APRIL 2015
VOLUME 20

Symantec

ISTR20

INTERNET SECURITY THREAT REPORT

GOVERNMENT

CHARTS & TABLES

Introduction

Symantec has established the most comprehensive source of Internet threat data in the world through the Symantec™ Global Intelligence Network, which is made up of more than 57.6 million attack sensors and records thousands of events per second. This network monitors threat activity in over 157 countries and territories through a combination of Symantec products and services such as Symantec DeepSight™ Intelligence, Symantec™ Managed Security Services, Norton™ consumer products, and other third-party data sources.

In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 66,400 recorded vulnerabilities (spanning more than two decades) from over 21,300 vendors representing over 62,300 products.

Spam, phishing, and malware data is captured through a variety of sources including the Symantec Probe Network, a system of more than 5 million decoy accounts, Symantec.cloud, and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary heuristic technology, is able to detect new and sophisticated targeted threats before they reach customers' networks. Over 8.4 billion email messages are processed each month and more than 1.8 billion web requests filtered each day across 14 data centers. Symantec also gathers phishing information through an extensive anti-fraud community of enterprises, security vendors, and more than 50 million consumers.

Symantec Trust Services secures more than one million web servers worldwide with 100 percent availability since 2004. The validation infrastructure processes over 6 billion Online Certificate Status Protocol (OCSP) look-ups per day, which are used for obtaining the revocation status of X.509 digital certificates around the world. The Norton™ Secured Seal is displayed almost one billion times per day on websites in 170 countries and in search results on enabled browsers.

These resources give Symantec analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the annual Symantec Internet Security Threat Report, which gives enterprises, small businesses, and consumers essential information to secure their systems effectively now and into the future.

Executive Summary

Governments around the world faced mounting cyber threats in 2014, while at the same time signficantly increasing their offensive capabiltiies. Cyber actors continued to target governments, public sector organizations and critical infrastructure. In response, some governments strengthened their cyber defenses, developed or improved their cybersecurity strategies, and took steps to enhance their protection capabilities.

The last year saw several headline-grabbing security stories: the Heartbleed bug affected millions of websites, the world got a close look at a stealthy, sophisticated tool for cyberespionage called "Regin," and a large financial institution acknowledged that data associated with 83 million customers was compromised in one of the largest data breaches in history.

Beneath the headlines, there were other big trends at work, notably the growth of the Internet of Things and the increasing shift from conventional PCs to mobile devices. Old threats remain—spam, phishing and the rest—but new technology creates new opportunities for adversaries and criminals. It also demands a layered security approach if individuals, companies, and governments want to stay safe online.

Sophisticated Cyberespionage

2014 was the year of Regin, Waterbug, Dragonfly and Turla—sophisticated, well-resourced, targeted, and persistent cyberespionage campaigns that used "professional-grade" malware and were likely created at the direction of nation states. The combination of spear-phishing, zero-day attacks, social engineering, and custom-coded malware that these campaigns use makes it very challenging to protect against these kinds of attack. Evidence that the Dragonfly campaign was surveying industrial control systems in several countries suggests that information may not be the only target of the creators of these tools. We also saw the emergence of denial-of-service-as-a-service that gave extortionists and hacktivists a powerful new tool for disrupting online services or connected infrastructure.

Threats are quickly diversifying and adapting to technology innovation. As the era of the Internet of Things, smart infrastructure, connected manufacturing, e-health, and hyper-connectivity approaches, it is increasingly clear that any device connected to the Internet will become a potential target for exploitation. Phones, tablets, and other connected devices already outnumber conventional PCs and their numbers are growing fast. Mobile phones have long been a target for cybercriminals and there are already 1 million malware-infected apps and more than 4.5 million apps that feature unwelcome "grayware"—programs that are not obviously malicious, but which can be annoying or even harmful to the user. Last year

saw a surge in proof-of-concept attacks on wearable devices, webcams, embedded devices such as routers and smart TVs, and even attacks on car informatics.

Our digital ecosystem is evolving faster than ever, but without proper security and policies in place it is also an enticing target for attackers. Given the growth in connectivity, the policies that governments around the world are putting in place on privacy, critical infrastructure protection, and digital trust should be scaled accordingly and remain technology neutral. All of these complex policy issues that once only concerned the ICT industry, are now relevant to every sector of the economy, from banking to healthcare to energy.

Cybercriminals Take Their Business to the Next Level

Criminal operations grow ever more sophisticated in 2014, with specializations, service providers and fluctuating markets mirroring the legitimate technology industry. A drive-by download web toolkit, for example, which includes updates and 24/7 support, can be rented for between $100 and $700 per week. Distributed denial-of-service (DDoS) attacks can be ordered from $10 to $1,000 per day. In terms of the buyer's market, credit card details can be bought for between $0.50 and $20 per card, and 1000 followers on a social network can cost as little as $2 to $12. The underground black market in malware and stolen identities continues to thrive, reflecting the continued widespread use of malware to attack computer and mobile device users around the world. There was a decline in the number of botnets, in part due to arrests and take-downs, such as the GameOver Zeus and ZeroAccess botnets. In 2014, Symantec formally partnered with Europol, the FBI, and other law enforcement agencies to take the fight to the cybercriminals. In light of the consistent growth of the cybercriminal market, we believe such cooperation will need to be strengthened and developed further.

Public-Private Partnerships

Many of these law enforcement actions were supported by Symantec as well as other private companies. Due to the borderless nature of cybercrime, efforts to thwart it require close cooperation and coordination between governments and industry. No single government or company can "go it alone" in the current threat landscape. The threats are too complex and the stakes are too high. Ultimately, to be successful in defeating cybercriminals and their networks, strong technical capabilities, effective defenses, industry collaboration and law enforcement cooperation are required.

Critical Infrastructure Protection (CIP)

The manufacturing industry saw the most growth in spear phishing, up from 13 to 20 percent, becoming the most targeted critical infrastructure sector in 2014. Spear phishing is prevalent enough within the industry that one out of every three organizations was targeted during the year. It was also the second-most likely source of compromised systems during the year, where 45.1 percent of the malicious activity recorded originated. Interestingly, manufacturing accounts for 96.3 percent of all source IP addresses logged preforming malicious activity in 2014. This indicates the activity is coming from a wide variety of systems within the manufacturing industry.

While manufacturing came second in the list of critical infrastructure sectors with compromised systems, the financial services sector topped the list with 52.8 percent of all CIP-related source activity. However, what's most concerning here is that financial services only accounted for 1.9 percent of the source IP addresses. This could indicate that while a much smaller number of systems are compromised within the financial services sector, they are performing a worrying amount of malicious activity. This is backed up by growth in spear phishing attacks in 2014, jumping from 14 percent in 2013 to 18 percent in 2014. In terms of risk, one out of every 4.8 organizations in this industry was targeted at some point within the year.

Spear phishing attacks against Public Administration (Government) organizations declined in 2014, dropping from 16 to 5 percent, though one in every 3.4 organizations was targeted by spear phishing attacks during the year. In terms of attacks targeting these organizations, 61 percent of the activity observed originated in the U.S. With 20 percent of activity recorded, China came in second.

In terms of the types of attacks carried out, the vast majority (95 percent) came from compromised web servers, particularly in the manufacturing, transportation, and Internet service provider sectors. However, peer-to-peer (P2P) communications dominated some individual industries, such as government, financial services, and healthcare. This could indicate an elevated presence of botnets within these industries, many of which depend on P2P communication protocols to operate. Denial of Service attacks topped the list for telecommunications and utility sectors.

Threat Intelligence and the Concept of Unified Security

Today's attackers are skilled enough and sufficiently resourced to have the persistence and patience to carry out their activities over a period of months or even years. They only have to be successful once in order to breach their targets' defenses; however, those targets must be able to resist each end every one of those assaults, every second of every day. Threat Intelligence is a vital component in understanding these potential threats, uncovering new attacks and better protecting critical digital assets. Threat intelligence can provide a prioritized list of suspicious incidents by correlating all available information from across an organization.

Advanced attackers use exploit toolkits not only against older vulnerabilities, but also new zero-day vulnerabilities, and being good at defense means making it harder to breach a network. The battle is asymmetric and attackers understand too well the defenses and their weaknesses. A unified security model is not just about investing in technology, but a holistic approach that combines threat intelligence, risk management and the most effective technical solutions available. A unified approach will not only help to reveal who is being targeted, but also analyze how and reflect on why. Understanding emerging threats is critical, and organizations should expect to be attacked – the question is not if, but when and how.

Unified security can leverage the combined visibility and threat intelligence gathered across an organization to block, detect and remediate attacks. It can help guide how to better protect confidential information and reduce risk. Supporting the continual assessment of not only the people and their skills, but also the processes and technology to ensure the best response is followed. Processes are continually updated and skills maintained. Ultimately, by making it harder to carry out a breach, attackers must work harder. No one wants to be the weakest link in the chain. This is the reality of the future of security.

2014 IN NUMBERS

46 2014 | **57** 2013

New Android Mobile Malware Families

277 2014 | **231** 2013

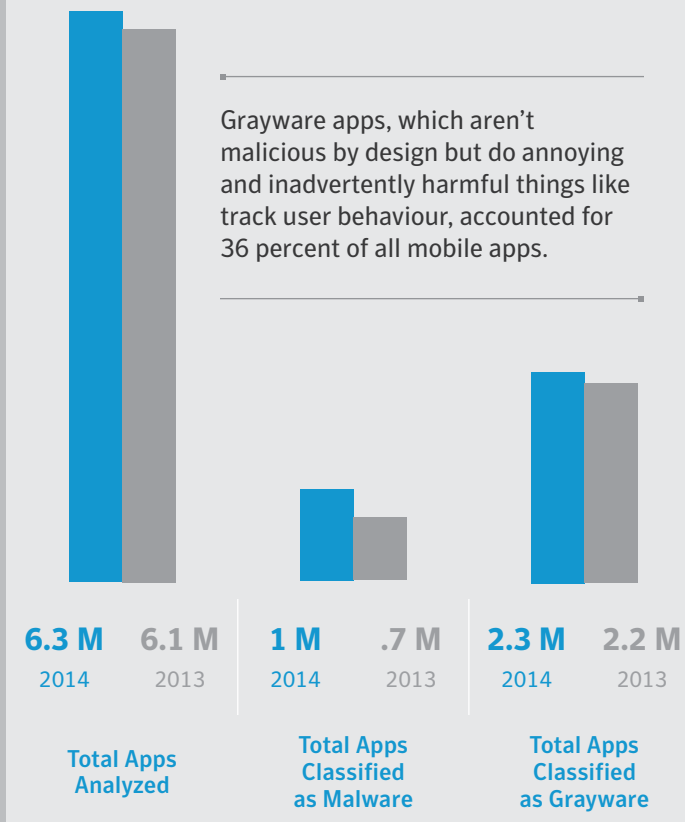
Cumulative Android Mobile Malware Families

48 2014 | **57** 2013

New Android Variants per Family

9,839 2014 | **7,612** 2013

Cumulative Android Mobile Malware Variants



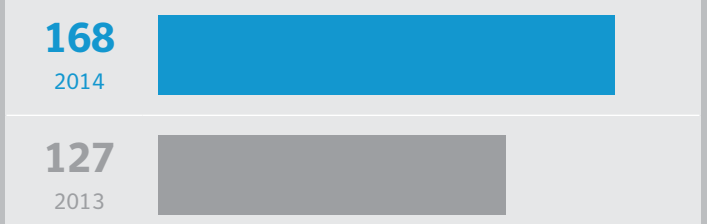
Grayware apps, which aren't malicious by design but do annoying and inadvertently harmful things like track user behaviour, accounted for 36 percent of all mobile apps.

6.3 M 2014 | **6.1 M** 2013 — Total Apps Analyzed

1 M 2014 | **.7 M** 2013 — Total Apps Classified as Malware

2.3 M 2014 | **2.2 M** 2013 — Total Apps Classified as Grayware

App Analysis by Symantec's Norton Mobile Insight



168 2014

127 2013

New Mobile Vulnerabilities

Symantec found that 17 percent of all Android apps (nearly one million total) were actually malware in disguise.

MOBILE DEVICES

76% 2014

77% 2013

Scanned Websites with Vulnerabilities

20% 2014

16% 2013

Percentage of Which Were Critical

6,549 2014

6,787 2013

New Vulnerabilities

496,657 2014

568,734 2013

Web Attacks Blocked per Day

1 in 1,126 2014

1 in 566 2013

Websites Found with Malware

Inverse Graph: Smaller Number = Greater Risk

1	SSL/TLS Poodle Vulnerability
2	Cross-Site Scripting
3	SSL v2 support detected
4	SSL Weak Cipher Suites Supported
5	Invalid SSL certificate chain

Top 5 Vulnerabilities Found Unpatched on Scanned Web Servers

Within four hours of the Heartbleed vulnerability becoming public, Symantec saw a surge of attackers stepping up to exploit it.

WEB THREATS

60% 2014 | **66%** 2013

Overall Email Spam Rate

1 in 965 2014

1 in 392 2013

Email Phishing Rate

Inverse Graph: Smaller Number = Greater Risk

28 Billion 2014 | **29 Billion** 2013

Estimated Global Spam Volume per Day

23% 2014 | **81%** 2013

Fake Offering Social Media Scams

70% 2014 | **2%** 2013

Manually Shared Social Media Scams

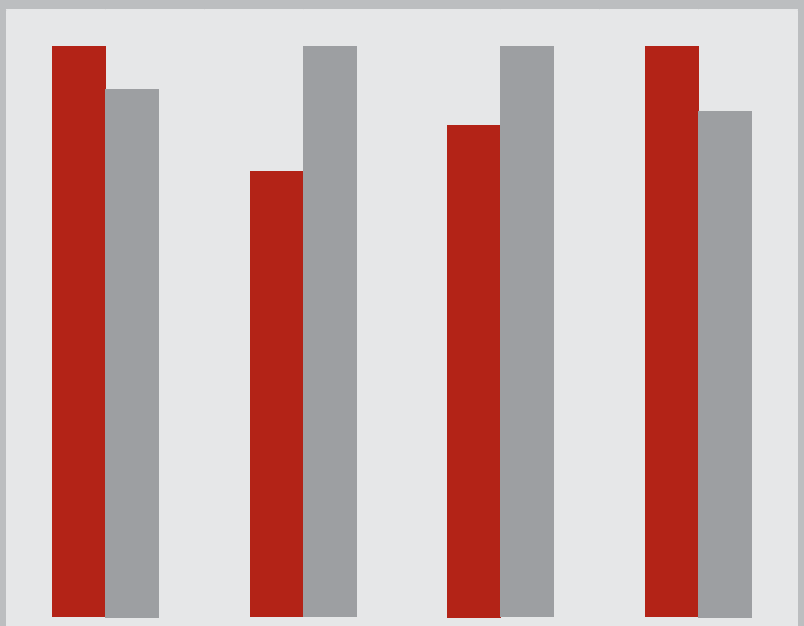
3,829 2014

6,993 2013

Average Number of Phishing URLs on Social Media

In 2014, Symantec observed that 70 percent of social media scams were manually shared.

SCAMS & SOCIAL MEDIA



2014	2013	2014	2013	2014	2013	2014	2013
841	779	18	23	25	29	9 Days	8 Days
Campaigns		Recipients per Campaign		Average Number of Attacks per Campaign		Average Duration of a Campaign	

Spear Phishing Email Campaigns

2014	2013
73	83

Spear Phishing Emails per Day

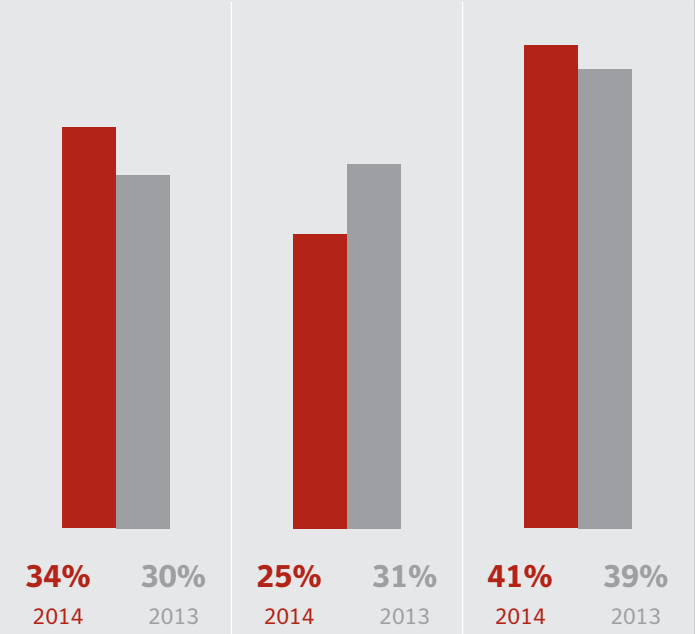
Industry	Risk Ratio	2014	2013
Mining	1 in 2.3	44%	37%
	1 in 2.7		
Wholesale	1 in 2.9	34%	29%
	1 in 3.4		
Manufacturing	1 in 3.0	33%	31%
	1 in 3.2		
Transportation, Communications, Electric, Gas & Sanitary Services	1 in 3.4	29%	26%
	1 in 3.9		
Public Administration (Government)	1 in 3.4	29%	32%
	1 in 3.1		

Risk Ratio of Spear-Phishing Attacks by Industry

Industry	2014	2013
Manufacturing	20%	13%
Services—Nontraditional	20%	14%
Finance, Insurance & Real Estate	18%	13%
Services—Professional	11%	15%
Wholesale	10%	5%

Top 10 Industries Targeted in Spear-Phishing Attacks

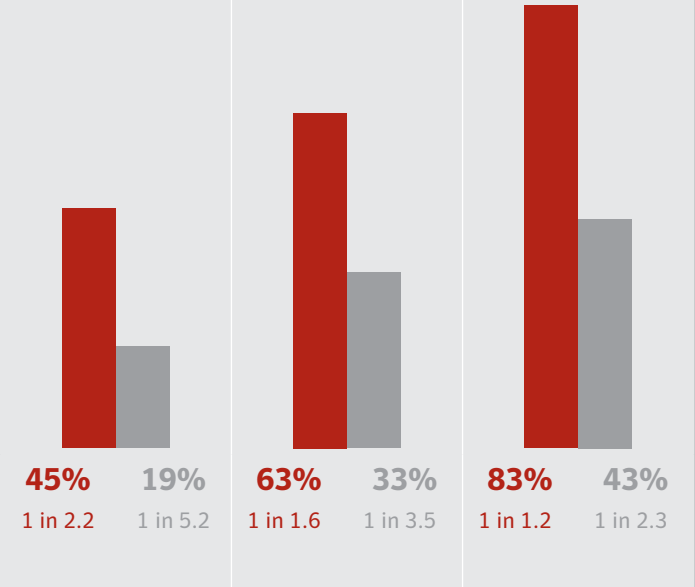
TARGETED ATTACKS



Distribution of Spear-Phishing Attacks by Organization Size

Small Businesses (SMBs) 1 to 250 Employees	Medium-Size Businesses 251 to 2,500 Employees	Large Enterprises 2,500+ Employees

Risk Ratio of Spear-Phishing Attacks by Organization Size



Individual Contributor	1 in 3.7	27%
Manager	1 in 3.8	26%
Intern	1 in 3.9	26%
Director	1 in 5.4	19%
Support	1 in 7.6	13%

Top 5 Risk Ratio of Spear-Phishing Attacks by Job Level

Sales/Marketing	1 in 2.9	35%
Finance	1 in 3.3	30%
Operations	1 in 3.8	27%
R&D	1 in 4.4	23%
IT	1 in 5.4	19%

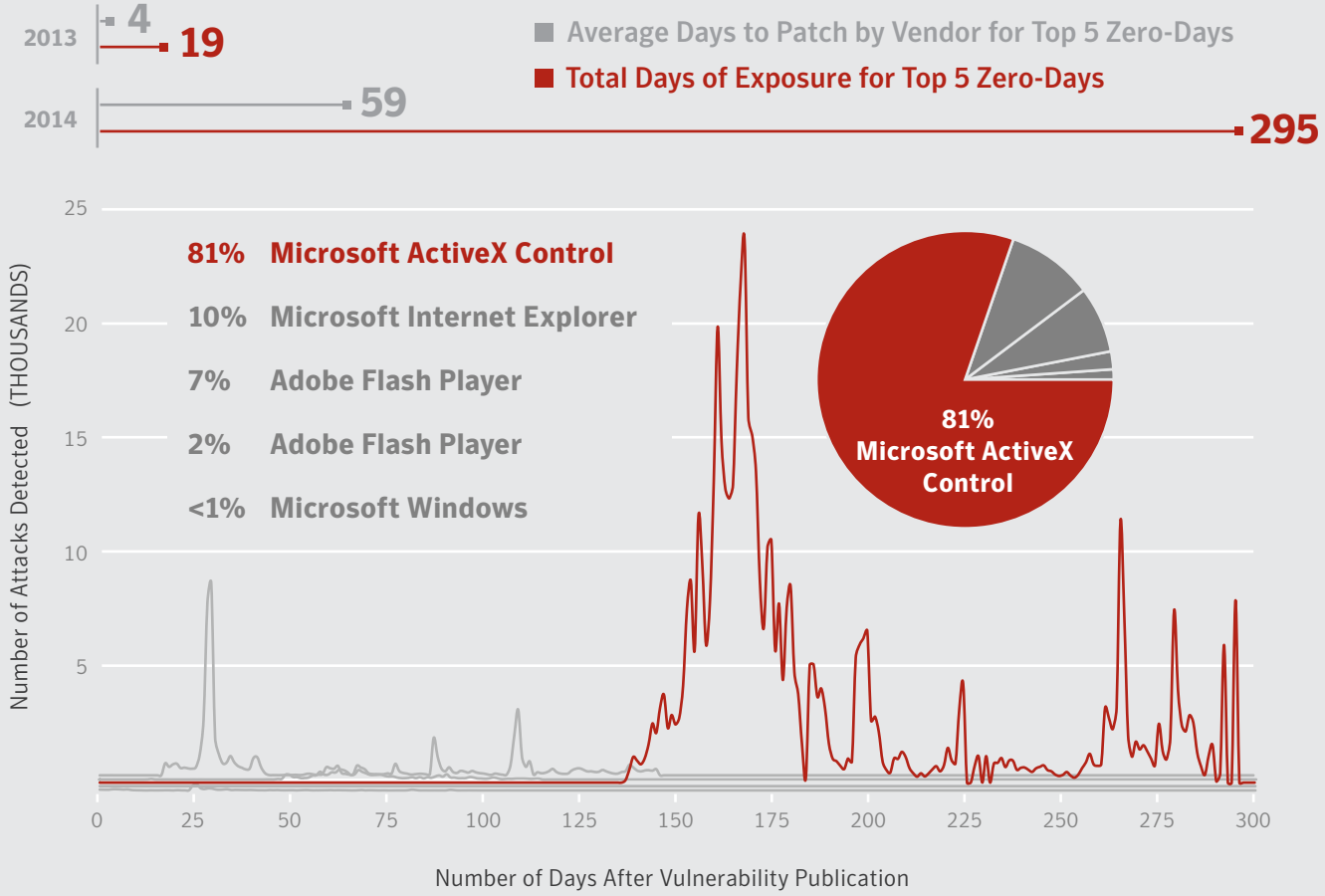
Top 5 Risk Ratio of Spear-Phishing Attacks by Job Role

.doc	39%
.exe	23%
.scr	9%
.au3	8%
.jpg	5%

Spear-Phishing Emails Used in Targeted Attacks

Last year, 60 percent of all targeted attacks struck small- and medium-sized organizations.

In total, the top five zero-days of 2014 were actively exploited by attackers for a combined 295 days before patches were available.



Top 5 Zero-Day Vulnerabilities – Days of Exposure and Days to Patch

Source: Symantec

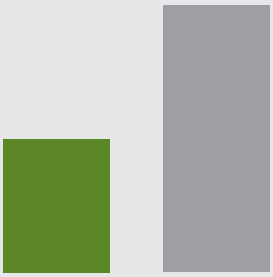
Zero-Day Vulnerabilities

312 2014 **253** 2013

Total Breaches

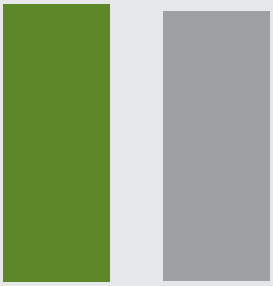
348 M 2014 **552 M** 2013

Total Identities Exposed



1.1 M 2014 **2.2 M** 2013

Average Identities Exposed per Breach



7,000 2014 **6,777** 2013

Median Identities Exposed per Breach

The number of breaches increased 23 percent in 2014. Attackers were responsible for the majority of these breaches.

4 2014

8 2013

Breaches with More Than 10 Million Identities Exposed

Healthcare	116	37%
Retail	34	11%
Education	31	10%
Gov. & Public	26	8%
Financial	19	6%

Top 5 Sectors Breached by Number of Incidents

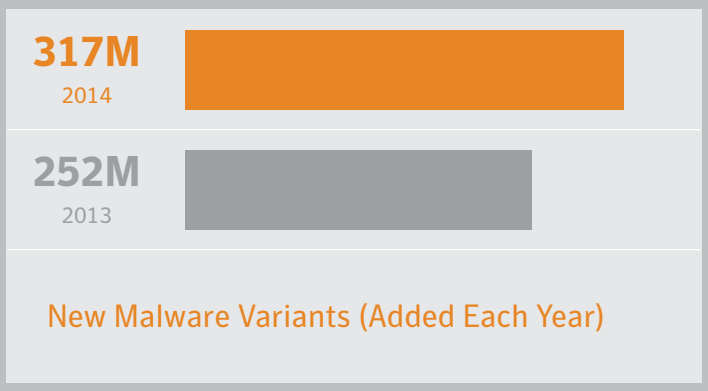
Retail	205M	59%
Financial	80M	23%
Computer Software	35M	10%
Healthcare	7M	2%
Gov. & Public	7M	2%

Top 5 Sectors Breached by Number of Identities Exposed

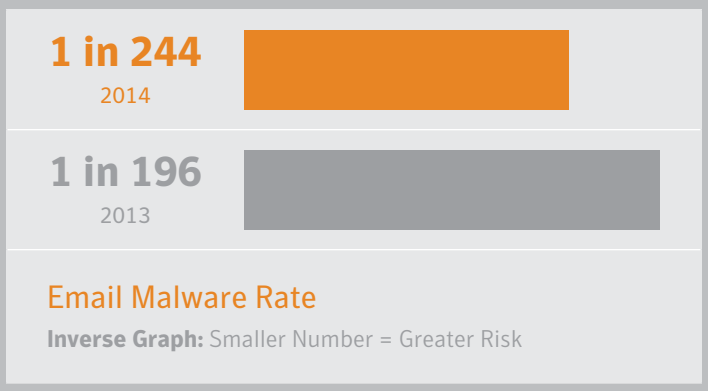
Real Names	69%
Gov. ID Numbers (e.g, SSN)	45%
Home Addresses	43%
Financial Information	36%
Birth Dates	35%

Top 10 Types of Information Exposed

DATA BREACHES

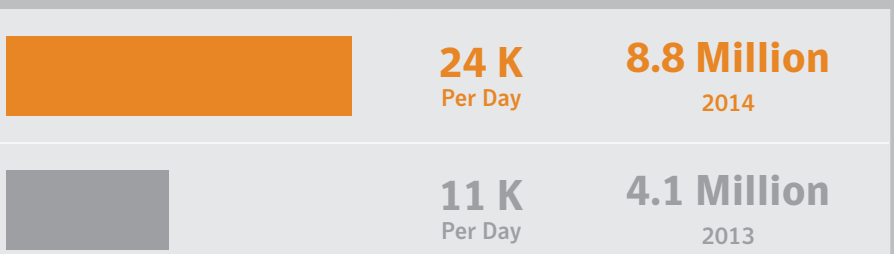


New Malware Variants (Added Each Year)



Email Malware Rate

Inverse Graph: Smaller Number = Greater Risk

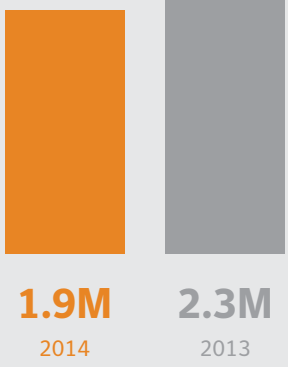


Ransomware Total

Item	2014 Cost
1,000 Stolen Email Addresses	$0.50 to $10
Credit Card Details	$0.50 to $20
Scans of Real Passports	$1 to $2
Stolen Gaming Accounts	$10 to $15
Custom Malware	$12 to $3500
1,000 Social Network Followers	$2 to $12
Stolen Cloud Accounts	$7 to $8
1 Million Verified Email Spam Mail-outs	$70 to $150
Registered and Activated Russian Mobile Phone SIM Card	$100

Value of Information Sold on Black Market

Ransomware attacks grew 113 percent in 2014, along with 45 times more crypto-ransomware attacks.



Number of Bots

In 2014, up to 28 percent of all malware was "virtual machine aware."

Email Malware as URL vs. Attachment

E-CRIME & MALWARE

MOBILE DEVICES & THE INTERNET OF THINGS

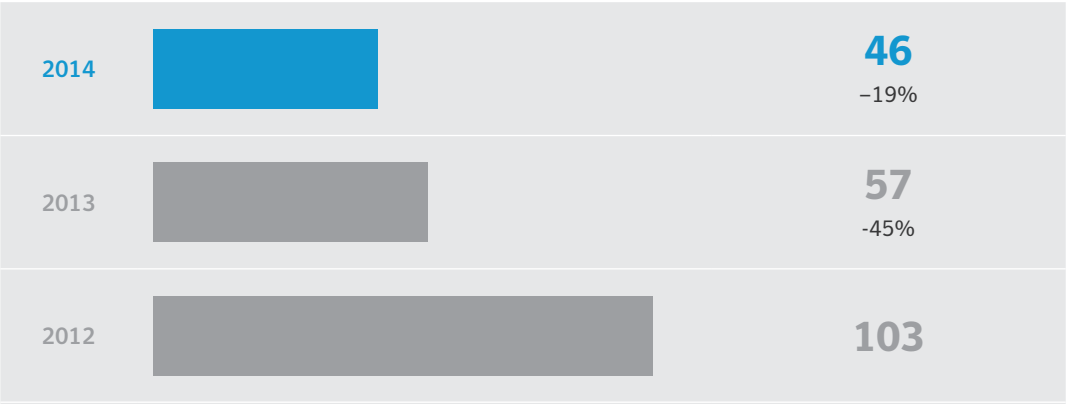
Mobile Devices and the Internet of Things

With billions of smartphones and potentially many billions of Internet-connected devices of all kinds, the focus of Internet security is shifting from the desktop and the data center to the home, the pocket, the purse, and, ultimately, the infrastructure of the Internet itself.

Mobile Malware

The tenth anniversary of mobile malware occurred in 2014. In 2004, researchers discovered SymbOS.Cabir,[1] a worm that spread through Bluetooth and targeted the Symbian OS, the most popular mobile operating system at the time.[2]

Today many apps contain malware. As of 2014, Symantec has identified more than 1 million apps that are classified as malware. This includes 46 new families of Android malware in 2014. In addition, there are perhaps as many as 2.3 million "grayware" apps that, while not technically malware, display undesirable behavior, such as bombarding the user with advertising.[3]



New Android Mobile Malware Families

Source: Symantec

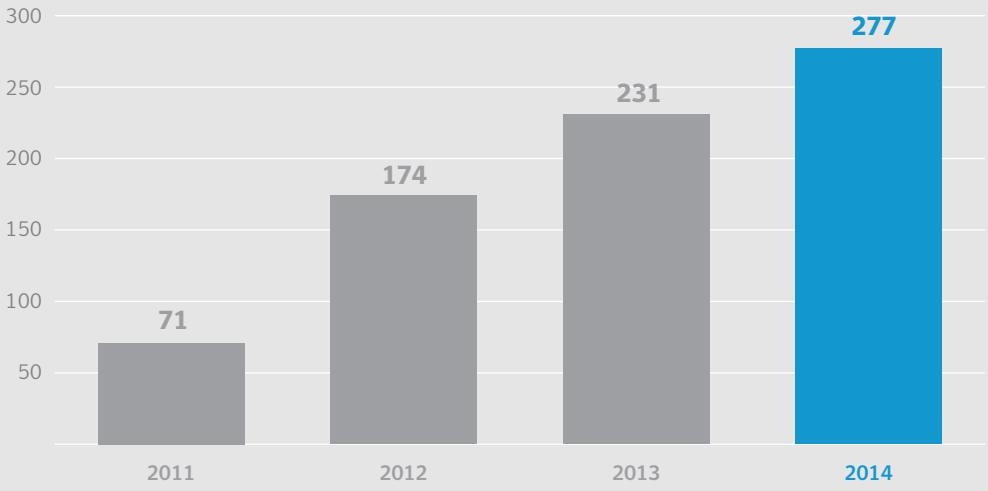
The falling number of families doesn't indicate that this problem is going away but just that the rate of innovation is slowing. This may be because existing malware is effective enough and there is less demand for new software. In addition, the overall trend masks significant fluctuations from month to month. The drop also suggests that developers are maximizing the number of variants per family, for example, by repackaging well-known games and apps with malware.

Symantec expects the growth in mobile malware to continue in 2015, becoming more aggressive in targeting a user's money. Already 51 percent of U.S. adults bank online and 35 percent use mobile phones to do so.[4] This creates an incentive for malware writers to target phones to capture bank details.[5] Today, Android malware can intercept text messages with authentication codes from your bank and forward them to attackers. Fake versions of legitimate banks' mobile applications also exist, hoping to trick users into giving up account details.

At a Glance

- *There are now more than 1 million malicious apps in existence.*
- *Proof-of-concept attacks on the Internet of Things are here, including wearables, Internet infrastructure, and even cars.*
- *Devices on the cusp of the Internet of Things, such as routers, network-attached storage devices, and embedded Linux devices, are already under attack.*

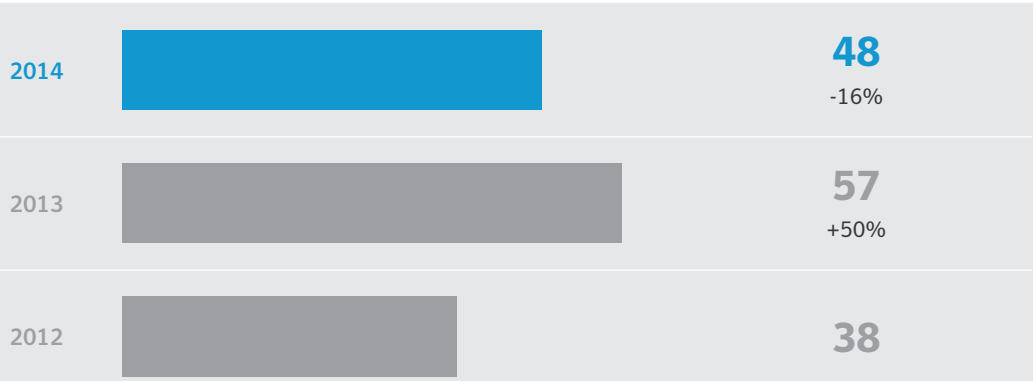
The falling number of families doesn't indicate that this problem is going away but just that the rate of innovation is slowing.



Cumulative Android Mobile Malware Families, 2011–2014

Source: Symantec

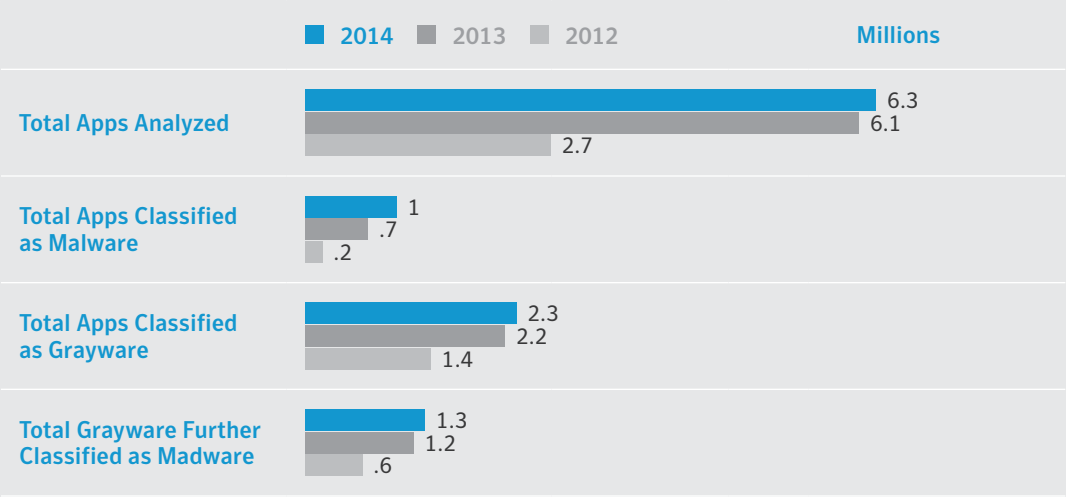
- *In 2014 there were 46 new mobile malware families discovered.*



New Android Variants per Family

Source: Symantec

- *There was a 16 percent drop in the number of Android variants per family in 2014.*

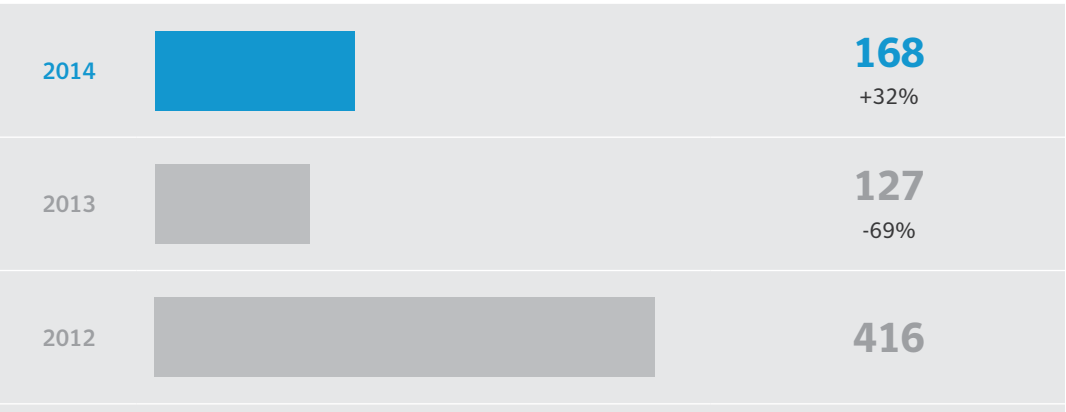


Malware Definition	Programs and files that are created to do harm. Malware includes computer viruses, worms, and Trojan horses.
Grayware Definition	Programs that do not contain viruses and that are not obviously malicious but that can be annoying or even harmful to the user (for example, hack tools, accessware, spyware, adware, dialers, and joke programs).
Madware Definition	Aggressive techniques to place advertising in your mobile device's photo albums and calendar entries and to push messages to your notification bar. Madware can even go so far as to replace a ringtone with an ad.

App Analysis by Symantec's Norton Mobile Insight

Source: Symantec

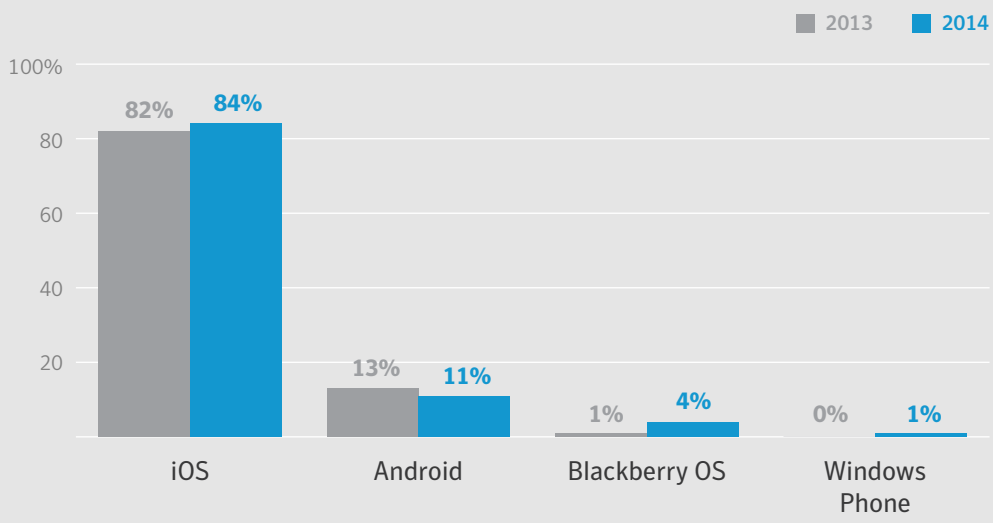
- *Of the 6.3 million apps analyzed in 2014, one million of these were classified as malware, while 2.3 million were classified as grayware.*
- *A further 1.3 million apps within the grayware category were classified as madware.*



New Mobile Vulnerabilities

Source: Symantec

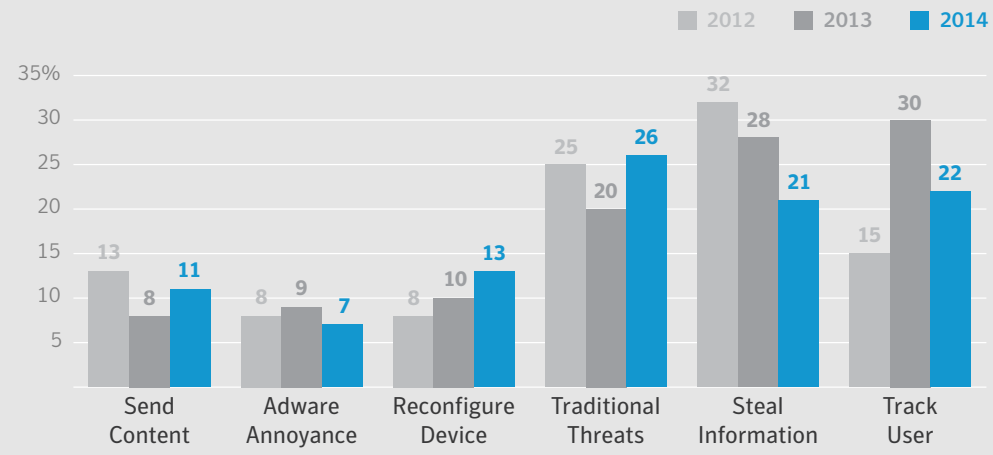
- *There were 168 mobile vulnerabilities disclosed in 2014, a 32 percent increase compared to 2013.*



Mobile Vulnerabilities by Operating System, 2013–2014

Source: Symantec

- *84% of mobile vulnerabilities related to Apple iOS in 2014, compared with 11% for Android, 4% for BlackBerry and 1% for Nokia.*



Send Content – Threats that send premium SMS, Spam and SEO Poisoning threats.
Adware/Annoyance – Threats that cause advertisement popups and unwanted information.
Reconfigure Device – Threats that modify user settings, and elevates privileges.
Traditional Threats – Threats like Backdoor Trojans, Downloaders, DDoS utility, Hacktool and Security Alerts.
Steal Information – Threats that steal device data, media files and any user credentials. Eg., Banking Trojan.
Track User – Threats that spy on users, tracks user location.

Mobile Threat Classifications, 2012–2014

Source: Symantec

- *Traditional threats increased 6 percentage points between 2013 and 2014, while threats that steal information from the device or track users declined in 2014.*

SMS and the Interconnected Threat to Mobile Devices

by Lamine Aouad, Slawomir Grzonkowski, Alejandro Mosquera, and Dylan Morss

The threat landscape is continually evolving, and with the emergence of cheaper and readily available technologies and communication channels, it naturally attracts malicious activity of all sorts. The shift from desktop PCs to mobile devices as primary computing devices is a perfect example of this. As more users rely on their mobile devices, more spam, scams, and threats are tailored to these devices.

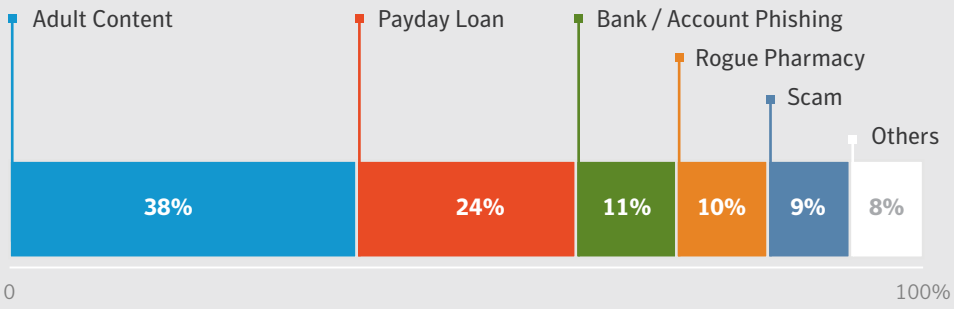
We suspect that the interconnectedness of apps on smartphones has played a big part in this increase. This interconnectedness has enabled a malicious source to send an SMS that will open in a mobile browser by default, which can be readily utilized to exploit the user.

SMS is far from a new technology; it's older than the smartphone itself. However, we've seen significant growth in this area of the mobile landscape when it comes to how scammers and attackers carry out their campaigns. SMS and other mobile messaging technologies are readily being used as a means to deliver all kinds of scam campaigns, such as adult content, rogue pharmacy, phishing and banking scams, payday loan spam, fake gifts, etc.

An important trend in 2014 was the proliferation of scam campaigns. Although this category was not the most prevalent, it certainly was one of the most dangerous threats using SMS messages as its vector of attack. These are targeted campaigns, of a range of scams and frauds, addressed to selected potential victims, mainly scraped off classified ad websites. Scammers send automated inquiries about the advert via SMS. They also offer fictitious items for sale, such as jobs and houses for rent, and interact with potential victims by SMS, and then they switch to email for communication. They typically use fake checks or spoofed payment notifications to make victims ship their items or to take victims' deposits. Naturally victims never hear back from them.

Another variant leads online dating users to fake age verification websites that charge for a premium adult subscription. For these adult scams, spammers initially targeted mobile dating apps users and moved to SMS afterward. These apps and social media sites were the main sources that dating scammers used in 2014.

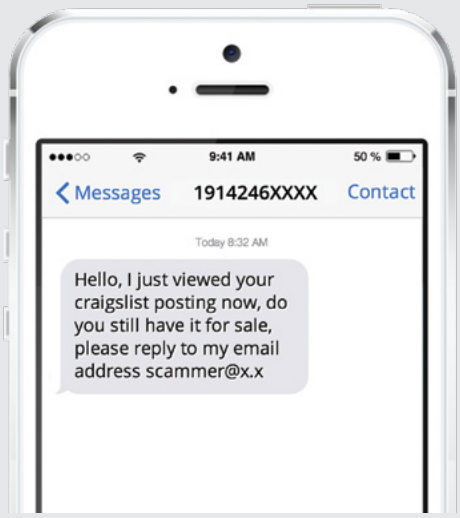
Most SMS scammers are posing as U.S. or Canadian citizens or businesses running from other countries (many were traced back to Nigeria). They abuse VoIP and cloud-based mobile carriers and messaging services (the top two services, namely Enflick and Integra5, accounted for more than 90 percent of their traffic). They also abuse all sorts of hosting, email, listing, and online payment and money transfer services. These scams are not new and have been running on email for quite some time; however, new mobile platforms and technologies make it easier for scammers to take advantage of the unsuspecting, especially when they are using a relatively trusted medium like SMS. Online buyers and sellers, as well as those looking for a job, apartment, or any other service, should pay close attention to the details of each communication and be aware that these scammers are constantly improving their fraudulent tactics.



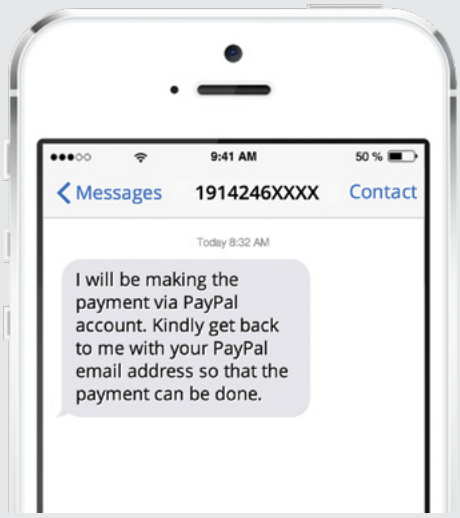
Top Categories of Observed SMS Spam, 2014

Source: Symantec

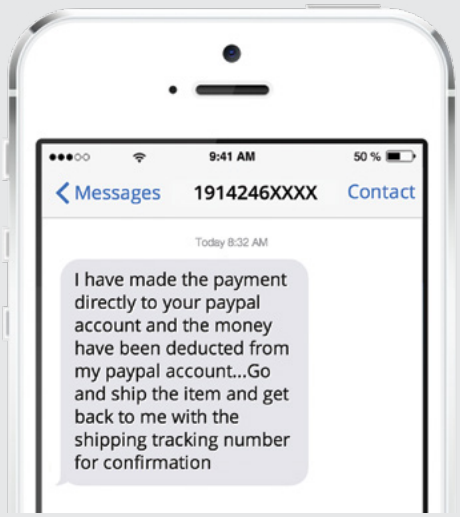
01 A typical Craigslist or PayPal[11] scam, for instance, would start with a message like the following sent to hundreds of people scraped off Craigslist:



02 The scammers have further discussions with the victim via email and follow up with a text message stating that they will be paying for the item and shipping via PayPal:



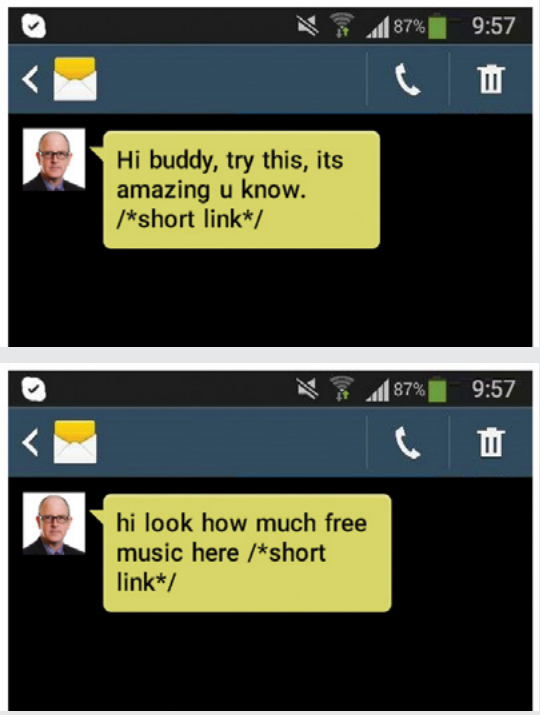
03 The scammers send a confirmation email to the victim's PayPal account, from a fake PayPal email address, claiming the funds have been deducted from his or her account and will be released to the victim once he or she ships the item:



04 If this is successful, the scammers can then track the items to their doorstep and the victim never receives any compensation for his or her items.

Users should also be aware of the continually evolving malware landscape. SMS has been seen as an infection and propagation vector for many Trojans, worms, and SMS agents. There are instances of malicious apps' propagating via SMS to infect new victims, which typically would be the contact list. These are very short messages that look legit but include links to malicious apps. Typical examples would look like the following text messages to the right. These malicious apps are monetized in different ways, mainly via premium services and SMS subscriptions. They also leak personal information and show affiliate ads.

The fact that an older technology, such as SMS, has become such a popular propagation technique for scams and other malicious activity highlights an important issue in the mobile threat landscape: communication is becoming more unified through new applications and services. In the future, the underlying delivery technology will be irrelevant, regardless if it's SMS, email, IM, or something new. As different apps and technologies are becoming more and more integrated, users will need to be aware that threats can be delivered across a variety of areas. ■



Mobile malware will become harder to remove, for example, by using PCs as a way to infect attached phones and by using bootkits to infiltrate a phone's operating system.[6] Like some rootkits for PCs, bootkits infect the master boot record of a device so that the malware runs before the operating system is even loaded. The first crypto-ransomware for Android devices appeared in 2014, giving criminals another way to earn money by infecting phones and tablets—extortion.[7]

There are also wider privacy issues at stake. Not only can apps gain access to users' private information, but the phones themselves can also be used to invade people's privacy. For example, this year researchers at Stanford University were able to pick up audio and identify who was speaking by using the gyroscope in a mobile phone.[8]

Mobile Apps and Privacy

An alarming percentage of apps collect and send personally identifiable information (PII) to app developers. A survey carried out by Symantec, and published in December 2014,[9] indicates that most consumers worry about app security and privacy risks. However, the findings also suggest consumers are their own worst enemies when it comes to mobile privacy.

Many consumers worry about device and data security, but, ironically, most are still willing to allow apps access to their personal information. In fact, according to the survey, 68 percent of people will willingly trade their privacy for a free app.

App users think they understand what they are agreeing to when downloading apps, but, in reality, they have little understanding of common app permission practices and behaviors. For instance, over half of respondents were unaware that apps could track their physical location (22 percent of the apps scanned by Norton Mobile Insight track this information).

Internet of Things

The first Internet-connected appliance was a Coke machine at Carnegie Mellon University back in 1982. It reported on stock levels and whether newly loaded drinks were chilled.[10] It was the snowflake that started an avalanche.

The Internet of Things (IoT), embedded computing devices with Internet connectivity, embraces a wide range of devices, including digital home thermostats, smart TVs, car systems (such as navigation, entertainment, and engine management computers), networking devices, smart watches, and activity trackers.

The diversity of threats mirrors the diversity of devices. In the past year, there has been a growing number of probing and experimental attacks on a range of devices, as well as a few serious attacks.

As the market for IoT devices has developed, it has become fragmented with a rich diversity in low-cost hardware platforms and operating systems. Some attacks are already capable of exploiting vulnerabilities in Linux-based IoT systems and routers; however, as market leaders emerge and their ecosystems grow stronger, attacks against some devices will undoubtedly escalate. This is likely to follow a path similar to the way that attacks against the Android platform reflected the growth in its popularity in recent years.

As the market for IoT devices has developed, it has become fragmented with a rich diversity in low-cost hardware platforms and operating systems.

Wearable Devices

Wearable fitness and personal health devices will be a $5 billion market by 2016[12] according to analysts at Gartner. There are devices and apps already available for measuring our steps, blood pressure, heart rate, and other intimate medical data, which can be stored online or on our phones.

With countless Internet-connected wearable devices on the market and more coming, including the highly anticipated Apple Watch, there is an obvious security and privacy threat.

Already, there have been proof-of-concept attacks on Fitbit devices[13] and Symantec researchers revealed significant vulnerabilities in many devices and applications in this area.[14] In a review of the 100 health apps in the App Store, 20 percent transmitted user credentials without encrypting them, more than half (52 percent) did not have any privacy policies, and, on average, each app contacted five Internet domains (typically a mix of advertising and analytics services).

The potential exposure of personal data from health-monitoring devices could have serious consequences for individuals, for example, if insurance companies started to use the data to adjust premiums, if people used hacked location data to track other people without their knowledge. In a fast-moving and early-stage industry, developers have a strong incentive to offer new functionality and features, but data protection and privacy policies seem to be of lesser priority.

Internet-Connected Everything

Computing and connectivity have enhanced our lives. Phones now play videos. Cars now have navigation and entertainment systems. In our homes, lighting, heating, and cooling can be controlled from an app. The possibilities are exciting, but there is also a dark side.

For example, in May 2014, the FBI and police in 19 countries arrested more than 90 people in connection with "creepware"—using Internet-connected webcams to spy on people.[15,16] Similarly, as cars get "smarter" (meaning more digital and more connected), they are also at greater risk. Researchers found that many cars are vulnerable to cyberattacks.[17] Researchers were even able to use a laptop to control a standard car.[18]

Automotive Security

by Shankar Somasundaram

The automotive industry is undergoing a number of big changes. Cars are already powerful networks on wheels, processing large quantities of data. In many cases, smartphones have already been integrated into car infotainment systems. Auto manufacturers are also integrating Internet connectivity into cars. This connectivity offers a variety of useful features to the cars, ranging from predictive maintenance to downloading new features on an on-demand basis. Standards around vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications are also being developed, with initial trials already underway. A number of players have also engaged in research on driverless cars, which is progressing rapidly, adding further computing power to the driving experience.

These developments have brought security and privacy issues in the automotive industry to the forefront. Attacks have already been demonstrated on different car manufacturers over the last couple of years.[19,20]

One attack surface is the websites and mobile apps provided by the car manufacturer, which could be used to configure or remotely control an Internet-enabled car. Symantec internal research has found that a number of these car manufacturers' websites are not very well authenticated. Another issue is that some of these websites and apps rely upon the car's unique vehicle identification number (VIN) to identify it. A car can be easily controlled by spoofing VINs through these websites and apps, by sending messages to the targeted cars. If this seems farfetched, keep in mind that in many cases a car's VIN can be located near the base of the windshield.

The most common attack surface is the OBD-II port, a diagnostic port that is kept in easily accessible locations within most cars, as per regulations for maintenance and software updates. The OBD-II port can be used to inject packets into the car's computer system, allowing control of the brakes, ignition control unit, etc. Technically speaking, an attacker could control any component within the car, even preventing the driver from accessing them via a denial-of-service attack. The general argument against the validity of such attacks has been that they require a physical connection to the auto. However, with insurance providers' and other players' providing wireless aftermarket units that can connect to the OBD-II port, such physical connectivity is no longer required.

If the back-end systems of companies providing devices that connect to a car's OBD-II port are compromised, then remote attacks on the car can be launched through these systems. In fact, compromised back-end systems, such as servers collecting and storing data from the devices, could become launch pads for attacks through multiple vendors, ranging from repair shops to the auto manufacturers themselves.

A compromised smartphone or malicious application on a phone is also a potential medium for attacking a car. For example, if a compromised device is charged via a vehicle's USB port, the vehicle is susceptible to being attacked. The increasing popularity of 4G, picocells,[21] and Home Node Bs[22] has also created a way to connect to and launch attacks over a cellular interface.

Another big threat vector is the infotainment unit, which controls the USB port, CD player, and other popular devices. Researchers at University of Washington and University of California, San Diego,[23] have demonstrated how attacks on a car can be carried out by compromising CD-ROMs or Bluetooth interfaces. Once the infotainment system is compromised, other units in the car can be attacked as well.

Another interesting, albeit less effective, threat has been tire pressure sensors. Attackers have demonstrated how wireless signals at the right frequency can be used to send conflicting signals to the tire pressure controller, possibly causing warning lights on the dashboard to turn on or, even worse, crash the controllers that connect to the tire pressure sensors, risking loss of control of the vehicle. However, such attacks need to be done at short range and require wireless expertise, in addition to particular hacking skills, making them more difficult to carry out.

While the above scenarios are critical from a security perspective, there are also issues around privacy. With the amount of data being generated by the car, as well as the user details that the car stores, questions like "Who owns the data?" and "How is the data being secured?" become critical issues. Privacy issues will start to get more severe as V2V and V2I technologies become more popular. In scenarios where user anonymity and privacy must be maintained, authentication will need to be carried out on an extremely large scale.

Symantec is conducting extensive research in this field, working directly with automobile manufacturers to perform vulnerability analysis of different features and components and providing aftermarket assessment. While auto manufacturers are separating out the critical and noncritical components of the car to ensure security, much more needs to be done. Symantec advocates end-to-end security to help address the problem. These solutions range from authentication, ensuring only signed code is executed, securing the infotainment and telematics units and applications that run on them, and then monitor them by using analytics to monitor abnormal activity, and ensuring the car's software can be updated remotely as needed. Some of these approaches must be incorporated during the design phase itself. How these solutions are implemented is equally important, since improper implementation could be just as ineffective as no security at all.

The future of Internet-enabled cars is bright and full of potential. The next phase of V2V communication, as well as driverless cars, will bring in a lot more connectivity. It will also increase the attack surface, as cars will autonomously communicate with each other and the infrastructure around them. It is all the more important that we understand and take action on the security issues now, before the challenges become too big to surmount. ■

The Network As the Target

The Internet is made up of hubs, switches, and routers that move information from place to place. These devices, from retail home routers to form-factor network-attached storage devices, are at the very least close cousins in the emerging IoT device space. They have processing, storage, and Internet connectivity and in many ways function just like more strictly defined IoT devices.

These types of devices are already under attack and can be seen as harbingers of what is to come in the larger IoT space.

For example, in August 2014 some Synology network-attached storage devices were infected by ransomware.[24] At the end of 2013, Symantec researchers discovered a new Linux worm called Darlloz[25] that targeted small Internet-enabled devices such as home routers, set-top boxes, and security cameras.[26] By March 2014, Symantec identified 31,716 devices that were infected with this malware.[27] Attackers can use freely available tools, such as the Shodan search engine, to search for Internet-enabled devices such as security cameras, heating control systems in buildings, and more.[28]

Symantec expects to see further malware development and attacks on the Internet of Things as criminals find new ways to make money from doing so. For example, some attackers have used Darlloz to mine for crypto-currencies similar to bitcoins. Other attackers have leveraged hacked routers to carry out distributed denial-of-service attacks.[29] Experience with PCs and, more recently, with mobile malware suggests that where there is opportunity created by technical exploits and motivation, such as greed, vindictiveness, or revenge, there will be cyberattacks. ■

Medical Devices – Safety First, Security Second

by Axel Wirth

Medical devices are notoriously insecure and easy to hack, as has been demonstrated for pacemakers and[30] insulin pumps,[31] as well as surgical and anesthesia devices, ventilators, infusion pumps, defibrillators, patient monitors, and laboratory equipment.[32]

The concerns voiced by security researchers, government regulators, and healthcare providers are well founded as any medical device cybersecurity incident could seriously harm patients. Because medical devices are so closely tied in with the care process any compromise may also adversely affect care delivery and hospital operations.

It is also a topic in the public eye, as we have seen through the press coverage of former Vice President Dick Cheney, who had the remote features of his pacemaker turned off.[33] These types of incidents were even dramatized in TV crime series like "Homeland" (Showtime) and "Person of Interest" (CBS).

2014 can be considered the year when medical device security became a mainstream topic and change started to happen. The US Department of Homeland Security,[34] the FBI,[35] and the FDA,[36] as well as international regulators issued warnings and expressed their concerns about the need to improve the cybersecurity of our medical device ecosystem.

There are reasons why medical devices are highly vulnerable:

- Medical devices have a long, useful life.
- The design, manufacturing, and sale of medical devices are highly regulated. Although regulations typically do not prevent manufacturers from including or updating device cybersecurity, they do mandate a time-consuming release process and test cycle, which can delay availability of security patches.
- Medical devices are used 24x7 and may be difficult to find time for upgrades, especially since groups of devices need to be upgraded together to maintain operational compatibility.
- Since medical devices are periodically on and off the hospital network as patient come and go, removal of malware from compromised devices may be operationally difficult. Given some malware's ability to reinfect cleaned devices, all vulnerable devices may need to be cleaned at once, requiring all impacted patients to come to the hospital at one time: a scheduling challenge in-and-of itself.

The most important risk scenarios to be aware of are those that target medical devices with the goal to harm a patient. Life-sustaining devices like pacemakers or insulin pumps can be hacked. Fortunately, to-date no such case has been reported outside proof-of-concept security research; however, the potential impact remains high.

Another situation that many healthcare providers struggle with are poorly patched devices, often running end-of-life operating systems. These highly vulnerable devices are a problem not because they are targeted, but because of their susceptibility to common malware. The impact is mainly operational, but cases have been reported where emergency patients have had to be rerouted to other hospitals due to malware infections of diagnostic equipment.[37]

Medical device vulnerabilities could also be used for an attack on a hospital. Attackers could exploit a device and use it as an entry point for a larger targeted attack, with the goal of damaging the reputation of a healthcare facility or instilling fear in the population as part of a hacktivist, cybervandalism, or even a cyberterrorism attack.

For practical and regulatory reasons, the responsibility for securing the actual device itself lies mainly with the manufacturers. However, hospitals also need to assure that their biomedical engineers are trained to work with their IT department to build secure networks for medical devices and include cybersecurity considerations in their buying decisions. Solutions to secure their devices and device networks do exist, and can be applied by manufacturers or healthcare providers.

- Asset management and risk analysis are critical to minimize the security risks of medical devices. Automated tools to support these activities do exist and standards and best practices are being put forward, for example the IEC 80001 series on risk management of medical device networks.
- Host Intrusion Detection and Prevention (HIDS/HIPS) is a security technology installed on the device itself that effectively excludes any undesired programs or an unauthorized user.
- Encryption can be used to protect patient data, but also to prevent data from being manipulated with the goal to change system settings.
- Device and software certificates can be used to control use of devices and deployment of device software and upgrades, minimizing the risk of unauthorized code being installed.
- Network-based security technologies, like Firewalls and Security Gateways, can be used to detect an external attack, but also to identify any devices that may be compromised by detecting connections to malicious external sources.

Medical device security is not only a challenge of today's healthcare ecosystem. Under the evolving umbrella of mobile health, or mHealth, new care delivery models will move devices into the patient's home. This will place medical devices on public networks, provide medical apps through consumer devices such as smartphones, and interlace personal data with clinical information.

With the evolving concept of "care is everywhere" we need to deal with cybersecurity, but also privacy concerns. The device will not only provide clinical information, but also information about patient behavior and location. Once again, it seems that regulations will have to catch up with technology. We will need new guidelines to address the new risks of information use, data ownership, and consent. ■

WEB THREATS

Web Threats

Web threats got bigger and much more aggressive in 2014 as holes in commonly used tools and encryption protocols were exposed and criminals made it harder to escape their malicious clutches.

The web presented an incredibly threatening landscape in 2014, a trend set to continue in 2015. Vulnerabilities and new variants of malware underlined that website security deserves full-time, business-critical attention.

At a Glance

- *The Heartbleed vulnerability left approximately half a million trusted websites at risk of significant data breaches in April.*[38]
- *The Heartbleed scare caused many more people to take note and improve standards in SSL and TLS implementation.*
- *Criminals are taking advantage of the technology and infrastructure that legitimate ad networks have created to distribute malicious attacks and scams.*
- *A big jump to 5 percent of total infected websites has bumped anonymizer sites into the top 10 types of infected sites for 2014.*
- *The total number of sites found with malware has virtually halved since 2013.*

Vulnerabilities

Vulnerabilities grabbed the headlines in 2014, and they continue to do so. At the time of writing, a new SSL/TLS vulnerability dubbed "FREAK" had been identified by several security researchers.[39] FREAK allows man-in-the-middle attacks on encrypted communications between a website visitor and website, which ultimately could allow attackers to intercept and decrypt communications between affected clients and servers. Once the encryption is broken by the attackers, they can steal passwords and other personal information and potentially launch further attacks against the affected website.

Looking back at 2014, three vulnerabilities disclosed in particular grabbed the news headlines.

Heartbleed

Heartbleed hit the headlines in April 2014, when it emerged that a vulnerability in the OpenSSL cryptographic software library meant attackers could access the data stored in a web server's memory during an encrypted session. This session data could include credit card details, passwords, or even private keys that could unlock an entire encrypted exchange.[40]

At the time, it was estimated that Heartbleed affected 17 percent of SSL web servers, which use SSL and TLS certificates issued by trusted certificate authorities.[41] This had a massive impact on businesses and individuals.

Not only was a great deal of sensitive data at risk, but the public also had to be educated about the vulnerability so they knew when to update their passwords. Website owners had to first update their servers to the patched version of OpenSSL, then install new SSL certificates, and finally revoke the old ones. Only then would a password change be effective against the threat, and communicating that to the general public posed a real challenge.

Fortunately, the response was swift and within five days none of the websites included in Alexa's top 1,000 were vulnerable to Heartbleed and only 1.8 percent of the top 50,000 remained vulnerable.[42]

ShellShock and Poodle

Heartbleed wasn't the only vulnerability to come to light in the online ecosystem in 2014. In September a vulnerability known as "Bash Bug" or "ShellShock," which affected most versions of Linux and Unix as well as Mac OS X, was discovered. ShellShock was a particularly good example that highlighted how quickly the security landscape could change for website owners; one day their servers are securely patched and up to date, and then, very suddenly, they are not and many of the initial patches are incomplete and must be patched again.

The easiest route of attack was through web servers, as attackers could use Common Gateway Interface (CGI), the widely used system for generating dynamic web content, to add a malicious

command to an environmental variable. The Bourne Again Shell (Bash),[43] the server component containing the vulnerability, would then interpret the variable and run it.[44]

Numerous threats took advantage of ShellShock, exposing servers and the networks to which they were connected, to malware that could infect and spy on multiple devices.

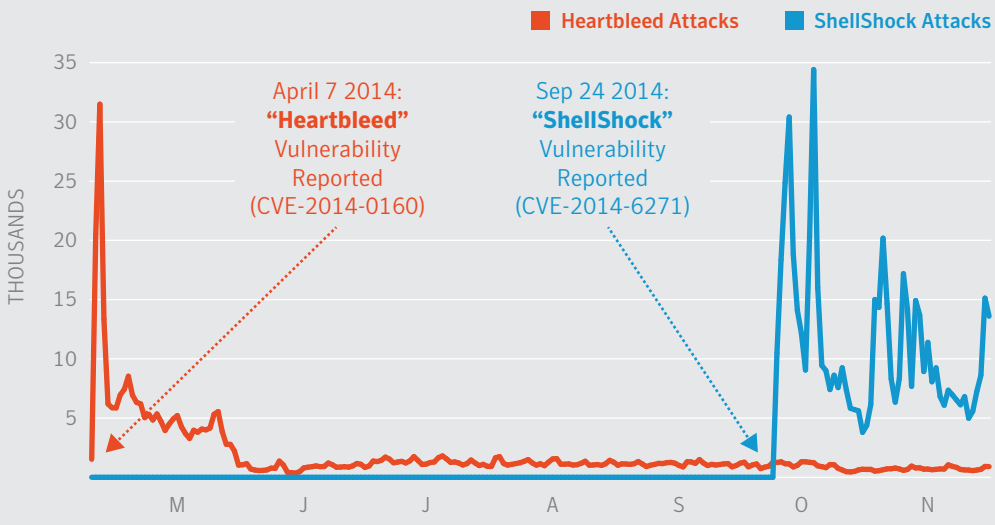
Attention then turned back to encryption in October 2014, when Google discovered a vulnerability known as Poodle. Potentially, this vulnerability allowed criminals to exploit servers that supported an older SSL protocol known as SSL 3.0. It interfered with the "handshake" process that verified the server's protocol forcing it to use SSL 3.0—even if a newer protocol was supported.[45]

A successful exploit allows attackers to carry out man-in-the-middle attacks to decrypt secure HTTP cookies, which then lets them steal information or take control of victims' online accounts. Fortunately, this was not as serious as Heartbleed. To take advantage of the Poodle vulnerability, the attacker would need to have access to the network between the client and server—for instance, through a public Wi-Fi hotspot.

Heartbleed and ShellShock could be viewed as a different class of vulnerability altogether.

High-Profile Vulnerabilities and Time to Patch

The attacks that quickly followed the announcement of these vulnerabilities were big news in and of themselves, albeit in a different manner than attention-grabbing zero-day vulnerabilities. Heartbleed and ShellShock could be viewed as a different class of vulnerability altogether, because they were used to compromise servers instead of end points. The key factor with these high-profile vulnerabilities was the prevalence of the software they affected, found in so many systems and devices. Given the software's widespread existence, these vulnerabilities instantly became hot targets for attackers, and both were exploited within hours of disclosure.



Heartbleed and ShellShock Attacks, April–November, 2014

Source: Symantec

The large spikes seen in the chart demonstrate that while Symantec signatures were in place to detect and block attacks almost immediately after disclosure, there were already a large number of attacks underway. Attackers were able to exploit the Heartbleed vulnerability within four hours of it becoming public.

The Vulnerability Rises

By Tim Gallo

Over the past few years the idea of vulnerability management has been frequently talked about but was often seen as an annoyance or a process that, while interesting, isn't as important as breach response or adversary tracking. However, 2014 gave vivid examples of the importance of addressing vulnerabilities. Three major vulnerabilities were in the news—and not just security industry news—including coverage by major media news outlets. They were colloquially known as Poodle, ShellShock, and Heartbleed.

The Heartbleed vulnerability even got its own logo.

Each of these vulnerabilities was discovered in areas traditionally not covered by most vulnerability management processes at the time. These processes have, as of late, been focused on laptops and servers, thanks to the regularity of publicized vulnerabilities by Adobe and Microsoft and these companies' speed in releasing patches. While we have seen, and will continue to see, new vulnerabilities in these applications, solid processes have been established here in patch deployment, vulnerability disclosure, and overall patch management processes.

It is this automation of patch deployment by operating system and application vendors that has forced attackers to shift their tactics somewhat. Attackers have moved to new methods of exploitation—or perhaps more accurately, they have moved back into the vulnerability research game. This shift back to combing through applications more thoroughly on the attacker's part has resulted in vulnerabilities being discovered in areas previously thought to be secure.

Let's take one of these vulnerabilities, ShellShock, as an example of what we will likely see in the coming years. ShellShock was, at best, a flawed feature and, at worst, a design flaw, in the Bourne Again Shell (Bash) that went overlooked for over 25 years before it was discovered to be exploitable, and subsequently disclosed publicly. ShellShock has been a part of the fabric of the Internet for most of the Internet's existence. In fact, the targets of ShellShock weren't just routers or Linux web servers but also email servers and even DDoS bots that utilize the shell—anything Unix-based that makes use of Bash.

We will likely continue to see vulnerabilities like this as the new normal for the coming years, for a few reasons. For starters, it is now apparent that the attackers are not going to rely on reusing the same old methods and the same old exploits. They are instead investing in researching new vulnerabilities in frequently used, older infrastructure that provides a broad attack surface.

These three high-profile vulnerabilities were also interesting because not only did they expose flaws in major components of Internet infrastructure, but they highlighted one of the dirty secrets of application development as well: code reuse. Code reuse is when a developer copies sections of code from existing applications for use in development of new applications. It is this practice, which has been around for as long as coding has existed, that can lead to vulnerabilities' being present in systems that may be completely unrelated.

When looking at the situation that led up to the Heartbleed discovery, legitimate uses of the OpenSSL library were a perfect example of code reuse. This code had long been seen as reliable and often went untested, as it was considered "a solved problem." However, new vulnerabilities in the library were discovered and developers around the globe had to scramble to determine if their code reuse implementations were vulnerable.

Additionally, we have seen a rise in bug bounty programs, and we no longer see governments threatening vulnerability researchers with jail time as in years past.[46] Therefore, the incentive to research vulnerabilities has increased and the repercussions of irresponsible disclosure, or even outright mercenary behavior, are no longer something researchers fear.

However, what we will also hopefully see is that remediation and better security practices will become more prevalent.

It takes the average IT professional only a few weeks of all-nighters to decide that planning ahead is far more advantageous. Better enforcement of configuration, policy, and patching across entire infrastructures will help. The moving of infrastructure to the cloud will help an overworked IT professional manage these issues as well.

As we look at the "detect and remediate" cycle of security, the return of vulnerabilities is a key point in understanding the threat landscape. To become more effective security professionals, we need to additionally think about how we "protect and respond" and "inform and assess" as well. That means we need to become better planners and testers, look to intelligence to help keep us informed, and know our environment well enough to understand whether that intelligence is actionable.

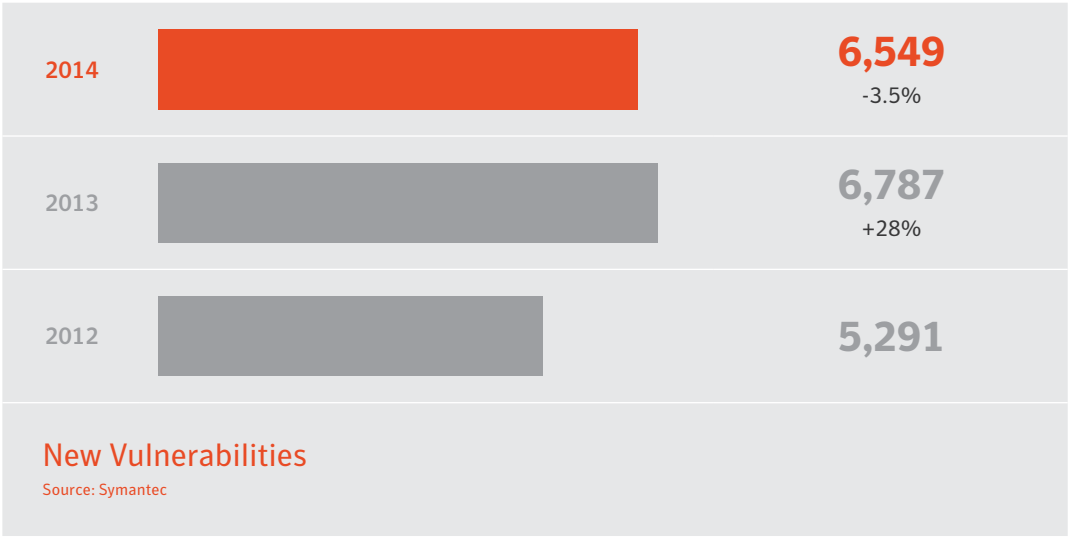
We need to better understand that the fabric of the Internet is likely still riddled with holes, and it is our responsibility to maintain vigilance in order to be prepared to deal with new vulnerabilities as they are disclosed in a process-oriented and programmatic manner. To not do so would be detrimental to our future. ■

SSL and TLS Certificates Are Still Vital to Security

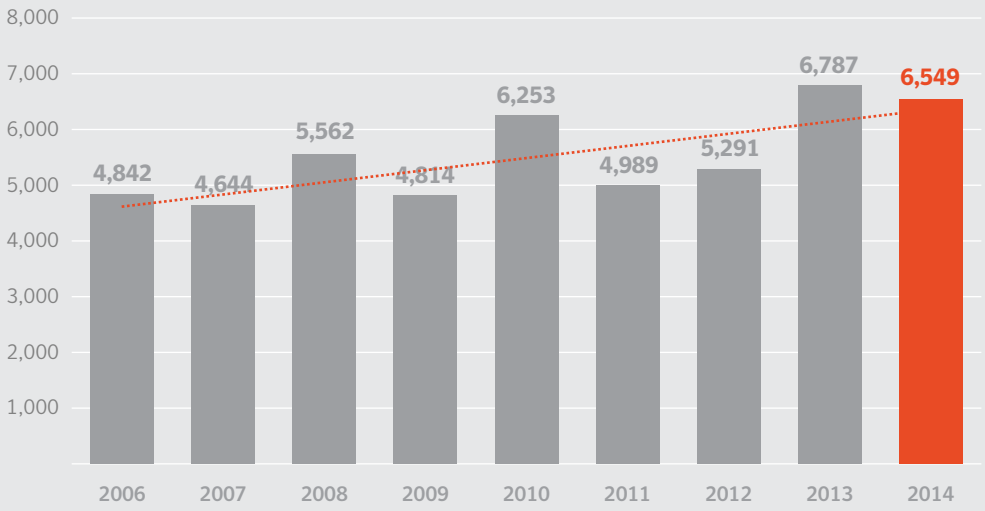
It's important to note that while online security was shaken in 2014, SSL certificates and their more modern counterparts, TLS certificates, still work and are still essential. In fact, the Heartbleed incident demonstrated just how quickly the online security community could respond to these types of threats.

Industry standards are also constantly improving thanks to the hard work and vigilance of organizations like the CA/Browser Forum, of which Symantec is a member. In other words, the foundations of Internet security, which keep your site and visitors safe, are still strong and are only getting stronger.

Vulnerabilities as a Whole



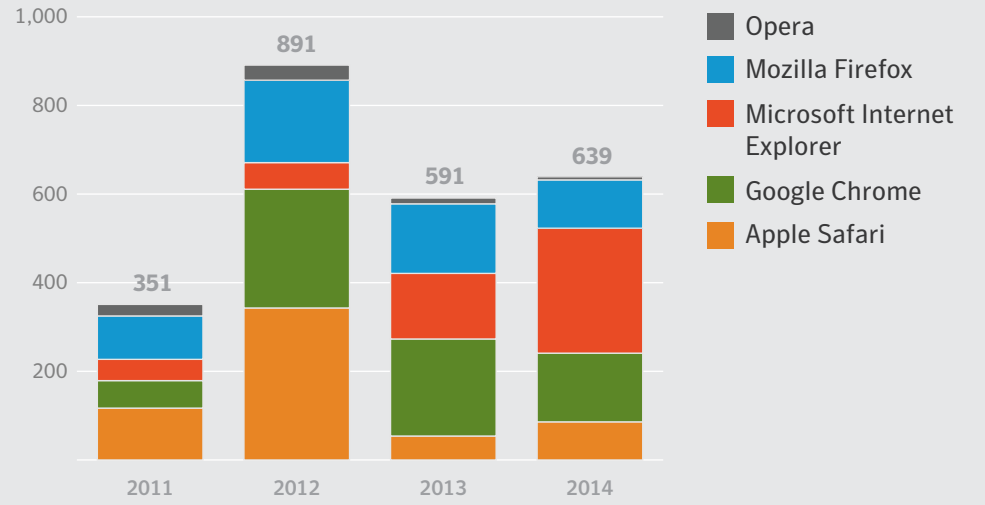
■ *The overall number of vulnerabilities declined 3.5 percent in 2014.*



Total Number of Vulnerabilities, 2006–2014

Source: Symantec

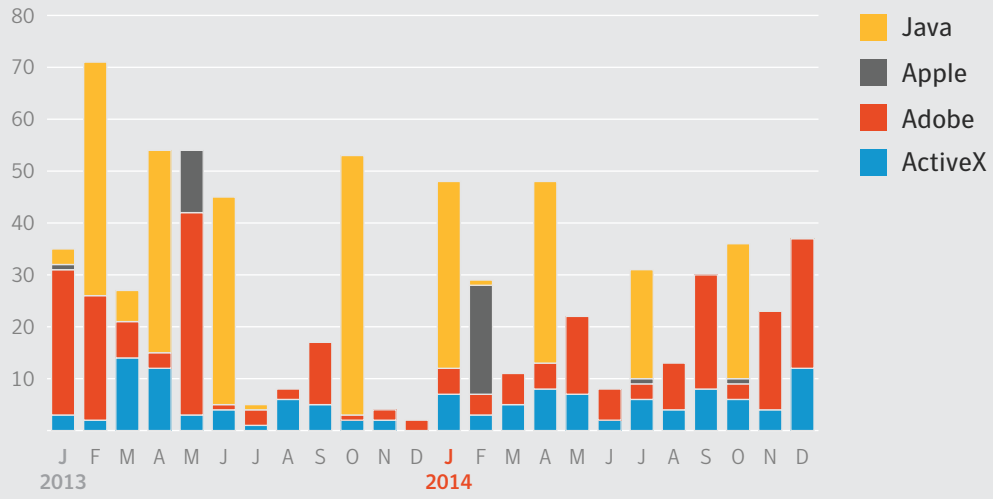
- *While reported vulnerabilities represent a general risk, zero-day vulnerabilities are potentially much more serious. These are vulnerabilities that are discovered only after they are exploited by attackers. See the chapter on Targeted Attacks for further coverage on zero-day vulnerabilities.*



Browser Vulnerabilities, 2011–2014

Source: Symantec

- *There was a 8 percent increase in the number of browser vulnerabilities reported in 2014.*
- *Microsoft Internet Explorer reported the largest number of vulnerabilities, followed by Google Chrome.*



Plug-in Vulnerabilities by Month, 2013–2014

Source: Symantec

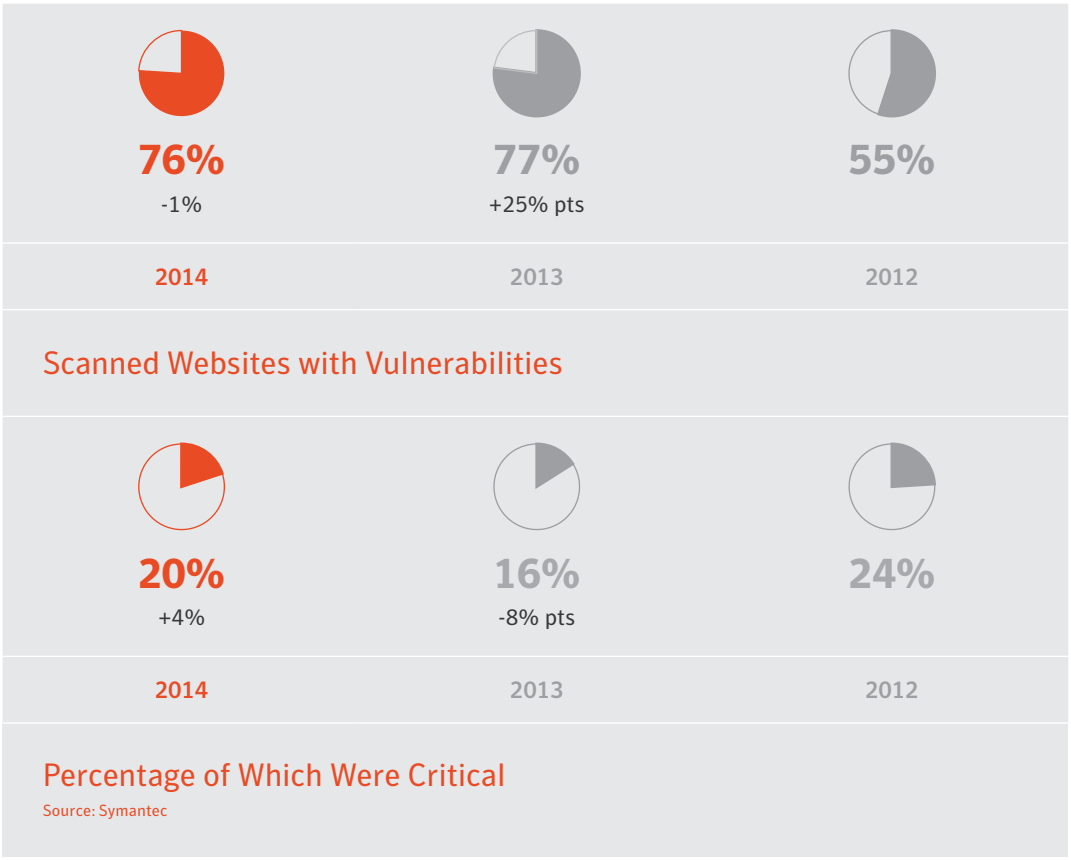
- *With a total of 336 vulnerabilities, there was a 10 percent decrease in the number of plug-in vulnerabilities reported in 2014.*
- *Adobe, with its Acrobat and Flash plugins, disclosed the largest number of vulnerabilities, followed by Oracle and its Java plug-in.*

Rank	Name
1	SSL/TLS Poodle Vulnerability
2	Cross-Site Scripting
3	SSL v2 support detected
4	SSL Weak Cipher Suites Supported
5	Invalid SSL certificate chain
6	Missing Secure Attribute in an Encrypted Session (SSL) Cookie
7	SSL and TLS protocols renegotiation vulnerability
8	PHP 'strrchr()' Function Information Disclosure vulnerability
9	http TRACE XSS attack
10	OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability

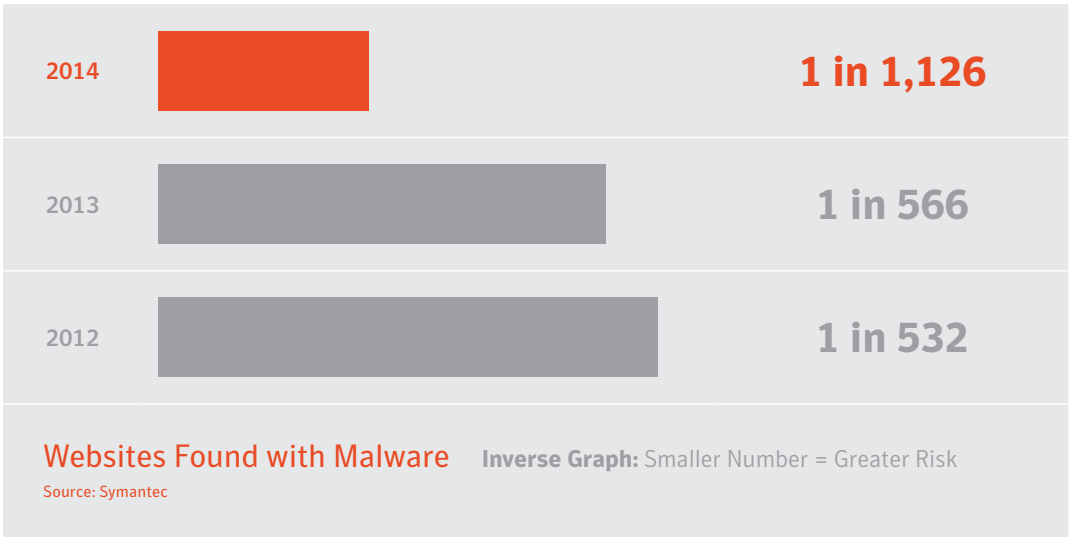
Top 10 Vulnerabilities Found Unpatched on Scanned Web Servers

Source: Symantec

- *As was the case in 2013, SSL and TLS vulnerabilities were most commonly exploited in 2014.*



- *In 2014, 20 percent (1 in 5) of all vulnerabilities discovered on legitimate websites were considered critical, meaning they could allow attackers to access sensitive data, alter the website's content, or compromise visitors' computers.*



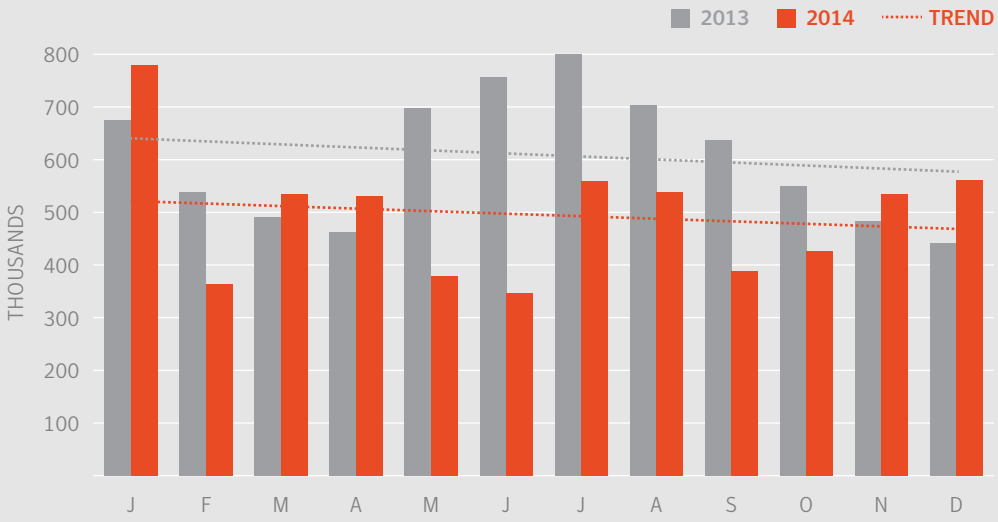
- *The number of websites found with malware decreased by nearly half in 2014.*

Rank	2014 Top 10 Most Frequently Exploited Categories of Websites	2014 Percentage of Total Number of Infected Websites	2013 Top 10	2013 Percentage
1	Technology	21.5%	Technology	9.9%
2	Hosting	7.3%	Business	6.7%
3	Blogging	7.1%	Hosting	5.3%
4	Business	6.0%	Blogging	5.0%
5	Anonymizer	5.0%	Illegal	3.8%
6	Entertainment	2.6%	Shopping	3.3%
7	Shopping	2.5%	Entertainment	2.9%
8	Illegal	2.4%	Automotive	1.8%
9	Placeholder	2.2%	Educational	1.7%
10	Virtual Community	1.8%	Virtual Community	1.7%

Classification of Most Frequently Exploited Websites, 2013–2014

Source: Symantec

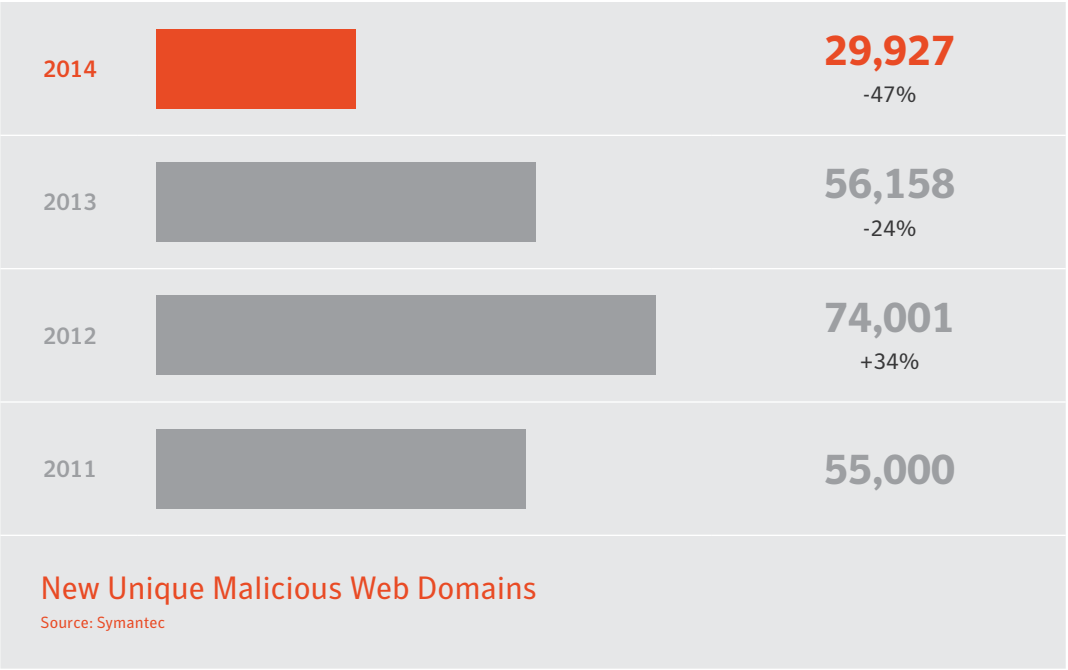
In terms of the type of websites most frequently exploited, it's interesting to note the inclusion of anonymizer websites in the top 10 this year. This is perhaps another case of criminals following the crowds as more people look to evade tracking by ISPs and others and increase their browsing privacy.



Web Attacks Blocked per Month, 2013–2014

Source: Symantec

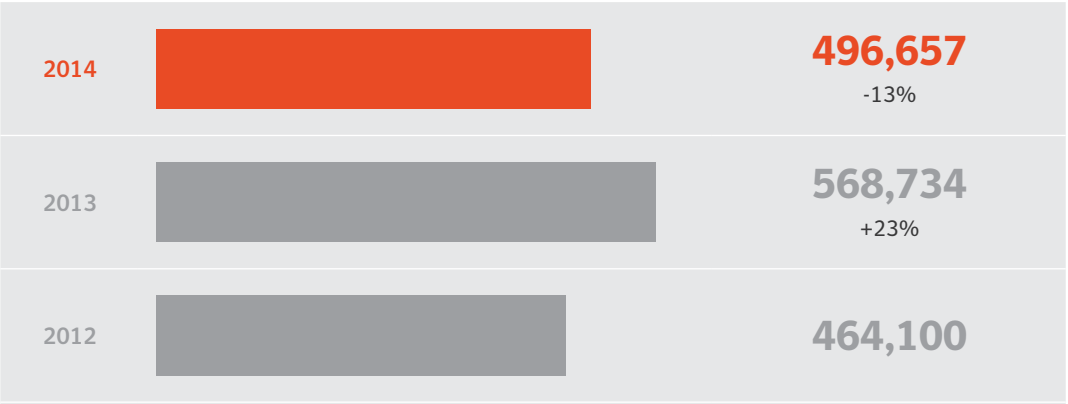
For the most part, the bulk of the 12.7% drop in the average number of daily attacks blocked occurred in the latter half of 2013. The decline in attacks throughout 2014 has been much more shallow than in 2013.



New Unique Malicious Web Domains

Source: Symantec

- *A 47 percent drop in unique malicious web domains in 2014 could indicate an increase in the use of cloud-based SaaS-type toolkits.*



Web Attacks Blocked per Day

Source: Symantec

- *The number of web attacks blocked per day dropped 13 percent in 2014.*

With minor fluctuations from year to year, the trend in the number of vulnerabilities continues upward. Remedies, workarounds, or patches are available for the majority of reported vulnerabilities. However, malware authors know that many people do not apply these updates and so they can exploit well-documented vulnerabilities in their attacks. In many cases, a specialist "dropper" scans for a number of known vulnerabilities and uses any unpatched security weakness as a back door to install malware. This, of course, underlines the crucial importance of applying updates.

This is how web exploit toolkits, such as Sakura and Blackhole, have made it easier for attackers to exploit an unpatched vulnerability published months or even years previously. Several exploits may be created for each vulnerability, and a web attack toolkit will perform a vulnerability scan on the browser to identify any potentially vulnerable plug-ins and the best attack that can be applied. Many toolkits won't utilize the latest exploits for new vulnerabilities if old ones will suffice. Exploits against zero-day vulnerabilities are uncommon and highly sought after by attackers, especially for use in watering-hole-style targeted attacks.

Compromised Sites

Three-quarters of the websites Symantec scanned for vulnerabilities in 2014 were found to have issues—about the same as last year. The percentage of those vulnerabilities classified as critical, however, increased from 16 to 20 percent.

In contrast, the number of websites actually found with malware was much lower than last year, down from 1 in 566 to 1 in 1,126. This seems to have had a knock-on effect on the number of web attacks blocked per day, which has also declined, though only by 12.7 percent, suggesting infected websites were, on average, responsible for more attacks in 2014. This is due to the fact that some web attack toolkits are designed to be used in the cloud, as software as a service (SaaS). For example, a compromised website may use an HTML iframe tag, or some obfuscated JavaScript, in order to inject malicious code from the SaaS-based exploit toolkit rather than launch the malicious attack directly from exploit code hosted on the compromised website. This growth in SaaS-based exploit toolkits is also evidenced in the decline in the number of new malicious domains used to host malware, which fell by 47 percent, from 56,158 in 2013 to 29,927 in 2014.

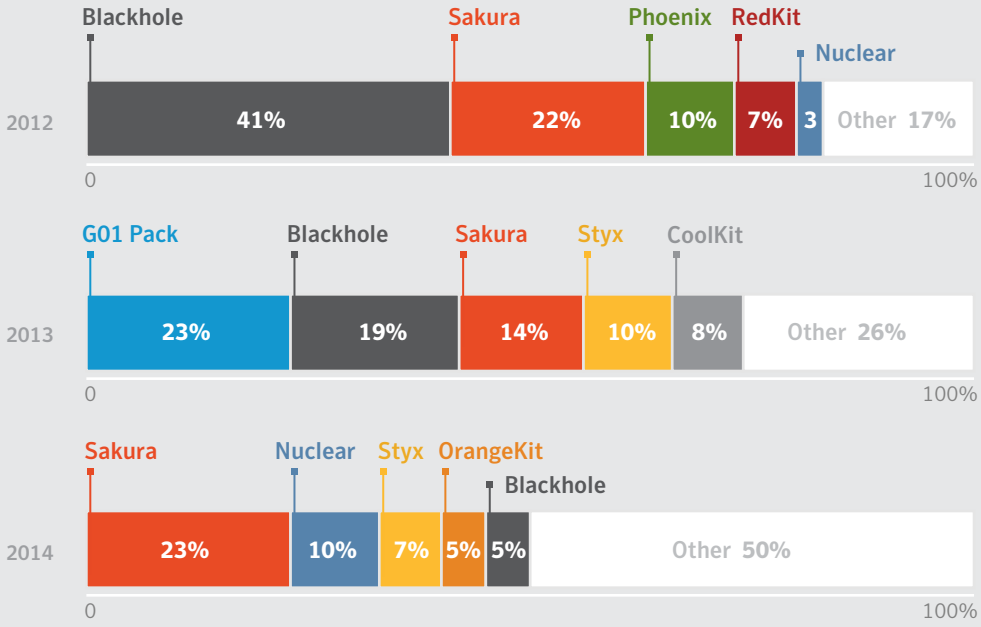
These SaaS toolkits are often located on bulletproof hosting services, with IP addresses that can change quickly and domain names that may be dynamically generated.

Web attack toolkits perform scans on the victims' computers, looking for vulnerable plug-ins in order to launch the most effective attack. Moreover, these SaaS toolkits are often located on bulletproof hosting services, with IP addresses that can change quickly and domain names that may be dynamically generated, making it more difficult to locate the malicious SaaS infrastructure and shut it down. Attackers are also able to control how the exploits are administered such as enabling the attacks only if a cookie has been set by the initial compromised website thereby preserving the malicious code from the prying eyes of search engines and security researchers.

With the majority of websites still accommodating vulnerabilities, it is apparent that many website owners are not keeping on top of vulnerability scans, although they may be paying more attention to malware scans that can potentially reveal malicious software. However, malware is often planted following previous exploitations of vulnerabilities, and prevention is always better than cure.

With so many potentially vulnerable websites, criminals in 2014 were achieving considerable success exploiting them, and many were also quick to take advantage of the SSL and TLS vulnerabilities. Moreover, the greater prevalence of social media scams and malvertising in 2014 suggests criminals are already turning to them as alternative methods of malware distribution.

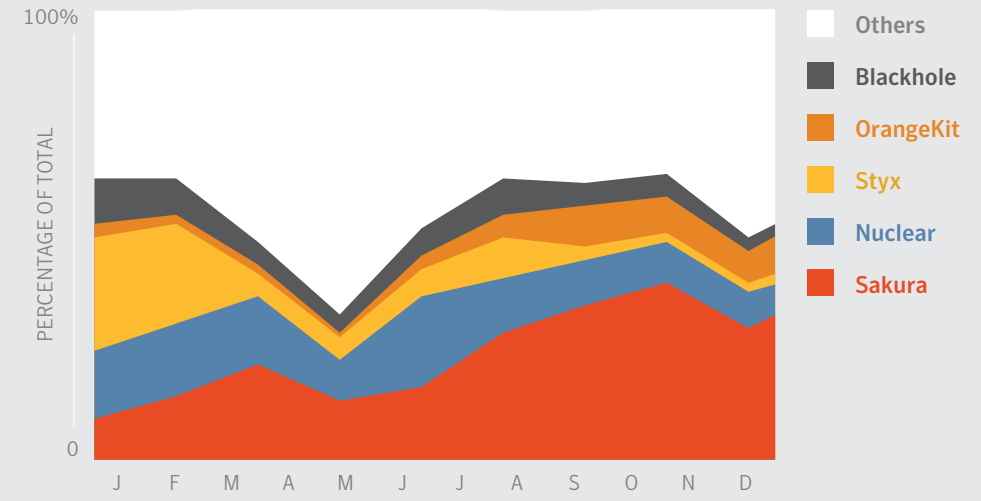
Web Attack Toolkits



Top 5 Web Attack Toolkits, 2012–2014

Source: Symantec

- *With half of active web attack toolkits falling into the "other" category, overall toolkit usage was much more fragmented in 2014 than in previous years.*
- *After the arrest of the alleged creator in late 2013, the Blackhole toolkit has dropped 14 percentage points in 2014, comprising only five percent of all web attack toolkit activity. At its peak, Blackhole make up 41 percent of all toolkit activity.*



Timeline of Web Attack Toolkit Use, Top 5, 2014

Source: Symantec

Example of a Browlock webpage demanding a fine for surfing pornography illegally.[47]

Malvertising

As we moved into 2014, we saw ransomware and malvertising cross paths, with the number of victims getting redirected to Browlock websites hitting new heights.

Browlock itself is one of the less aggressive variants of ransomware. Rather than malicious code that runs on the victim's computer, it's simply a webpage that uses JavaScript tricks to prevent the victim from closing the browser tab. The site determines where the victim is and presents a location-specific webpage, which claims the victim has broken the law by accessing pornography websites and demands that they pay a fine to the local police.

The Browlock attackers appear to be purchasing advertising from legitimate networks to drive traffic to their sites. The advertisement is directed to an adult webpage, which then redirects to the Browlock website. The traffic that the Browlock attackers purchased comes from several sources, but primarily from adult advertising networks.[48]

To escape, victims merely need to close their browser. However, the large financial investment criminals are making to direct traffic to their site suggests people are just paying up instead. Perhaps this is because the victim has clicked on an advert for a pornographic site before ending up on the Browlock webpage: guilt can be a powerful motivator.

As we moved into 2014, we saw ransomware and malvertising cross paths, with the number of victims getting redirected to Browlock websites hitting new heights.

Malvertising at Large

It's not just ransomware that is spread through malvertising: malicious advertisements also redirect to sites that install Trojans. Some malicious advertisements even use drive-by attacks to infect a victim's device without the user clicking on the advertisements.

The appeal for criminals is that malvertising can hit major, legitimate websites drawing in high volumes of traffic. Ad networks also tend to be highly localized in their targeting, meaning

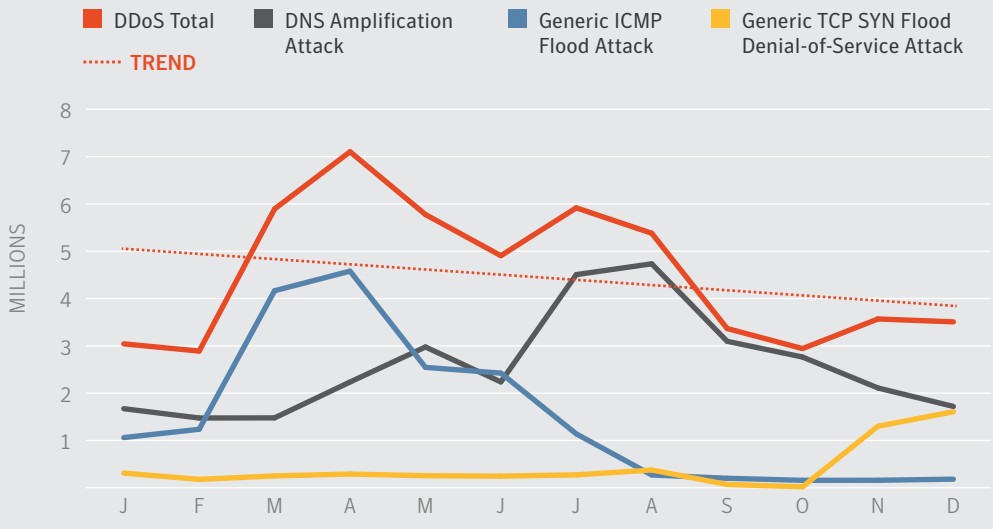
criminals can tailor their scams to specific victims—for example, people searching for financial services. Legitimate ad networks sometimes inadvertently do all the work for the criminals.

Criminals also switch tactics to avoid detection. For example, they'll run a legitimate ad for a few weeks, to appear aboveboard, and then convert it to a malicious ad. In response, ad networks need to run scans regularly rather than just when a new ad is uploaded.

For website owners, it's hard to prevent malvertising, as they have no direct control over the ad networks and their customers. However, site managers can reduce risk by choosing networks that restrict ad functionality so advertisers can't embed malicious code in their promotions. And of course, when selecting an ad network, due diligence goes a long way.

Denial of Service

Denial-of-service attacks give attackers another way to target individual organizations. By overloading critical systems, such as websites or email, with Internet traffic as a way to block access, denial-of-service attacks can wreak financial havoc and disrupt normal operations. Distributed denial-of-service (DDoS) attacks are not new, but they are growing in intensity and frequency.[49] For example, Symantec saw a 183 percent increase in DNS amplification attacks between January and August 2014.[50] According to a survey by Neustar, 60 percent of companies were impacted by a DDoS attack in 2013 and 87 percent were hit more than once.[51] Motives include extortion for money, diversion of attention away from other forms of attack, hacktivism, and revenge. Increasingly, would-be deniers of service can rent attacks of a specified duration and intensity for as little as $10–$20 in the online black market. ■



DDoS Attack Traffic Seen by Symantec's Global Intelligence Network, 2014

Source: Symantec

- *DDoS traffic saw peaks in April and July of 2014.*
- *There was a 183 percent increase in DNS amplification attacks between January and August 2014.*

SOCIAL MEDIA & SCAMS

Social Media and Scams

In 2014 criminals hijacked the power of "social proof"—the idea that we attribute more value to something if it's shared or approved by others. The classic example is of two restaurants: one with a big queue, the other empty. People would rather wait in the queue because popularity suggests quality.

Criminals exploited this theory by hacking real accounts on platforms like Snapchat so that when you saw an endorsement for a scam product or link, you'd trust it because it seemed to come from someone you actually knew.

The public also undervalued their data in 2014, freely giving away email addresses and login credentials without checking that they were on a legitimate website.

While scammers certainly evolved their tactics and ventured onto new platforms in 2014, a lot of their success continued to come from people's willingness to fall for predictable and easily avoided scams.

Social Media

Criminals will go wherever there are people to be scammed. There are large numbers of people using well-established social media platforms, and, as such, they play host to plenty of scams. The rise in popularity of messaging and dating apps means scammers have taken note and taken advantage, and a variety of scams are being seen on these platforms.

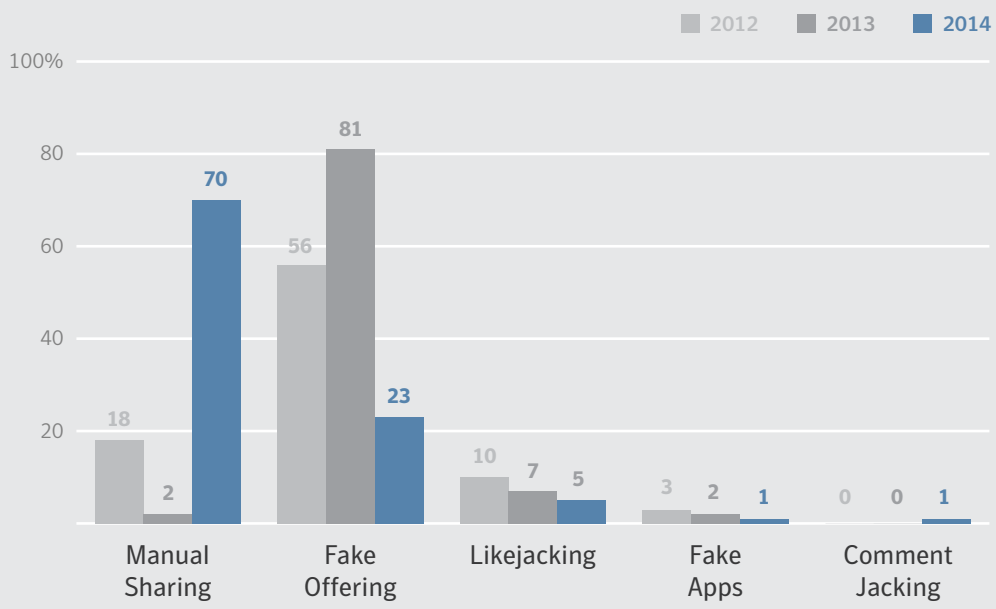
Facebook, Twitter, and Pinterest

The big shift in social media scams this year has been the uptick in manual sharing scams. This is where people voluntarily and unwittingly share enticing videos, stories, pictures, and offers that actually include links to malicious or affiliate sites.

At a Glance

- *Social media scammers go after payouts from affiliate programs by offering false promises of weight loss, money, and sex to drive clicks and sign-ups.*
- *Many people use the same password on multiple networks, meaning criminals have been able to spam multiple accounts thanks to a single hack.*
- *Scammers take advantage of the power of social proof by relying on real people rather than bot networks to share their scams.*
- *Many phishing scams play on either fears generated by hacking and health-scare stories or intrigue piqued by scandalous celebrity stories, both real and fake.*

In 2014 criminals hijacked the power of "social proof"—the idea that we attribute more value to something if it's shared or approved by others.



Manual Sharing – These rely on victims to actually do the work of sharing the scam by presenting them with intriguing videos, fake offers or messages that they share with their friends.

Fake Offering – These scams invite social network users to join a fake event or group with incentives such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.

Likejacking – Using fake “Like” buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user’s newsfeed, spreading the attack.

Fake Apps – Users are invited to subscribe to an application that appears to be integrated for use with a social network, but is not as described and may be used to steal credentials or harvest other personal data.

Comment Jacking – This attack is similar to the "Like" jacking where the attacker tricks the user into submitting a comment about a link or site, which will then be posted to his/her wall.

Social Media, 2012–2014

Source: Symantec

In 2014, 70 percent of social media threats required end users to propagate them, compared with only 2 percent in 2013.

Affiliate Programs: The Fuel That Drives Social Media Scams

By Satnam Narang

If you have used a social network in the past decade, chances are you've seen one of the following offers appear in your news feeds and timelines:

- Free smartphones, airline tickets, or gift cards
- Unbelievable news about celebrities (sex tapes, death)
- Unbelievable world news (specifically, natural disasters)
- Proposals to get naked on a webcam or propositions from alleged sex workers

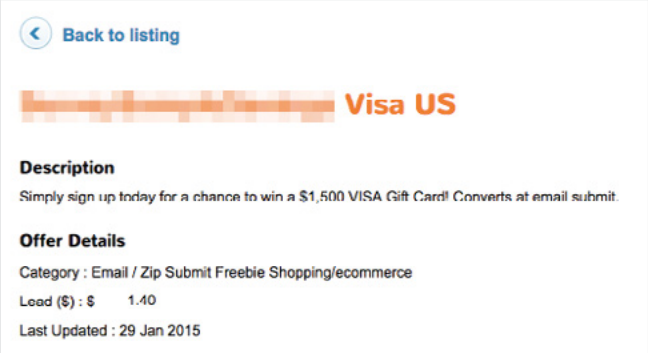
It has become clear that as any social networking platform becomes popular, scammers are never far behind. While each platform may be different and each scam slightly varied, the constant is that affiliate networks are the driving force behind them.

Affiliate marketing is a popular way for companies to increase their business on the Internet. A business uses affiliates to help market and sell their products. For instance, an affiliate could feature a book on their webpage and provide a link directly to a vendor that sells that book. And for every sale, the affiliate receives a small commission.

While legitimate vendors use affiliates, so do illegitimate ones. And in some cases the vendor is legitimate, but some of their affiliates are willing to use unscrupulous methods to profit from an affiliate program.

Affiliates participate in an affiliate program by appending a special ID to the URLs that are used when a customer clicks an advertisement. The unique ID helps keep track of where the click comes from. This affiliate ID enables merchants to track the contributions from affiliates and thus pay out commissions.

Scammers monetize on social media by leveraging affiliate networks. When a user is asked to fill out a survey or sign up for a premium offer to a service, he or she becomes the referral for an affiliate program. By tricking users into participating in a survey and/or signing up for a premium service, the scammer makes money.



Details on these semi-legitimate affiliates and their payouts are murky. Many won't share details, making it hard to estimate just how much money an affiliate can make. However, most affiliate networks put up bids from merchants, which state clearly what action is required for a conversion. In the example above, a $1,500 Visa gift card advertisement will convert when the referrer submits his or her email address. This particular merchant values each email conversion at $1.40 when paying affiliates.

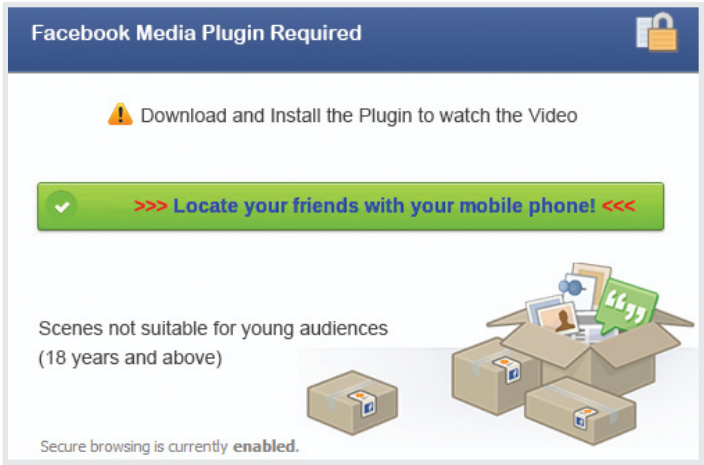
On the popular dating application Tinder, we found affiliate links to adult dating services and webcam sites. These sites promote their affiliate payouts directly. One site pays affiliates up to $6 for every user who signs up for an account and up to $60 if a user signs up for a premium service, which typically involves paying for a subscription using a credit card.

Based on the pricing structure, convincing users to sign up for the premium service could be highly profitable. However, scammers drive so much traffic to these sites that sign-ups for an account, at only $6 each, are enough to create a handsome profit. The users who do sign up for a premium service are just the icing on the cake.

Legitimate merchants, and some affiliate networks, have tried to tackle scams on their platforms, but as long as there is money to be made from these shady affiliate programs, they will persist. As a merchant, it is important to know the affiliates you work with and ensure they are being transparent with you about their practices.

End users should be mindful when using any social network, keeping an eye out for free offers for gadgets, gift cards, and airline tickets or for invitations from attractive women to join adult dating and webcam sites. If you are asked to fill out a survey or sign up for a service using a credit card, you are most likely being scammed. As the old adage goes, if it sounds too good to be true, it probably is. ■

Facebook share dialog with fake comments and shares.



Scam site asks users to install fake Facebook media plug-in.

For example, scammers took advantage of the death of Robin Williams by sharing what was supposed to be his goodbye video. Users were told they had to share the video with their friends before they could view it, and were instructed to fill out surveys, download software, or were redirected to a fake news website. There was no video.[52]

With manual sharing there's no hacking or jacking necessary—people and their networks do all the work for the criminals. Other social media scams require a bit more work on the part of the criminal. Likejacking and comment jacking, for example, ask victims to click what appears to be a "continue" or "verification" button to access some enticing content but actually masks the fact the victim is liking or commenting on the post to increase its popularity and reach.

Instagram

Instagram, the picture-sharing platform, now has more monthly active users than Twitter, and legitimate brands use it as a marketing channel.[53,54] Among the scams seen on Instagram in 2014 were those where criminals tried to monetize prepopulated accounts and mimic offers employed by legitimate corporate users.

In one scam, fake accounts are created, purporting to be lottery winners who are sharing their winnings with anyone who will become a follower. In another scam, scammers pretend to be well-known brands giving away gift cards. Instagram users are told to follow the fake accounts and add their personal information, like email addresses, in the comments to receive incentives.

> Once a fake account has enough followers, the criminals change the name, picture, and bio, so when the incentive fails to materialize, people can't locate the account to mark it as spam.

Victims often think nothing of giving away their details. According to our Norton Mobile Apps Survey Report, 68 percent of people surveyed will willingly trade in various types of private information for a free app.[55] In fact, some even send $0.99 to the scammers in order to cover the return postage for the so-called offer. (The offer never arrives, of course.) It's such a small amount, so people don't worry, but they're giving away more details, and scammers are getting an extra cash bonus.[56]

This is particularly prevalent on Instagram, partly because there is no verified check for legitimate accounts. And as soon as one person falls for the scam, that person's friends who follow his or her stream will see the posted picture and often jump on board too.

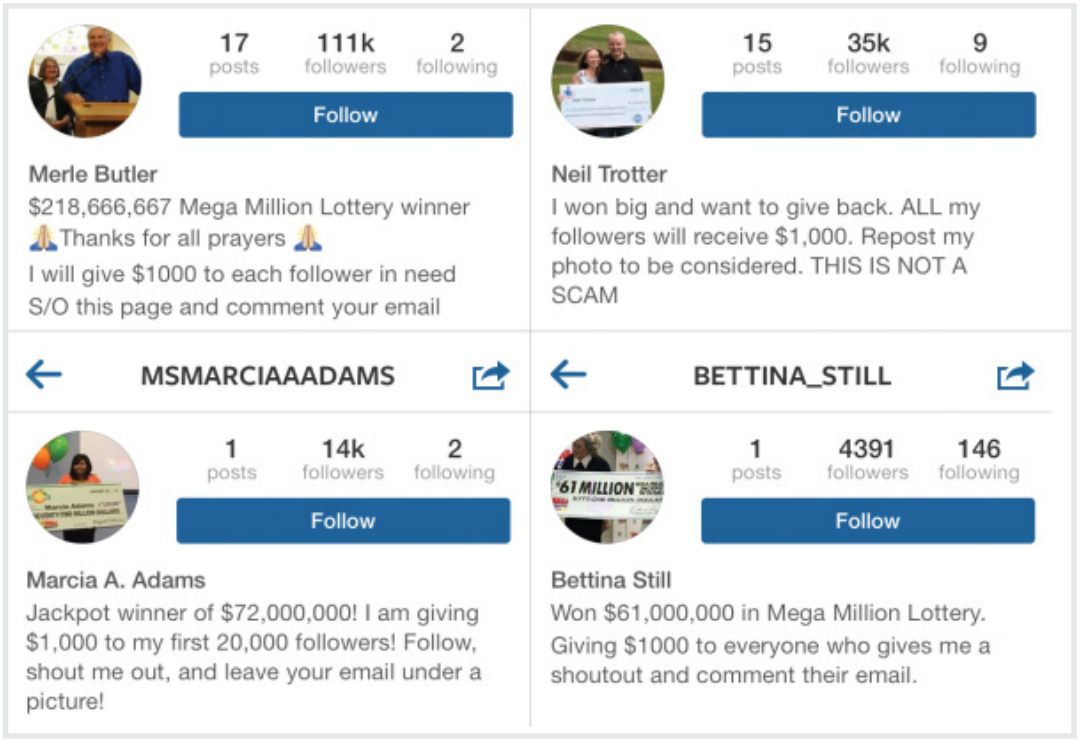
Once a fake account has enough followers, the criminals change the name, picture, and bio, so when the incentive fails to materialize, people can't locate the account to mark it as spam. Criminals then sell this altered account with all its followers to the highest bidder.

Shortly afterward a new account usually pops up in the guise of the original fake profile, claiming the old account was hacked, and the process starts all over again.

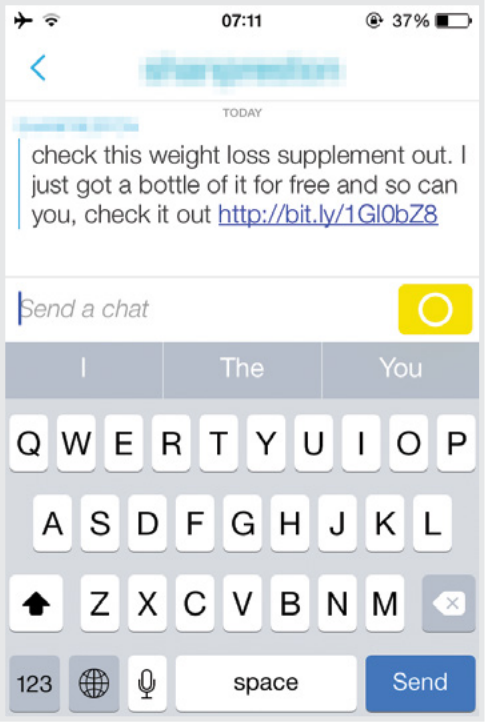
Messaging Platforms

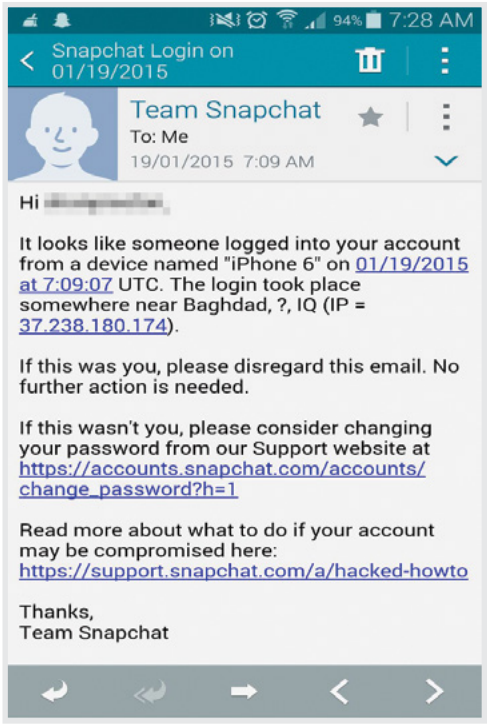
This year Snapchat, the social app that allows people to send images and videos that self-destruct within 10 seconds of the recipient's opening the message, was hit particularly hard.

In October 2014, several Snapchat accounts were hacked and people reported receiving messages from their friends with a live link promoting diet pills. Snapchat claims these accounts were compromised because certain users reused the same password on multiple websites, one of which had been breached.[57]

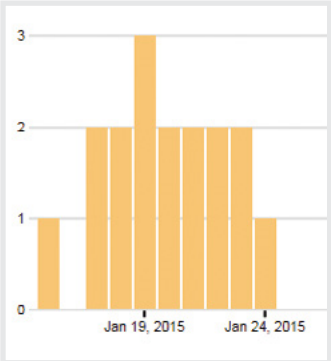


Instagram accounts impersonating real-life lottery winners.[58]





An example of a legitimate user account being compromised to send spam to the victim's circle of friends. The legitimate owner of the compromised account was quickly notified by Snapchat.



Example of click-through rates for the URL included in the Snapchat spam example above.

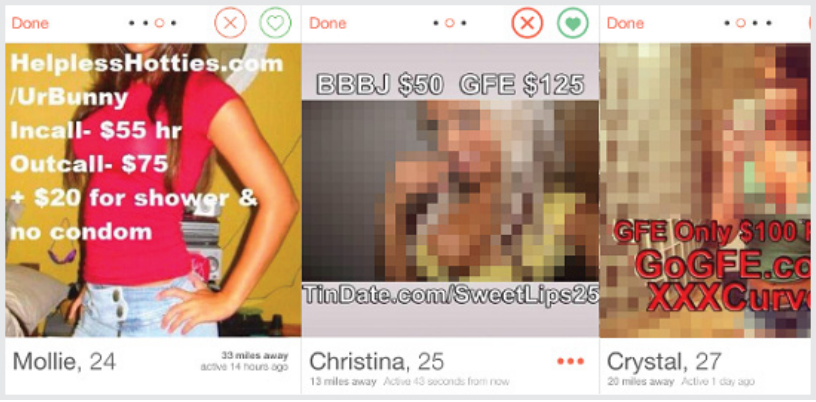
URL shortening services are popular among spammers and social networking users alike because they provide a shortened link. For spammers, they have an added benefit: they obfuscate the domain name of the spam website behind them. Additionally, by appending "+" to the end of a Bitlink, spammers and their affiliates now have easy access to click-through statistics and other demographics.

Short URLs are frequently seen not only in email spam but also in SMS spam and some of the newer forms of spam spread through social networks.

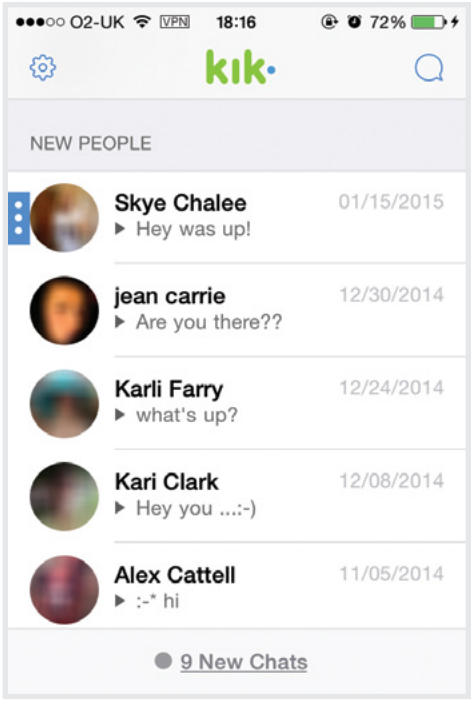
In October 2014 Symantec also saw an incident, referred to online as "The Snappening," when supposedly destroyed Snapchat images began appearing online. This originated from an unapproved third-party app that some people used to archive their Snapchat photos.

Often, the security and privacy policies of emerging social media platforms aren't as strong as they could or should be, and users don't help the situation by replicating their passwords across multiple platforms and using unverified third-party apps to enhance their experience.

Unless users begin to think about the risk they're exposing themselves to, we're likely to see similar account hijacking stories in 2015 on whatever the next big platforms turn out to be.



Historical overview of fake prostitution profiles on Tinder.[59]



Examples of spam "cam girl"-type messages appearing as new chats on Kik Messenger.

Dating Scams

Sexual content has always gone hand in hand with cybercrime, and 2014 was no different.

In 2014, adult-themed scams embraced popular dating apps, with examples appearing on Tinder and on messaging services, such as Snapchat and Kik Messenger. The goal is to get people to click through and sign up for external websites, at which point scammers earn a commission as part of an affiliate program.[60]

Some affiliate programs will pay out for every victim who clicks through, and others will pay out only if a victim signs up and hands over credit card details. Some sites pay $6 per lead for a successful sign-up and up to $60 if a lead becomes a premium member.[61] These schemes can be, in other words, a profitable monetization strategy for online criminals. (See "Affiliate Programs: The Fuel That Drives Social Media Scams" for more on affiliate marketing.)

The scam usually starts with the profile of an attractive young girl offering adult webcam time, sexting, or hookups. In Tinder there have also been cases of profile pictures overlaid with text offering prostitution services. Scammers put the text within the image in an attempt to beat spam filters.

The recipient then clicks through to or manually visits an affiliate website if he or she wants to continue the encounter. In reality these "hot chicks" are nothing more than scripted bots with sexy profile pictures, and there's no one waiting on the other side.

These promises of sexual content prove popular with the public: one particular campaign, associated with a site called blamcams, resulted in nearly half a million clicks across seven URLs in less than four months.[62] For scammers tied to affiliate programs or who use links to fake webcam sites to phish for credit card details, that's a good source of income.

Malcode in Social Media

It's worth noting that while most sharing scams are concerned with gaining clicks and sign-ups for affiliate programs, there was a case in 2014 where a Facebook scam redirected to the Nuclear exploit kit. When successful, this scam gives attackers control of a victim's computer and allows them to send out spam email and malicious files.[63]

People need to be wary of links posted by friends that seem unusually sensational and, rather than clicking on the link, should go directly to a trusted news source and search for the story there.

The Rise of "Antisocial Networking"

Privacy concerns—both about government surveillance and oversharing with service providers—have triggered the launch of new social networks that prioritize secrecy, privacy, and/or anonymity, such as Secret, Cloaq, Whisper, ind.ie, and PostSecret. These types of applications are havens for gossip, confessions, and, sometimes, the darker side of human nature. Some argue that secrecy is the key to the next phase of social networking.[64,65] Critics say that anonymous forums, such as 4chan, create safe havens for trolls, bullies, and criminals.[66] Existing social networks, such as Twitter and Facebook, have responded to these concerns with greater disclosure and by sharpening up their privacy policies. For example, Facebook now publishes its number of government data requests,[67] Twitter is considering a "whisper mode,"[68] and Google has enhanced encryption on its Gmail email service.[69]

Some argue that secrecy is the key to the next phase of social networking.

While the desire to remain anonymous may be very attractive for some individuals, there is always a downside that we must keep in mind. Some organizations have very strict guidelines and policies that govern how their employees must conduct themselves online, but many are still adapting to these new environments where people can potentially say whatever they like with impunity. Businesses should ensure their electronic communication policies address these concerns and technologies are in place for monitoring potential breaches of the rules. While it may not be appropriate to block access, it may prove invaluable to be able to monitor such activities.

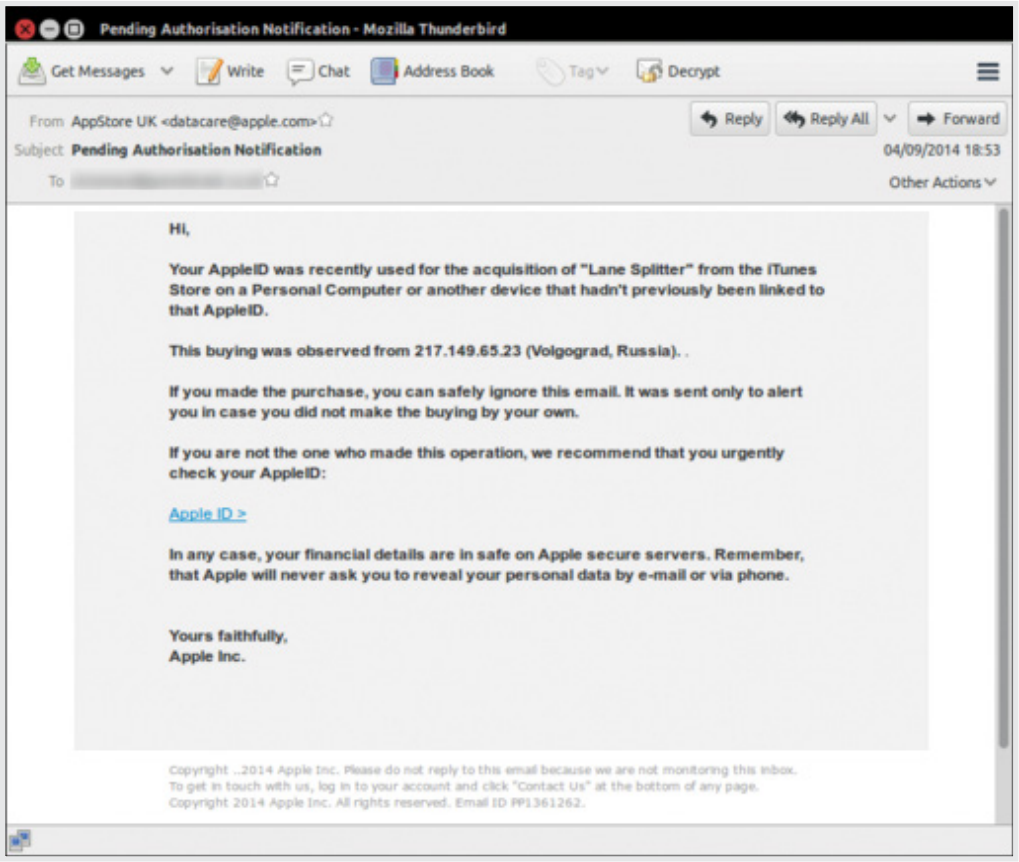
Phishing

There was a dip between June and September, but the overall phishing rate in 2014 was 1 in 965, compared with 1 in 392 in 2013. Phishing attacks toward the end of the year were boosted by the surge in Apple ID phishing schemes that emerged after the headline-grabbing hack that saw several nude pictures of celebrities stolen and published. Apple IDs have always been a target for phishers, but this news story meant people were particularly receptive to messages purporting to be about the security of their iCloud accounts.

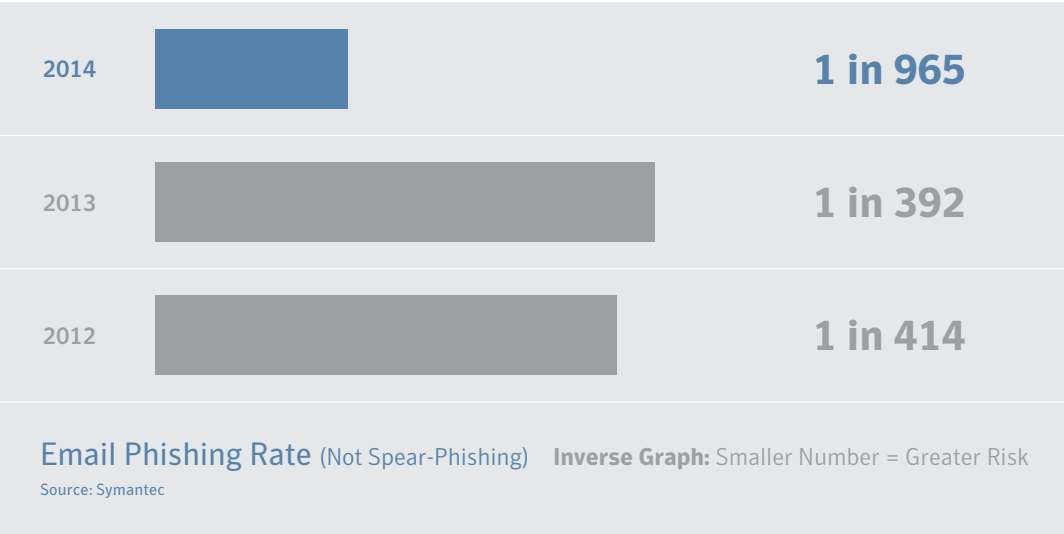
The Kelihos botnet looked to exploit the public's fear by sending messages that claimed a purchase had been made on the victim's iCloud account from an unusual device and IP address. The victim was encouraged to urgently check his or her Apple ID by clicking an accompanying link, which led to a phishing page. Masquerading as an Apple website, the site asked the user to submit his or her Apple ID and password, which was then harvested by criminals for exploit or resale.[70]

Most phishing scams are distributed through phishing emails or URLs on social media sites. On social media there's often a news hook, like the Ebola outbreak or some kind of celebrity scandal, that encourages people to click on links that require them to "log in" before they can see the details or video promised.

Email distribution involves news hooks but is used to phish for professional account logins such as banking details, LinkedIn accounts, cloud file storage, or email accounts.[71] Some emails pose as security updates or unusual activity warnings that require you to fill in your details on a phishing site, which then immediately sends your details to the criminals.



- *Sample of phishing email sent to victims.*[72]
- *Variations on this theme appeared throughout 2014, with criminals aiming to acquire social media, banking and email login details.*



- *The email phishing rate dropped to 1 in 965 emails in 2014. In 2013 this rate was 1 in 392 emails.*

Phishing in Countries You Might Not Expect

By Nicholas Johnston

Symantec sees a significant proportion of global email traffic, and recently we were surprised to see phishing attacks targeting institutions in rather unexpected locations.

Angola and Mozambique are two southern African countries, on opposite sides of the vast continent. These countries aren't the first places that spring to mind when you think of phishing, where the goal is to gather sensitive information in order to make money. Mozambique is still a developing country, and despite having an abundance of natural resources, remains heavily dependent on foreign aid. Its per-capita GDP is around $600. Angola fares better than Mozambique; its per-capita GDP is just under $6,000. These are statistically poor countries. (For comparison, global average per-capita GDP figure stands at $10,400, and the U.S. GDP stands around $52,800.)

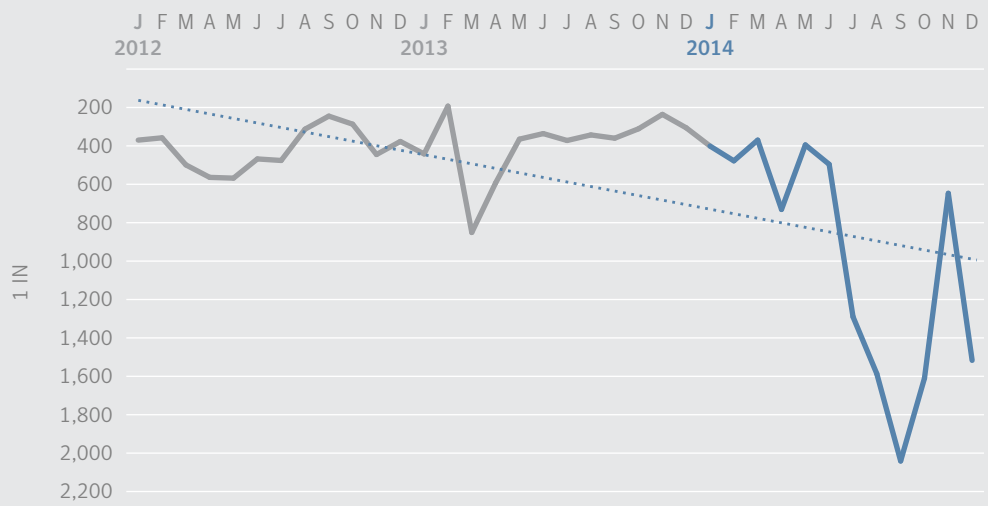
Both of these countries have recently been subjected to phishing campaigns. For instance, one recent phishing campaign was targeted at a major African financial institution, appearing to come from a Mozambique bank, with the email subject, "Mensagens & alertas: 1 nova mensagem!" (Messages & alerts: 1 new message!) A URL contained within the body lead to a fake version of the bank's Web site, asking the target to enter a number of banking details that would allow the attacker to take over the account.

Why are financial institutions in these countries being targeted? It's impossible to be sure, but one of the main dangers of phishing is the ease at which attackers can set up phishing sites. Over the year we've found many "phish kits"--zip files containing phishing sites, ready to be unzipped on a freshly-compromised web server. Additionally, since Angola and Mozambique both speak Portuguese, campaigns from one country can easily be used in the other with only minor changes to the content within them.

From an attacker's perspective, phishing has very low barriers to entry. By targeting smaller or more niche institutions, phishers can avoid competition with their peers. Phishing awareness in developing countries is likely to be lower than in the US or Europe for example.

In all likelihood, the phishing scams targeting Angola and Mozambique probably originate from those countries or neighboring ones. Phishers who target people in developed countries won't be interested in the comparatively low potential profits from phishing accounts in Angola or Mozambique—but those low (by Western standards) profits can still be attractive to someone living in Angola, Mozambique or nearby countries with similar living standards. It might also be easier for phishers based in Angola or Mozambique to use stolen credentials locally rather than selling them on.

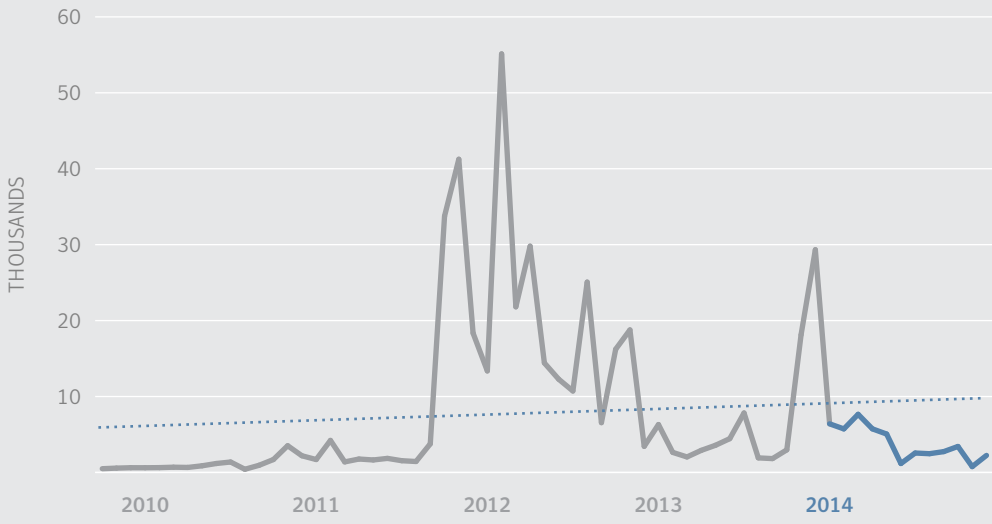
As people increasingly interact with companies and services online, we expect phishing to increase—there are more targets and barriers of entry that will continue to get lower. Even institutions in the very small and relatively isolated east Himalayan Kingdom of Bhutan have been targeted in phishing attacks. This only demonstrates that nowhere is safe from phishing. ■



Phishing Rate, 2012–2014 **Inverse Graph:** Smaller Number = Greater Risk

Source: Symantec

- *There was a significant drop in the phishing rate during the late summer, early autumn of 2014.*



Number of Phishing URLs in Social Media, 2009–2014

Source: Symantec

- *The number of phishing URLs on social media remained low throughout 2014 when compared to 2013 and the peak year of 2012.*

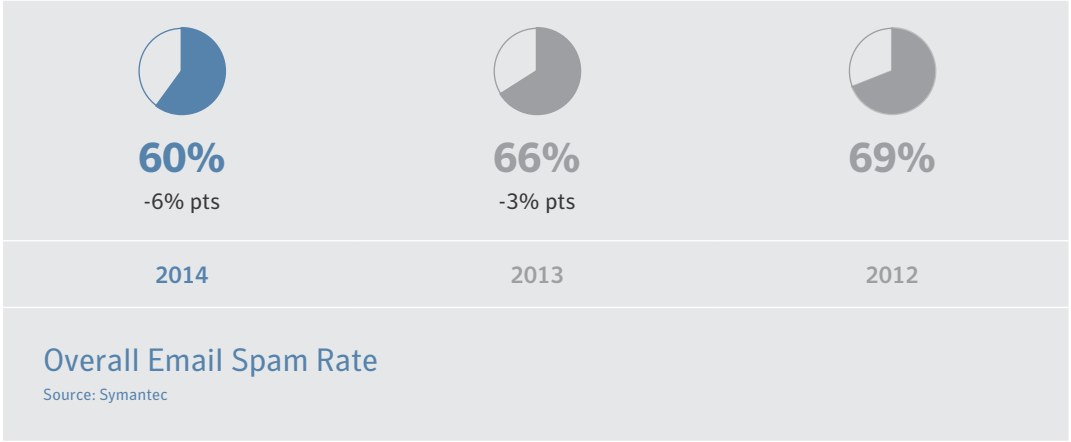
The origins of these phishing sites are often obscured to prevent security warnings when victims open their browsers, and this year saw a new leap forward for the criminals with the use of AES (Advanced Encryption Standard).

This encryption is designed to make the analysis of phishing sites more difficult, and a casual analysis of the page will not reveal any phishing-related content, as it is contained in the unreadable encrypted text. Browser and security software warnings are therefore less likely to appear.

Email Scams and Spam

The shift away from email isn't happening with just phishing attacks; the global spam rate is declining too. The result is more victims are likely to fall for the scam, and it's harder to track.[73]

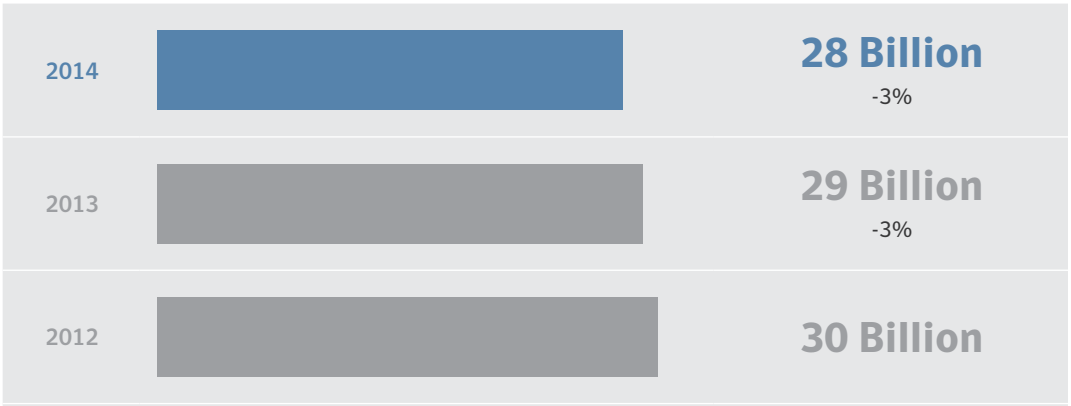
The shift away from email isn't happening with just phishing attacks; the global spam rate is declining too.



Overall Email Spam Rate

Source: Symantec

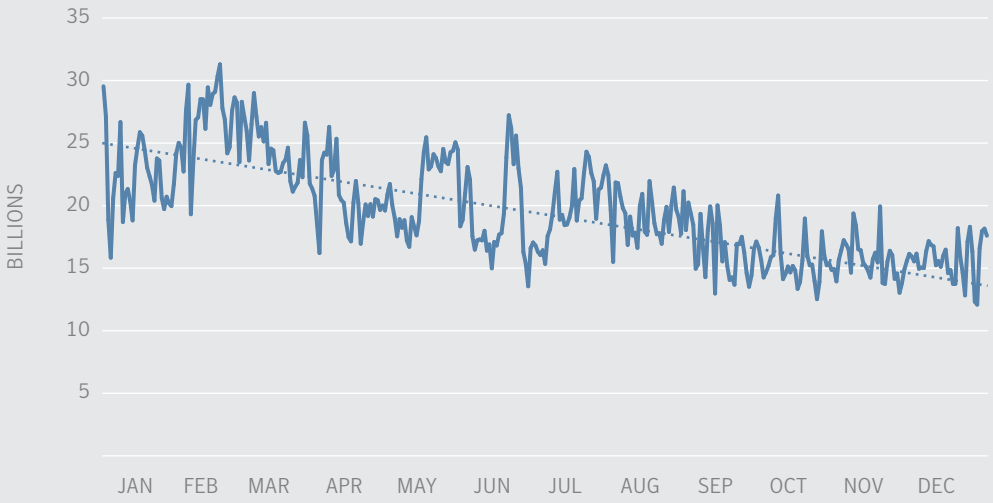
- *The overall email spam rate further declined in 2014, dropping six percentage points to 60 percent.*



Estimated Global Email Spam Volume per Day

Source: Symantec

- *The global spam volume per day dropped three percent for the second year in a row.*



Global Spam Volume per Day, 2014

Source: Symantec

Over the last three years, the overall spam rate has dropped from 69 percent in 2012, to 66 percent in 2013 and 60 percent in 2014. While this is good news overall, there are still a lot of scams out there being sent by email, and criminals are still making money.

In October 2014, Symantec reported an increase in a particular scam where emails were sent, often to a recipient working in the finance department of a company, requesting payment by credit card or the completion of a wire transfer. The sender details were sometimes faked or made to look like they had come from the CEO or another high-ranking member of the victim's company. Money transfer details were either sent in an attachment, or required the victim to email back and request them.[74]

The rise in this type of scam is likely because scams based on malicious attachments can be more easily filtered by corporate security systems, but many organizations are still not undertaking this simple action despite the majority of malicious emails relying on potentially harmful attachments.

In contrast, a sharp rise in malicious URLs versus attachments at the end of the year was related to a change in tactics and a surge in socially engineered spam emails. ■

TARGETED ATTACKS

Targeted Attacks

In 2014, Symantec analyzed several cyberespionage attacks and gathered data on the tactics used to infiltrate thousands of well-defended organizations around the world. This research shows a worrying increase in sophistication.

Imagine you're the CISO for an Eastern European diplomatic corps. In 2014, You suspect that computers in your embassies across Europe have been infected with a back door Trojan. You call in a security firm to investigate and they confirm your worst suspicions. Upon investigation you find that a carefully targeted spear-phishing campaign sent emails to staff members with a stealthy Trojan payload that infected the computers. The use of zero-day exploits, carefully crafted emails, and cunning watering hole website attacks meant that the attacks evaded detection long enough to compromise more than 4,500 computers in more than 100 countries.[75] It's a worrying scenario but not a hypothetical one. This is a description of the Waterbug attack.

It's similar to other targeted attacks such as Turla and Regin, and due to the targets chosen and the sophistication of the attack methods, Symantec believes that a state-sponsored group is behind Waterbug.[76]

In view of the growing sophistication of these attacks, good IT security is essential and broad cybersecurity practices should be the norm. Well-funded state actors are not the only threat. Patriotic hackers, hacktivists, criminal extortionists, data thieves, and other attackers use similar techniques but with fewer resources and perhaps less sophistication.

Email-based attacks continue much as before. Web-based attacks are growing increasingly sophisticated. Espionage attacks use more exploit kits, bundling together exploits rather than using just one attack. Exploit kits have been used in e-crime for many years, but cyberespionage attackers are now using them too.

At a Glance

- *More state-sponsored cyberespionage came to light in 2014.*
- *Attackers are using increasingly well-crafted malware that displays sophisticated software engineering and professionalism.*
- *Campaigns such as Dragonfly, Waterbug, and Turla infiltrated industrial systems, embassies, and other sensitive targets.*
- *The number of spear-phishing campaigns increased by 8 percent in 2014, while the number of daily attacks decreased as attackers become more patient, lying in wait and crafting more subtle attacks boosted by longer-term reconnaissance.*

In view of the growing sophistication of these attacks, good IT security is essential and broad cybersecurity practices should be the norm.

Cyberespionage

In 2014, Symantec security experts spent nearly eight months dissecting one of the most sophisticated pieces of cyberespionage malware ever seen. Known as Regin, it gave its owners powerful tools for spying on governments, infrastructure operators, businesses, researchers, and private individuals. Attacks on telecom companies appeared to be designed to gain access to calls being routed through their infrastructure.[77]

Regin is complex, with five stealth stages of installation. It also has a modular design that allows for different capabilities to be added and removed from the malware. Both multistage loading and modularity have been seen before, but Regin displays a high level of engineering capability and professional development. For example, it has dozens of modules with capabilities such as remote access, screenshot capture, password theft, network traffic monitoring, and deleted file recovery.[78]

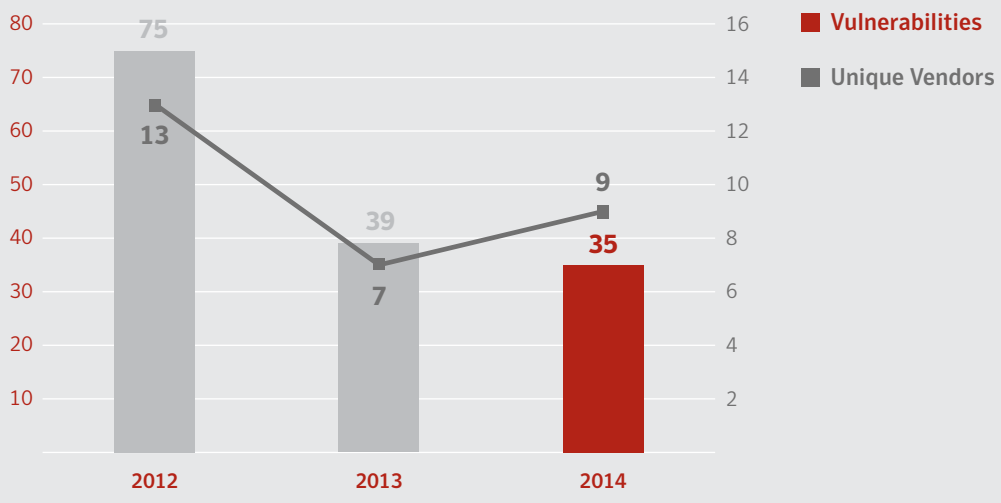
It took months, if not years, to develop Regin, implying a significant investment of resources. It is highly suited to persistent long-term surveillance operations, and its level of sophistication implies that a nation state created it.

Symantec saw a similar level of commitment in another cyberespionage campaign known as Turla.[79] The attackers used spear-phishing and watering hole attacks (see below) to target the governments and embassies of former Eastern Bloc countries. Once installed, it gave attackers remote access to infected computers, allowing them to copy files, delete files, and connect to servers, among other things. Because of the targets chosen and the sophistication of the malware, Symantec believes that a state-sponsored group was behind these attacks too.[80]

More recently, a highly resourced attack group dubbed the "Equation Group" was exposed,[81] revealing that espionage attacks in previous years, including 2014, had probably employed highly specialized techniques. Moreover, as espionage attack groups continue to improve their methods, they can also take advantage of the black market in exploits, zero-day attacks, and custom code. The exposé of the Equation Group further highlights the professionalism behind the development of these specialized attacks, as espionage attack groups benefit from the same traditional software development practices as legitimate software companies.

Industrial Cybersecurity

As more devices are being connected to the Internet, new avenues of attack and, potentially, sabotage open up. This is especially true for industrial devices known as industrial control systems (ICSs), commonly used in areas of industrial production and utility services throughout the world. Many of these devices are Internet enabled, allowing for easier monitoring and control of the devices.



Vulnerabilities Disclosed in ICS Including SCADA Systems

Source: Symantec

The chart shows the number of disclosed vulnerabilities that were associated with ICS and supervisory control and data acquisition (SCADA) systems, including the number of vendors involved each year.

Securing Industrial Control Systems

By Preeti Agarwal

Targeted attacks have evolved from novice intrusion attempts to become an essential weapon in cyberespionage. Industrial control systems (ICS) are prime targets for these attackers, with motives for executing attacks at a national security level. These trends are leading countries to reinforce their investment and build strategies to improve ICS security.

The term "industrial control system" refers to devices that control, monitor, and manage critical infrastructure in industrial sectors, such as electric, water and wastewater, oil and natural gas, transportation, etc. Various types of ICSs include supervisory control and data acquisition (SCADA), programmable logic controllers (PLC), distributed control systems (DCS), to name a few.

Attacks targeting ICSs have become a common occurrence and can potentially have serious social and economic impacts. But these attacks often go undisclosed, limiting the PR fallout for the victim, and underreporting the extent of the problem.

There have been numerous attacks, with intentions ranging from cyberespionage to damaging the utilities in ICSs. In 2010 Stuxnet was discovered, a threat designed to attack specific SCADA systems and damaged the physical facilities of Iran's nuclear system. Since then a myriad of weaponized malware has been seen in the threat landscape, and 2014 was no exception. The attackers behind Dragonfly, a cyberespionage campaign against a range of targets, mainly in the energy sector, managed to compromise a number of strategically important ICSs within these organizations and could have caused damage or disruption to the energy supply in the affected countries, had they used the sabotage capabilities open to them.

More recently, Sandworm launched a sophisticated and targeted malware campaign compromising the human-machine interface (HMI) of several well-known ICS vendors. Attackers used the internet connected HMIs to exploit vulnerabilities in the ICS software. Such intrusions could have been reconnaissance for another attack.

The most recent addition to emerge in 2014 was an incident where a blast furnace at a German steel mill suffered massive damage following a cyber-attack on the plant's network.[82]

Attacks against ICSs have matured and become more frequent, making the security of these systems essential and a pressing issue.

Many ICSs are installed and operate for many years. This often leads to security policies rooted in a security-through-obscurity approach, using physical isolation, proprietary protocols, and specialized hardware in the hopes that this will keep them secure. Many of these systems were developed before Internet-based technologies were used in businesses and were designed with a focus on reliability, maintainability and availability aspects, with little-or-no emphasis on security. However, compelling needs for remote accessibility and corporate connectivity have changed the attack surface dramatically, exposing new vulnerabilities in these systems to attacks.

The primary entry point for these attacks today is poorly protected Internet-accessible, critical infrastructure devices. In order to provide remote accessibility, elements of SCADA systems, used to monitor and control the plants and equipment, are connected to the Internet through corporate networks. These SCADA elements expose the control network and pose a risk of attacks like scanning, probing, brute force attempts, and unauthorized access of these devices.

One way to leverage these devices in an attack is through the HMI, often accessible from the corporate network. An attacker can compromise the corporate hosts by exploiting any existing day-zero vulnerability, discover any hosts that have access into the control network, and attempt to leverage this information as a way into the ICSs.

Another way to leverage ICSs is through an HMI connected directly to Internet. These Internet-facing devices can be easily discovered over the Internet using common search engines. Once a control device is identified it can be compromised by exploiting vulnerabilities or through an improper configuration. The level of knowledge required for launching these attacks is fairly low.

Apart from these entry points, ICSs and their software have several inherent vulnerabilities, opening doors for adversaries. Many of the proprietary web applications available have security vulnerabilities that allow buffer overflows,

SQL injection, or cross-site scripting attacks. Poor authentication and authorization techniques can lead the attacker to gain access to critical ICS functionalities. Weak authentication in ICS protocols allows for man-in-the-middle attacks like packet replay and spoofing. An attacker can end up sending rogue commands to PLCs or fake statuses to HMIs.

Ladder logic used to program the PLCs is a critical asset in ICS environments. Compromises to an engineering work station used for developing and uploading this PLC ladder logic can lead to reverse engineering, which can be used to craft attacks.

Securing ICS environments requires a comprehensive security plan that would help an organization define its security goals in terms of standards, regulatory compliance, potential risk factors, business impacts, and required mitigation steps. Building a secure ICS environment requires integrating security into each phase of the industrial processes starting from planning to the day-to-day operations.

Network-level segregation between the control network and corporate network should be an absolute requirement as it greatly reduces the chances of attacks originating from within corporate networks. However practical considerations require ICS connectivity from the corporate network. In such cases the access points should be limited, protected by a firewall, and should make use of trusted communication channels like a VPN.

ICS environments are evolving, with vendors extending support for security software on the control devices for general purpose SCADA servers and engineering workstations. However systems like PLCs and DCSes still use vendor-specific customized operating systems. These control systems, once installed, have zero tolerance for downtime, limited resources and time-dependent code. This limits opportunities to deploy traditional enterprise-security solutions designed for IT computer systems. Given these challenges there is no silver bullet solution for ICS security. Rather security has to be implemented end-to-end at each layer, including the network perimeter, access points to the corporate and external network, the network level, the host-based level, and the application level.

In addition, the control devices themselves should also be secure by design. Manufacturers are responsible to ensure that security is built into the control devices before shipping.

Looking ahead we will likely see a trend towards an increase in the use of mobile technology allowing remote HMI access and control options. While the solution is very compelling from administrative efficiency perspective, it will launch a new attack surface associated with the mobile usage model.

It's also possible that we will see the development of generalized techniques for attacking ICSs. As a result we may see a rise in freely available ICS exploit kits. This trend would no doubt increase ICS attack numbers.

As we saw with Stuxnet, which reincarnated itself with multiple variants, ICS-focused threats that followed had similarities in attack vectors and artifacts, making use of common ICS protocols and general-purpose Trojans. It is highly likely that there are threats out there on ICSs, installed stealthily, that have not yet been detected, sitting passively at the moment. Attackers may find a reason to make these passive attacks active at any point in time. It's entirely possible that we will see an onset of more critical infrastructure vulnerabilities being utilized, to dangerous ends. ■

Symantec saw more attacks against industrial control systems in 2014. For example, the Dragonfly cyberespionage campaign attacked a range of targets, including energy grid operators, electricity generators, petroleum pipeline operators, and industrial equipment manufacturers.[83] The majority of victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland.

By attacking industrial control systems Dragonfly is following in the footsteps of Stuxnet, which targeted the Iranian nuclear program. However, Dragonfly appears to have less destructive goals. Initially it appeared to focus on espionage and persistent access rather than the ultimate goal of sabotage. However, it gives the well-resourced group that created it insight into important industrial systems and— hypothetically—the ability to deliver a more destructive attack if required.

Using custom-written malware and malware bought "off the shelf" from Russian-language forums, Dragonfly was spread using a combination of email-based spear-phishing and web-based watering hole attacks that targeted its principal victims through smaller, less well-protected companies in their supply chain.

It can be difficult for companies to protect legacy systems when they can't afford any downtime for patching or when they use proprietary or poorly protected technology. For example, OLE for Process Control[84] (OPC) is a widely used protocol in industrial automation systems. It is a well-documented open standard, but there is little provision for encryption, authentication, or other security measures, making it vulnerable to rogue software. One of the goals of Dragonfly was to collect information about OPC systems in target companies.

By specifically exploiting the ICS vendors' software update servers, the Dragonfly attacks introduced a new dimension to the watering hole attack method. Watering hole-based attacks exploit vulnerabilities in third-party websites that the real target of the attack will visit, through which the attacker may inject malware into the targeted organization. With Dragonfly, the attackers compromised the supply chain by exploiting the software update servers for the ICS software employed by its victims, marking a new milestone in new watering hole-style attacks.

Reconnaissance Attacks

Besides attacks using spear-phishing campaigns and watering holes—attacks that require the human element of social engineering to succeed—attackers continue to attack targeted organizations from other angles in order to gain a foothold in their network. They can do this by attacking the perimeter of the network, looking for holes in their defenses and exploiting them.

Now more than ever, reconnaissance plays a big part in an attacker gaining access to a targeted organization's network. This is generally the first step in the hacking process: gaining information about the systems and looking for any weaknesses that can be exploited.

Now more than ever, reconnaissance plays a big part in an attacker gaining access to a targeted organization's network.

The popularity of reconnaissance is clear when looking at the top zero-day exploits in 2014. Far and away, the most commonly used zero-day vulnerability was CVE-2013-7331. This wasn't a run-of-the-mill "exploit and gain access to a vulnerable system" exploit either. It only supports the attacker gathering intelligence on the targeted network. However, it is quite useful for planning further attacks. Armed with information such as the targeted internal network's host names, IP addresses, and various internal path names, an attacker could easily figure out his or her plan of attack.

This zero-day exploit was also left unpatched for a significant period of time. Not only was the CVE for this vulnerability allocated in 2013, only to be disclosed in February 2014, but the patch to mitigate it wasn't released until September 2014. This left a huge window of 204 days between public disclosure and the patch's release for the attackers to exploit vulnerable systems.

The best explanation for this extended period of exposure is the perceived severity of the threat. Since this particular exploit did not allow an attacker to directly take control of a vulnerable computer, perhaps it was not considered as important to address as other vulnerabilities. Attackers clearly noticed this and were able to take advantage of the vulnerability and the information it gained them about targeted networks, indirectly helping them in their malicious goals.

This is a portion of the threat landscape that may be deserving of more attention across the security industry. While a vulnerability that simply returns information about the network, computer, or device may not be considered as severe as one that allows privilege escalation, it can still be just as dangerous if it points attackers toward vulnerable systems they wouldn't have discovered without it.

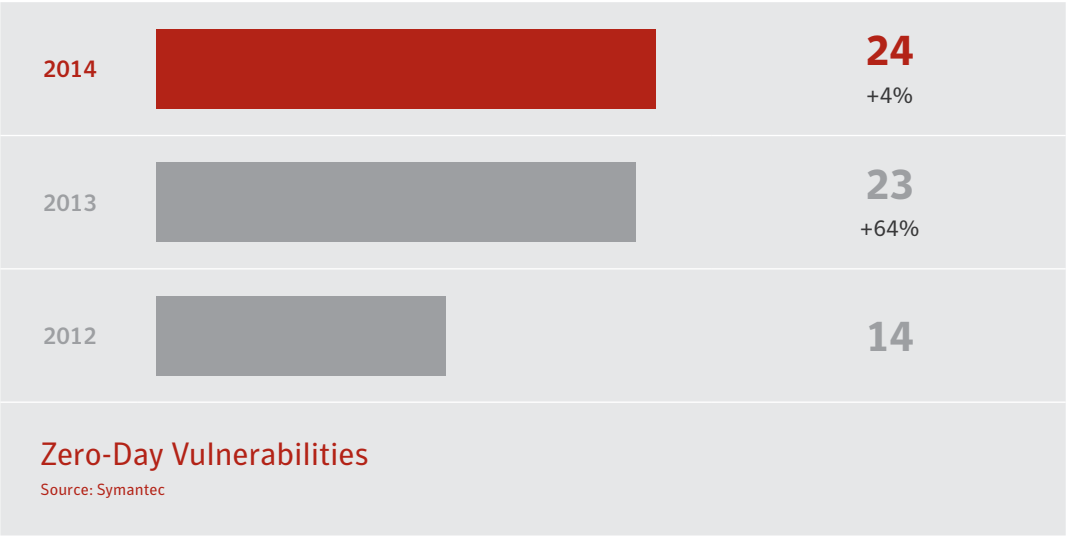
Attackers were able to take advantage of the vulnerability and the information it gained them about targeted networks, indirectly helping them in their malicious goals.

Watering Hole Attacks

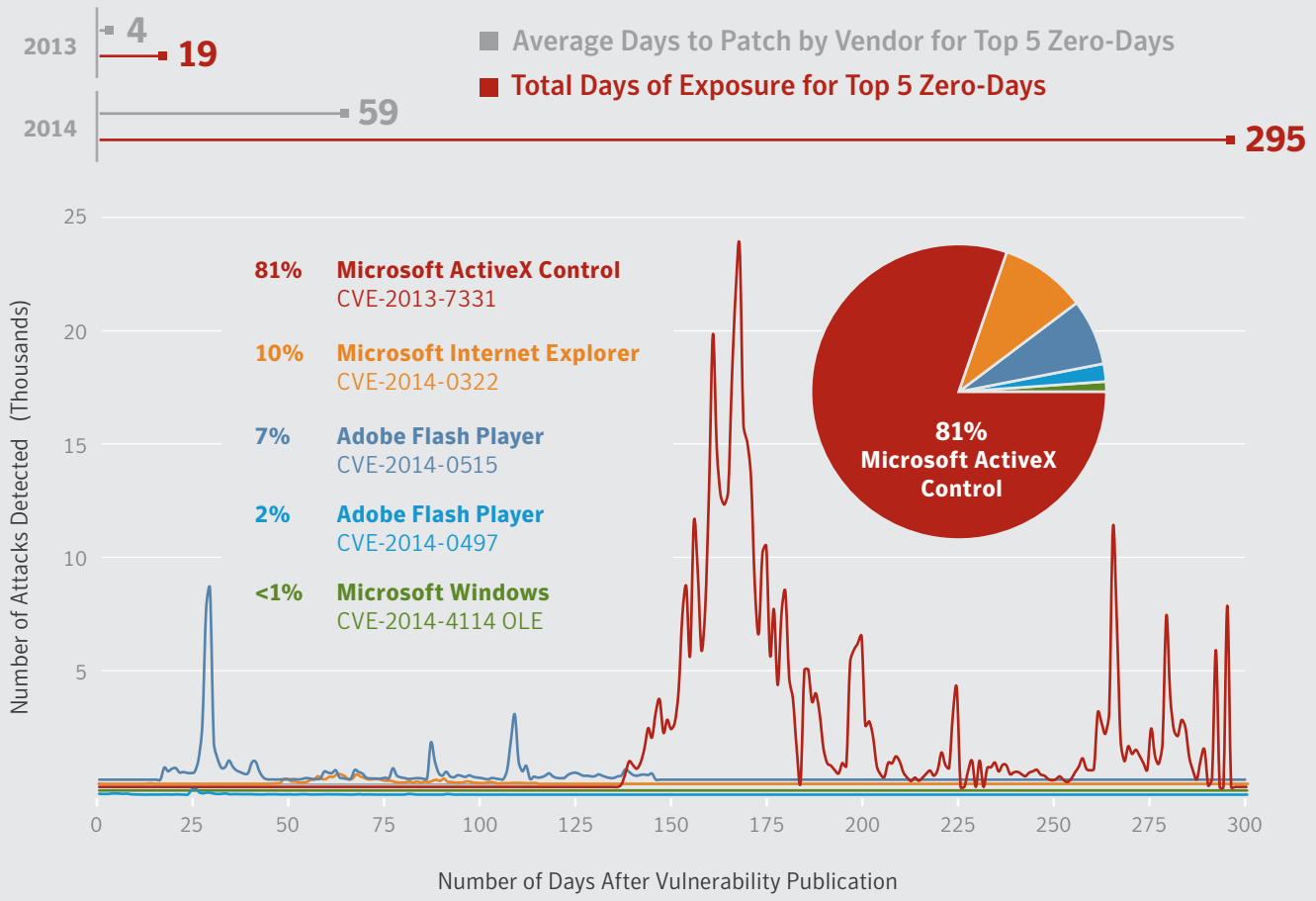
The professional hackers-for-hire group known as Hidden Lynx, first uncovered in September 2013, continued their operations in 2014. This group took advantage of a significant zero-day vulnerability (CVE-2014-0332)[85] through a watering hole-style attack. The attack ultimately opened a back door on any computer that visited the compromised site while the watering hole was active, through which subsequent attacks and exfiltration could take place.

This vulnerability was also discovered in watering hole attacks against organizations involved with the French aerospace industry and a variety of Japanese websites. However, it is likely that these attacks are separate from the Hidden Lynx group and other actors were involved in their use.[86]

Another significant watering hole attack took advantage of a zero-day vulnerability in Adobe Flash (CVE-2014-0515) and coupled it with a specific piece of software produced by a legitimate vendor. This particular attack appears to have been highly targeted, as the target organization would have needed both pieces of software installed in order for the attack to be successful.



There was a four percent increase in the number of zero-day vulnerabilities discovered in 2014.



Top 5 Zero-Day Vulnerabilities – Days of Exposure and Days to Patch

Source: Symantec

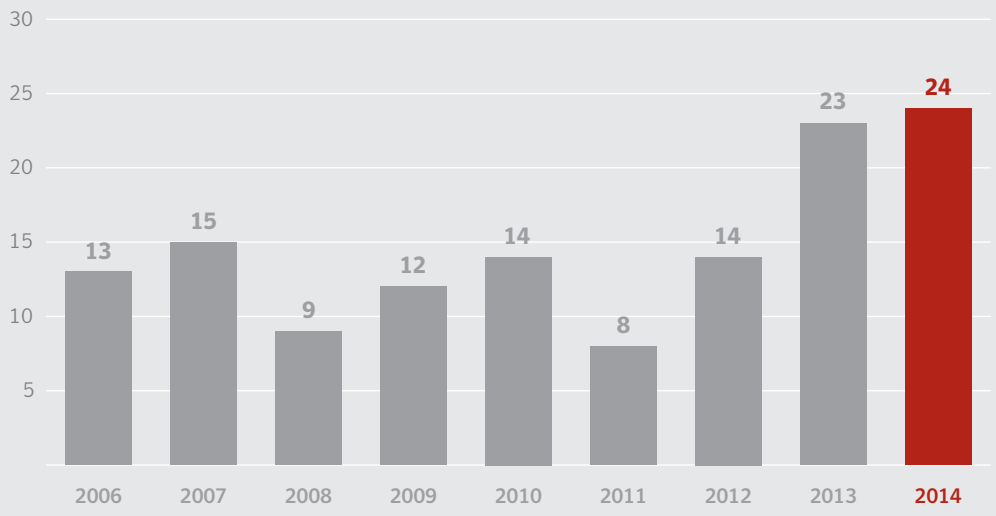
- *The total number of days between the vendor's publication date and the subsequent patch date for the top five most frequently exploited zero-day vulnerabilities grew from 19 days in 2013 to 295 days in 2014. Fifty-seven percent of the attacks exploiting these top five zero-day vulnerabilities were blocked by Symantec Endpoint technology in the first 90 days, often before a patch was made available.*

In a different case, a previously undiscovered vulnerability in Microsoft Windows allowed the Sandworm cyberespionage group to install malware on targeted organizations,[87] including NATO, as well as several Ukrainian and Western European government organizations, energy companies, and telecommunications companies.

The Elderwood platform was first identified in 2012 but continues to be maintained. At the start of 2014, for example, it exploited three new zero-day vulnerabilities to attack its victims.[88] Twenty-four zero-day vulnerabilities were discovered in 2014, just one more than the all-time high of 2013, indicating a new norm in zero-day vulnerabilities being discovered and exploited. There may be many more that remain undiscovered and attackers are keeping to themselves for now.

The value and importance of an exploit for a zero-day vulnerability for an attacker comes in two ways. First, any unpublished vulnerability has enormous value if it can be exploited by an attacker to gain remote access or perform reconnaissance. Second, an exploit can reap enormous reward by taking advantage of the delay between a vendor's becoming aware of the vulnerability and the time taken to provide a patch. It can take several days, weeks, or even months for a patch to be available and even longer before it is widely deployed.

For the top five most frequently exploited zero-day vulnerabilities published in 2014, the total number of days between the vendor publication date and the patch date grew to 295 days, up from 19 in 2013. The average time taken between publication and patch also grew, to 59 days, up from 4 in 2013. The most frequently exploited zero-day in 2014, CVE-2013-7331, was first identified in 2013, hence its classification; however, its existence was not disclosed to the public until the following year. It was a further 204 days before the vendor was able to publish a patch. The number two and three most frequent zero-day exploits also had long time-to-patch windows of 22 and 53 days, respectively. Both of these windows are larger than the average seen in 2013.



Zero-Day Vulnerabilities, Annual Total, 2006–2014

Source: Symantec

■ *Twenty-four zero-days were discovered in 2014, consistent with the all-time high of 2013.*

Shifting Targets and Techniques

By the Symantec Managed Adversary & Threat Intelligence team

As Symantec has worked to protect our customers over the years, we have noted that our cyber adversaries demonstrate considerable agility and adaptability. This is enabling a proliferation of targeted attacks by actors other than governments, who were previously believed to have had a monopoly on this capability and intent. This remains the case in 2014. Symantec follows and reports on adversaries—those actors conducting malicious attacks—as well as their tools, techniques, and activities through its DeepSight Adversary Intelligence service.[89] Two of the changes we observed in 2014 relate to shifting techniques and targets.

Cybercriminals are increasingly combining malicious activity with benign behavior to target networks globally. One technique that actors use when targeting environments is to limit the use of malware and detectable attack tools in order to avoid detection and subsequent security improvements made by defenders. While intrusions involving spear-phishing emails containing malware and second-stage-attack malware to maintain network access remain prevalent, the use of privileged user accounts with tools that generate legitimate network activity, such as network administration tools, has become common. Symantec has discovered and exposed such network intrusions and methods of maintaining persistence within enterprise customers in the retail sector this year, and expects increasing adoption of this technique across the adversary community.

To mitigate the risk of these types of attacks, defenders, in addition to relying on signature-based detection, should identify and minimize risks from legitimate but unnecessary services running on their networks that could be utilized by attackers for lateral movement, privilege escalation and exfiltration. They should also address risks from asymmetric attack vectors such as network connectivity with less well-defended parties, such as vendors.

While attacks against financial and other high-profile industries continue unabated, a number of cyber espionage campaigns discovered in 2014 targeted key sectors—such as energy and manufacturing—that use industrial control system (ICS) technologies to automate physical processes. Over the last year, Symantec detected multiple campaigns against ICS technologies such as actors using BlackEnergy malware to exploit specialized ICS software programs, and the Dragonfly group using Trojanized ICS software bundles that distribute Backdoor.Oldrea[90] (a.k.a. Havex, and used by the Dragonfly group) to perform reconnaissance on ICS network protocols and ports. Given the potential impact such attacks can have on targeted enterprises and nations, it is reasonable to expect certain categories of adversaries will continue to enhance their capabilities to exploit ICS weaknesses.

Defenders of ICS technologies should not rely on the limited connectivity and unique architectures of these environments for protection. Given the sensitivity of the assets, strong security controls should be implemented and the deterministic nature of the environment leveraged to identify abnormal behavior through security monitoring. ■

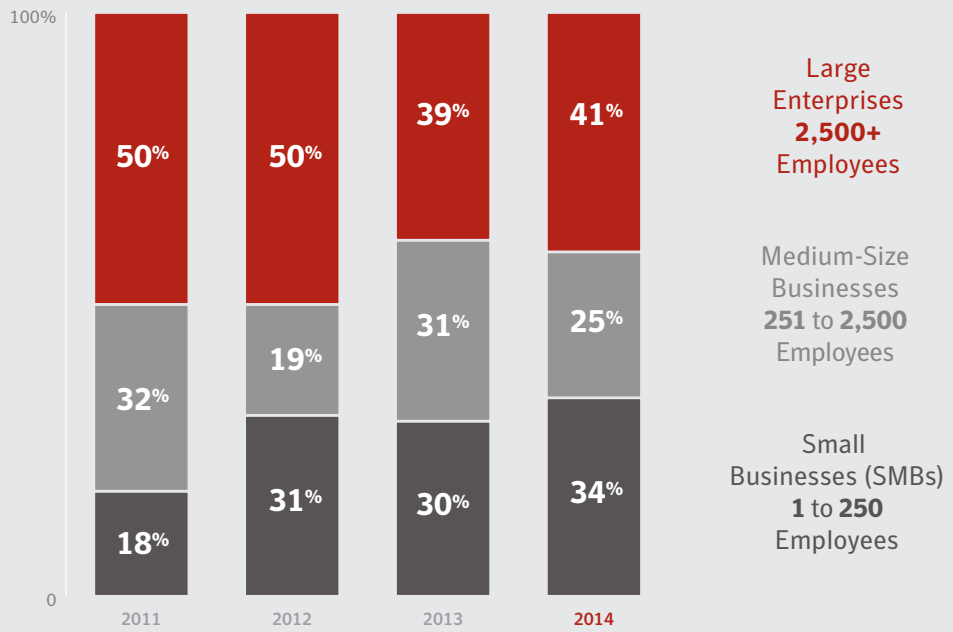
It is this weakness—the window of vulnerability—that the espionage attack groups depend on for their success. For example, a website already compromised to host a watering hole exploit may stop using a zero-day exploit once the software vendor publishes information about the vulnerability's existence, even though a patch may not yet be available. The attackers may then switch over to using another as-of-yet undiscovered exploit, a further example of the enormous resources at their disposal.

Threat Intelligence

Threat intelligence is now a vital component for any organization to understand regarding the potential threats against their networks. Investing in great technology solves only part of the problem, and a combination of threat intelligence, risk management, and the best technical solutions will help not only reveal who is being targeted but also how and why. Understanding the threats is critical, as businesses should now expect to be attacked. The question is not "if" but "when."

Advanced attackers use exploit toolkits against not only older vulnerabilities but also new zero-day ones, and being good at defense means being harder to breach. Threat intelligence can provide a prioritized list of suspicious incidents by correlating all available information from across the enterprise. A continual assessment of not only the people and their skills but also the processes will ensure the best response is followed and that processes are continually updated and skills are maintained. If businesses can become harder to breach, the attackers will have to work harder; don't be the weakest link in the supply chain.

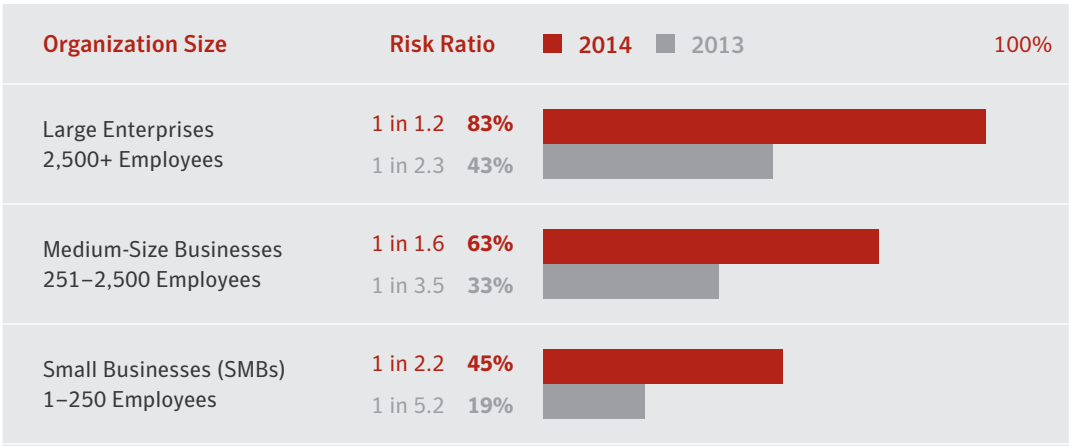
Techniques Used In Targeted Attacks



Distribution of Spear-Phishing Attacks by Organization Size

Source: Symantec

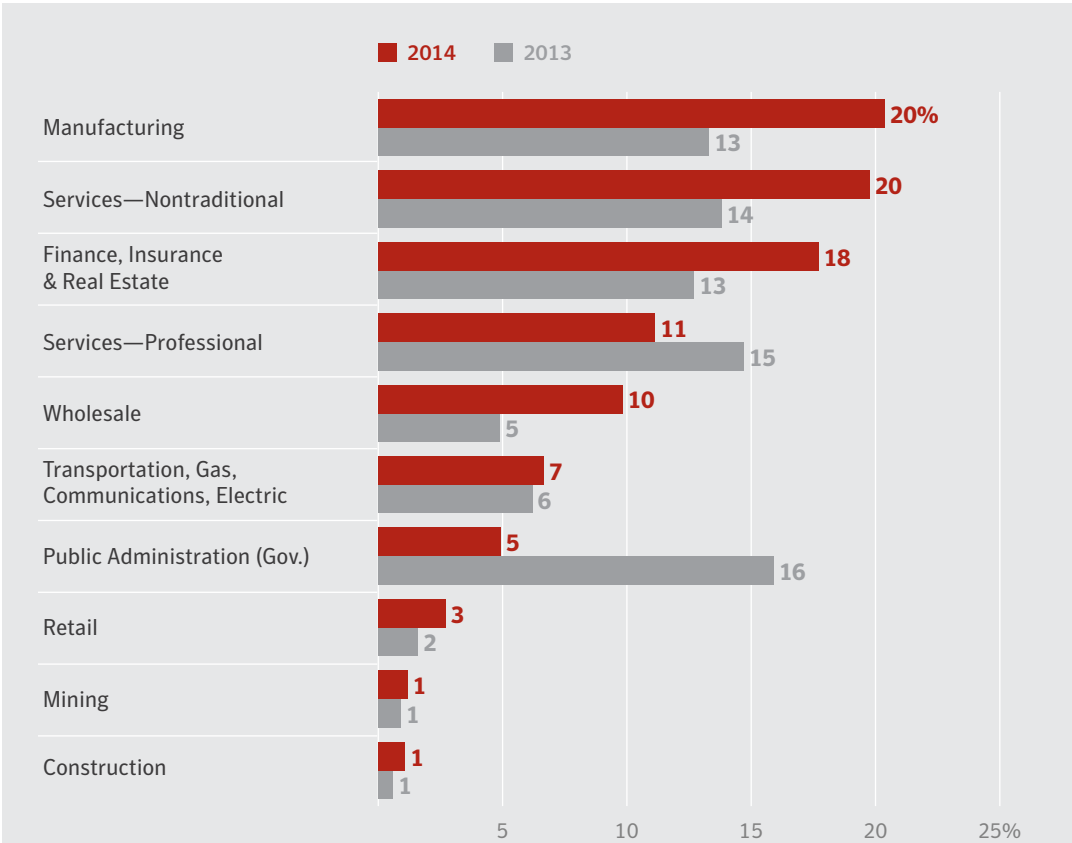
■ *Forty-one percent of spear-phishing emails were directed at large enterprises in 2014. As in 2013, spear-phishing attacks on small- and medium-size businesses in 2014 show that being small and relatively anonymous is no protection. In fact, attacks in 2014 confirm that determined attackers often attack a target company's supply chain as a way of outflanking its security.*



Risk Ratio of Spear-Phishing Attacks by Organization Size

Source: Symantec

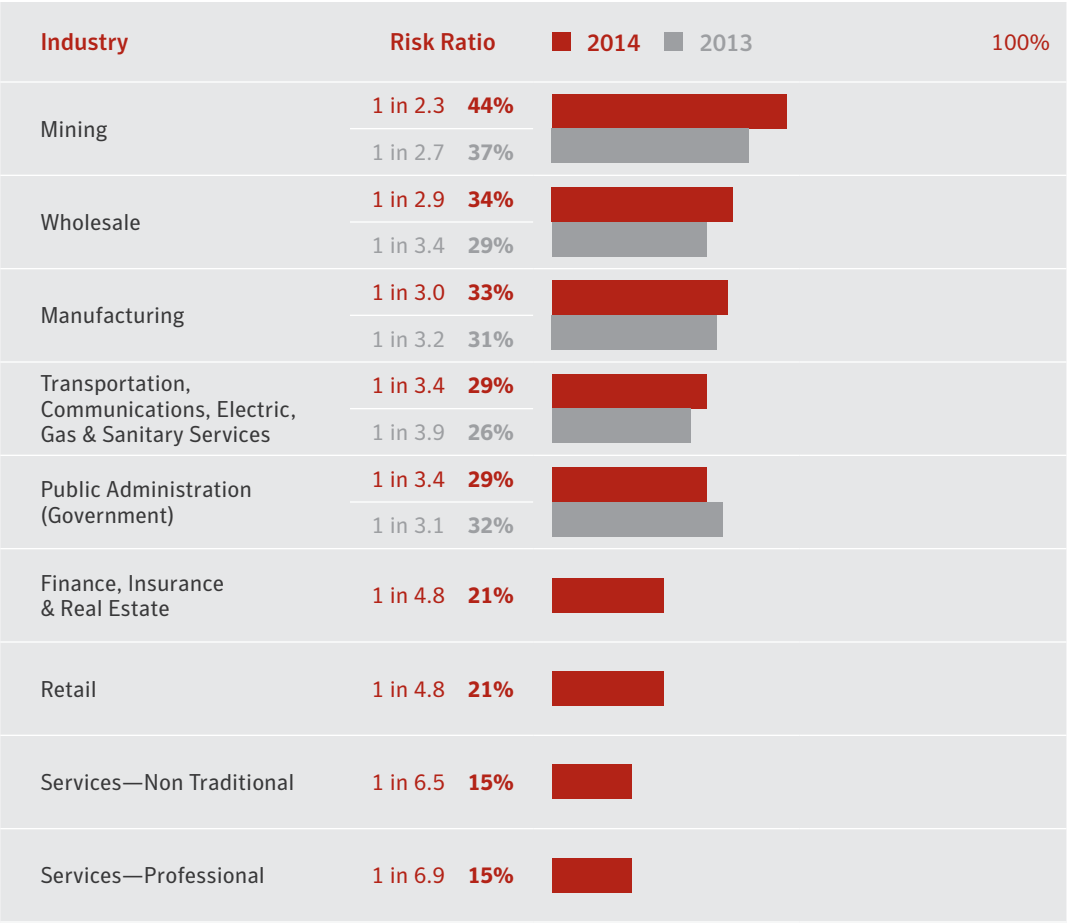
In 2014, 83 percent of large enterprises were targeted in spear-phishing campaigns, compared with 43 percent in 2013.



Top 10 Industries Targeted in Spear-Phishing Attacks, 2013–2014

Source: Symantec

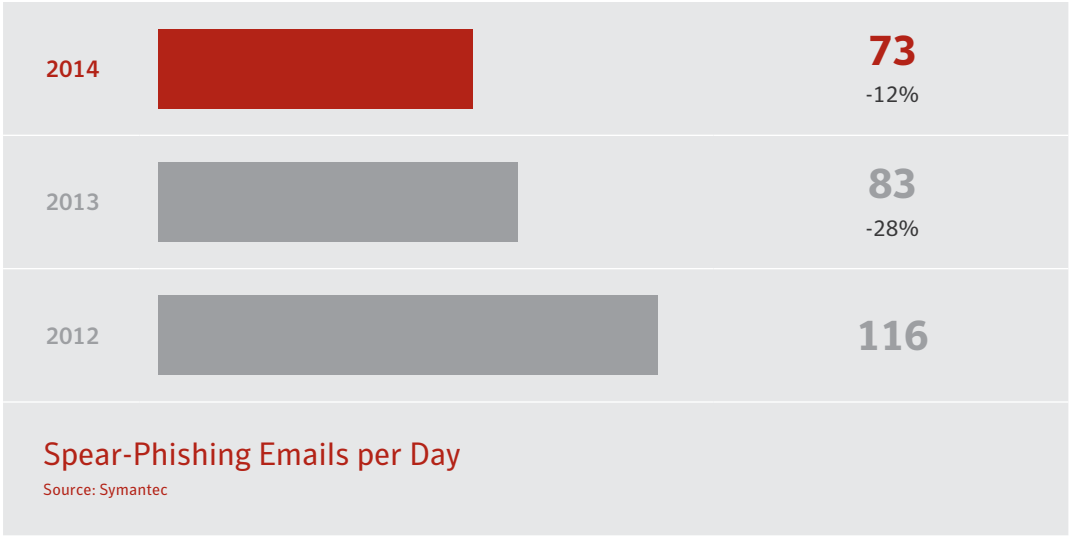
Overall in 2014, the manufacturing sector was targeted with the greatest volume of spear-phishing attacks, as 1 in 5 (20 percent) were directed at manufacturing organizations.



Risk Ratio of Spear-Phishing Attacks by Industry

Source: Symantec

- *The mining industry was the most heavily targeted in 2014, with 43 percent (1 in 2.3) of mining organizations being targeted at least once during the year. The mining classification includes energy extraction organizations, as well as those mining metals and quarrying minerals.*



Spear-Phishing Emails per Day

Source: Symantec

- *The number of spear-phishing emails detected by Symantec fell slightly, but there are no signs that the intensity of targeted attacks is also falling. The number of overall email campaigns has increased, and spear-phishing emails have become subtler, using custom-written malware and carefully crafted, socially engineered messages in order to bypass security.*

	2014	Change	2013	Change	2012
Campaigns	841	+8%	779	+91%	408
Recipients per Campaign	18	-22%	23	-80%	111
Average Number of Email Attacks per Campaign	25	-14%	29	-76%	122
Average Duration of a Campaign	9 Days	+13%	8 Days	+32%	3 Days

Spear-Phishing Email Campaigns, 2012–2014

Source: Symantec

- *In 2014, there was an 8 percent increase in targeted attacks via spear-phishing campaigns, despite an overall decline by 12 percent in the number of spear-phishing emails sent daily. Spear-phishing attacks in 2014 were less spam-like, with fewer high-volume recipients. Attackers have taken more time to plan and coordinate attacks before launching them, paying particular attention to reconnaissance. Symantec has also observed several "distributed targeted attacks" being coordinated between groups of attackers seemingly working together. These attacks have been planned and distributed in such a way that even if they were of relatively high volume, they wouldn't have qualified as spam.*

Spear-Phishing Email Word Cloud

Most commonly used words in spear-phishing attacks

Job Role	Risk Ratio		2014 100%
Sales/Marketing	1 in 2.9	35%	
Finance	1 in 3.3	30%	
Operations	1 in 3.8	27%	
R&D	1 in 4.4	23%	
IT	1 in 5.4	19%	
Engineering	1 in 6.4	16%	
HR & Recruitment	1 in 7.2	14%	
Other	1 in 9.3	11%	

Risk Ratio of Spear-Phishing Attacks by Job Role

Source: Symantec

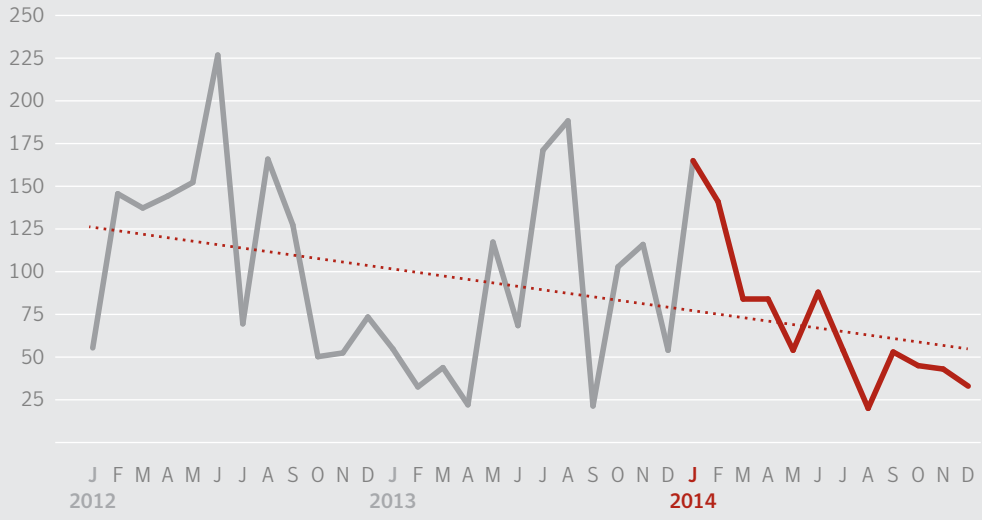
- *Individuals in sales/marketing job roles were the most targeted in 2014, with 1 in 2.9 of them being targeted at least once; this is equivalent to 35 percent of sales/marketing personnel.*

Job Level	Risk Ratio	2014	100%
Individual Contributor	1 in 3.7	27%	
Manager	1 in 3.8	26%	
Intern	1 in 3.9	26%	
Director	1 in 5.4	19%	
Support	1 in 7.6	13%	
Other	1 in 9.3	11%	

Risk Ratio of Spear-Phishing Attacks by Job Level

Source: Symantec

Individual contributors were the most frequently targeted level of seniority in 2014, with 1 in 3.7 of them being targeted at least once; this is equivalent to 27 percent of individuals at that level.



Average Number of Spear-Phishing Attacks per Day, 2012–2014

Source: Symantec

The average number of spear-phishing attacks per day continued to decline in 2014.

Rank	Attachment Type	2014 Overall Percentage	Attachment Type	2013 Overall Percentage
1	.doc	38.7%	.exe	31.3%
2	.exe	22.6%	.scr	18.4%
3	.scr	9.2%	.doc	7.9%
4	.au3	8.2%	.pdf	5.3%
5	.jpg	4.6%	.class	4.7%
6	.class	3.4%	.jpg	3.8%
7	.pdf	3.1%	.dmp	2.7%
8	.bin	1.9%	.dll	1.8%
9	.txt	1.4%	.au3	1.7%
10	.dmp	1.0%	.xls	1.2%

Analysis of Spear-Phishing Emails Used in Targeted Attacks, 2013–2014

Source: Symantec

- *Microsoft Office document file attachments overtook executable files to become the most frequently used type of attachments used in spear-phishing attacks. They were used in 39 percent of attacks during 2014. Malicious document attachments could also be rendered safe before reaching the email gateway through the use of strong cloud-based filtering that can identify and eliminate spear-phishing attacks before they reach the corporate network.*
- *At least 32 percent of spear-phishing attacks could be prevented if companies blocked executable-type file attachments and screensavers at the email gateway.*

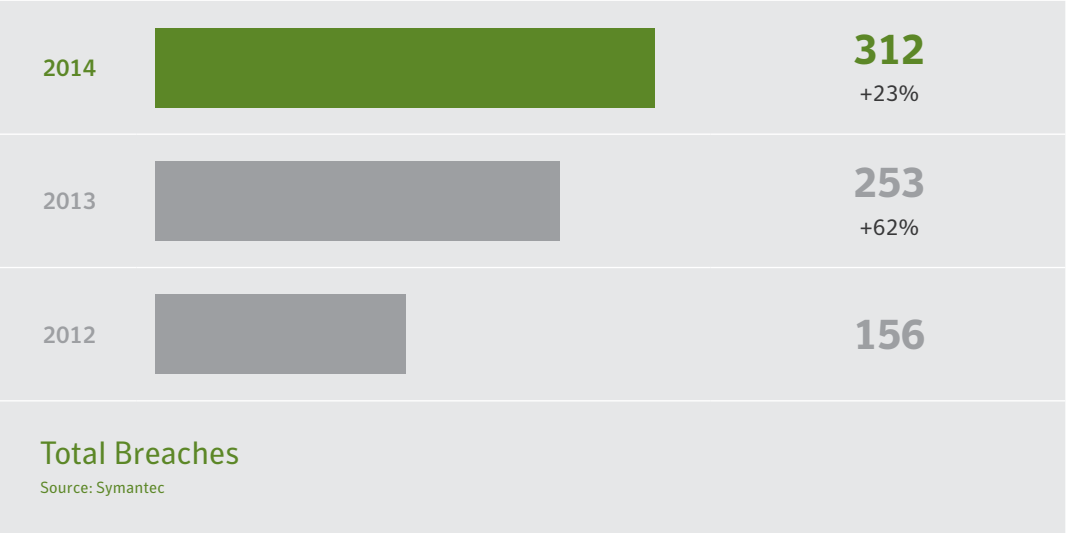
DATA BREACHES & PRIVACY

Data Breaches

In 2014, cybercriminals continued to steal private information on an epic scale, by direct attack on institutions such as banks and retailers' point-of-sale systems.

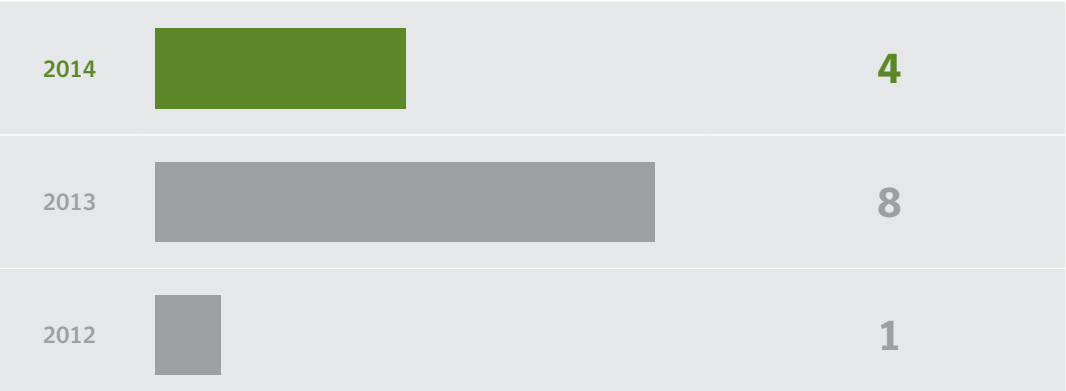
While there were fewer "mega breaches" in 2014, data breaches are still a significant issue. The number of breaches increased 23 percent and attackers were responsible for the majority of these breaches.

Fewer identities were reported exposed in 2014, in part due to fewer companies reporting this metric when disclosing that a breach took place. This could indicate that many breaches—perhaps the majority—go unreported or undetected.[91,92]



Total Breaches

Source: Symantec



Breaches with More Than 10 Million Identities Exposed

Source: Symantec

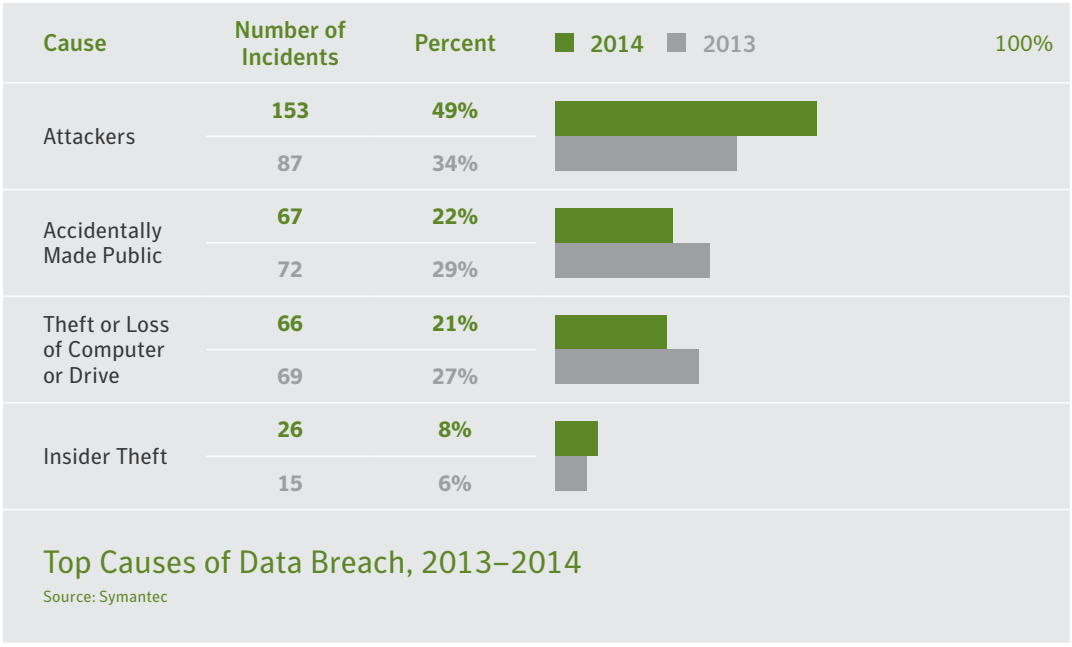
At a Glance

- *There were fewer mega breaches (with more than 10 million identities disclosed) in 2014 than 2013.*
- *The overall number of data breaches increased.*
- *Attackers are responsible for the majority—49 percent—of breaches.*
- *Attacks on point-of-sale systems have grown in scale and sophistication.*
- *According to a survey carried out by Symantec, 57 percent of respondents are worried their data is not safe.*

- *While 2014 had fewer mega breaches (greater than 10 million identities exposed per breach), the total number of breaches increased 23 percent, suggesting breach activity continues to rise.*

The release of nearly 200 celebrity photographs on the website 4chan in August 2014 received wide media coverage and increased consumer anxiety about privacy. According to Apple, the images were obtained using highly tailored targeted attacks on individual accounts rather than general weaknesses in the company's security.[93]

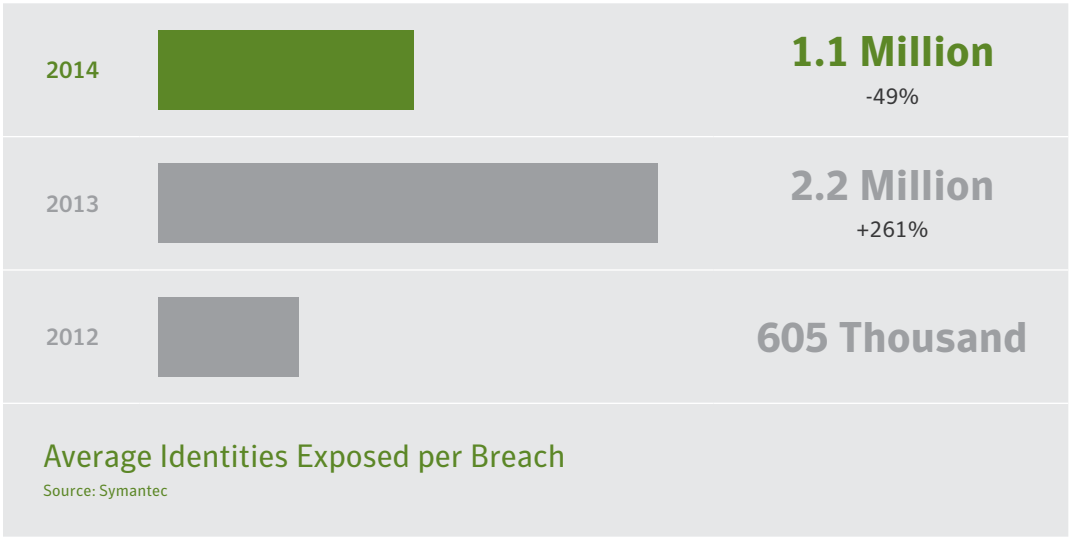
People's personal and financial information continues to command high prices on the black market, and that means cybercriminals will continue to target major institutions for large scores and small companies for small, easy ones. Many breaches are preventable with the right security measures, including elements such as data loss prevention, encryption, and intrusion detection systems, as well as with effective security policies and training.



Top Causes of Data Breach, 2013–2014

Source: Symantec

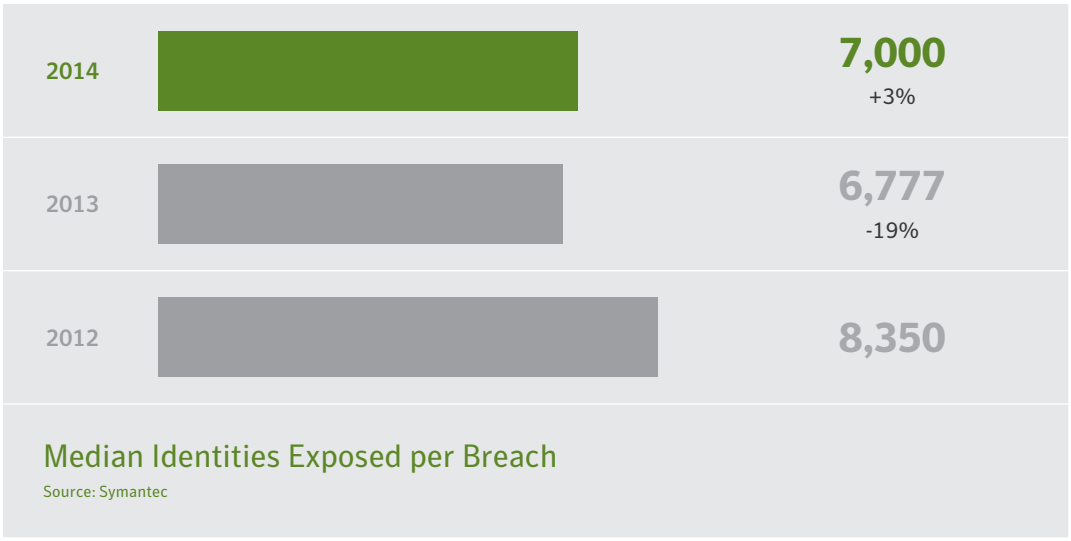
- *At 49 percent, the majority of breaches were caused by attackers, up from 34 percent in 2013. However, a further 22 percent of breaches were classified as "accidentally made public," and 21 percent were due to theft or loss of a computer or drive. These latter types of data exposure are preventable if data is encrypted, effectively eliminating the impact of the data's falling into the wrong hands. The good news is that this is down from 56 percent in 2013.*



Average Identities Exposed per Breach

Source: Symantec

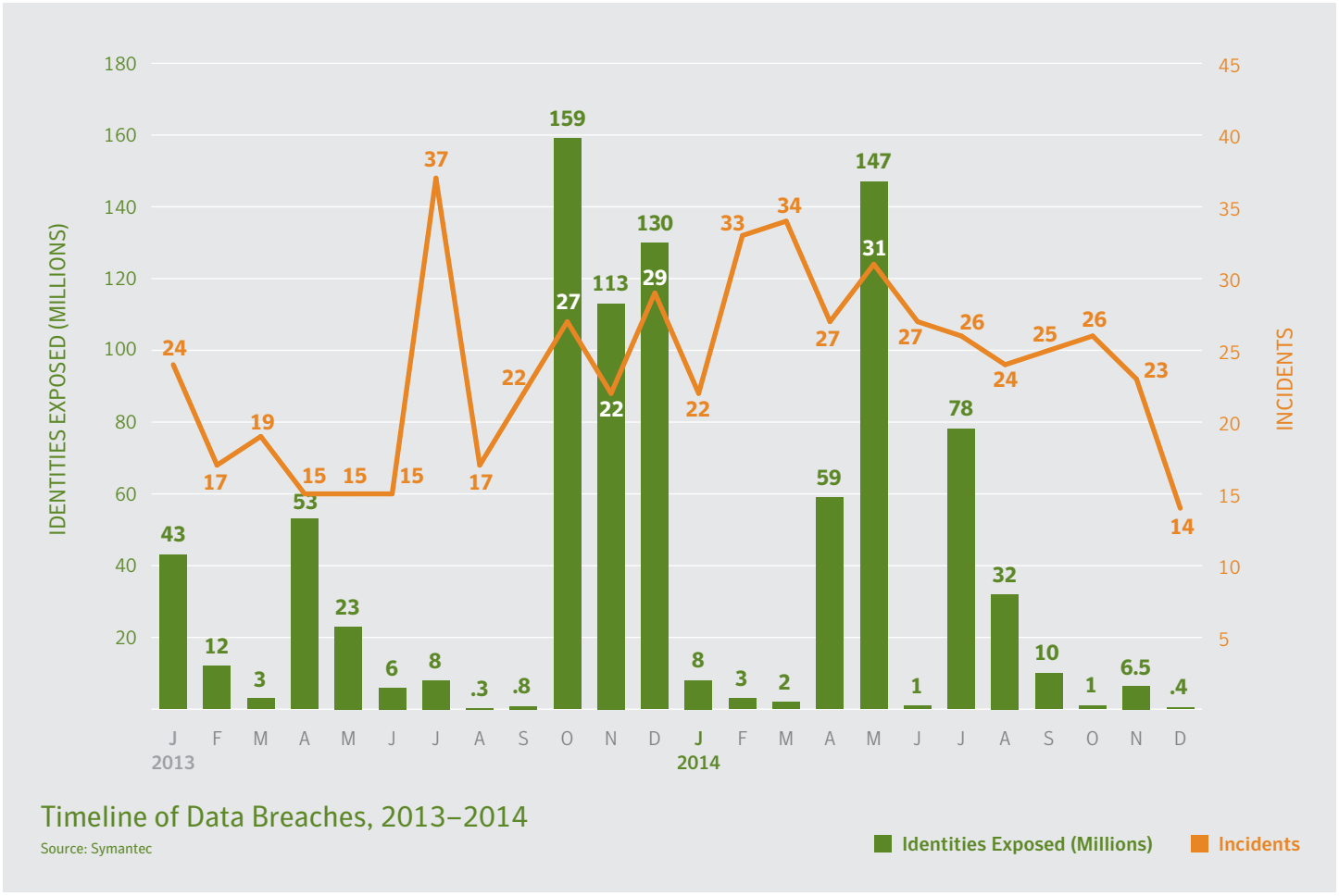
- *The average number of identities exposed per breach declined in 2014 due to fewer mega breaches compared to 2013.*



Median Identities Exposed per Breach

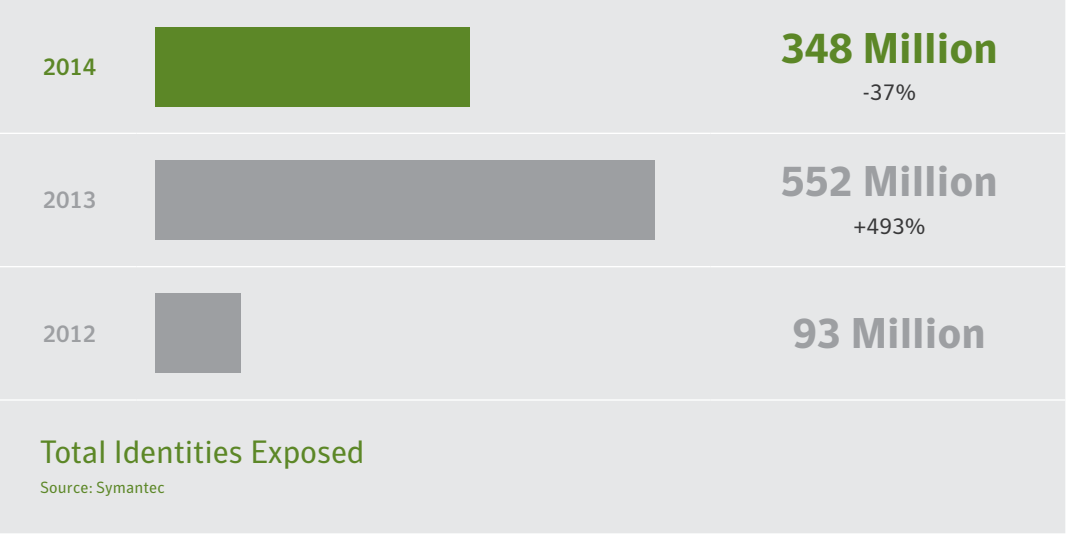
Source: Symantec

- *The median number of identities exposed has increased three percent in 2014.*



Timeline of Data Breaches, 2013–2014

Source: Symantec



Total Identities Exposed

Source: Symantec

- *One significant downturn in 2014 is the number of identities exposed as the result of a data breach. In 2013 we reported that there were 552 million identities exposed. In 2014 this is down significantly, to 348 million identities.*

On the surface it appears that there were far fewer identities exposed in 2014. The fact that there were fewer breaches reported containing more than 10 million identities plays a part in this drop, if anything for sheer volume. It is also possible that large organizations sat up and took notice of the major breaches that occurred toward the end of 2013, implementing security policies that reduced the risk of a data breach, such as rolling out a data loss prevention (DLP) solution that prevents most data from being exfiltrated, even if attackers succeed in penetrating the network.

While these items no doubt played a part, our numbers point to another possibility: the number of organizations that are withholding information on the number of identities exposed is increasing. In 2013, 34 out of 253 breaches, or 13 percent, did not report the number of identities exposed. In comparison, 61 out of 312, or 20 percent, of breaches disclosed in 2014 didn't include this information. This equates to 1 in 5 breaches not reporting on the breadth of data exposed.

It's difficult to definitively explain why this information is not being shared publicly. In some cases it's possible the organizations find it too challenging to determine the number of identities exposed. In others, this information likely remains undisclosed to help save face in what clearly has a negative impact on an organization's public reputation.

What is most concerning, however, is this trend could point to a situation where a large number of breaches are not being disclosed to the public at all. While there are many industries, such as healthcare and some government organizations where a breach must legally be reported, most industries do not have such laws. As a result, some organizations may decide to withhold information about a breach to protect their reputations, and they do not face penalties as a result. This may change in the coming years, as many governing agencies around the world are already looking at bringing in regulation surrounding the proper disclosure of data breaches.

Rank	Sector	Number of Incidents	Percentage of Incidents	100%
1	Healthcare	116	37%	
2	Retail	34	11%	
3	Education	31	10%	
4	Gov. & Public Sector	26	8%	
5	Financial	19	6%	
6	Computer Software	13	4%	
7	Hospitality	12	4%	
8	Insurance	11	4%	
9	Transportation	9	3%	
10	Arts and Media	6	2%	

Top 10 Sectors Breached by Number of Incidents

Source: Symantec

- *For the fourth year in a row, the healthcare sector reported the largest number of data breaches.*

Rank	Sector	Number of Identities Exposed	Percentage of Identities Exposed	100%
1	Retail	205,446,276	59%	
2	Financial	79,465,597	23%	
3	Computer Software	35,068,405	10%	
4	Healthcare	7,230,517	2%	
5	Gov. & Public Sector	7,127,263	2%	
6	Social Networking	4,600,000	1%	
7	Telecom	2,124,021	.6%	
8	Hospitality	1,818,600	.5%	
9	Education	1,359,190	.4%	
10	Arts and Media	1,082,690	.3%	

Top 10 Sectors Breached by Number of Identities Exposed

Source: Symantec

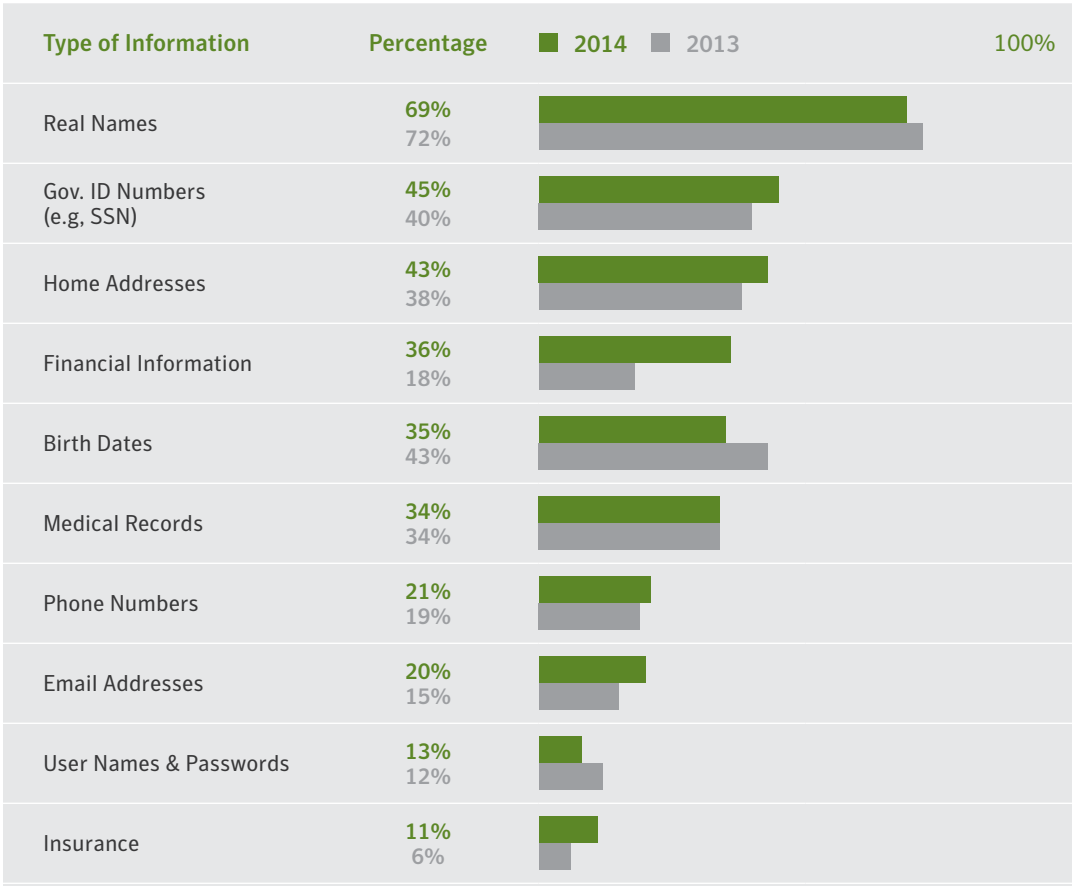
- *The retail sector was responsible for 59 percent of all identities exposed in 2014, followed by the financial sector, with 23 percent.*

Retailers Under Attack

Attackers clearly have retailers in their cross hairs, if the increase in data breaches containing financial information is any indication. The retail industry again has the dubious distinction of being the industry liable for the largest number of identities exposed, accounting for almost 60 percent of all identities reported exposed, up from 30 percent in 2013. Financial information has moved to the fourth most common type of information exposed in a breach. In 2013, 17.8 percent of breaches contained financial information, but in 2014 this number jumped to 35.5 percent.

This financial information can range from bank account details to tax-related documents, but, in most cases, this information is credit or debit card details. Online retailers play a significant part, but so do attacks on point-of-sale systems: the credit card swipe machines that have become so ubiquitous in our retail lives.

Although the first attacks on retail point-of-sale systems date back to 2005, Symantec saw an upsurge in attacks in 2014. It is now one of the biggest sources of stolen payment card data[94] and is at the root of 2013's and 2014's biggest data breaches.



Top 10 Types of Information Exposed

Source: Symantec

Real names, government ID numbers, and home addresses were the top three types of information breached in 2014. The exposure of financial information grew from 17.8 percent to 35.5 percent in 2014, the largest increase within the top 10 list of information types exposed.

Point-of-sale systems are vulnerable because of widespread lack of security, including poor or nonexistent encryption of data, software vulnerabilities, reliance on out-of-date software such as Microsoft Windows XP (which Microsoft stopped supporting in 2014), and the slow adoption of chip-and-PIN technology outside Europe. With new ways to pay, such as Apple Pay, and chip-and-PIN cards finally being adopted in the United States, point-of-sale data should become more secure over the next few years.

Nonetheless, point-of-sale systems are likely to remain a top target for attacks in the near term. Credit card companies are quick to spot anomalous spending patterns, as are observant card owners. This means that criminals need a steady supply of "fresh" card numbers, and the online economy provides a ready market of buyers and sellers.[95]

Privacy and the Importance of Data Security

The prevalence of data breaches over the past number of years has certainly had an impact on consumers' views concerning their private information. Symantec carried out a survey on the topic of privacy within the European Union, publishing some interesting findings in the "State of Privacy Report 2015." [96]

For instance, 59 percent of respondents have experienced a data protection issue in the past. These issues include not only being notified of a data breach by a company that they use but also having an email or social media account hacked, having bank details stolen, being a victim of online identify theft, getting a computer virus, or responding to an online scam or fake email.

Overall, 57 percent of respondents are worried their data is not safe. This is no small matter, as data security is very important to consumers, considering that 88 percent say this is an important factor when choosing a company to do business with—more important than the quality of the product (86 percent) or the customer service experience (82 percent).

On top of that, only 14 percent of respondents were happy to share their data with third parties, with 47 percent being unhappy to share any data and 35 percent requiring some form of check on exactly what data would be shared.

Those surveyed also indicated that they are actively adopting a self-moderation approach to their personal data and taking the matter into their own hands. According to Symantec's research, over half of those surveyed (57 percent) are now avoiding posting personal details online. Another popular approach to self-moderation could also have chilling repercussions for business, as 1 in 3 consumers admitted they provide false information in order to protect their privacy.

1 in 3 consumers admitted they provide false information in order to protect their privacy.

On another note, attackers have become more patient, breaching organizations' defenses and lying in wait, building up knowledge of behavior patterns from activity on the network and learning who does what and how. In this way, attackers are better able to target consumers while impersonating and exploiting them. Attackers often use legitimate, stolen credentials and use patience in conducting such attacks, as opposed to springing attacks immediately following a breach. By carefully monitoring these cycles of behavior for a long time, cybercriminals make sure their attacks appear like normal patterns of behavior.

The traditional perimeter for an organization is no longer as clear as it once was—the boundaries are blurred—and mobile devices make this even more difficult to manage. Data is increasingly stored not only on mobile devices but also in the cloud. Mobile devices have become the key to accessing this data since passwords are more likely to be cached on mobile devices, which are less likely to be encrypted than a stolen laptop. ■

Data Breaches in the Healthcare Industry


By Axel Wirth and David Finn

Driven by market forces and the desire to improve health delivery, reduce costs, and comply with government mandates, healthcare providers are adopting electronic records and digital clinical systems in record numbers. In addition, an aging population requiring management of chronic diseases, new diagnostic methodologies delivering higher-quality results, and an increasing number of covered patients are leading to rapidly growing data volumes. This all results in a more complex IT infrastructure, increasing needs for integration and exchange of information, new care delivery and reimbursement models, and the accumulation of data. These combined trends are making the healthcare industry more attractive to attackers and have put providers at an increasing risk of data breaches, both intentional and accidental.

Symantec saw a 25 percent increase in the number of healthcare data breaches in 2014, two percentage points higher than the rate across all industries. Unlike data breaches as a whole, human error and device theft—related or unrelated to the data present—still make up the majority of these incidents. Lost or stolen devices are accountable for the largest portion of breaches in the healthcare industry. According to the Norton Cybercrime Index, 44 percent of healthcare breaches were the result of lost or stolen devices, a 10 percent increase over the previous year. The number of identities being accidentally exposed publicly as the result of error was also up approximately 11 percent in 2014.

However, targeting patient medical information for purposes of medical identity theft, financial fraud, or health insurance fraud has become an increasing problem. Specifically interested in personally identifiable information (PII) or protected health information (PHI), thieves appear to have more incentive to either hack into healthcare organizations or attempt to hire insiders to obtain electronic copies or printouts of patient records. In fact, the number of data breaches in the healthcare industry that were the result of insider theft nearly doubled in 2014. Data breaches that were the result of attacks were up 82 percent in 2014.

More advanced attacks may target larger volumes of electronic records for identity theft, such as in the retail sector. There are also other criminal activities, including extortion, blackmail, or celebrity snooping. However, an unprecedented number of cases have been reported around the globe and across all types of healthcare organizations, from large academic medical centers to small community hospitals, when compared with any other industry. Neither location nor size provides any protection, as in the case of a 22-bed rural community hospital in Southern Illinois, which received stolen patient data in an email with the request to pay a ransom or the information would be made public.[97]

A number of hospitals have mature cybersecurity programs in place, but many are still struggling with basic goals like implementing encryption to protect data on lost or stolen mobile devices, laptops, or data carriers. Too many healthcare organizations are still underinvesting in cybersecurity, making them an easy target for cybercriminals' increasingly sophisticated and targeted attacks.

Unfortunately, for the most part, the healthcare industry is not prepared to face today's cybersecurity risks, no matter if they are hospitals, pharmaceutical or biotech companies, medical device manufacturers, health insurers, national health agencies, or employers.

Many organizations, such as the SANS Institute, U.S. Department of Homeland Security, FBI, and FDA, have all issued dire warnings about the cybersecurity risks to the healthcare industry. And this is not just a U.S.-centric issue, as breaches have been reported in many other countries. There is a thriving underground market for medical information, and criminals are monetizing it in many ways and for many reasons.

First, medical data sets tend to be more complete when compared to what can be obtained elsewhere. They include demographics, government ID numbers, bank and credit card accounts, insurance plan credentials, disease statuses, and physical descriptors. This data can be used for identify theft, financial fraud, prescription fraud, obtaining medical services, or reselling the data on the black market. Physical characteristics of patients could be misused to obtain passports, visas, or other identity cards.[98] In short, it is enticing for malicious agents due to the breadth and depth of the data.

Medical identity theft has been shown to be much more costly to the victims in ways other than just financial. Incorrect data in your medical records could lead to incorrect or delayed diagnoses or treatments, could affect job prospects, and could be difficult to correct. Unlike financial fraud, where consumers have limited liability, there is little protection against healthcare fraud and the long-term consequences.[99]

Where credit card numbers may fetch $0.50 to $1 in the underground economy, basic identity and insurance information can be valued up to $10[100] or even as high as $50[101] based on its completeness, which may even include ready-made insurance membership cards, driver's licenses, and credit cards.

Breach numbers in healthcare are high and they are trending up. Traditionally, device loss or theft has been the predominant challenge for healthcare organizations, but we are now seeing an increase in targeted attacks on healthcare organizations, resulting in breaches with a significant impact on healthcare providers and patients. Overall, unintentional causes, such as losing devices or accidentally exposing data, are still the most common, but breaches caused by malicious actors, such as attackers or insider thieves, are increasing far more rapidly. This trend highlights the need for healthcare organizations to ensure there are processes in place to handle theft or loss, as well as policies to protect against outside agencies attempting to gain access to lucrative data. ■

E-CRIME & MALWARE

E-Crime and Malware

Every day, personal banking details are phished by fake emails and websites. Computers infected with malware are used to send out spam or contribute to distributed denial-of-service (DDoS) attacks. Perhaps the most unlucky see all their files encrypted and their computer made unusable by ransomware.

Email continues to be an effective delivery vehicle for spam, phishing, and malware, and overall, the proportion of emails that include malware is rising. Cybercriminals rely on an underground online economy to buy and sell services and malware and to fence stolen credit cards and botnets.

Working with security firms, including Symantec, law enforcement has continued to disrupt botnets and make arrests. This has produced noticeable, if temporary, improvements on the overall levels of cybercrime.

The Underground Economy

The underground black market is thriving. In the darker corners of the Internet, there's a huge trade in stolen data, malware, and attack services.[102] Criminals are moving their illegal marketplaces further from public gaze, including using the anonymous Tor network and limiting access to an invitation-only basis.[103] Price changes give some indication of supply and demand. Overall, email prices have dropped considerably, credit card information has declined a little, and online bank account details have remained stable.

Underground economy prices for credit cards in various countries.

At a Glance

- *Prices are holding steady in the underground economy, suggesting continuing high levels of demand for stolen identities, malware, and e-crime services.*
- *The number of vulnerabilities is down relative to 2013, but the general trend is still upward.*
- *The number of new malware variants grew by 317,256,956 in 2014—a 26 percent increase compared with 2013.*
- *Ransomware is getting nastier and increasing in volume. The amount of crypto-ransomware has also grown over 45 times larger than in 2013.*
- *The number of bots declined by 18 percent in 2014.*

Cybercriminals rely on an underground online economy to buy and sell services and malware.

Cybercriminals can also buy malware, attack kits, and vulnerability information off the shelf. They can even buy "crimeware as a service," which comes with the entire infrastructure to run online scams.

These markets allow a division of labor. Some people specialize in writing Trojans and viruses, and others in malware distribution, botnets, or monetizing stolen credit card details. Some of these markets have existed for at least 10 years, but Symantec sees increasing professionalization of all the elements. Any product or service directly linked to monetary profit for the buyer retains a solid market price.[104]

A drive-by download web toolkit, which includes updates and 24/7 support, can be rented for between $100 and $700 per week. The online banking malware SpyEye (detected as Trojan.Spyeye) is offered from $150 to $1,250 on a six-month lease, and DDoS attacks can be ordered from $10 to $1,000 per day.[105]

Item	2014 Cost	Uses
1,000 Stolen Email Addresses	$0.50 to $10	Spam, Phishing
Credit Card Details	$0.50 to $20	Fraudulent Purchases
Scans of Real Passports	$1 to $2	Identity Theft
Stolen Gaming Accounts	$10 to $15	Attaining Valuable Virtual Items
Custom Malware	$12 to $3500	Payment Diversions, Bitcoin Stealing
1,000 Social Network Followers	$2 to $12	Generating Viewer Interest
Stolen Cloud Accounts	$7 to $8	Hosting a Command-and-Control (C&C) Server
1 Million Verified Email Spam Mail-outs	$70 to $150	Spam, Phishing
Registered and Activated Russian Mobile Phone SIM Card	$100	Fraud

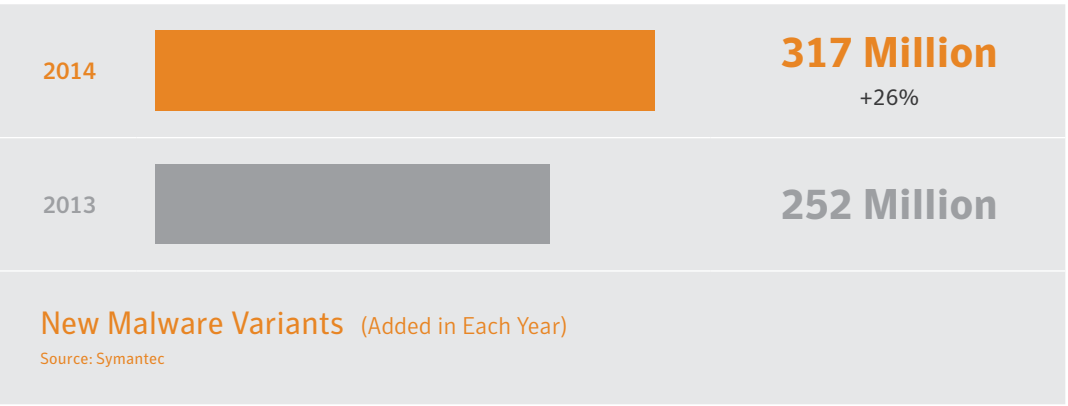
Value of Information Sold on Black Market

Source: Symantec

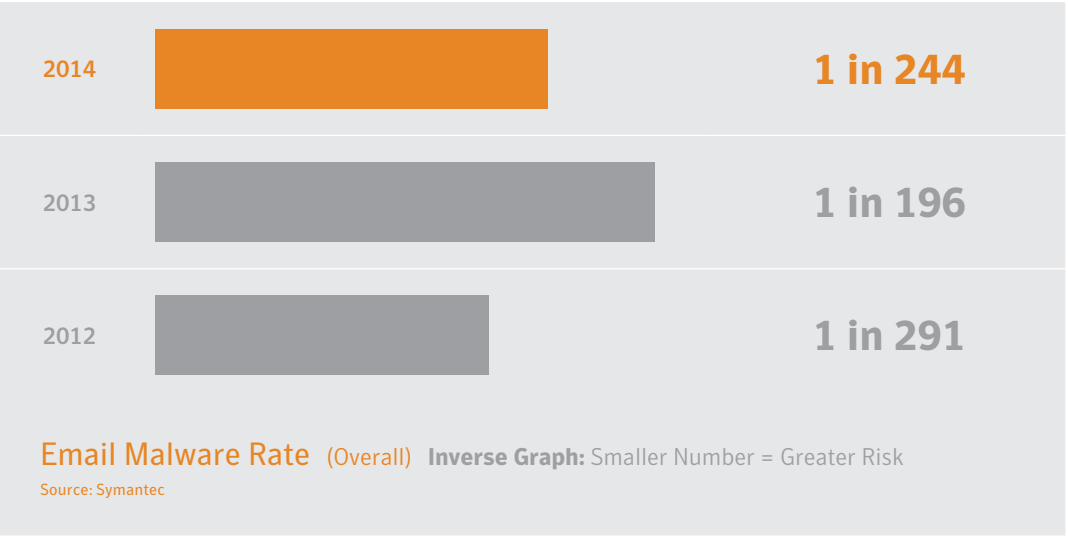
Malware

At the end of 2013, Russian authorities arrested "Paunch," the alleged author of the Blackhole exploit kit, which was responsible for a large number of infections worldwide.[106,107] It was a small victory in a long war against malware in all its forms.

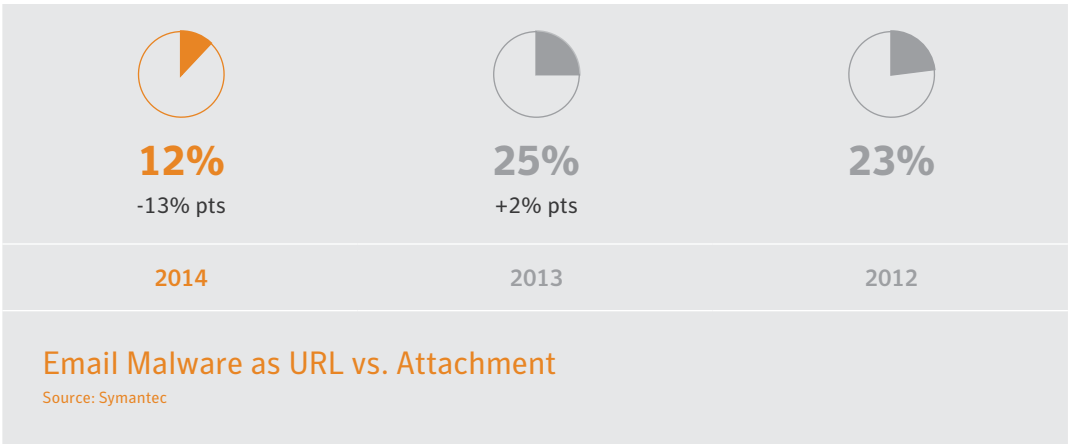
Inevitably, other attack kits have come up to fill the void. Malware designed to steal bank details continues to be prevalent. Malware targeting new "markets" appeared in 2014, with the Snifula banking Trojan attacking Japanese financial institutions[108] and an indigenous group of attacks emerging in the Middle East using malware called njRAT.[109]



- *With more than 317 million new pieces of malware created in 2014, or close to 1 million new pieces of unique malware each day, the overall total number of malware is now 1.7 billion.*



- *The email malware rate dropped to 1 in 244 emails in 2014. While lower than 2013, this is still higher than the rate of 1 in 291 emails seen in 2012.*



Email Malware as URL vs. Attachment

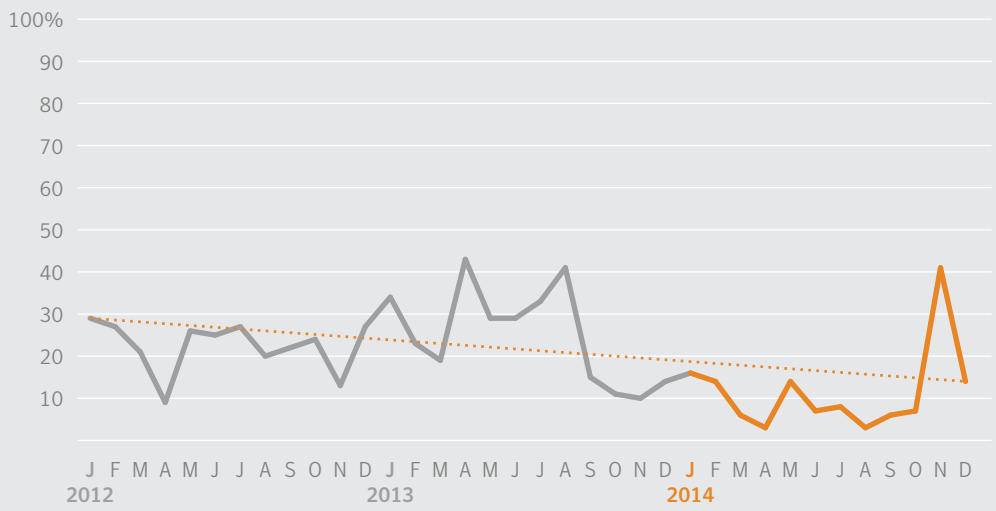
Source: Symantec

- *Twelve percent of email-borne malware in 2014 contained a malicious link rather than being attached to an email, compared with 25 percent in 2013.*

In October 2014, only seven percent of malicious spam emails contained URL links. That number jumped to 41 percent in November and continued to climb in early December, thanks to a surge in social engineering–themed messages, including malicious fax and voice mail notification emails.

The links in these emails use hijacked domains and have a URL path that leads to a PHP landing page. If the user clicks on the links, they are led to a malicious file. In particular, we have seen Downloader.Ponik and Downloader.Upatre being used in these emails. These are well-known Trojans that are used for downloading additional malware onto compromised computers, including information stealers like Trojan.Zbot (also known as Zeus).[110]

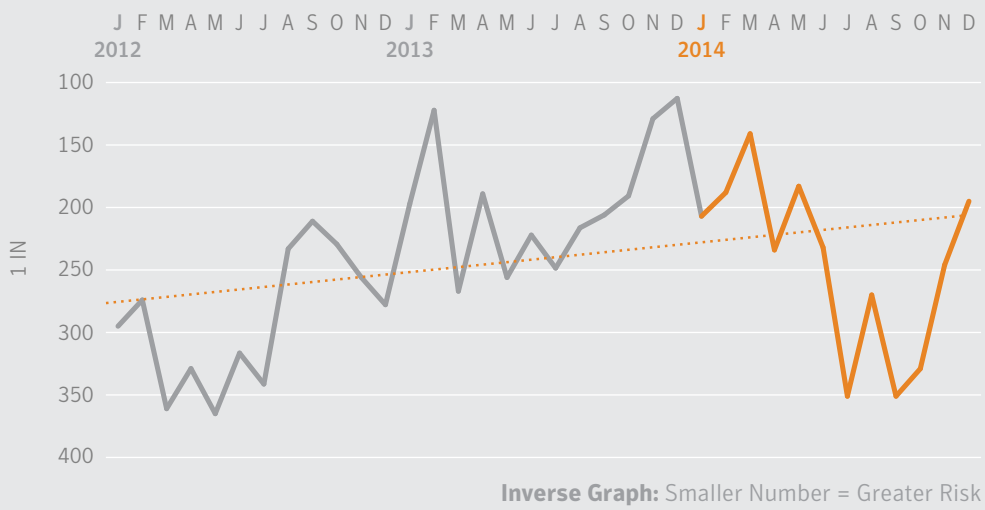
Overall, the number of emails distributing malware has declined in 2014, after appearing to have peaked in 2013.



Percent of Email Malware as URL vs. Attachment by Month, 2012–2014

Source: Symantec

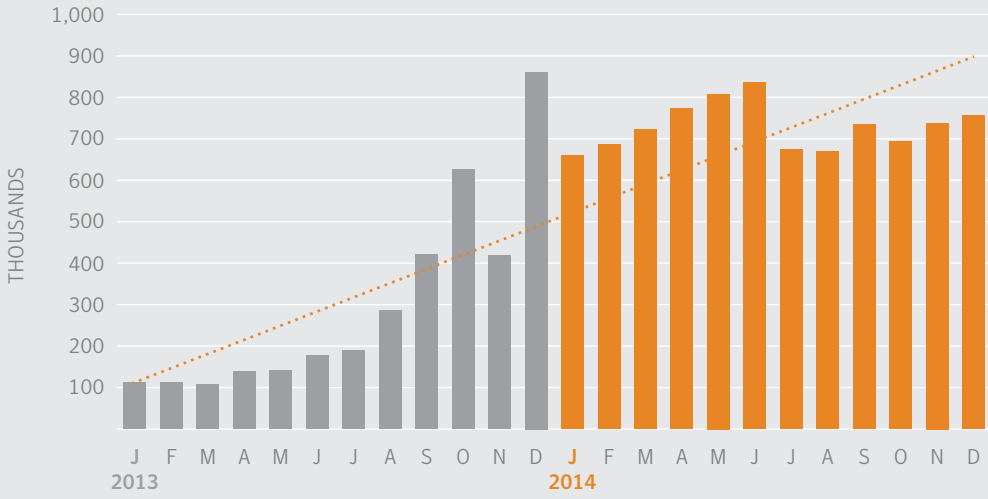
- *In November 2014, the percent of email malware that contains a URL jumped to 41 percent, the highest seen since August 2013.*
- *The sudden increase, and subsequent decline, was attributed to the activity of the Cutwail botnet.*



Proportion of Email Traffic in Which Malware Was Detected, 2012–2014

Source: Symantec

- *There was a significant drop in the email malware rate during the late summer, early autumn of 2014.*



Ransomware Over Time, 2013–2014

Source: Symantec

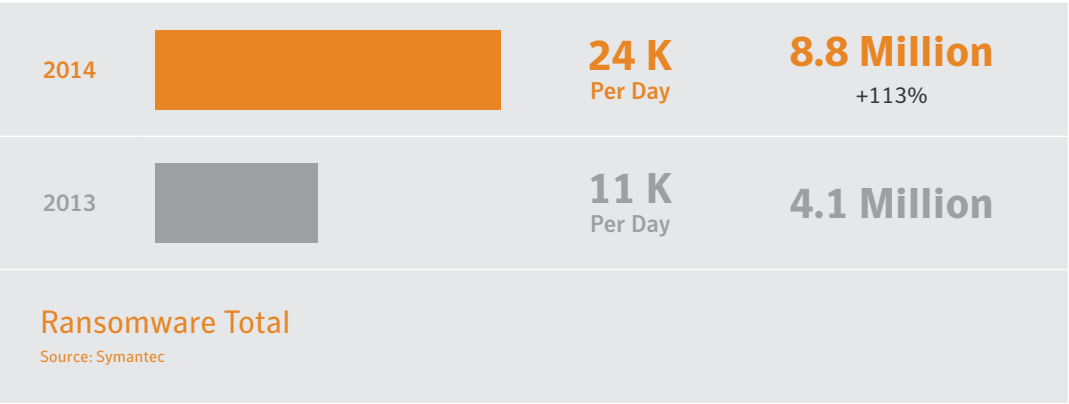
- *On average there were 729,167 ransomware attacks per month in 2014.*

Ransomware

Ransomware attacks more than doubled in 2014, from 4.1 million in 2103, up to 8.8 million. More concerning is the growth of file-encrypting ransomware (what Symantec refers to as "crypto-ransomware"), which expanded from 8,274 in 2013 to 373,342 in 2014. This is 45 times more crypto-ransomware in the threat landscape within a one-year span. In 2013, crypto-ransomware accounted for 0.2 percent (1 in 500) of ransomware and was fairly uncommon; however, by the end of 2014 it accounted for 4 percent (1 in 25) of all ransomware.

On a human level, ransomware is one of the nastiest forms of attack for victims. Criminals use malware to encrypt the data on victims' hard drives—family pictures, homework, music, that unfinished novel—and demand payment to unlock the files. The best, and pretty much only, defense is to keep a separate backup of your files, preferably offline, to restore from.

There are many ransomware variants, and no operating system guarantees immunity.[111] And while the advice remains the same—do not pay the criminals—many businesses and individuals simply want or need their files back. So they pay, and thus the scam remains profitable.



Criminals use malware to encrypt the data on victims' hard drives—family pictures, homework, music, that unfinished novel—and demand payment to unlock the files.

Crypto-Ransomware

The bad news is that, while ransomware has doubled, between 2013 and 2014 Symantec saw the amount of crypto-ransomware in the threat landscape grow to be over 45 times larger.[112]

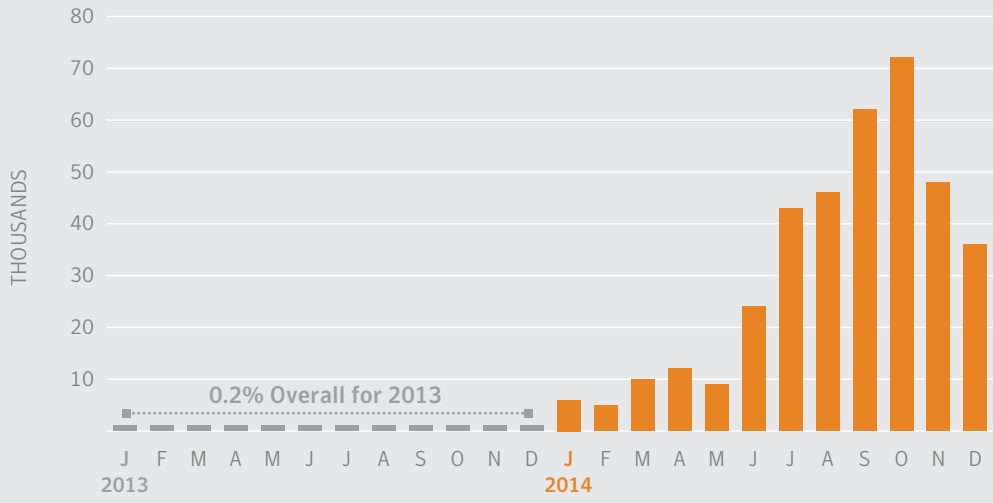
There are several different crypto-ransomware families, such as Cryptolocker,[113] Cryptodefense,[114] and Cryptowall,[115] but their method of exploitation is the same. Rather than locking your desktop behind a ransom wall, crypto-ransomware encrypts your personal files and holds the private keys to their decryption for ransom at a remote site. This is a much more vicious attack than traditional ransomware.

Methods of infection vary, but commonly it's via a malicious email attachment purporting to be an invoice, energy bill, or image. The delivery often forms part of a service actually provided by different criminals from those executing the crypto-ransomware. This is just one of the darker sides of the underground economy, where criminals offer services such as "I can infect X computers for a fixed price of Y."

CryptoDefense, brought to light back in March, is a perfect example of just how serious crypto-ransomware is and how hard the criminals behind it are to track. It's delivered via malicious email attachments and encrypts a victim's files with public-key cryptography using strong RSA 2048 encryption.

In order to pay the ransom, the victim has to visit a webpage on the Tor network.[116] The payment is then requested in bitcoins. These are typical moves of a crypto-ransomware criminal, making it incredibly difficult to track and shut down such scams.

And then we get to the crux of the entire scam: the profit. Symantec estimated that the cybercriminals behind CryptoDefense earned over $34,000 in just one month.[117] It's no wonder crypto-ransomware is considered to be the most effective cybercrime operation out there at the moment.



Crypto-Ransomware, 2013–2014

Source: Symantec

In 2013, crypto-ransomware accounted for approximately 0.2 percent of all ransomware attacks. By the end of 2014 this figure grew to 4 percent.[118]

Digital Extortion: A Short History of Ransomware

By Peter Coogan

In 2014, crypto-ransomware was rarely out of the news. The latest and deadliest trend in the ongoing ransomware saga, crypto-ransomware differs from its standard ransomware siblings, which simply lock the device, in that it encrypts data files on the compromised device and, in most cases, leaves victims with no way to rescue their data. Both crypto-ransomware and ransomware, however, are in the business of extorting ransom from victims for the removal of the infection.

These types of malware have been around for over a decade but have grown in prevalence over the past few years. This growth is the result of cybercriminals' shifting from the creation of fake antivirus software to the more lucrative ransomware. While we can trace an evolution from fake antivirus, to ransomware, and then on to crypto-ransomware, malware authors rarely rest on their laurels. We can clearly see new areas of the threat landscape where these digital extortionists are heading.

Fake antivirus (a.k.a. FakeAV or rogue security software) is a misleading application that fraudulently deceives or misleads a user into paying for the removal of malware. While this software has been around for quite some time now— its prevalence peaked around 2009, a Symantec report at that time observed 43 million rogue security software installation attempts from over 250 distinct programs, at a cost of $30 to $100 for anyone who purchased the software.[119]

Ransomware is malicious software that locks and restricts access to infected computers. The malicious software then displays an extortion message using a social engineering theme that demands a ransom payment to remove the restriction. In 2012 Symantec reported on the growing menace of ransomware, with fraudsters charging in the range of €50 to €100 in Europe or up to $200 in the U.S. for the removal of restrictions.[120]

Now, after the emergence and perceived success of the now-infamous Trojan.Cryptolocker[121] in 2013, malware authors have been turning their attention to writing new crypto-ransomware-style threats. This has led to a surge in new crypto-ransomware families seen in 2014 that incorporate new innovations, platforms, and evasion tactics alongside both old and new tricks in an attempt to extort money from victims.

One of the more prolific new crypto-ransomware threats in 2014 was Trojan.Cryptodefense[122] (a.k.a. Cryptowall). This threat appeared in late February 2014 and was initially marketed as Cryptodefense. It employed techniques such as the use of Tor and bitcoins for anonymity, strong RSA-2048 encryption of data, and pressure tactics to scare victims into payment. With an initial ransom demand of $500/€500, it soon increased to $1,000/€1,000 if payment was not forthcoming. However, following analysis, it was found that the malware author's poor implementation of the cryptographic functionality had left hostages with the key to their own escape, in the form of the private encryption key being left on the system. After this information was made public, the issue was fixed by the malware authors and it was rebranded as Cryptowall. Since then, Cryptowall has continued to evolve by weaponizing itself further, with an elevation of privilege exploit, anti-analysis checks, and the use of Invisible Internet Project (I2P) for communication anonymization. The known earnings of Cryptowall were at least $34,000 in its first month, [123] with researchers determining that it made in excess of $1 million over a six-month period.[124]

The Windows PC landscape has been a lucrative area for ransomware authors, and this will likely continue to be the case. However, in 2014 the attackers behind these digital extortion tools began to tackle new platforms. We saw the Reveton gang release Android ransomware known as Android.Lockdroid.G[125] (a.k.a. Koler). Through their use of a Traffic Distribution System (TDS), the Reveton gang performed a three-pronged ransomware attack. Depending on certain conditions, such as the browser being used to view a website controlled by the gang, traffic would be redirected to a fitting ransomware.

Ransomware had suddenly become platform independent. Android users would be redirected to download Android.Lockdroid.G. Internet Explorer users were redirected to the Angler Exploit kit, delivering a payload of Trojan.Ransomlock.G.[126] and other browsers used on Windows, Linux, or Mac to Browlock,[127] another form of ransomware that

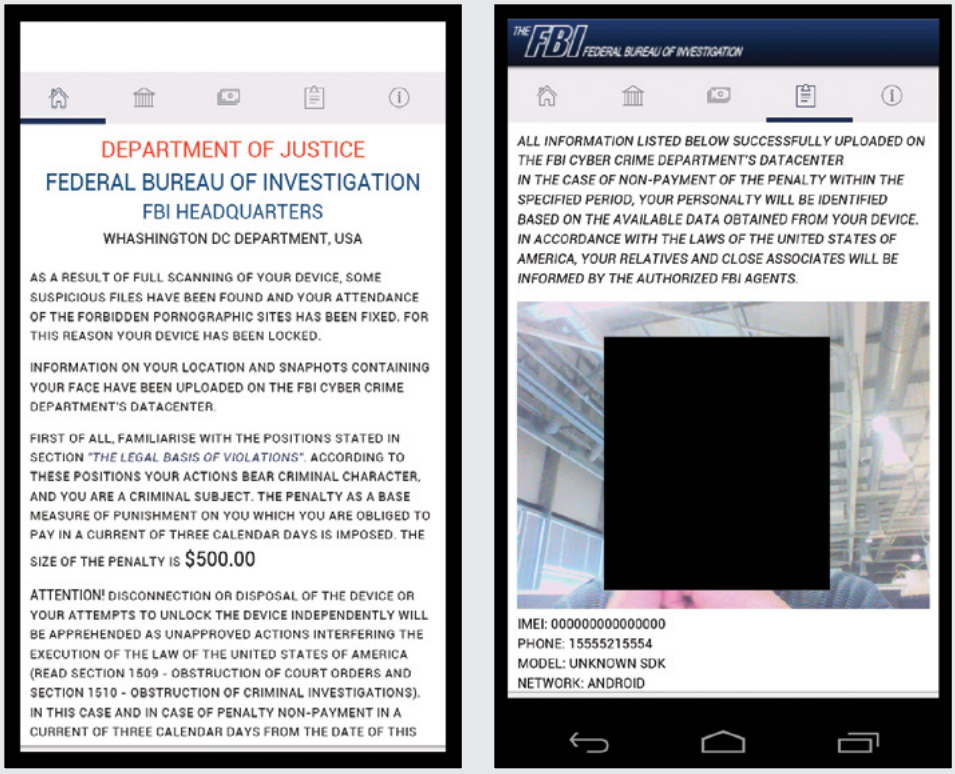
attempts to lock the computer and extort money from users by simply using tools in their web browser.

In June 2014, the first file-encrypting ransomware for Android, known as Android.Simplocker,[128] was discovered. With a demand initially in Russian, by July 2014 an updated English version (Android.Simplocker.B[129]) was being seen that employed an FBI social engineering theme. October 2014 saw the emergence of Android.Lockdroid.E[130] (a.k.a. Porndroid), which once again used a fake FBI social engineering theme. This threat, however, also used the device's camera to take a picture, which would then be displayed alongside the ransom demand. Android.Lockdroid further spawned new variants that included worm-like capabilities, allowing self-replication via SMS messages sent to contacts in the address book on an infected device, along with a social engineering catch.

Ransomware authors even began looking past mobile devices to see where else they could possibly extort money, and they realized that network-attached storage (NAS) devices, where large quantities of files are stored, could also be targeted. Trojan.Synolocker[131] (a.k.a. Synolocker) targeted Synology NAS devices by using a previously unknown vulnerability in Synology's DiskStation manager software to gain access to the devices and then encrypt all the files, holding them for ransom. These devices have since been patched against further attacks, but this case highlights that ransomware attackers are continuing to look for new areas to attack.

So why are we seeing such rapid changes in ransomware? Ransomware is a lucrative business for cybercriminals, with ransom demands ranging anywhere from $100 to $500. During 2014 we also saw bitcoins become the ransom payment method of choice by most new ransomware. Given bitcoin's strong anonymity, it allows cybercriminals to easily hide and launder their ill-gotten gains.

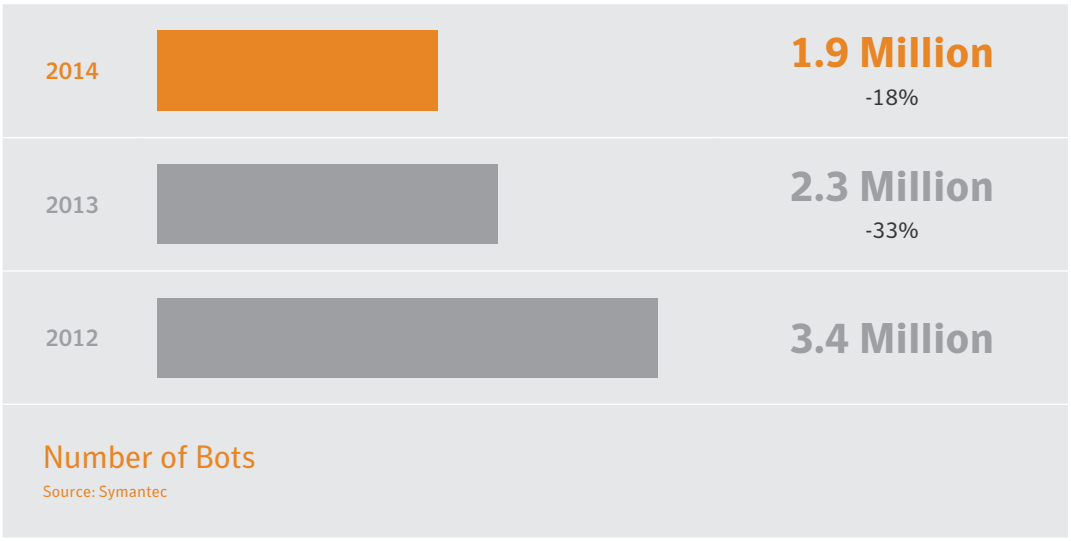
While we have observed a surge in new ransomware families, Symantec has also seen an increase in the overall growth path. Since 2013, there has been a 113 percent rise in the occurrence of ransomware attacks. However, given the lucrative nature of these threats and the number of new ransomware families appearing, it is unlikely that ransomware-type scams will drop off the threat landscape anytime soon, with future growth being more likely. ■



"Porndroid" Android ransomware threat.

Bots and Botnets

The number of bots declined by 18 percent in 2014 compared to the previous year. In large measure, this is because the FBI, the European Cybercrime Centre (EC3) at Europol, and other international law enforcement agencies, working with Symantec and other tech firms, have been active in disrupting and shutting them down. Most notably, the Gameover Zeus botnet was shut down in 2014. It was responsible for millions of infections worldwide since its arrival in 2011.[132,133] This is one in a series of botnet takedowns over the past couple of years[134,135] that have seen IT firms and law enforcement working together effectively.



Number of Bots

Source: Symantec

- *The decline in bots in 2014 was, in part, fueled by the disruption of the Gameover Zeus botnet with "Operation Tovar." This botnet had largely been used for banking fraud and distribution of the CryptoLocker ransomware.*

Country/Region	2014 Bots Rank	2014 Bots Percentage	2013 Bots Rank	2013 Bots Percentage
China	1	16.5%	2	9.1%
United States	2	16.1%	1	20.0%
Taiwan	3	8.5%	4	6.0%
Italy	4	5.5%	3	6.0%
Hungary	5	4.9%	7	4.2%
Brazil	6	4.3%	5	5.7%
Japan	7	3.4%	6	4.3%
Germany	8	3.1%	8	4.2%
Canada	9	3.0%	10	3.5%
Poland	10	2.8%	12	3.0%

Malicious Activity by Source: Bots, 2013–2014

Source: Symantec

- *The United States and China, two of the most populated countries with the greatest concentration of Internet-connected users, swapped the number one and two places in 2014. This switch can likely be attributed to the takedown of the Gameover Zeus botnet.*

Spam Botnet Name	Percentage of Botnet Spam	Estimated Spam per Day	Top Sources of Spam From Botnet		
			Rank #1	Rank #2	Rank #3
KELIHOS	51.6%	884,044	Spain 10.5%	United States 7.6%	Argentina 7.3%
UNKNOWN/ OTHER	25.3%	432,594	United States 13.5%	Brazil 7.8%	Spain 6.4%
GAMUT	7.8%	133,573	Russia 30.1%	Vietnam 10.1%	Ukraine 8.8%
CUTWAIL	3.7%	63,015	Russia 18.0%	India 8.0%	Vietnam 6.2%
DARKMAILER5	1.7%	28,705	Russia 25.0%	Ukraine 10.3%	Kazakhstan 5.0%
DARKMAILER	0.6%	9,596	Russia 17.6%	Ukraine 15.0%	China 8.7%
SNOWSHOE	0.6%	9,432	Canada 99.9%	United States 0.02%	Japan 0.01%
ASPROX	0.2%	3,581	United States 76.0%	Canada 3.4%	United Kingdom 3.3%
DARKMAILER3	0.1%	1,349	United States 12.7%	Poland 9.6%	South Korea 9.1%
GRUM	0.03%	464	Canada 45.7%	Turkey 11.5%	Germany 8.5%

Top 10 Spam-Sending Botnets, 2014

Source: Symantec

OSX as a Target

Over the past few years Apple has sat up and taken notice of the threats that have been targeting OS X, rolling out a couple of much-needed security features to the operating system. XProtect scans downloaded files for signs of malware, warning users if they download a malicious file known to Apple. Using code signing Gatekeeper limits what apps can be run within an OS X computer. There are varying degrees of protection with Gatekeeper, ranging from limiting installation to apps from the official Mac App Store, developers identified as trustworthy by Apple, or any developer that signs their apps.

However, while these security features have made it more difficult for threats to gain a foothold in OS X, threats have nevertheless succeeded in getting past them. As with any signature-based security solution, apps have managed to compromise computers before signatures could be put in place to block them. Malicious apps have also appeared with legitimate developer signatures, by either stealing legitimate credentials or creating false ones.

The most common threats seen in 2014 had similar behaviors to those found on other operating systems. There were Trojans that arrived via browser exploits. Notorious threats such as Flashback, which infected over 600,000 Macs in 2012, are still fairly prevalent, with variants taking up the number three and 10 spots in 2014. Threats that modify settings, such as DNS, browser, or search settings on the OS X computer, also rank highly.

Two notable threats highlighted a significant issue in the OS X threat landscape: pirated OS X apps that contain malware.

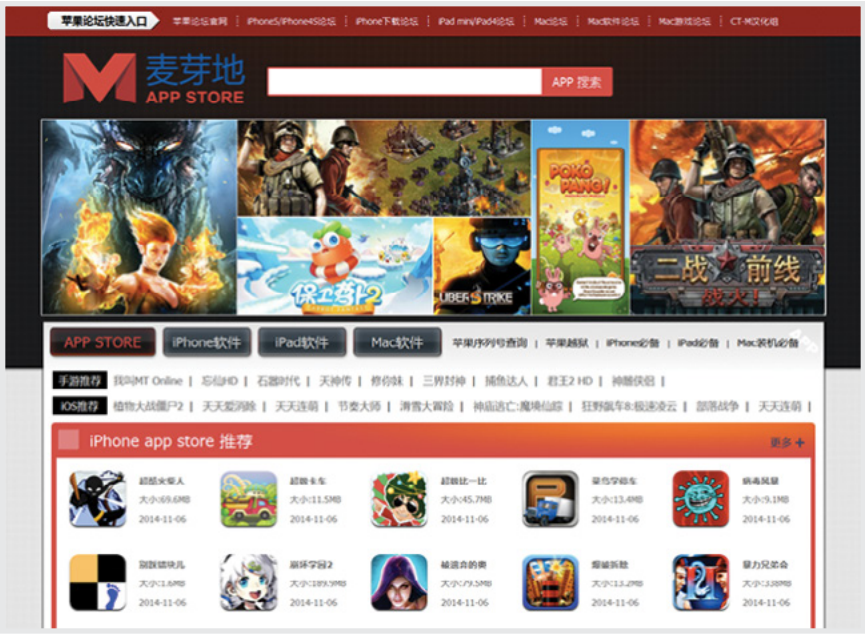
OSX.Wirelurker is a dual-threat Trojan horse, impacting both Macs running OS X and any iOS devices connected to a compromised computer. This threat gained major attention when it was discovered within 467 OS X applications hosted on a third-party OS X app store in China. These malicious apps were downloaded more than 356,000 times before Apple stepped in and blocked them to prevent them from running.

Rank	Malware Name	Percentage of Mac Threats 2014	Malware Name	Percentage of Mac Threats 2013
1	OSX.RSPlug.A	21.2%	OSX.RSPlug.A	35.2%
2	OSX.Okaz	12.1%	OSX.Flashback.K	10.1%
3	OSX.Flashback.K	8.6%	OSX.Flashback	9.0%
4	OSX.Keylogger	7.7%	OSX.HeIIRTS	5.9%
5	OSX.Stealbit.B	6.0%	OSX.Crisis	3.3%
6	OSX.Klog.A	4.4%	OSX.Keylogger	3.0%
7	OSX.Crisis	4.3%	OSX.MacControl	2.9%
8	OSX.Sabpab	3.2%	OSX.FakeCodec	2.3%
9	OSX.Netweird	3.1%	OSX.Iservice.B	2.2%
10	OSX.Flashback	3.0%	OSX.Inqtana.A	2.1%

Top 10 Mac OS X Malware Blocked on OS X Endpoints, 2013–2014

Source: Symantec

Two notable threats highlighted a significant issue in the OS X threat landscape: pirated OS X apps that contain malware.



Third-party app store, Maiyadi, which was found to be hosting apps with OS X malware in 2014.

OSX.Luaddit (a.k.a. iWorm) is a threat that added compromised computers to an OS X botnet. This threat was found bundled with pirated copies of commercial products like Adobe Photoshop, Microsoft Office, and Parallels.[136] These apps were posted to torrent sites and were downloaded thousands of times.

Type	Name (Order by: Uploaded, Size, ULed by, SE, LE) View: Single / Double	SE	LE
Applications (Mac)	Adobe Illustrator CS6 Mac OSX Uploaded 07-31 05:19, Size 1.42 GiB, ULed by aceprog	217	15
Applications (Mac)	Parallels Desktop 9 Mac OSX Uploaded 07-31 00:19, Size 418.43 MiB, ULed by aceprog	41	1
Applications (Mac)	Adobe Photoshop CC 2014 Mac OSX Uploaded 07-29 05:19, Size 801.44 MiB, ULed by aceprog	342	21
Applications (Mac)	Adobe Photoshop CS6 Mac OSX Uploaded 07-26 23:18, Size 988.02 MiB, ULed by aceprog	269	15
Applications (Mac)	Adobe Photoshop CS6 for Mac OSX Uploaded 07-26 23:11, Size 988.02 MiB, ULed by aceprog	80	6
Applications (Mac)	Microsoft Office 2011 Mac OSX Uploaded 07-20 19:04, Size 910.84 MiB, ULed by aceprog	449	5

Examples of OS X torrents that contain malware.

In terms of other notable OS X threats, OSX.Stealbit.A and OSX.Stealbit.B are bitcoin-stealing threats that monitor browsing traffic, looking for login credentials to major bitcoin websites. The latter was one of the top five OS X threats seen in 2014.

OSX.Slordu is a back door Trojan horse that appears to be used for gathering information about the compromised computer. What is interesting about this threat is it appears to be an OS X port of a popular Windows back door.

OSX.Ventir is a modular threat, equipped with option components that can open a back door, log keystrokes, or contain spyware capabilities. Depending on what the attacker wishes to gain from the compromised computer, different modules could be downloaded and installed in OS X.

OSX.Stealbit.A is a bitcoin-stealing threat that monitors browsing traffic, looking for login credentials to major bitcoin websites.

Malware on Virtualized Systems

Virtualization is no protection against malware. Increasingly, malware can detect whether it is running on a virtual machine and, instead of quitting, it can change its behavior to reduce the risk of detection.[137] Historically the proportion of malware that detected whether or not it was running on VMware hovered around 18 percent but spiked at the beginning of 2014 to 28 percent.[138]

Virtualization is no protection against malware. Increasingly, malware can detect whether it is running on a virtual machine and, instead of quitting, it can change its behavior to reduce the risk of detection.

But this type of functionality is not being used just to avoid security researchers. Once installed on a virtual machine, malware can hop to other virtual machines on the same hardware or infect the hypervisor, massively increasing the risk and the difficulty of removal.[139] This behavior has already been seen in the wild: the W32.Crisis malware tries to infect virtual machine images stored on a host computer.[140]

For IT managers, this kind of attack poses special risks. It is unlikely to be detected by perimeter security, such as intrusion detection systems or firewalls that use virtual machines for detecting threats in virtual "sandboxes." Virtual machines may not have the same level of protection as traditional clients or servers because of the (false) assumption that malware doesn't attack virtual machines. Organizations need to consider technology such as network hardware, hypervisors, and software-defined networks in their security plans and patch cycles. ■

APPENDIX

Looking Ahead

Threat Intelligence and Unified Security

Today's attackers are skilled enough and sufficiently resourced to have the persistence and patience to carry out their espionage activities over a period of months or even years. They have only to be successful once in order to breach their targets' defenses; however, those targets must be able to resist each and every one of those assaults, every second of every day. Threat intelligence is a vital component in understanding these potential threats, uncovering new attacks, and better protecting critical company assets. Threat intelligence can provide a prioritized list of suspicious incidents by correlating all available information from across the enterprise.

Advanced attackers use exploit toolkits against not only older vulnerabilities but also new, zero-day ones, and being good at defense means being harder to breach. The battle is an asymmetric one, and attackers already understand the defenses and their weaknesses. A unified security model is not just about investing in great technology. It also takes a holistic approach that combines threat intelligence, risk management, and the very best technical solutions. A unified approach will not only help reveal who is being targeted but also how and why. Understanding the new threats is critical, and businesses should now expect to be attacked—the question is not "if" but "when" and "how."

Unified security can leverage the combined visibility and threat intelligence gathered across the enterprise to block, detect, and remediate attacks. It can help guide how to better protect confidential information and reduce risk, supporting the continual assessment of not only people and their skills but also processes and technology to ensure the best response is followed. Processes are continually updated and skills maintained. Ultimately, by becoming harder to breach, attackers must work harder; no one wants to be the weakest link in the supply chain. This, we believe, is the future of security.

Security Gamification

As the 15th-century security consultant Niccolo Machiavelli observed, "Men are so simple and yield so readily to the desires of the moment that he who will trick will always find another who will suffer to be tricked."

Internet security relies on the human element as much as it does on technology. If people were more skillful, they could help reduce the risks they faced. This is as true of consumers' avoiding scams as it is of government employees' avoiding the social engineering in targeted attacks.

In this context, gamification can be used to turn "the desires of the moment" into lasting changes of behavior by using the psychological rewards and instant gratification of simple computer games. Gamification could be used, for example, to train people to be wary of phishing emails or to generate, remember, and use strong passwords.

Symantec sees a big market opportunity and a great need for this kind of training in the coming years.

Security Simulation

Companies can prepare for security breaches and understand their defenses better using simulations and security "war games." By extending conventional penetration testing into a simulated response and remediation phase, companies can train their people and improve their readiness. This message is not lost on governments. In January 2015, UK Prime Minister David Cameron and U.S. President Barack Obama agreed to carry out "war game" cyberattacks on each other. Companies should follow their example in 2015.

Determined Attackers Will Likely Succeed

In the battle between attackers and corporate IT security, the bad guys have to be lucky only once. The IT department has to be lucky all the time. With this in mind, IT managers (and indeed consumers) need to plan for the worst. There is no magic-bullet technology that will guarantee immunity from Internet crime or determined, targeted attacks. So assume you've been hacked or you're about to be hacked. Switch from a binary "safe"/"not safe" view to a nuanced, almost medical approach to trends, symptoms, behavioral prevention, diagnostics, and treatment.

On a technical level, it means ensuring you have effective data loss prevention software on each endpoint, gateway, and email server to prevent data exfiltration. It also means that backup and disaster recovery become much more important, as do detection and response planning. This is not a counsel of despair—we should never make it easy for attackers by giving up on prevention—but it is better to be wise before the event than sad after it.

Data Sharing Between Companies Is Essential

Data sharing between companies is essential to security. Historically, companies have been afraid to share too much information with other companies, so they've effectively fought individual battles against the bad guys and depended on their own internal resources. We believe they need to pool their threat intelligence and their experience to combat the criminals. Tools that allow them to do this while retaining some IP protection will become increasingly important. For example, security electronic data exchanges could share hashes, binary attributes, symptoms, and so on, without revealing corporate secrets or information that could be useful in an attack.

Insecure Operating Systems

A quarter of PC users were running Windows XP and Office 2003 in July 2014[141] even as their software went out of support and Microsoft stopped updating it. A lot of people are still in denial about this change. This leaves them unpatched as new threats emerge. Over the next year, this presents a significant security risk. For embedded devices running out-of-date operating systems, companies will need to find new ways of protecting them until they can be replaced or upgraded.

Internet of Things

As consumers buy more smart watches, activity trackers, holographic headsets, and whatever new wearable devices are dreamed up in Silicon Valley and Shenzhen, the need for improved security on these devices will become more pressing. It's a fast-moving environment where innovation trumps privacy. Short of government regulation, a media-friendly scare story, or greater consumer awareness of the dangers, it is unlikely that security and privacy will get the attention they deserve. The market for Internet of Things–ready devices is growing but is still very fragmented, with a rich diversity in low-cost hardware platforms and operating systems. As market leaders emerge and certain ecosystems grow, the attacks against these devices will undoubtedly escalate, as has already happened with attacks against the Android platform in the mobile arena in recent years.

Best Practice Guidelines for Businesses

Employ defense-in-depth strategies

Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls as well as gateway antivirus, intrusion detection or protection systems (IPS), website vulnerability with malware protection, and web security gateway solutions throughout the network.

Monitor for network incursion attempts, vulnerabilities, and brand abuse

Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation. Track brand abuse via domain alerting and fictitious website reporting.

Antivirus on endpoints is not enough

On endpoints, it is important to have the latest versions of antivirus software installed. Deploy and use a comprehensive endpoint security product that includes additional layers of protection including:

- Endpoint intrusion prevention that protects unpatched vulnerabilities from being exploited, protects against social engineering attacks, and stops malware from reaching endpoints;
- Browser protection for avoiding obfuscated web-based attacks;
- File and web-based reputation solutions that provide a risk-and-reputation rating of any application and website to prevent rapidly mutating and polymorphic malware;
- Behavioral prevention capabilities that look at the behavior of applications and prevent malware;
- Application control settings that can prevent applications and browser plug-ins from downloading unauthorized malicious content;
- Device control settings that prevent and limit the types of USB devices to be used.

Secure your websites against MITM attacks and malware infection

Avoid compromising your trusted relationship with your customers by:

- Implementing Always On SSL (SSL protection on your website from logon to logoff);
- Scanning your website daily for malware;
- Setting the secure flag for all session cookies;
- Regularly assessing your website for any vulnerabilities (in 2013 1 in 8 websites scanned by Symantec was found to have vulnerabilities);
- Choosing SSL Certificates with Extended Validation to display the green browser address bar to website users;
- Displaying recognized trust marks in highly visible locations on your website to show customers your commitment to their security.

Protect your private keys

Make sure to get your digital certificates from an established, trustworthy certificate authority that demonstrates excellent security practices. Symantec recommends that organizations:

- Use separate Test Signing and Release Signing infrastructures;
- Secure keys in secure, tamper-proof, cryptographic hardware devices;
- Implement physical security to protect your assets from theft.

Use encryption to protect sensitive data

Implement and enforce a security policy whereby any sensitive data is encrypted. Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution. Ensure that customer data is encrypted as well. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization. Use Data Loss Prevention to help prevent data breaches: Implement a DLP solution that can discover where sensitive data resides, monitor its use, and protect it from loss. Data loss prevention should be implemented to monitor the flow of information as it leaves the organization over the network, and monitor traffic to external devices or websites.

Best Practice Guidelines for Businesses

- DLP should be configured to identify and block suspicious copying or downloading of sensitive data;
- DLP should also be used to identify confidential or sensitive data assets on network file systems and computers.

Ensure all devices allowed on company networks have adequate security protections

If a bring your own device (BYOD) policy is in place, ensure a minimal security profile is established for any devices that are allowed access to the network.

Implement a removable media policy

Where practical, restrict unauthorized devices such as external portable hard-drives and other removable media. Such devices can both introduce malware and facilitate intellectual property breaches, whether intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.

Be aggressive in your updating and patching

Update, patch, and migrate from outdated and insecure browsers, applications, and browser plug-ins. This also applies to operating systems, not just across computers, but mobile, ICS, and IoT devices as well. Keep virus and intrusion prevention definitions at the latest available versions using vendors' automatic update mechanisms. Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.

Enforce an effective password policy

Ensure passwords are strong; at least 8-10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple websites and sharing of passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days.

Ensure regular backups are available

Create and maintain regular backups of critical systems, as well as endpoints. In the event of a security or data emergency, backups should be easily accessible to minimize downtime of services and employee productivity.

Restrict email attachments

Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments. Ensure that mail servers are adequately protected by security software and that email is thoroughly scanned.

Ensure that you have infection and incident response procedures in place

- Keep your security vendor contact information handy, know who you will call, and what steps you will take if you have one or more infected systems;
- Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss;
- Make use of post-infection detection capabilities from web gateway, endpoint security solutions and firewalls to identify infected systems;
- Isolate infected computers to prevent the risk of further infection within the organization, and restore using trusted backup media;
- If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied.

Educate users on basic security protocols

- Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless the download has been scanned for viruses;
- Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends;

- Deploy web browser URL reputation plug-in solutions that display the reputation of websites from searches;
- Only download software (if allowed) from corporate shares or directly from the vendor website;
- If Windows users see a warning indicating that they are "infected" after clicking on a URL or using a search engine (fake antivirus infections), educate users to close or quit the browser using Alt-F4, CTRL+W or the task manager.

Building Security into devices

- The diverse nature of ICS and IoT platforms make host-based IDS and IPS, with customizable rulesets and policies that are unique to a platform and application, suitable solutions. However, manufacturers of ICS and IoT devices are largely responsible for ensuring that security is built into the devices before shipping. Building security directly into the software and applications that run on the ICS and IoT devices would prevent many attacks that manage to side-step defenses at the upper layers. Manufacturers should adopt and integrate such principles into their software development process.

20 Critical Security Controls

Overview

The Council on Cybersecurity 20 Critical Security Controls is a prioritized list designed to provide maximum benefits toward improving risk posture against real-world threats. This list of 20 control areas grew out of an international consortium of U.S. and international agencies and experts, sharing from actual incidents and helping to keep it current against evolving global cybersecurity threats.

Many organizations face the challenges and increasing threats to their cybersecurity by strategically choosing a security controls framework as a reference for initiating, implementing, measuring and evaluating their security posture, and managing risk. Over the years, many security control frameworks have been developed (e.g. NIST), with the common goal of offering combined knowledge and proven guidance for protecting critical assets, infrastructure and information. Based on the information we have today about attacks and threats, what are the most important steps that enterprises should take now, to secure systems and data?

The Critical Security Controls are designed to provide organizations the information necessary to increase their security posture in a consistent and ongoing fashion. The Controls are a relatively small number of prioritized, well-vetted, and supported set of security actions that organizations can take to assess and improve their current security state.

To implement the Controls you must understand what is critical to your business, data, systems, networks, and infrastructures, and you must consider the adversary actions that could impact your ability to be successful in the business or operations.

Top 5 Priorities

We emphasize the use of the first five Controls for every organization. This helps establish a foundation of security and has the most immediate impact on preventing attacks. From this foundation organizations can apply other Controls as they meet the business need of the organization.

In the following pages you will see a table that outlines the areas identified in the ISTR and ties them to Critical Security Controls:

01

Inventory of Authorized and Unauthorized Devices

Reduce the ability of attackers to find and exploit unauthorized and unprotected systems: Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices.

02

Inventory of Authorized and Unauthorized Software

Identify vulnerable or malicious software to mitigate or root out attacks: Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.

03

Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers

Prevent attackers from exploiting services and settings that allow easy access through networks and browsers: Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.

04

Continuous Vulnerability Assessment and Remediation

Proactively identify and repair software vulnerabilities reported by security researchers or vendors: Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.

05

Malware Defense

Block malicious code from tampering with system settings or content, capturing sensitive data, or from spreading: Use automated antivirus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis.

Critical Control Protection Priorities

	HARDEN DEFENSES	ENHANCE DETECTION	REDUCE IMPACT
INTERNET OF THINGS	04 05 06 07	01 09 10 11 14 18	12 13 17 19
MOBILE THREATS	02 03 04 05 06 07	01 10	08 17
PROTECT WEB SERVERS	02 03 04 05 06 10 11	01 14 16 18 20	08 12 17 13
WEB-BASED ATTACKS	02 03 04 05 06	01 14 16	12 13 15 17
SPAM & PHISHING	02 05	01 09 20	12 13
TARGETED ATTACKS	02 03 04 05 06 11	01 14 16 18 20	12 13 15 17
DATA BREACHES	02 03 04 05 06 10 11 07	01 14 16 09 18 20	08 12 17 13 15 19
MALWARE THREATS	02 03 04 05	01 14 16 09 18 20	08 12 17 13
BOTS	02 03 04 05	01 14 18	17 13 19

Critical Controls

01

Inventory of Authorized and Unauthorized Devices

Reduce the ability of attackers to find and exploit unauthorized and unprotected systems: Use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices.

02

Inventory of Authorized and Unauthorized Software

Identify vulnerable or malicious software to mitigate or root out attacks: Devise a list of authorized software for each type of system, and deploy tools to track software installed (including type, version, and patches) and monitor for unauthorized or unnecessary software.

03

Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers

Prevent attackers from exploiting services and settings that allow easy access through networks and browsers: Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.

04

Continuous Vulnerability Assessment and Remediation

Proactively identify and repair software vulnerabilities reported by security researchers or vendors: Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.

05

Malware Defense

Block malicious code from tampering with system settings or content, capturing sensitive data, or from spreading: Use automated antivirus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media.

06

Application Software Security

Neutralize vulnerabilities in web-based and other application software: Carefully test internally-developed and third-party application software for security flaws, including coding errors and malware. Deploy web application firewalls that inspect all traffic, and explicitly check for errors in all user input (including by size and data type).

07

Wireless Device Control

Protect the security perimeter against unauthorized wireless access: Allow wireless devices to connect to the network only if they match an authorized configuration and security profile and have a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points.

08

Data Recovery Capability

Minimize the damage from an attack: Implement a trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more frequently. Regularly test the restoration process.

09

Security Skills Assessment and Appropriate Training to Fill Gaps

Find knowledge gaps, and eradicate them with exercises and training: Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.

10

Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Preclude electronic holes from forming at connection points with the Internet, other organizations, and internal network segments: Compare firewall, router, and switch configurations against standards for each type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates.

Critical Controls

11

Limitation and Control of Network Ports, Protocols, and Services

Allow remote access only to legitimate users and services: Apply host-based firewalls, port-filtering, and scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file and print services, and domain name system (DNS) servers to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.

12

Controlled Use of Administrative Privileges

Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open a malicious email, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.

13

Boundary Defense

Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines: Establish a multi-layered boundary defense by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks ("extranets").

14

Maintenance, Monitoring, and Analysis of Security Audit Logs

Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed, and activity on victim machines: Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run bi-weekly reports to identify and document anomalies.

15

Controlled Access Based on the Need to Know

Prevent attackers from gaining access to highly sensitive data: Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to nonpublic data and files.

16

Account Monitoring and Control

Keep attackers from impersonating legitimate users: Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees or contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.

17

Data Loss Prevention

Stop unauthorized transfer of sensitive data through network attacks and physical theft: Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize exposure to attackers. Monitor people, processes, and systems, using a centralized management framework.

18

Incident Response Management

Protect the organization's reputation, as well as its information: Develop an incident response plan with clearly delineated roles and responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

19

Secure Network Engineering

Keep poor network design from enabling attackers: Use a robust, secure network engineering process to prevent security controls from being circumvented. Deploy a network architecture with at least three tiers: DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks.

20

Penetration Tests and Red Team Exercises

Use simulated attacks to improve organizational readiness: Conduct regular internal and external penetration tests that mimic an attack to identify vulnerabilities and gauge the potential damage. Use periodic red team exercises—all-out attempts to gain access to critical data and systems to test existing defense and response capabilities.

Best Practice Guidelines for Consumers

Protect Yourself

Use a modern Internet security solution that includes the following capabilities for maximum protection against malicious code and other threats:

- Antivirus (file- and heuristic-based) and behavioral malware prevention can prevent unknown malicious threats from executing;
- Bi-directional firewalls will block malware from exploiting potentially vulnerable applications and services running on your computer;
- Browser protection to protect against obfuscated web-based attacks;
- Use reputation-based tools that check the reputation and trust of a file and website before downloading, and that check URL reputations and provide safety ratings for websites found through search engines;
- Consider options for implementing cross-platform parental controls, such as Norton Online Family.[142]

Update Regularly

Keep your system, program, and virus definitions up-to-date – always accept updates requested by the vendor. Running out-of-date versions can put you at risk from being exploited by web-based attacks. Only download updates from vendor sites directly. Select automatic updates wherever possible.

Be Wary of Scareware Tactics

Versions of software that claim to be free, cracked or pirated can expose you to malware, or social engineering attacks that attempt to trick you into thinking your computer is infected and getting you to pay money to have it removed.

Use an Effective Password Policy

Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary. Do not use the same password for multiple applications or websites. Use complex passwords (upper/lowercase and punctuation) or passphrases.

Think Before You Click

Never view, open, or copy email attachments to your desktop or execute any email attachment unless you expect it and trust the sender. Even when receiving email attachments from trusted users, be suspicious.

- Be cautious when clicking on URLs in emails or social media communications, even when coming from trusted sources and friends. Do not blindly click on shortened URLs without expanding them first using a preview tool or plug-in.
- Use a web browser plug-in or URL reputation site that shows the reputation and safety rating of websites before visiting. Be suspicious of search engine results; only click through to trusted sources when conducting searches, especially on topics that are hot in the media.
- Be suspicious of warnings that pop up asking you to install media players, document viewers and security updates. Only download software directly from the vendor's website.
- Be aware of files you make available for sharing on public sites, including gaming, bitTorrent, and any other peer-to-peer (P2P)exchanges. Keep Dropbox, Evernote, and other usages to a minimum for pertinent information only.

Guard Your Personal Data

Limit the amount of personal information you make publicly available on the Internet (in particular via social networks). This includes personal and financial information, such as bank logins or birth dates.

- Review your bank, credit card, and credit information frequently for irregular activity. Avoid banking or shopping online from public computers (such as libraries, Internet cafes, and similar establishments) or from unencrypted Wi-Fi connections.
- Use HTTPS when connecting via Wi-Fi networks to your email, social media and sharing websites. Check the settings and preferences of the applications and websites you are using.
- Look for the green browser address bar, HTTPS, and recognizable trust marks when you visit websites where you log in or share any personal information.
- Configure your home Wi-Fi network for strong authentication and always require a unique password for access to it.

Best Practice Guidelines for Website Owners

Despite this year's vulnerabilities, when it comes to protecting your website visitors and the information they share with you, SSL and TLS remain the gold standard.

In fact, due to the publicity that Heartbleed received, more companies than ever have started hiring SSL developers to work on fixes and code. This has focused more eyes on the SSL libraries and common good practices in implementation.

Get Stronger SSL

SSL certificate algorithms become stronger than ever in 2014. Symantec, along with several other CAs, has moved to SHA-2 as default and is winding down support for 1024-bit roots.[143] Microsoft and Google announced SHA-1 deprecation plans that may affect websites with SHA-1 certificates expiring as early as January 1, 2016.[144] In other words, if you haven't migrated to SHA-2, visitors using Chrome to access your site will likely see a security warning and as of January 1, 2017, your certificates just won't work for visitors using Internet Explorer.

Symantec is also advancing the use of the ECC algorithm—a much stronger alternative to RSA. All major browsers, even mobile, support ECC certificates on all the latest platforms, and there are three main benefits to using it:

1. Improved Security

Compared to an industry-standard RSA-2048 key, ECC-256 keys are 10,000 times harder to crack.[145] In other words, it would take a lot more computing power and a lot longer for a brute-force attack to crack this algorithm.

2. Better Performance

Website owners used to worry that implementing SSL certificates would slow their sites. This led to many sites' having only partial-on SSL, which creates serious vulnerabilities. ECC requires much less processing power on the website than does RSA and can handle more users and more connections simultaneously. This makes the implementation of always-on SSL not only sensible but viable too.

3. Perfect Forward Secrecy (PFS)

Although PFS is an option with RSA-based and ECC-based certificates, performance is much better with ECC-based certificates. Why does that matter? Without PFS, if hackers got hold of your private keys, they could retrospectively decrypt any and all data they captured. Considering the Heartbleed vulnerability made this a very real possibility for so many websites, this is a problem. With PFS, however, if hackers crack or get hold of your SSL certificate private keys, they can decrypt only information protected with those keys—not historical data—from that point on.

Use SSL Correctly. As we realized in 2014, SSL is only as good as its implementation and maintenance. So be sure to:

Implement Always-On SSL. Use SSL certificates to protect every page of your website so that every interaction a visitor has with your site is authenticated and encrypted.

Keep Servers Up to Date. This applies beyond server SSL libraries: any patches or updates should be installed as soon as possible. They're released for a reason: to reduce or eliminate a vulnerability.

Display Recognized Trust Marks. (such as the Norton Secured Seal) in highly visible locations on your website to show customers your commitment to their security.

Scan Regularly. Keep an eye on your web servers and watch for vulnerabilities or malware.

Keep Server Configuration Up to Date. Make sure that old, unsecure versions of the SSL protocol (SSL2 and SSL3) are disabled, and newer versions of the TLS protocol (TLS1.1 and TLS1.2) are enabled and prioritized. Use tools like Symantec's SSL Toolbox to verify proper server configuration.[146]

Educate Employees

Basic common sense and the introduction of some good security habits can go a long way toward keeping sites and servers safe this year:

- Ensure employees don't open attachments from senders they don't know.
- Educate them on safe social media conduct: offers that look too good probably aren't legitimate; hot topics are prime bait for scams; not all links lead to real login pages.
- Encourage them to adopt two-step authentication on any website or app that offers it.
- Ensure they have different passwords for every email account, application, and login—especially for work-related sites and services.
- Remind then to use common sense—having antivirus software doesn't mean it's OK to go on malicious or questionable websites.

Get Safe or Get Shamed

Attackers have become more aggressive, more sophisticated, and more ruthless than ever in their attempts to exploit the Internet for ill gains. There is, however, plenty that individuals and organizations can do to limit attackers' impact.

SSL and website security are now in the public consciousness, and if you're not doing your part you could find yourself being publicly shamed on HTTP Shaming, a site set up by software engineer Tony Webster.[147]

When it comes to businesses and their websites, good security processes and implementations are all that stand in the way of total financial and reputational ruin. So get secure in 2015 with Symantec.

Footnotes

01 http://www.symantec.com/security_response/writeup.jsp?docid=2004-061419-4412-99

02 http://www.symantec.com/connect/blogs/tenth-anniversary-mobile-malware

03 http://www.symantec.com/connect/blogs/grayware-casting-shadow-over-mobile-software-marketplace

04 http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/

05 http://www.symantec.com/connect/blogs/future-mobile-malware

06 Ibid

07 http://www.symantec.com/connect/blogs/simplocker-first-confirmed-file-encrypting-ransomware-android

08 https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-michalevsky.pdf

09 http://www.slideshare.net/symantec/norton-mobile-apps-survey-report

10 https://www.cs.cmu.edu/~coke/history_long.txt

11 PayPal has a Buyer and Seller Protection Program to help protect against scams like this. For more information, see the following link. https://www.paypal.com/webapps/mpp/paypal-safety-and-security

12 Garter, Market Trends: Enter the Wearable Electronics Market With Products for the Quantified Self, Angela McIntyre and Jessica Ekholm, 01 July 2013

13 https://securityledger.com/2013/05/fitbitten-researchers-exploit-health-monitor-to-earn-workout-rewards/

14 http://www.symantec.com/connect/blogs/how-safe-your-quantified-self-tracking-monitoring-and-wearable-tech

15 http://www.cnn.com/2014/05/19/justice/us-global-hacker-crackdown/

16 http://www.symantec.com/connect/blogs/creepware-who-s-watching-you

17 http://www.wired.com/2014/08/car-hacking-chart/

18 http://www.bbc.co.uk/news/technology-23443215

19 http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/

20 http://www.cbsnews.com/news/car-hacked-on-60-minutes/

21 http://en.wikipedia.org/wiki/Picocell

22 http://en.wikipedia.org/wiki/Home_Node_B

23 http://www.autosec.org/pubs/cars-usenixsec2011.pdf

24 https://www.synology.com/en-us/company/news/article/Synology_Encourages_Users_to_Update_as_SynoLocker_Ransomware_Affects_Older_DSM_Versions/Synology%C2%AE%20Encourages%20Users%20to%20Update%20as%20SynoLocker%20Ransomware%20Affects%20Older%20DSM%20Versions

25 http://www.symantec.com/security_response/writeup.jsp?docid=2013-112710-1612-99

26 http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices

27 http://www.symantec.com/connect/blogs/iot-worm-used-mine-cryptocurrency

28 http://www.symantec.com/connect/blogs/internet-things-new-threats-emerge-connected-world

29 http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/

30 "A Heart Device Is Found Vulnerable to Hacker Attacks"; New York Times; Mar. 2008; http://www.nytimes.com/2008/03/12/business/12heart-web.html?_r=0

31 https://www.gartner.com/doc/2537715/market-trends-enter-wearable-electronics

32 U.S. Department of Homeland Security, Industrial Control System Cyber Emergency Response Team, (ICS-CERT); ALERT-13-164-01; https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01

33 U.S. "Yes, terrorists could have hacked Dick Cheney's heart"; The Washington Post; Oct. 21, 2013; http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/

34 "Feds Probe Cybersecurity Dangers in Medical Devices"; IEEE Spectrum; Oct. 27, 2014; http://spectrum.ieee.org/tech-talk/biomedical/devices/feds-probe-cybersecurity-dangers-in-medical-devices

35 "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain"; U.S. Federal Bureau of Investigation (FBI) Cyber Division, Private Industry Notice #140408-009; April 8, 2014

36 "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff"; U.S. Food and Drug Administration, Center for Devices and Radiological Health (FDA CDRH); October 2, 2014; http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

37 "Medical-device security isn't tracked well, research shows"; Network World; July 19, 2012; http://www.networkworld.com/article/2189998/data-center/medical-device-security-isn-t-tracked-well--research-shows.html

38 http://www.symantec.com/connect/blogs/freak-vulnerability-can-leave-encrypted-communications-open-attack

39 Ibid

40 http://www.symantec.com/connect/blogs/heartbleed-bug-poses-serious-threat-unpatched-servers

41 http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html

42 http://www.symantec.com/connect/blogs/heartbleed-reports-field

43 For those unfamiliar with UNIX terminology, a shell is a command line user interface for interacting with the operating system. In this case, Bash is one of the most widely used shells in all of the UNIX and Linux worlds.

44 http://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability

45 http://www.symantec.com/connect/blogs/poodle-vulnerability-old-version-ssl-represents-new-threat

46 http://www.wired.com/2013/03/att-hacker-gets-3-years

47 http://www.symantec.com/connect/blogs/massive-malvertising-campaign-leads-browser-locking-ransomware
48 Ibid
49 http://www.symantec.com/connect/blogs/denial-service-attacks-short-strong
50 Ibid
51 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf
52 http://www.symantec.com/connect/blogs/robin-williams-goodbye-video-used-lure-social-media-scams
53 http://blog.instagram.com/post/104847837897/141210-300million
54 https://investor.twitterinc.com/releasedetail.cfm?ReleaseID=878170
55 http://www.slideshare.net/symantec/norton-mobile-apps-survey-report
56 http://www.symantec.com/connect/blogs/instagram-scam-lottery-winners-impersonated-offer-money-followers
57 http://www.symantec.com/connect/blogs/hacked-snapchat-accounts-use-native-chat-feature-spread-diet-pill-spam
58 http://www.symantec.com/connect/blogs/instagram-scam-lottery-winners-impersonated-offer-money-followers
59 http://www.symantec.com/connect/blogs/tinder-spam-year-later-spammers-still-flirting-mobile-dating-app
60 http://www.symantec.com/connect/blogs/adult-webcam-spam-all-roads-lead-kik-messenger
61 http://www.symantec.com/connect/blogs/tinder-spam-year-later-spammers-still-flirting-mobile-dating-app
62 Ibid
63 http://www.symantec.com/connect/blogs/facebook-scam-leads-nuclear-exploit-kit
64 http://www.wired.com/2014/02/can-anonymous-apps-give-rise-authentic-internet/
65 http://www.technologyreview.com/review/531211/confessional-in-the-palm-of-your-hand/
66 See many issues highlighted on See many issues highlighted on http://en.wikipedia.org/wiki/4chan
67 https://www.facebook.com/about/government_requests
68 http://thenextweb.com/twitter/2014/04/30/twitter-ceo-dick-costolo-whisper-mode-encourage-friends-privately-discuss-public-conversations/
69 http://techcrunch.com/2014/03/20/gmail-traffic-between-google-servers-now-encrypted-to-thwart-nsa-snooping/
70 http://www.symantec.com/connect/blogs/apple-ids-targeted-kelihos-botnet-phishing-campaign
71 http://www.symantec.com/connect/blogs/linkedin-alert-scammers-use-security-update-phish-credentials
72 http://www.symantec.com/connect/blogs/apple-ids-targeted-kelihos-botnet-phishing-campaign
73 http://www.symantec.com/connect/blogs/fresh-phish-served-helping-aes
74 http://www.symantec.com/connect/blogs/scammers-pose-company-execs-wire-transfer-spam-campaign
75 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf
76 Ibid
77 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf
78 http://www.symantec.com/en/uk/outbreak/?id=regin
79 http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats
80 Ibid
81 http://www.symantec.com/connect/blogs/equation-advanced-cyberespionage-group-has-all-tricks-book-and-more
82 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf
83 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
84 http://en.wikipedia.org/wiki/OLE_for_Process_Control
85 http://www.symantec.com/connect/blogs/emerging-threat-ms-ie-10-zero-day-cve-2014-0322-use-after-free-remote-code-execution-vulnerabi
86 http://www.symantec.com/connect/blogs/zero-day-internet-vulnerability-let-loose-wild
87 http://www.symantec.com/connect/blogs/sandworm-windows-zero-day-vulnerability-being-actively-exploited-targeted-attacks
88 http://www.symantec.com/connect/blogs/how-elderwood-platform-fueling-2014-s-zero-day-attacks
89 http://www.symantec.com/deepsight-products/
90 http://www.symantec.com/security_response/writeup.jsp?docid=2013-052817-2105-99
91 http://www.insurancejournal.com/news/west/2014/03/07/322748.htm
92 http://www.ponemon.org/news-2/7
93 https://www.apple.com/uk/pr/library/2014/09/02Apple-Media-Advisory.html
94 http://securityresponse.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/attacks_on_point_of_sale_systems.pdf
95 http://www.symantec.com/connect/blogs/demystifying-point-sale-malware-and-attacks
96 http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf
97 “Illinois hospital reports data blackmail”; PC World; Dec. 15, 2014; http://www.pcworld.com/article/2859952/illinois-hospital-reports-data-blackmail.html
98 “Medical identity theft proves lucrative in myriad ways”; Fierce Health IT; Oct. 21, 2014; http://www.fiercehealthit.com/story/medical-identify-theft-proves-lucrative-myriad-ways/2014-10-21?utm_medium=nl&utm_source=internal
99 “The Growing Threat of Medical Identity Fraud: A Call to Action”; Medical Identity Fraud Alliance (MIFA); July 2013; http://medidfraud.org/wp-content/uploads/2013/07/MIFA-Growing-Threat-07232013.pdf

100 "Your medical record is worth more to hackers than your credit card"; Reuters; Sept. 24, 2014; http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

101 "Stolen EHR Charts Sell for $50 Each on Black Market"; MedScape; April 18, 2014; http://www.medscape.com/viewarticle/824192

102 http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services

103 Ibid

104 Ibid

105 Ibid

106 http://en.wikipedia.org/wiki/Blackhole_exploit_kit

107 http://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/

108 http://www.symantec.com/connect/blogs/snifula-banking-trojan-back-target-japanese-regional-financial-institutions

109 http://www.symantec.com/connect/blogs/simple-njrat-fuels-nascent-middle-east-cybercrime-scene

110 http://www.symantec.com/connect/blogs/malicious-links-spammers-change-malware-delivery-tactics

111 http://www.symantec.com/connect/blogs/windows-8-not-immune-ransomware-0

112 http://www.symantec.com/connect/blogs/australians-increasingly-hit-global-tide-cryptomalware

113 http://www.symantec.com/security_response/writeup.jsp?docid=2013-091122-3112-99

114 http://www.symantec.com/security_response/writeup.jsp?docid=2014-032622-1552-99

115 http://www.symantec.com/security_response/writeup.jsp?docid=2014-061923-2824-99

116 Tor is a combination of software and an open network that protects users against traffic analysis and helps to preserve their anonymity and privacy online. While not inherently criminal, it also helps to protect the anonymity of criminals in this case.

117 http://www.symantec.com/connect/blogs/cryptodefense-cryptolocker-imitator-makes-over-34000-one-month

118 http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network

119 http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_report_on_rogue_security_software_exec_summary_20326021.en-us.pdf

120 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf

121 http://www.symantec.com/security_response/writeup.jsp?docid=2013-091122-3112-99

122 http://www.symantec.com/security_response/writeup.jsp?docid=2014-032622-1552-99

123 http://www.symantec.com/connect/blogs/cryptodefense-cryptolocker-imitator-makes-over-34000-one-month

124 http://www.secureworks.com/cyber-threat-intelligence/threats/cryptowall-ransomware/

125 http://www.symantec.com/security_response/writeup.jsp?docid=2014-050610-2450-99

126 http://www.symantec.com/security_response/writeup.jsp?docid=2011-051715-1513-99

127 http://www.symantec.com/connect/blogs/massive-malvertising-campaign-leads-browser-locking-ransomware

128 http://www.symantec.com/security_response/writeup.jsp?docid=2014-060610-5533-99

129 http://www.symantec.com/security_response/writeup.jsp?docid=2014-072317-1950-99

130 http://www.symantec.com/security_response/writeup.jsp?docid=2014-103005-2209-99

131 http://www.symantec.com/security_response/writeup.jsp?docid=2014-080708-1950-99

132 http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network

133 http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/

134 http://www.computerweekly.com/news/2240185424/Microsoft-partnership-takes-down-1000-cybercrime-botnets

135 http://www.computerweekly.com/news/2240215443/RSA-2014-Microsoft-and-partners-defend-botnet-disruption

136 http://www.thesafemac.com/iworm-method-of-infection-found/

137 http://www.symantec.com/connect/blogs/does-malware-still-detect-virtual-machines

138 Ibid

139 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/threats_to_virtual_environments.pdf

140 Ibid

141 http://www.informationweek.com/software/operating-systems/windows-xp-stayin-alive/d/d-id/1279065

142 For more information about Norton Online Family, please visit https://onlinefamily.norton.com/

143 http://www.symantec.com/page.jsp?id=1024-bit-certificate-support

144 http://www.symantec.com/en/uk/page.jsp?id=sha2-transition

145 http://www.symantec.com/connect/blogs/introducing-algorithm-agility-ecc-and-dsa

146 https://ssltools.websecurity.symantec.com/checker/views/certCheck.jsp

147 http://arstechnica.com/security/2014/08/new-website-aims-to-shame-apps-with-lax-security/

Credits

Paul Wood, Executive Editor
Ben Nahorney, Editorial Content
Kavitha Chandrasekar, Analyst
Scott Wallace, Graphics & Design
Kevin Haley, Technical Advisor

Contributors

Alejandro Mosquera
Anand Kashyap
Axel Wirth
Bartlomiej Uscilowski
Candid Wueest
David Finn
Dylan Morss
Efrain Ortiz
Gavin O'Gorman
Kent McMullen
Lamine Aouad
Michael Klieman
Nicholas Johnston
Peter Coogan
Pierre-Antoine Vervier
Pravin Bange
Preeti Agarwal
Satnam Narang
Shankar Somasundaram
Slawomir Grzonkowski
Stephen Doherty
Tim Gallo
Vaughn Eisler

With Support From

Albert Cooley
Eric Chien
Gary Krall
Himanshu Dubey
Jason Theodorson
Kevin Thompson
Marianne Davis
Rick Andrews
William Wright

Special Thanks To

Alejandro Borgia
Anna Sampson
Camille Van Duyn
Charlie Treadwell
Cheryl Elliman
Darbi Booher
David Gantman
Fred Unterberger
Gerritt Hoekman
Gina Fiorentino
Jasmin Kohan
Jeff Scheel
Jennifer Duffourg
Jim Kunkle
Linda Smith Munyan
Mara Mort
Mary Verducci
Melissa Orr
Nisha Ramachandran
Piero DePaoli
Solange Deschatres

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenues of $6.7 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

More Information

- Symantec Worldwide: http://www.symantec.com/
- ISTR and Symantec Intelligence Resources: http://www.symantec.com/threatreport/
- Symantec Security Response: http://www.symantec.com/security_response/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/
- Norton Cybercrime Index: http://us.norton.com/cybercrimeindex/

Symantec Corporation World Headquarters

350 Ellis Street

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com

For specific country offices
and contact numbers,
please visit our website.
For product information in the U.S.,
call toll-free 1 (800) 745 6054.

04/15 21347926

APRIL 2015
VOLUME 20

Symantec

ISTR20

INTERNET SECURITY THREAT REPORT

APPENDICES

CHARTS & TABLES

APPENDIX A: THREAT ACTIVITY TRENDS

Appendix A: Threat Activity Trends

Threat Activity Trends

The following section of the Symantec Global Internet Security Threat Report provides an analysis of threat activity, data breaches, and web-based attacks, as well as other malicious actions that Symantec observed in 2014. The malicious actions discussed in this section also include phishing, malicious code, spam zombies, bot-infected computers, and attack origins. Attacks are defined as any malicious activity carried out over a network that has been detected by an intrusion detection system (IDS) or firewall. Definitions of the other types of malicious activities can be found in their respective sections within this report.

This section will discuss the following metrics, providing analysis and discussion of the trends indicated by the data:

- Malicious Activity by Source
- Malicious Web-Based Attack Prevalence
- Analysis of Malicious Web Activity by Attack Toolkits
- Analysis of Web-Based Spyware, Adware and Potentially Unwanted Programs
- Analysis of Web Policy Risks from Inappropriate Use
- Analysis of Website Categories Exploited to Deliver Malicious Code
- Bot-Infected Computers
- Analysis of Mobile Threats
- Data Breaches and Identity Theft

Malicious Activity by Source

Background

- Malicious activity usually affects computers that are connected to high-speed broadband Internet, because these connections are attractive targets for attackers. Broadband connections provide larger bandwidth capacities than do other connection types, plus faster speeds, the potential for constantly connected systems, and typically a more stable connection. Symantec categorizes malicious activities as follows:
- Malicious code: This includes programs such as viruses, worms, and Trojans that are covertly inserted into programs. The purposes of malicious code include destroying data, running destructive or intrusive programs, stealing sensitive information, and compromising the security or integrity of a victim's computer data.
- Spam zombies: These are remotely controlled, compromised systems specifically designed to send out large volumes of junk or unsolicited email messages. These email messages can be used to deliver malicious code and phishing attempts.
- Phishing hosts: Phishing hosts are computers that provide website services in order to illegally gather sensitive user information while pretending that the attempt is from a trusted, well-known organization by presenting a website designed to mimic the site of a legitimate business.
- Bot-infected computers: Malicious programs have been used to compromise computers to allow an attacker to control the targeted system remotely. Typically, a remote attacker controls a large number of compromised computers over a single reliable channel in a botnet, which can then be used to launch coordinated attacks.
- Network attack origins: These measure the originating sources of attacks from the Internet. For example, attacks can target SQL protocols or buffer overflow vulnerabilities.
- Web-based attack origins: These measure attack sources that are delivered via the web or through HTTP. Typically, legitimate websites are compromised and used to attack unsuspecting visitors.

Methodology

These metrics assess the sources from which the largest amount of malicious activity originates. To determine malicious activity by source, Symantec has compiled geographical data on numerous malicious activities, namely malicious code reports, spam zombies, phishing hosts, bot-infected computers, network attack origins, and web-based attack origins. The proportion of each activity originating from each source is then determined. The mean of the percentages of each malicious activity that originates in each source is calculated. This average determines the proportion of overall malicious activity that originates from the source in question, and rankings are determined by calculating the mean average of the proportion of these malicious activities that originated in each source.

Geography	2014 World Rank	2014 Overall Average	2013 World Rank	2013 Overall Average	Change
United States	1	20.7%	1	20.3%	0.4%
China	2	10.6%	2	9.4%	1.2%
India	3	4.0%	3	5.1%	-1.1%
Netherlands	4	3.6%	4	3.5%	0.1%
Germany	5	3.3%	5	3.3%	0.0%
Taiwan	6	2.6%	9	2.5%	0.1%
United Kingdom	7	2.6%	7	2.6%	0.0%
Russia	8	2.5%	6	2.6%	-0.1%
Vietnam	9	2.4%	12	2.2%	0.2%
Brazil	10	2.3%	8	2.5%	-0.2%

Malicious Activity by Source: Overall Rankings, 2013-2014

Source: Symantec

Geography	2014 Malicious Code Rank	2014 Malicious Code %	2013 Malicious Code Rank	2013 Malicious Code %	Change
United States	1	19.8%	1	16.9%	2.9%
India	2	12.2%	2	15.3%	-3.1%
China	3	6.5%	3	5.9%	0.6%
Japan	4	3.8%	5	3.4%	0.4%
United Kingdom	5	3.5%	7	2.8%	0.7%
Netherlands	6	3.3%	8	2.8%	0.5%
Indonesia	7	3.2%	4	4.0%	-0.8%
Australia	8	3.0%	11	2.1%	0.9%
Germany	9	2.9%	9	2.7%	0.2%
Vietnam	10	2.4%	6	2.8%	-0.4%

Malicious Activity by Source: Malicious Code, 2013-2014

Source: Symantec

Geography	2014 Spam Rank	2014 Spam %	2013 Spam Rank	2013 Spam %	Change
Vietnam	1	10.1%	7	5.0%	5.1%
Netherlands	2	8.0%	2	8.2%	-0.2%
Iran	3	6.2%	5	5.3%	0.9%
Russia	4	6.2%	3	6.6%	-0.4%
Germany	5	5.8%	13	2.6%	3.2%
India	6	5.8%	1	9.8%	-4.0%
Argentina	7	5.1%	11	3.1%	2.0%
Spain	8	4.1%	12	2.9%	1.2%
United States	9	3.9%	9	4.3%	-0.4%
Taiwan	10	3.6%	4	5.5%	-1.9%

Malicious Activity by Source: Spam Zombies, 2013-2014

Source: Symantec

Geography	2014 Phishing Hosts Rank	2014 Phishing Hosts %	2013 Phishing Hosts Rank	2013 Phishing Hosts %	Change
United States	1	46.6%	1	39.4%	7.2%
Germany	2	5.4%	2	6.5%	-1.1%
United Kingdom	3	3.9%	3	3.8%	0.1%
Netherlands	4	3.2%	6	2.5%	0.7%
France	5	3.2%	5	2.6%	0.6%
Hong Kong	6	3.1%	19	1.1%	2.0%
Canada	7	2.5%	4	2.8%	-0.3%
Russia	8	2.5%	7	2.5%	0.0%
China	9	2.2%	9	2.2%	0.0%
Croatia	10	2.2%	70	0.1%	2.1%

Malicious Activity by Source: Phishing Hosts, 2013-2014

Source: Symantec

Geography	2014 Bots Rank	2014 Bots %	2013 Bots Rank	2013 Bots %	Change
China	1	16.5%	2	9.1%	7.3%
United States	2	16.1%	1	20.0%	-3.9%
Taiwan	3	8.5%	4	6.0%	2.5%
Italy	4	5.5%	3	6.0%	-0.5%
Hungary	5	4.9%	7	4.2%	0.6%
Brazil	6	4.3%	5	5.7%	-1.4%
Japan	7	3.4%	6	4.3%	-0.8%
Germany	8	3.1%	8	4.2%	-1.0%
Canada	9	3.0%	10	3.5%	-0.5%
Poland	10	2.8%	12	3.0%	-0.2%

Malicious Activity by Source: Bots, 2013-2014

Source: Symantec

Geography	2014 Web Attacking Countries Rank	2014 Web Attacking Countries %	2013 Web Attacking Countries Rank	2013 Web Attacking Countries %	Change
United States	1	21.1%	1	26.2%	-5.1%
China	2	6.6%	2	7.4%	-0.8%
Costa Rica	3	6.6%	68	0.03%	6.6%
Japan	4	3.2%	6	1.4%	1.8%
Netherlands	5	2.3%	3	2.8%	-0.5%
India	6	1.1%	4	1.6%	-0.5%
Philippines	7	1.1%	12	0.9%	0.2%
Brazil	8	1.0%	10	0.9%	0.1%
Korea, South	9	0.8%	7	1.4%	-0.6%
Germany	10	0.8%	5	1.6%	-0.8%

Malicious Activity by Source: Web Attack Origins, 2013-2014

Source: Symantec

Geography	2014 Network Attacking Countries Rank	2014 Network Attacking Countries %	2013 Network Attacking Countries Rank	2013 Network Attacking Countries %	Change
China	1	28.7%	1	26.6%	2.1%
United States	2	16.6%	2	15.2%	1.4%
Netherlands	3	4.2%	3	3.9%	0.3%
Russia	4	3.2%	5	3.1%	0.1%
United Kingdom	5	3.0%	4	3.3%	-0.3%
France	6	2.6%	7	2.6%	0.0%
Korea, South	7	2.4%	15	1.8%	0.6%
India	8	2.4%	9	2.4%	0.0%
Australia	9	2.2%	11	2.0%	0.2%
Japan	10	2.1%	10	2.2%	-0.1%

Malicious Activity by Source: Network Attack Origins, 2013-2014

Source: Symantec

Commentary

- In 2014, the United States and China remained the top two sources overall for malicious activity. The overall average proportion of attacks originating from the United States in 2014 increased by 0.4 percentage point compared with 2013, while the same figure for China saw an increase by 1.2 percentage points compared with 2013. Countries ranking in the top 10 for 2013 continued to appear in the same range in 2014.
- The United States remains in first position as a source of all activities except for spam zombies, bots, and network attacks. Vietnam remains in first position for spam zombies, and China remains primary for bots and network attacks.
- Of all bot activity, 16.5 percent originated in China: China was the main source of bot-infected computers, an increase of 7.3 percentage points compared with 2013.
- Of all web-based attacks, 21.1 percent originated in the United States: Web-based attacks originating from the United States decreased by 5.1 percentage points in 2014.
- Of all network attacks, 28.7 percent originated in China: China has the largest population of Internet users not only in the Asia region but also globally, which attributes to the high rates of attacks.
- Of all phishing websites, 46.6 percent were hosted in the United States: The United States is the second largest population of Internet users in the world, which could be one of the reasons that it accounts for highest number of phishing websites.

- Of all spam zombies, 10.1 percent were located in Vietnam, an increase of 5.1 percentage points compared with 2013. The proportion of spam zombies located in the United States dipped by 0.4 percentage point to 3.9 percent, resulting in the United States being ranked in ninth position in 2014, the same as in 2013.
- Of all malicious code activities, 19.8 percent originated from the United States, an increase of 2.9 percentage points compared with 2013, giving the country the same ranking as in 2013. With 12.2 percent of malicious activity originating in India, the country was ranked in second position.

Malicious Web-Based Attack Prevalence

Background

The circumstances and implications of web-based attacks vary widely. Web-based attacks may target specific businesses or organizations, or they may be widespread attacks of opportunity that exploit current events, zero-day vulnerabilities, or recently patched and publicized vulnerabilities that many users have yet to protect themselves against. While major attacks may have individual importance and often receive significant attention when they occur, examining web-based attacks overall provides insight into the threat landscape and how attack patterns may be shifting. Analysis of the underlying trend can provide insight into potential shifts in web-based attack usage and can assist in determining whether attackers are more or less likely to employ these attacks in the future. To see which vulnerabilities are being exploited by web-based attacks, see Appendix D: Vulnerability Trends.

Methodology

This metric assesses changes to the prevalence of web-based attack activity by comparing the overall volume of malicious activity in each month during the current and previous reporting periods. The data is obtained from Symantec Endpoint Protection and Norton Network Threat Protection IPS Signature detections.

Month	2014	2013
January	779,337	674,293
February	364,110	539,069
March	534,089	491,713
April	530,227	463,152
May	379,156	697,823
June	346,572	756,068
July	558,450	799,486
August	537,762	702,893
September	387,889	637,823
October	427,094	135,451
November	534,822	483,999
December	561,513	442,298

Malicious Website Activity, 2013-2014

Source: Symantec

Commentary

- The average number of malicious websites blocked each day dipped by approximately 12.7 percent, from approximately 568,700 in 2013 to 496,700 in 2014.
- The highest level of activity was in January, with approximately 779,300 blocks per day.
- The lowest rate of malicious activity was 346,600 blocks per day in June 2014.
- Further analysis of malicious code activity may be found in Appendix B: Malicious Code Trends, “Top Malicious Code Families.”

Analysis of Malicious Web Activity by Attack Toolkits

Background

The increasing pervasiveness of web browser applications, along with increasingly common, easily exploited web browser application security vulnerabilities, has resulted in the widespread growth of web-based threats. Attackers wanting to take advantage of client-side vulnerabilities no longer need to actively compromise specific networks to gain access to those computers. Enterprises and consumers who visit mainstream websites hosting web attack toolkits are silently infected with a variety of malware. Symantec analyzes attack activity to determine which types of attacks and toolkits these predators are utilizing. This can provide insight into emerging web attack trends and may indicate the types of attacks with which attackers are having the most success.

Methodology

This metric assesses the top web-based attack activity grouped by exploit "web kit" families. These attacks originated from compromised legitimate sites and intentionally malicious sites set up to target Internet users in 2014. To determine this, Symantec ranked attack activity by the number of incidents associated with each toolkit.

Month	Sakura	Nuclear	Styx	OrangeKit	Blackhole	Others
January	9.48%	15.19%	25.09%	3.14%	10.08%	37.02%
February	14.43%	15.79%	21.85%	2.28%	8.23%	37.43%
March	21.48%	15.24%	4.77%	1.53%	5.01%	51.98%
April	12.76%	8.81%	5.27%	1.04%	4.42%	67.69%
May	16.45%	19.95%	6.22%	2.72%	5.60%	49.06%
June	28.04%	12.47%	9.14%	5.18%	8.14%	37.03%
July	34.21%	10.10%	3.45%	9.07%	5.35%	37.83%
August	38.86%	9.06%	1.71%	8.24%	4.70%	37.44%
September	29.38%	8.30%	1.89%	6.99%	2.54%	50.90%
October	37.85%	4.31%	2.73%	11.33%	1.65%	42.12%
November	19.31%	1.93%	1.44%	3.82%	1.03%	72.48%
December	19.72%	1.05%	2.03%	9.37%	3.36%	64.48%

Malicious Website Activity: Attack Toolkit Trends, 2014

Source: Symantec

Toolkit	% of Attacks
Sakura	22.76%
Nuclear	9.98%
Styx	7.23%
OrangeKit	5.27%
Blackhole	5.07%
Other	49.70%

Malicious Website Activity: Overall Frequency of Major Attack Toolkits, 2014

Source: Symantec

Commentary

- G01 Pack Exploit Kit virtually disappeared from the detections of web attack kits in 2014, though ranked first in 2013 with 23 percent of total attacks blocked. Sakura ranked first in 2014, with 23 percent of attacks blocked. The Nuclear toolkit that didn't appear in the top five in 2013 ranked second in 2014, with 10 percent.
- Blackhole has reappeared, ranking fifth in 2014.

Analysis of Web-Based Spyware, Adware and Potentially Unwanted Programs

Background

One of the main goals of a drive-by web-based installation is the deployment of malicious code, but often a compromised website is also used to install spyware or adware code. This is because the cybercriminals pushing the spyware and adware in this way are being paid a small fee for each installation. Most adware vendors, such as those providing add-in toolbars for web browsers, are not aware of how their code came to be installed on users' computers; the expectation is that it is with the permission of the end user, but this is typically not the case in a drive-by installation and may be in breach of the vendors' terms and conditions of use.

Methodology

This metric assesses the prevalence of web-based spyware and adware activity by tracking the trend in the average number of spyware- and adware-related websites blocked each day by users of Symantec.cloud web security services. Underlying trends observed in the sample data provide a reasonable representation of overall malicious web-based activity trends.

Rank	Spyware Name	Percent
1	Adware.Adpeak.E	23.6%
2	Application.SearchProtect.R	10.4%
3	Adware.Crossid	9.6%
4	Application.Downloader.SS	7.5%
5	Adware.Adpeak.C	6.5%
6	Adware.SwiftBrowse.E	3.5%
7	Application.SearchProtect.AD	2.9%
8	Adware.NewNextMe.A	2.5%
9	Adware.Multiplug.DH	2.4%
10	Adware.BrowseFox.U	2.4%

Potentially Unwanted Programs: Spyware and Adware Blocked, 2014

Source: Symantec.cloud

Commentary

- It is sometimes the case that "potentially unwanted programs" are legitimate programs that have been installed as part of a drive-by download and the installation is performed without the permission of the user. This is typically when the third party behind the installation is being rewarded for the number of installations of a particular program, irrespective of whether the user has granted permission. It is often without the knowledge of the original vendor and may be in breach of its affiliate terms and conditions.
- The most frequently blocked installation of potentially unwanted programs in 2014 was for the adware Adpeak.E.
- In 2014, seven of the top 10 potentially unwanted programs were classified as adware, compared with nine in 2013.
- In 2014, 31.6 percent of spyware and adware was detected using generic techniques, compared with 1.8 percent in 2013.

Analysis of Web Policy Risks from Inappropriate Use

Background

Many organizations implement an acceptable usage policy to limit employees' use of Internet resources to a subset of websites that have been approved for business use. This enables an organization to limit the level of risk that may arise from users' visiting inappropriate or unacceptable websites, such as those containing sexual images and other potentially illegal or harmful content. Often there will be varying degrees of granularity imposed on such restrictions, with some rules being applied to groups of users, while other rules may apply only at certain times of the day. For example, an organization may wish to limit employees' access to video-sharing websites to Friday lunchtime only but may also allow any member of the PR and marketing teams access at any time during the week. This enables an organization to implement and monitor its acceptable usage policy and reduce its exposure to certain risks that may also expose the organization to legal difficulties.

Methodology

This metric assesses the classification of prohibited websites blocked by users of Symantec. cloud web security services. The policies are applied by the organization from a default selection of rules that may also be refined and customized. This metric provides an indication of the potential risks that may arise from uncontrolled use of Internet resources.

Rank	Category	2014	2013	Change
1	Social Networking	37.4%	39.0%	-1.5%
2	Advertisement & Popups	23.8%	24.4%	-0.5%
3	Computing & Internet	4.6%	4.5%	0.1%
4	Streaming Media	4.0%	5.2%	-1.2%
5	Hacking	3.4%	0.0%	3.4%
6	Hosting Sites	3.1%	3.7%	-0.6%
7	Portal	2.5%	0.8%	1.7%
8	Chat	1.7%	2.9%	-1.2%
9	Search	1.2%	2.8%	-1.6%
10	Entertainment	1.2%	1.1%	0.1%

Web Policies That Triggered Blocks, 2013-2014

Source: Symantec.cloud

Commentary

- The most frequently blocked traffic was categorized as social networking, and it accounted for 37 percent of policy-based filtering activity that was blocked, equivalent to approximately one in every 2.5 websites blocked. Many organizations allow access to social networking websites but in some cases implement policies to permit access only at certain times of the day. This information is often used to address performance management issues, perhaps in the event of lost productivity due to social networking abuse.
- Twenty-four percent of web activity blocked through policy controls was related to advertisements and pop-ups. Web-based advertisements pose a potential risk through the use of "malvertisements," or malicious advertisements. These may occur as the result of a legitimate online ad provider's being compromised or a banner ad's being used to serve malware on an otherwise harmless website.
- Activity related to streaming media policies resulted in 4 percent of policy-based filtering blocks in 2014. Streaming media is increasingly popular when there are major sporting events or high-profile international news stories. This activity often results in an increased number of blocks, as businesses seek to preserve valuable bandwidth for other purposes. This figure was likely to have been higher in 2012 due to the staging of the Olympics in London.

Analysis of Website Categories Exploited to Deliver Malicious Code

Background

As organizations seek to implement appropriate levels of control in order to minimize risk levels from uncontrolled web access, it is important to understand the level of threat posed by certain classifications of websites and categories. This provides insight on the types of legitimate websites that may be more susceptible to being compromised and therefore could expose users to greater levels of risk.

Methodology

This metric assesses the classification of malicious websites blocked by users of Norton Safe Web[1] technology. Data is collected anonymously from customers voluntarily contributing to this technology, including through Norton Community Watch. Norton Safe Web is processing billions of rating requests each day and monitoring millions of daily software downloads.

This metric provides an indication of the levels of infection of legitimate websites that have been compromised or abused for malicious purposes. The malicious URLs identified by the Safe Web technology were classified by category using the Symantec RuleSpace[2] technology. RuleSpace proactively categorizes websites into nearly 100 categories in 30 languages.

Rank	Top 10 Most Frequently Exploited Categories of Websites	% of Total Number of Infected Websites
1	Technology	21.5%
2	Hosting	7.3%
3	Blogging	7.1%
4	Business	6.0%
5	Anonymizer	5.0%
6	Entertainment	2.6%
7	Shopping	2.5%
8	Illegal	2.4%
9	Placeholder	2.2%
10	Virtual Community	1.8%

Malicious Web Activity: Categories That Delivered Malicious Code, 2014

Source: Symantec

Rank	Top-10 Most Frequently Exploited Categories of Websites	Average Number of Threats Found on Infected Website	Top 3 Threat Types Detected		
1	Technology	1.4	Virus: 50%	Browser Exploit: 37%	Phish: 6%
2	Hosting	1.2	Browser Exploit: 52%	Virus: 34%	Phish: 9%
3	Blogging	1.4	Virus: 57%	Browser Exploit: 36%	Phish: 3%
4	Business	1.5	Browser Exploit: 68%	Phish: 17%	Virus: 8%
5	Anonymizer	6.5	Security Risk: 58%	Virus: 39%	Browser Exploit: 3%
6	Entertainment	1.8	Browser Exploit: 69%	Virus: 13%	Phish: 11%
7	Shopping	1.7	Browser Exploit: 60%	Virus: 17%	Phish: 14%
8	Illegal	2.1	Virus: 40%	Browser Exploit: 35%	Phish: 16%
9	Placeholder	2.1	Browser Exploit: 50%	Virus: 16%	Security Risk: 5%
10	Virtual Community	1.2	Virus: 89%	Browser Exploit: 9%	Phish: 1%

Malicious Web Activity: Malicious Code by Number of Infections per Site for Top-10 Most Frequently Exploited Categories, 2014

Source: Symantec.cloud

Commentary

- Of all malicious website activity, 21.5 percent was classified in the technology category.
- Websites classified as Anonymizers were found to host the greatest number of threats per site among all categories, with an average of 6.5 threats per website, the majority of which related to security risks (58 percent).
- The Illegal category includes sites that fall into the following subcategories: activist groups, cyberbullying, malware accomplice, password cracking, potentially malicious software and unwanted programs, remote access programs, and several other types of phishing- and spam-related content.
- The Placeholder category refers to any domain name that is registered but may be for sale or has recently expired and is redirected to a domain parking page.
- Anonymizers are sites that provide anonymous access to websites through a PHP or CGI proxy, allowing users to gain access to websites blocked by corporate and school proxies as well as parental control filtering solutions. Examples include:
  - Transparent proxy servers
  - Elite, disguised, distorting, and high-anonymity proxy servers
  - Websites explaining how to surf the web anonymously

Bot-Infected Computers

Background

Bot-infected computer programs, or bots, are programs that are covertly installed on a user's machine in order to allow an attacker to control the targeted system remotely through a communication channel, such as Internet Relay Chat (IRC), peer to peer (P2P), or Hypertext Transfer Protocol (HTTP). These channels allow the remote attacker to control a large number of compromised computers over a single, reliable channel in a botnet, which can then be used to launch coordinated attacks.

Bots allow for a wide range of functionality, and most can be updated to assume new functionality by downloading new code and features. Attackers can use bots to perform a variety of tasks, such as setting up denial-of-service attacks against an organization's website, distributing spam and phishing attacks, distributing spyware and adware, propagating malicious code, and harvesting confidential information from compromised computers that may be used in identity theft—all of which can lead to serious financial and legal consequences. Attackers favor bot-infected computers with a decentralized command and control model because they are difficult to disable and allow the attackers to hide in plain sight among the massive amounts of unrelated traffic occurring over the same communication channels, such as P2P. Most important, botnet operations can be lucrative for their controllers because bots are also inexpensive and relatively easy to propagate.

Methodology

A bot-infected computer is considered active on a given day if it carries out at least one attack on that day. This does not have to be continuous; a single such computer can be active on a number of different days. A distinct bot-infected computer is one that was active at least once during the period. The bot-infected computer activities that Symantec tracks can be classified as active attacker bots or bots that send out spam (that is, spam zombies).

Distributed denial-of-service (DDoS) campaigns may not always be indicative of bot-infected computer activity. DDoS activity can occur without the use of bot-infected computers. For example, the use of publicly available software such as Low Orbit Ion Cannon (LOIC), when used in a coordinated effort and in sufficiently large numbers, may disrupt some businesses' website operations.

The following analysis reveals the average life span of a bot-infected computer for the highest populations of bot-infected computers. To be included in the list, the geography must account for at least 0.1 percent of the global bot population.

Rank	Geography	Average Life Span of Bot (Days) - 2014	% of World Bots - 2014	Average Life Span of Bot (Days) - 2013	% of World Bots - 2013
1	Romania	23	0.2%	20	0.2%
2	United States	21	16.1%	13	20.0%
3	Indonesia	15	0.2%	15	0.1%
4	Pakistan	14	0.1%	15	0.1%
5	Iran	14	0.1%	9	0.1%
6	New Zealand	13	0.1%	10	0.2%
7	Israel	13	0.9%	8	1.0%
8	Bulgaria	13	0.2%	14	0.1%
9	Korea, South	13	1.2%	9	1.0%
10	Denmark	12	0.1%	7	0.2%

Top-10 Bot Locations by Average Lifespan of Bot, 2013-2014

Source: Symantec

Commentary

- Bots located in Romania were active for an average of 23 days in 2014, compared with 20 days in 2013; 0.2 percent of bots were located in Romania, compared with 0.19 percent in 2013.
- Although it still takes longer to identify and clean a bot-infected computer in Romania than it does in the United States, the number of infections in the United States is more than 100 times greater than that in Romania. One factor contributing to this disparity may be a low level of user awareness of the issues involved, combined with the lower availability of remediation guidance and support tools in the Romanian language.
- In the United States, which was home to 16 percent of the world's bots in 2014, the average life span of a bot was 21 days.
- All other countries outside the top 10 had bot life spans of 12 days or less. The overall global average bot life span was 7.5 days, slightly higher than in 2013, when it was six days.

Analysis of Mobile Threats

Background

Since the first smartphone arrived in the hands of consumers, speculation about threats targeting these devices has abounded. While threats targeted early "smart" devices such as those based on Symbian and Palm OS in the past, none of these threats ever became widespread and many remained proof of concept. Recently, with the growing uptake of smartphones and tablets and their increasing connectivity and capability, there has been a corresponding increase in attention, from both threat developers and security researchers.

While the number of immediate threats to mobile devices remains relatively low in comparison to threats targeting PCs, there have been new developments in the field, and as malicious code for mobile begins to generate revenue for malware authors, there will be more threats created for these devices, especially as people increasingly use mobile devices for sensitive transactions such as online shopping and banking.

As with desktop computers, the exploitation of a vulnerability can be a way for malicious code to be installed on a mobile device.

Methodology

In 2014, there was an increase in the number of vulnerabilities reported that affected mobile devices. Symantec documented 168 vulnerabilities in mobile device operating systems in 2014, compared with 127 in 2013 and 416 in 2012.

Symantec tracks the number of threats discovered against mobile platforms by tracking malicious threats identified by Symantec's own security products and confirmed vulnerabilities documented by mobile vendors.

Currently most malicious code for mobile devices consists of Trojans that pose as legitimate applications. These applications are uploaded to mobile application ("app") marketplaces in the hope that users will download and install them, often trying to pass themselves off as legitimate apps or games. Attackers have also taken popular legitimate applications and added supplementary code to them. Symantec has classified these threats into a variety of categories based on their functionality.

Month	2014	2013
January	3	4
February	2	1
March	4	7
April	2	5
May	3	4
June	4	9
July	4	8
August	2	2
September	3	7
October	5	4
November	8	2
December	6	4

Android Mobile Threats: Newly Discovered Malicious Code, 2013-2014

Source: Symantec

Month	2014	2013
January	46	53
February	60	133
March	41	107
April	80	44
May	53	78
June	40	56
July	7	20
August	7	107
September	25	36
October	204	48
November	22	93
December	3	33

Android Mobile Threats: Average Number of Malware Variants per Family, 2013–2014

Source: Symantec

Platform	Number of Threats	Percent of Threats
Android	45	94%
Symbian	0	0%
Windows	0	0%
iOS	3	6%

Mobile Threats: Malicious Code by Platform, 2014

Source: Symantec

High-level Risk Categories	Track User	Steal Information	Send Content	Traditional Threats	Reconfigure Device	Adware/ Annoyance
Percent of Actions Found in Threats (2014)	22%	21%	11%	26%	13%	7%
Percent of Actions Found in Threats (2013)	30%	23%	8%	20%	10%	9%

Mobile Threats: Malicious Code Actions in Malware, 2013-2014

Source: Symantec

Detailed Threat Categories	Percent Found in Threats, 2014	Percent Found in Threats, 2013
Steals Device Data	36%	17%
Spies On User	36%	28%
Sends Premium SMS	16%	5%
Downloader	18%	8%
Back door	18%	12%
Tracks Location	9%	3%
Modifies Settings	20%	8%
Spam	7%	3%
Steals Media	0%	3%
Elevates Privileges	7%	2%
Banking Trojan	7%	3%
SEO Poisoning	0%	0%
Adware/ Annoyance	13%	9%
DDOS Utility	0%	0%
Hacktool	0%	0%

Mobile Threats: Malicious Code Actions—Additional Detail, 2013-2014

Source: Symantec

Platform	Documented Vulnerabilities	Percent
Apple iOS/iPhone/iPad	140	84%
Android	19	11%
BlackBerry	7	4%
Windows Mobile	1	1%

Mobile Threats: Documented Mobile Vulnerabilities by Platform, 2014

Source: Symantec

Month	Documented Vulnerabilities
January	2
February	6
March	28
April	19
May	1
June	29
July	6
August	1
September	53
October	7
November	16
December	0

Mobile Threats: Documented Mobile Vulnerabilities by Month, 2014

Source: Symantec

The following are specific definitions of each subcategory:

- Steals device data—gathers information that is specific to the functionality of the device, such as International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), operating system, and phone configuration data
- Spies on user—intentionally gathers information from the device to monitor a user, such as phone logs and SMSs, and sends it to a remote source
- Sends premium SMSs—sends SMSs to premium-rate numbers that are charged to the user's mobile account
- Downloader—can download other risks onto the compromised device
- Back door—opens a back door on the compromised device, allowing attackers to perform arbitrary actions
- Tracks location—gathers GPS information from the device specifically to track the user's location
- Modifies settings—changes configuration settings on the compromised device
- Spam—sends spam email messages from the compromised device
- Steals media—sends media, such as pictures, to a remote source
- Elevates privileges—attempts to gain privileges beyond those laid out when installing the app bundled with the risk
- Banking Trojan—monitors the device for banking transactions, gathering sensitive details for further malicious actions
- SEO poisoning—periodically sends the phone's browser to predetermined URLs in order to boost search rankings

Apps with malicious intentions can present serious risks to users of mobile devices. These metrics show the different functions that these bad apps performed during the year. The data was compiled by analyzing the key functionality of malicious apps.

Symantec has identified five primary mobile risk types:

- Steal information—Most common among bad apps is the collection of data from the compromised device. This is typically done with the intent to carry out further malicious activities, in much the way an information-stealing Trojan might. This includes both device- and user-specific data, ranging from configuration data to banking details. This information can be used in a number of ways, but for the most part it is fairly innocuous, with IMEI and IMSI numbers taken by attackers as a way to uniquely identify a device. More concerning is data gathered about the device software, such as operating system (OS) version or applications installed, to carry out further attacks (say, by exploiting a software vulnerability). Rarer but of greatest concern is when user-specific data, such as banking details, is gathered in an attempt to make unauthorized transactions. While this category covers a broad range of data, the distinction between device and user data is given in more detail in the subcategories below.
- Track user—The next most common purpose is to track a user's personal behavior and actions. These apps take data specifically in order to spy on the individual using the phone. This is done by gathering up various communication data, such as SMSs and phone call logs, and sending it to another computer or device. In some instances they may even record phone calls. In other cases these apps track GPS coordinates, essentially keeping tabs on the location of the device (and its user) at any given time. Gathering pictures taken with the phone also falls into this category.

- Send content—The third largest in the group of risks is apps that send out content. These risks are different from the first two categories because their direct intent is to make money for the attacker. Most of these apps will send a text message to a premium SMS number, ultimately appearing on the mobile bill of the device's owner. Also within this category are apps that can be used as email spam relays, controlled by the attackers and sending unwanted emails from addresses registered to the device. Another example in this category is constantly sent HTTP requests in the hope of bumping up certain pages within search rankings.
- Traditional threats—The fourth group contains more traditional threats, such as back doors and downloaders. Attackers often port these types of apps from PCs to mobile devices.
- Change settings—Finally, there are a small number of apps that focus on making configuration changes. They attempt to elevate privileges or simply modify various settings within the OS. The goal for this final group seems to be to perform further actions on the compromised devices.

Commentary

- Forty-six new Android malware families were identified in 2014, compared with 57 in 2013.
- The average number of variants per family in 2014 was 48, compared with 57 in 2013. Similar to the overall number of new mobile malware families, the number of variants for each family is also lower in 2014 compared with the previous year.
- As we have seen in previous years, a high number of vulnerabilities for a mobile OS do not necessarily lead to malware that exploits those vulnerabilities. Overall, there were 168 mobile vulnerabilities published in 2014, compared with 127 in 2013, an increase of 32 percent.
- Further analysis of mobile malware and spyware indicated the most common type of activity undertaken on a compromised device was done to spy on the user, at 36 percent in 2014 compared with 28 percent in 2013. Thirty-six percent of malicious mobile activity was designed to steal data in 2014, compared with 17 percent in 2013.

Data Breaches and Identity Theft

Background

Hacking continued to be the primary cause of data breaches in 2014. In 2014, there were four data breaches that netted hackers 10 million or more identities, the largest of which was a massive breach of 145 million identities. Comparatively, there were eight breaches in 2013 of more than 10 million identities. As a result, the overall average number of identities exposed has decreased, from 2,181,891 identities per breach in 2013 to 1,116,767 in 2014.

As the overall average size of a breach has decreased, the median number of identities stolen has slightly increased, from 6,777 in 2013 to 7,000 in 2014. Using the median can be helpful in this scenario since it ignores the extreme values caused by the notable, rare events that resulted in the largest numbers of identities' being exposed. In this way, the median may be more representative of the underlying trend. While the number of incidents has increased, the number of identities exposed is still in the order of thousands, but there were fewer incidents that resulted in extremely large volumes of identities' being exposed in 2014 than in the previous year.

Hacking was the chief cause of most data breaches in 2014, and it consequently received a great deal of media attention. Hacking can undermine institutional confidence in a company, exposing its attitude toward security. The loss of personal data in a highly public way can result in damage to an organization's reputation. Hacking accounted for 49 percent of data breaches in 2014, according to Norton Cybercrime Index (CCI) data. As data breach notification legislation becomes more commonplace, we are likely to see the number of data breaches rise. Such legislation is often used to regulate the responsibilities of organizations after a data breach has occurred and may help mitigate against the potential negative impact on the individuals concerned.

The healthcare, retail, and education sectors were ranked highest for the number of data breach incidents in 2014; the top three accounted for 58 percent of all data breaches. However, the retail, computer software, and financial sectors accounted for 92 percent of all the identities exposed in 2014.

Methodology

The information analyzed regarding data breaches that could lead to identity theft is procured from the Norton CCI. The Norton CCI is a statistical model that measures daily the levels of threats, including malicious software, fraud, identity theft, spam, phishing, and social engineering. Data for the CCI is primarily derived from the Symantec Global Intelligence Network, one of the industry's most comprehensive sources of intelligence about online threats, along with certain other data from ID Analytics.[3] The data breach section of the Norton CCI is derived from data breaches that have been reported by legitimate media sources and have exposed personal information, including names, addresses, Social Security numbers, credit card numbers, and medical histories. Using publicly available data, the Norton CCI determines the sectors that were most often affected by data breaches and the most common causes of data loss.

The sector that experienced the loss, along with the cause of the loss that occurred, is determined through analysis of the organization reporting the loss and the method that facilitated the loss.

The data also reflects the severity of the breach by measuring the total number of identities exposed to attackers, using the same publicly available data. An identity is considered to be exposed if personal or financial data related to the identity is made available through the data breach. Data may include names, government-issued identification numbers, credit card information, home addresses, or email information. A data breach is considered deliberate when the

cause of the breach is due to hacking, insider intervention, or fraud. A data breach is considered to be caused by hacking if data related to identity theft is exposed by attackers' (external to an organization) gaining unauthorized access to computers or networks.

It should be noted that some sectors may need to comply with more stringent reporting requirements for data breaches than may others. For instance, government organizations are more likely to report data breaches, either due to regulatory obligations or in conjunction with publicly accessible audits and performance reports.[4] Conversely, organizations that rely on consumer confidence may be less inclined to report such breaches for fear of negative consumer, industry, or market reaction. As a result, sectors that are neither required nor encouraged to report data breaches may be underrepresented in this data set.

Date	Identities Exposed	Incidents
January	8,100,970	22
February	3,238,996	33
March	1,743,522	34
April	58,745,468	27
May	147,621,411	31
June	1,213,567	27
July	77,979,705	26
August	31,563,950	24
September	10,194,376	25
October	1,136,601	26
November	6,484,574	23
December	408,016	14

Timeline of Data Breaches Showing Identities Breached in 2014, Global

Source: Symantec

- There were 312 data breach incidents recorded by the Norton Cybercrime Index for 2014 and a total of 348 million identities exposed as a result.
- The average number of identities exposed per incident was 1,116,767, compared with 2,181,891 in 2013 (a decrease of more than 49 percent).
- The median number of identities exposed was 7,000, compared with 6,777 in 2013. The median is a useful measure, as it eliminates extreme values caused by the most notable incidents, which may not necessarily be typical.
- The number of incidents that resulted in 10 million or more identities' being exposed was four, compared with eight in 2013.

Rank	Sector	Number of Incidents	% of Incidents
1	Healthcare	116	37.2%
2	Retail	34	10.9%
3	Education	31	9.9%
4	Government and Public Sector	26	8.3%
5	Financial	19	6.1%
6	Computer Software	13	4.2%
7	Hospitality	12	3.8%
8	Insurance	11	3.5%
9	Transportation	9	2.9%
10	Arts and Media	6	1.9%

Top 10 Sectors Breached by Number of Incidents

Source: Symantec

Rank	Sector	Number of Identities Exposed	% of Identities Exposed
1	Retail	205,446,276	59.0%
2	Financial	79,465,597	22.8%
3	Computer Software	35,068,405	10.1%
4	Healthcare	7,230,517	2.1%
5	Government and Public Sector	7,127,263	2.0%
6	Social Networking	4,600,000	1.3%
7	Telecom	2,124,021	0.6%
8	Hospitality	1,818,600	0.5%
9	Education	1,359,190	0.4%
10	Arts and Media	1,082,690	0.3%

Top 10 Sectors Breached by Number of Identities Exposed

Source: Symantec

- Healthcare, retail, and education were ranked highest for the number of data breach incidents in 2014; the top three accounted for 58 percent of all data breaches.
- The retail, computer software, and financial sectors accounted for 92 percent of all the identities exposed in 2014.
- This highlights that sectors involved in the majority of data breaches don't necessarily result in the largest caches of stolen identities, with the exception of retail.

Cause of Breach	Average Identities per Incident
Administration and human resources	9,090
Agriculture	5,480
Community and non-profit	193,722
Computer hardware	52,876
Computer software	2,697,570
Education	43,845
Financial	4,182,400
Government	274,126
Healthcare	62,332
Hospitality	151,550
Insurance	13,240
Internet service provider	212,500
Retail	6,042,538
Social networking	1,533,333
Telecom	424,804
Transportation	91,671
Arts and media	180,448
Manufacturing	2,492
Business consulting	19,154
Architectural	52,660

Average Number of Identities Exposed per Data Breach by Notable Sector

Source: Symantec

- The highest average number of identities exposed per breach in 2014 was in the retail and financial sectors, with between 4 million and 6 million identities exposed in each breach, on average.
- The largest breach incident in 2014 occurred in the retail sector, with an incident resulting in 145 million identities' reportedly being exposed.

Cause of Breach	Number of Incidents	% of Incidents
Attackers	153	49.0%
Accidentally made public	67	21.5%
Theft or loss of computer or drive	66	21.2%
Insider theft	26	8.3%

Top Causes for Data Breaches by Number of Breaches

Source: Symantec

Cause of Breach	Number of Identities Exposed	% of Identities Exposed
Attackers	286,398,409	82.2%
Accidentally made public	60,019,573	17.2%
Theft or loss of computer or drive	1,049,498	0.3%
Insider theft	963,676	0.3%

Top Causes for Data Breaches by Number of Identities Exposed

Source: Symantec

Cause of Breach	Average Identities per Incident
Hackers	1,871,885
Accidentally made public	895,815
Theft or loss	15,901
Insider theft	37,064

Average Number of Identities Exposed per Data Breach, by Cause

Source: Symantec

- Hacking was the leading cause of reported identities exposed in 2014: Hackers were also responsible for the largest number of identities exposed, as well as for 49 percent of the incidents and 82 percent of the identities exposed in data breach incidents during 2014.
- The average number of identities exposed per data breach for hacking incidents was approximately 1.8 million.

Type of Information	Number of Incidents	% of Data Types
Real Names	215	68.9%
Gov ID numbers (Soc Sec)	140	44.9%
Home Address	134	42.9%
Financial Information	110	35.3%
Birth Dates	109	34.9%
Medical Records	105	33.7%
Phone Numbers	66	21.2%
Email Addresses	61	19.6%
User names & Passwords	40	12.8%
Insurance	35	11.2%
Driver's licenses	16	5.1%

Types of Personal Information Exposed in Data Breach Incidents

Source: Symantec

- The most common type of personal information exposed in data breaches during 2014 was real names, where 69 percent of the incidents in 2014 included this type of information's being exposed.
- Government ID numbers (including Social Security numbers) were identified in 45 percent of the identity breaches during 2014, compared with birth dates in 35 percent and user names and passwords in 13 percent.

APPENDIX B: MALICIOUS CODE TRENDS

Appendix B: Malicious Code Trends

Malicious Code Trends

Symantec collects malicious code information from our large global customer base through a series of opt-in anonymous telemetry programs, including Norton Community Watch, Symantec Digital Immune System, and Symantec Scan and Deliver technologies. Millions of devices, including client devices, servers, and gateway systems, actively contribute to these programs. New malicious code samples, as well as detection incidents from known malicious code types, are reported back to Symantec. These resources give Symantec's analysts unparalleled sources of data to identify, analyze, and provide informed commentary on emerging trends in malicious code activity in the threat landscape. Reported incidents are considered potential infections if infections could have occurred in the absence of security software to detect and eliminate threats.

Malicious code threats are classified into four main types—back doors, viruses, worms, and Trojans:

- Back doors allow an attacker to remotely access compromised computers.
- Viruses propagate by infecting existing files on affected computers with malicious code.
- Worms are malicious code threats that can replicate on infected computers or in a manner that facilitates their being copied to another computer (such as via USB storage devices).
- Trojans are malicious code that users unwittingly install onto their computers, most commonly through either opening email attachments or downloading from the Internet. Trojans are often downloaded and installed by other malicious code as well. Trojan horse programs differ from worms and viruses in that they do not propagate themselves.

Many malicious code threats have multiple features. For example, a back door will always be categorized in conjunction with another malicious code feature. Typically, back doors are also Trojans; however, many worms and viruses also incorporate back door functionality. In addition, many malicious code samples can be classified as both worms and viruses due to the way they propagate. One reason for this is that threat developers try to enable malicious code with multiple propagation vectors in order to increase their odds of successfully compromising computers in attacks.

The following malicious code trends were analyzed for 2014:

- Top Malicious Code Families
- Analysis of Malicious Code Activity by Geography, Industry Sector, and Company Size
- Propagation Mechanisms
- Targeted Attacks Intelligence: Going from Isolated Attacks to Coordinated Campaigns Orchestrated by Threat Actors

Top Malicious Code Families

Background

Symantec analyzes new and existing malicious code families to determine attack methodologies and vectors that are being employed in the most prevalent threats. This information also allows system administrators and users to gain familiarity with threats that attackers may favor in their exploits. Insight into emerging threat development trends can help bolster security measures and mitigate future attacks.

The endpoint is often the last line of defense and analysis; however, the endpoint can often be the first line of defense against attacks that spread using USB storage devices and insecure network connections. The threats found here can shed light on the wider nature of threats confronting businesses, especially from blended attacks and new threats facing mobile workers. Attacks reaching the endpoint are likely to have already circumvented other layers of protection that may be deployed, such as gateway or cloud-based filtering.

Methodology

A malicious code family initially consists of a distinct malicious code sample. As variants to the sample are released, the family can grow to include multiple variants. Symantec determines the most prevalent malicious code families by collating and analyzing anonymous telemetry data gathered for the reporting period.

Malicious code is classified into families based on variants in the signatures assigned by Symantec when the code is identified. Variants appear when attackers modify or improve existing malicious code to add or change functionality. These changes alter existing code enough that antivirus sensors may not detect the threat as an existing signature.

Overall, the top 10 list of malicious code families accounted for 33 percent of all potential infections blocked in 2014.

Rank	Name	Type	Propagation Mechanisms	Impacts/Features	% Overall
1	W32.Ramnit	Virus/ Worm	Executable files and removable drives	Infects various file types, including executable files, and copies itself to removable drives. It then relies on AutoPlay functionality to execute when the removable drive is accessed on other computers.	10.4%
2	W32.Sality	Virus/ Worm	Executable files and removable drives	Uses polymorphism to evade detection. Once running on an infected computer it infects executable files on local, removable and shared network drives. It then connects to a P2P botnet, downloads and installs additional threats. The virus also disables installed security software.	5.9%
3	W32.Almanahe	Virus/ Worm	CIFS/mapped drives/ removable drives/ executables	Disables security software by ending related processes. It also infects executable files and copies itself to local, removable, and shared network drives. The worm may also download and install additional threats.	4.0%
4	W32.Downadup	Worm/ Back door	P2P/CIFS/remote vulnerability	The worm disables security applications and Windows Update functionality and allows remote access to the infected computer. Exploits vulnerabilities to copy itself to shared network drives. It also connects to a P2P botnet and may download and install additional threats.	3.9%
5	W32.SillyFDC	Worm	Removable drives	Downloads additional threats and copies itself to removable drives. It then relies on AutoPlay functionality to execute when the removable drive is accessed on other computers.	3.4%
6	W32.Virut	Virus/ Back door	Executables	Infects various file types including executable files and copies itself to local, removable, and shared network drives. It also establishes a back door that may be used to download and install additional threats.	2.3%
7	W32.Chir	Worm	SMTP engine	Searches across the network and accesses files on other computers. However, due to a bug, these files are not modified in any way.	1.3%
8	W32.Imaut	Worm	IM	Downloads and installs additional threats as well as disables security software by ending security related processes. Sends instant messages containing a malicious URL that, if clicked, will trigger an attack on the recipient and install a copy of the worm.	0.8%
9	W32.Mabezat	Virus/Worm	SMTP/CIFS/ removable drives	Copies itself to local, removable, and shared network drives. Infects executables and encrypts various file types. It may also use the infected computer to send spam email containing infected attachments.	0.7%
10	W32.Changeup	Worm	Removable and mapped drives/ File sharing programs/Microsoft Vulnerability	The primary function of this threat is to download more malware on to the compromised computer. It is likely that the authors of the threat are associated with affiliate schemes that are attempting to generate money through the distribution of malware.	0.2%

Overall Top Malicious Code Families, 2014

Source: Symantec

Rank	Malware	% of Email Malware	Equivalent Ratio in Email
1	Trojan.Zbot	6.0%	1 in 16.8
2	Trojan.Zbot-SH	4.3%	1 in 23.0
3	Exploit/Link.G	3.2%	1 in 31.1
4	VBS.Downloader.Trojan	2.5%	1 in 40.0
5	Exploit/Link.D	1.5%	1 in 67.5
6	Court.Fakeavlock	0.9%	1 in 107.2
7	Exploit/Link-Downloader	0.9%	1 in 113.9
8	Trojan.Dropper	0.9%	1 in 116.3
9	JS/Selfaltering.dam	0.6%	1 in 164.2
10	W97M.Downloader	0.5%	1 in 185.4

Relative Proportion of Top 10 Malicious Code Blocked in Email Traffic by Symantec.cloud in 2014, by Percentage and Ratio

Source: Symantec.cloud

Commentary

- Ramnit overtook Sality again to become the most prevalent malicious code family in 2014.[5] Ranked first in 2011, 2012, and 2013, it was the top malicious code family by volume of potential infections again in 2014.
- Samples of the Ramnit family of malware were responsible for significantly more potential infections (10.4 percent) than was the second-ranked malicious code family in 2014, Sality[6] (5.9 percent).
- First discovered in 2010, W32.Ramnit has remained a prominent feature of the threat landscape.
- Ramnit spreads by encrypting and then appending itself to DLL, EXE, and HTML files. It can also spread by copying itself to the recycle bin on removable drives and creating an AUTORUN.INF file so that the malware is potentially automatically executed on other computers. This can occur when an infected USB device is attached to a computer. The reliable simplicity of spreading via USB devices and other media makes malicious code families such as Ramnit and Sality (as well as SillyFDC[7] and others) effective vehicles for installing additional malicious code on computers.
- The Sality family of malware remains attractive to attackers because it uses polymorphic code that can hamper detection. Sality is also capable of disabling security services on affected computers. These two factors may lead to a higher rate of successful installations for attackers. Sality propagates by infecting executable files and copying itself to removable drives such as USB devices. Similar to Ramnit, Sality also relies on AUTORUN.INF functionality to potentially execute when those drives are accessed.

- Overall in 2014, 1 in 244 emails was identified as malicious, compared with 1 in 196 in 2013; 12 percent of email-borne malware contained hyperlinks that referenced malicious code, in contrast with malware that was contained in an attachment to the email. This figure was 25.4 percent in 2013, an indication that cybercriminals are attempting to circumvent security countermeasures by changing the vector of attacks from purely email to the web.
- In 2014, 13.9 percent of malicious code detected that year was identified and blocked using generic detection technology. Many new viruses and Trojans are based on earlier versions, where code has been copied or altered to create a new strain, or variant. Often these variants are created using toolkits, and hundreds of thousands of variants can be created from the same piece of malware. This has become a popular tactic to evade signature-based detection, as each variant would traditionally need its own signature to be correctly identified and blocked. By deploying techniques such as heuristic analysis and generic detection, it's possible to correctly identify and block several variants of the same malware family, as well as identify new forms of malicious code that seek to exploit certain vulnerabilities that can be identified generically.
- Trojan.Zbot was the most frequently blocked malware in email traffic by Symantec.cloud in 2014, with Trojan.Zbot-SH taking the second position. It was the reverse ranking in 2013.

Analysis of Malicious Code Activity by Geography, Industry Sector, and Company Size

Background

Malicious code activity trends can also reveal patterns that may be associated with particular geographical locations or hotspots. This may be a consequence of social and political changes in the region, such as increased broadband penetration and increased competition in the marketplace, which can drive down prices, thereby increasing adoption rates. There may be other factors at work based on the local economic conditions. Similarly, the industry sector may also have an influence on an organization's risk factor; certain industries may be exposed to different levels of threat by the nature of their business.

Moreover, the size of an organization can also play a part in determining its exposure to risk. Small and medium businesses (SMBs) may find themselves the targets of malicious attacks by virtue of the relationships they have with other organizations. For example, a company may be subjected to an attack because it is a supplier to a larger organization, and attackers may seek to take advantage of this relationship in forming the social engineering behind subsequent attacks on the main target, using the SMB as a springboard for these later attacks. SMBs are perceived to be softer targets, as they are less likely to have the same levels of security as larger organizations, which have larger budgets applied to their security countermeasures.

Methodology

Analysis of malicious code activity by geography, industry, and size is based on the telemetry analysis from Symantec.cloud clients for threats detected and blocked against those organizations in email traffic during 2014.

This analysis looks at the profile of organizations being subjected to malicious attacks, not the source of the attacks.

Industry	2014	2013
Public Administration	1 in 88.9	1 in 95.4
Agriculture, forestry & fishing	1 in 149.5	1 in 415.5
Services – Professional	1 in 171.2	1 in 396.5
Services – Non-Traditional	1 in 186.2	1 in 401.8
Finance, insurance & Real Estate	1 in 204.0	1 in 426.8
Nonclassifiable Establishments	1 in 213.9	1 in 460.2
Construction	1 in 217.7	1 in 471.8
Wholesale	1 in 223.2	1 in 435.0
Transportation & Communication	1 in 289.0	1 in 480.5
Mining	1 in 427.3	1 in 426.8

Proportion of Email Traffic Identified as Malicious by Industry Sector, 2014

Source: Symantec.cloud

Company Size	2014	2013
1-250	1 in 142.3	1 in 332.1
251-500	1 in 135.2	1 in 359.4
501-1000	1 in 203.3	1 in 470.3
1001-1500	1 in 180.6	1 in 356.9
1501-2500	1 in 218.4	1 in 483.5
2501+	1 in 284.7	1 in 346.5

Proportion of Email Traffic Identified as Malicious by Organization Size, 2014

Source: Symantec.cloud

Country/Region	2014	2013
United Kingdom	1 in 78.6	1 in 198.9
Saudi Arabia	1 in 167.8	1 in 869.1
Kenya	1 in 177.4	1 in 1011.7
Hong Kong	1 in 180.3	1 in 440.7
Nigeria	1 in 193.9	1 in 970.3
Austria	1 in 197.1	1 in 300.7
Ireland	1 in 199.5	1 in 440.6
South Africa	1 in 214.7	1 in 272.8
Hungary	1 in 221.5	1 in 306.8
Thailand	1 in 227.7	1 in 929.2

Proportion of Email Traffic Identified as Malicious by Geographic Location, 2014

Source: Symantec.cloud

Commentary

* The rate of malicious attacks carried out by email has increased for four of the top 10 geographies being targeted, and six new countries appeared in the top 10 list in 2014: Saudi Arabia, Kenya, Hong Kong, Nigeria, Ireland, and Thailand.

* Businesses in the United Kingdom were subjected to the highest average ratio of malicious email-borne threats in 2014, with 1 in 78.6 emails blocked as malicious, compared with 1 in 198.9 in 2013.

* Globally, organizations in the government and public sector were subjected to the highest level of malicious attacks in email traffic, with 1 in 88.9 emails blocked as malicious in 2014, compared with 1 in 95.4 in 2013.

* Malicious email threats have increased for all sizes of organizations, with 1 in 284.7 emails being blocked as malicious for large enterprises with more than 2,500 employees in 2014, compared with 1 in 346.5 in 2013.

* One in 142.3 emails was blocked as malicious for SMBs with 1–250 employees in 2014, compared with 1 in 332.1 in 2013.

Propagation Mechanisms

Background

Worms and viruses use various means to spread from one computer to another. These means are collectively referred to as propagation mechanisms. Propagation mechanisms can include a number of different vectors, such as instant messaging (IM), Simple Mail Transfer Protocol (SMTP), common Internet file system (CIFS),[8] peer-to-peer (P2P) file transfers, and remotely exploitable vulnerabilities.Some malicious code may even use other malicious code as a propagation vector by locating a computer that has been compromised through a back door server and using it to upload and install itself.

Methodology

This metric assesses the prominence of propagation mechanisms used by malicious code. To determine this, Symantec analyzes the malicious code samples that propagate and ranks associated propagation mechanisms according to the related volumes of potential infections observed during the reporting period.[9]

Rank	Propagation Mechanisms	2014 Percentage	Change	2013 Percentage
1	Executable file sharing The malicious code creates copies of itself or infects executable files. The files are distributed to other users, often by copying them to removable drives such as USB thumb drives and setting up an autorun routine.	65%	-5%	70%
2	File transfer, CIFS is a file sharing protocol that allows files and other resources on a computer to be shared with other computers across the Internet. One or more directories on a computer can be shared to allow other computers to access the files within. Malicious code creates copies of itself on shared directories to affect other users who have access to the share.	31%	-1%	32%
3	Remotely exploitable vulnerability The malicious code exploits a vulnerability that allows it to copy itself to or infect another computer.	22%	-1%	23%
4	File transfer, email attachment The malicious code sends spam email that contains a copy of the malicious code. Should a recipient of the spam open the attachment the malicious code will run and their computer may be compromised.	7%	-1%	8%
5	File transfer, non-executable file sharing The malicious code infects non-executable files.	4%	+1%	3%
6	Peer to Peer file sharing	2%	-1%	3%
7	SQL The malicious code accesses SQL servers, by exploiting a latent SQL vulnerability or by trying default or guessable administrator passwords, and copies itself to the server.	1%	+0%	1%
8	File Transfer, Instant Messenger The malicious code sends or modifies instant messages that contains a copy of the malicious code. Should a recipient of the spam open the attachment the malicious code will run and their computer may be compromised.	1%	+0%	1%
9	File transfer, HTTP, embedded URI, email message body The malicious code sends spam email containing a malicious URI that, when clicked by the recipient, will launch an attack and install a copy of the malicious code.	<1%	=	<1%
10	File transfer, MMS attachment. The malicious code sends an MMS attachment, when clicked by the recipient, will launch an attack and install a copy of the malicious code.	<1%	=	<1%

Propagation Mechanisms

Source: Symantec

Commentary

As malicious code continues to become more sophisticated, many threats employ multiple mechanisms:

- Executable file sharing activity decreases: In 2014, 65 percent of malicious code propagated as executables, a small decrease from 70 percent in 2013. This propagation mechanism is typically employed by viruses and some worms to infect files on removable media. For example, variants of Ramnit and Sality use this mechanism, and both families of malware were significant contributing factors in this metric, as they were ranked as the two most common potential infections blocked in 2014.
- Remotely exploitable vulnerabilities decrease: At 22 percent, the percentage of malicious code that propagated through remotely exploitable vulnerabilities in 2014 was 1 percentage point lower than in 2013. Examples of attacks employing this mechanism include Downadup, which gained some momentum and is still a major contributing factor to the threat landscape, but was ranked fourth in 2013.
- File transfer using CIFS is in decline: The percentage of malicious code that propagated through CIFS file transfer fell by 1 percentage point between 2013 and 2014, a similar decline as between 2012 and 2013. Fewer attacks exploited CIFS as an infection vector in 2014.
- File transfer via email attachments also decreased: It is worth noting that file transfer via email attachments slightly decreased in 2014 compared with 2013, with 1 in 244 emails being identified as malicious in 2014, compared with 1 in 196 in 2013. In 2014, 12 percent of email attacks used malicious URLs, compared with 25 percent in 2013, showing an overall decrease in malicious emails.

Targeted Attacks Intelligence: Going from Isolated Attacks to Coordinated Campaigns Orchestrated by Threat Actors

Over the year 2014, Symantec could identify about 26,000 spear phishing emails that were deemed targeted by our threat analysts. However, this does not mean that we were facing the same number of attackers. Intuitively, we can easily imagine that some of these targeted attacks or intrusions may originate from the same hackers or threat group. Some of these threat actors may have different skills, exhibit various behaviors, and pursue different goals. To get a better understanding of this threat landscape, it is important to be able to differentiate between them and identify series of related attacks that might have been sourced by the same (group of) attackers. This will help us get a better understanding of attackers' tactics, techniques, and procedures (TTPs) and their motivation, which can ultimately be used to proactively detect them when attackers are coming back with new exploits or if they use slightly adapted techniques to attempt to compromise other customers.

However, finding groups of related attacks and attributing them to a specific threat actor or hacker group, based solely on intrusion activity or logging data, are challenging. The main reason is that skilled attackers can and do obviously update at least part of their attack tools and methodology in order to maximize their chances of successfully compromising the organization(s) they are targeting. While changing all aspects of their attack tools or exploit kits might have a prohibitive cost, chances are that they will adapt their methods over time by investing their resources into developing new exploits and adapting their intrusion tools.

As a result, it might be challenging for us, as defenders, to determine whether two spear phishing attacks were conducted by the same person, by different people who are collaborating, or by two unrelated hackers who decide independently to compromise the same company or even the same computer. Nevertheless, with enough information, analytical experience, and the technological tools to piece it all together, it might be possible to reconstruct attack campaigns from raw email data and additional meta-data on the malware or the exploit crafted together with the email. Consider an analogy with a serial killer in the real world, who leaves behind traces of his crime at different crime scenes. While individual crimes may vary in many details (such as the crime location, the victim's gender and age, the weapon or vehicle used, the various signs left at the crime scene, and how the crime scene was framed by the criminal), investigators might be able to collect different pieces of evidence that, when put together appropriately, could enable them to reconstruct the whole puzzle and ultimately identify which criminal was behind a series of crimes, based on the identified modus operandi and through the combination of all available pieces of evidence.

How Symantec is able to differentiate between distinct targeted attack campaigns using advanced TRIAGE technology

Symantec advanced TRIAGE data analytics technology aims at reproducing, in an automated fashion, a forensics methodology similar to the one performed by crime investigators, yet in the digital world. This framework has been designed to help analysts answer fundamental questions about cyberattacks, such as:

- Campaign analysis: Which series of attacks might be related to each other, even though they may be targeting different organizations—on the same or different dates—and using different malware or different exploits?
- What are the attackers' TTPs? How many different groups of attackers can we identify based on their modus operandi?
- What are the characteristics and dynamics of attack campaigns run by the same hacker groups? For example, what is their prevalence, size, and scale, or their sophistication?

Symantec uses the term attack campaign to refer to a series of spear phishing emails (or email intrusions) that:

1. Show clear evidence that the subject and target have been deliberately selected
2. Contain at least 3–4 strong correlations to other emails, such as the email topic, sender address, recipient domain, source IP address, attachment MD5, etc.

Attack campaigns may be sent on a single day or spread across multiple days; however, emails within the same campaign are always linked by a number of similar traits and thus form a sort of "chain of attacks."

One of the challenges to identifying such attack campaigns is that intrusions sourced by the same attackers (group) may have varying degrees of correlation. Without knowing in advance which features or indicators one should use to correlate attacks, this makes it very tedious for analysts to identify groups of related attacks. Figure 1 illustrates graphically this challenge of varying correlations between three different intrusions that were identified as parts of the same campaign. For example, intrusions 1 and 2 are linked by a different set of email features than are intrusions 2 and 3. This means that attackers may change any one feature when targeting different companies over time. Since we don't know in advance what their next move is, we have to rely on advanced correlation mechanisms that enable us to identify groups of related attacks (for example, originating from a specific threat group) without knowing which set of features should be used to associate these attacks with a particular group.

Phase	Email feature	Intrusion 1	Intrusion 2	Intrusion 3
Reconnaissance	**Recipient**	[user1]@org1.**gov.xy**	[user2]@**org2.gov.xy**	[user3]@**org2.gov.xy**
Weaponization	**Attach_name**	**Global Pulse Project***.pdf		Agenda - G20***.pdf
	Attach MD5	**dd2ed3f7dead4a[***]**		2e36081dd7f62e[***]
Delivery	**Date**	2011-05-13	2011-05-14	2011-07-02
	From addr.	[Att1]@domain1.com	[Att2]@domain2.com	
	Sender IP	**74.125.83.*** **		74.125.82.***
	Subject	FW:Project Document	Project Document	G20 Ds Finance Key Info – Paris July 2011
	Email body	[body1]		[body2]
Exploitation	**AV signature**	**CVE-2011-0611.C**		
Persistence	**C&C domains**	www.webserver.***		[N/A]

Figure 1: Illustration of varying correlations between different intrusions of the same campaign

By leveraging our TRIAGE data analytics technology, we can automatically group targeted attacks based on common elements likely reflecting the same root cause. As a result, we are able to identify complex patterns showing various types of relationships among series of targeted attacks, giving insight into the manner by which attack campaigns are orchestrated by various threat actors. The TRIAGE approach is illustrated in Figure 2.

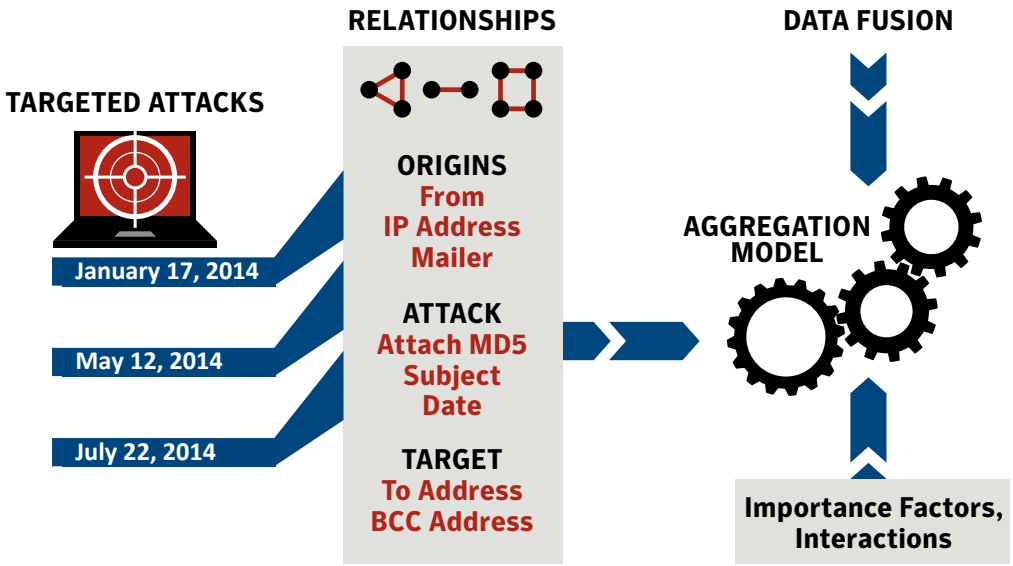


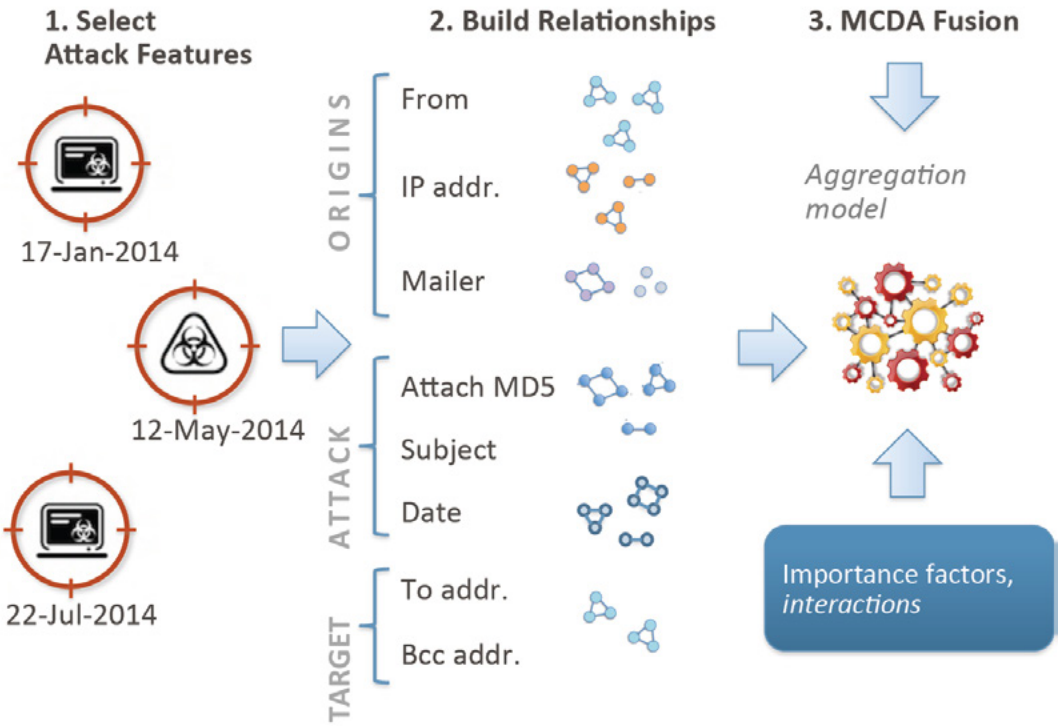
Figure 2: Illustration of TRIAGE methodology

It is worth mentioning that our TRIAGE framework was recently enhanced with novel visualizations thanks to VIS-SENSE,[10] a European research project aimed at developing visual analytics technologies for network security applications. Since its original conception, TRIAGE has been successfully used to analyze the behavior of cybercriminals involved in various types of Internet attack activities, such as rogue antivirus websites,[11] spam botnets operations,[12] scam campaigns,[13] spam campaigns launched from hijacked networks,[14] and targeted attacks performed via spear phishing emails.[15,16]

Insights into targeted attack campaigns

In 2014 Symantec's TRIAGE technology identified 841 clusters of spear phishing attacks (hereafter called attack campaigns, as defined previously), which quite likely reflect different waves of attacks launched by the same groups of individuals. Indeed, within the same cluster, attacks are linked by at least 3–4 characteristics among the following ones:

- The origins of the attack (like the email "From" address and source IP address used by the attacker)
- The attack date
- The characteristics of the malicious file attached to the email (for example, MD5 checksum; AV signature; file name; some meta-data coming from both static and dynamic analysis, such as document type or domains and IPs contacted by the malware)
- The email subject
- The targeted recipient (To" or "BCC" address fields in the email)

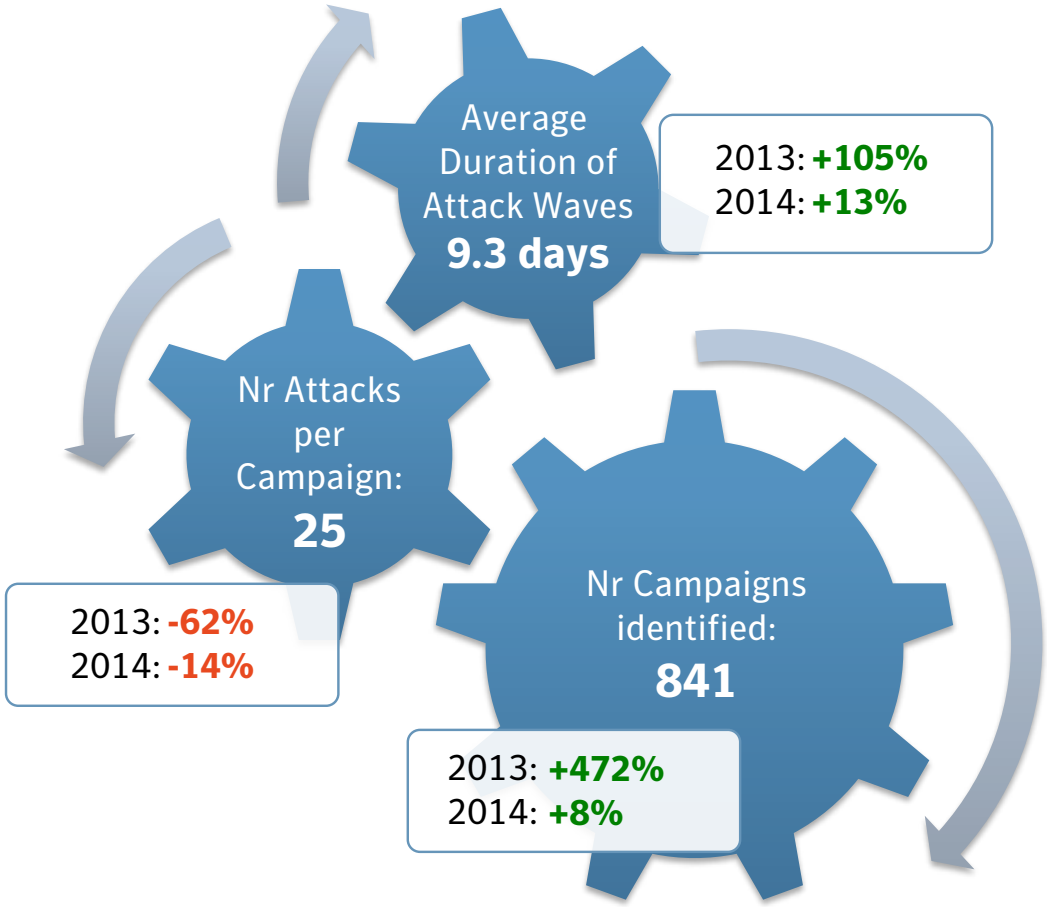


- *Figure 3: Illustration of Symantec's TRIAGE methodology*

Figure 4 and Figure 5 highlight some global metrics calculated across all attack campaigns identified by TRIAGE. To give more perspective to these figures, we compare them with statistics calculated in the past two years (since 2013), which can generate some insights about the characteristics and evolution of spear phishing campaigns. More specifically, we can clearly identify the following new trends:

- Spear phishing email campaigns have been increasingly prevalent since 2011, with a slight increase (8 percent) in the number of spear phishing campaigns compared with 2013! Considering the 16 percent decrease in the number of observed (individual) spear phishing emails since 2013, the increased number of spear phishing campaigns indicates that spear phishing emails have become a more prevalent technique among cybercriminal groups to launch targeted attacks. As companies and organizations have become more and more aware of the importance of securing their networks and systems against the wide range of Internet attacks, more cybercriminal groups appear to be leveraging spear phishing emails to infiltrate networks.
- Because the average number of attacks per campaign has significantly decreased, we can say they are performed at a smaller scale, likely in an effort by attackers to remain as stealthy as possible and not to raise too much suspicion. Because of the way TRIAGE identifies campaigns of spear phishing emails, we can also say that campaigns are more diverse in terms of the attackers perpetrating them, the companies or organizations that are targeted, the content of attacks (for example, the email, the exploit[s] used, the contacted C&C server[s], etc.), or a combination thereof.

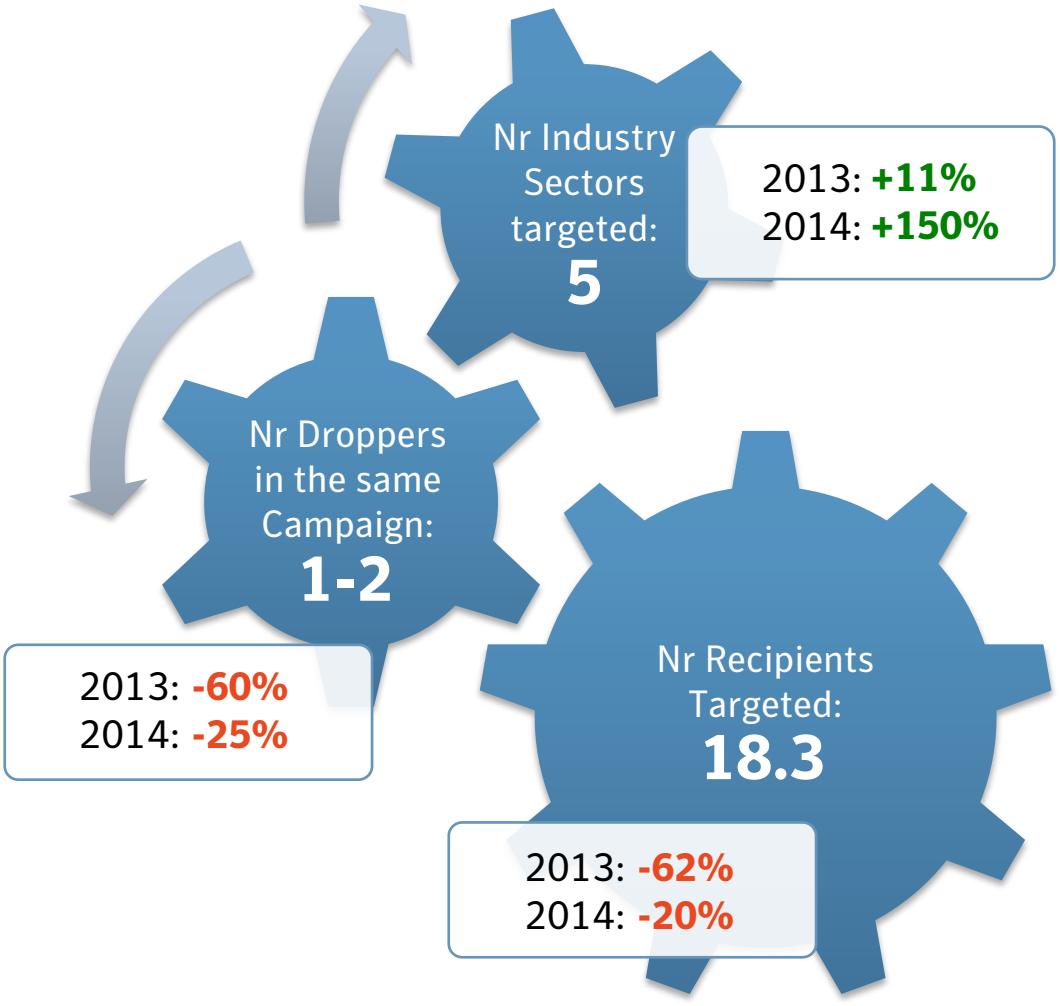
- We observe also that the average duration of a spear phishing campaign has increased a lot (9.3 days on average), which suggests that these campaigns have been increasingly persistent over the past few years (attackers won't give up after the first attempt! On the contrary, they will persist much longer to try to penetrate the premises of a company or an organization). The decreased number of attacks per campaign combined with the longer average duration of campaigns also likely indicates the will of attackers to remain under the radar by launching fewer attacks over a longer period of time.



- *Figure 4: Global metrics calculated across all identified campaigns (1)*

Figure 5 further highlights other interesting aspects of these targeted attack campaigns:

- If we look now at the average number of recipients targeted during the same campaign, this number has dropped significantly compared with 2013. This means that spear phishing campaigns are more and more focused, targeting fewer individuals, and conducted over a long period of time!
- Similarly, we observed that the average number of distinct droppers used in the same campaign has dropped by 25 compared with 2013. This tends to show that campaigns are usually tied to very few attacks (one or two on average) used against many targets. This makes spear phishing campaigns more consistent attack-wise and thus slightly less stealthy. Note that different droppers may sometimes contain the very same exploit, which was simply repacked in different documents (pdf, doc, xls, etc). The availability of and easy access to these exploits (for example, via tools like Metasploit) for a wide range of vulnerabilities (including zero-day vulnerabilities) then make targeted attacks via spear phishing emails a method of choice for attackers to breach a company's or organization's network.
- Finally, the average number of different industries targeted during the same campaign has increased by 150 compared with 2013, showing a significant broader diversification in spear phishing attacks!



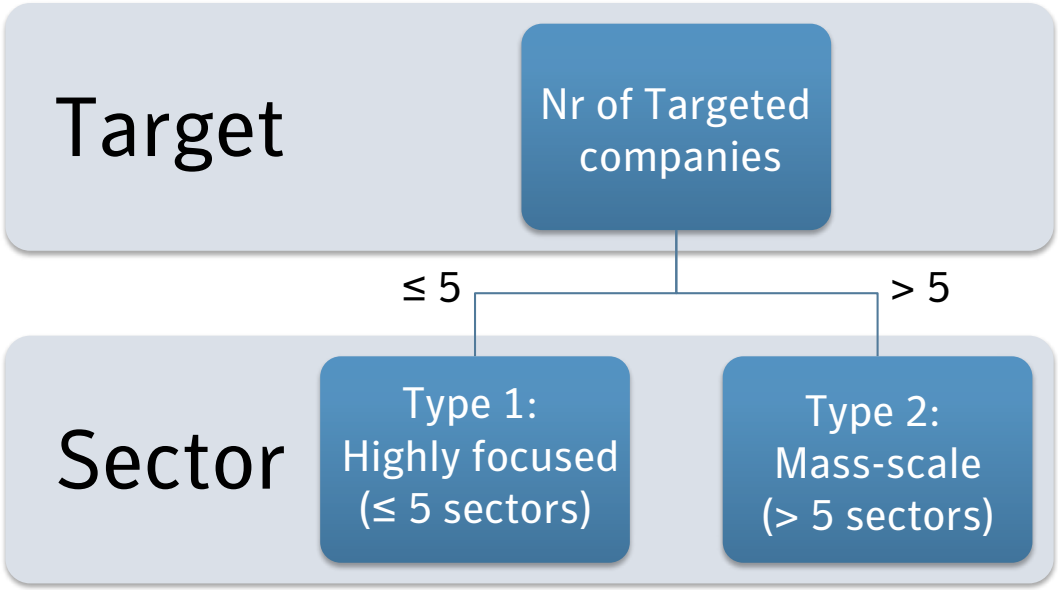
- *Figure 5: Global metrics calculated across all identified campaigns (2)*

Highly Focused versus Mass-Scale Campaigns

The 841 distinct campaigns of spear phishing attacks were then further classified into two groups:

- Type 1: Highly focused and targeted campaigns
- Type 2: Mass-scale organizational targeted attacks (MOTAs)

To this end, we used a combination of two criteria: the number of targeted companies and the number of distinct industry sectors associated with them. Type 1 campaigns were defined as spear phishing campaigns that targeted five (or fewer) distinct companies in five (or fewer) different sectors. Spear phishing campaigns not matching these criteria were deemed Type 2 campaigns (that is, they fit the profile of MOTAs) because they targeted a more significant set of different industries having very different lines of business.



- *Figure 6: Criteria used to classify targeted attack campaigns according to their scale*

Based on the classification defined previously, we found that in 2014 about three-fifths of spear phishing campaigns were highly focused and targeted a smaller number of companies active in the same or closely related sectors. The other two-fifths of the campaigns were still targeted (in the sense of being in low-copy number and showing some evidence of a selection of a subject in relation with the recipient activity), but these campaigns involved more large-scale attacks, in the sense that they were targeting more companies and organizations active in different sectors.

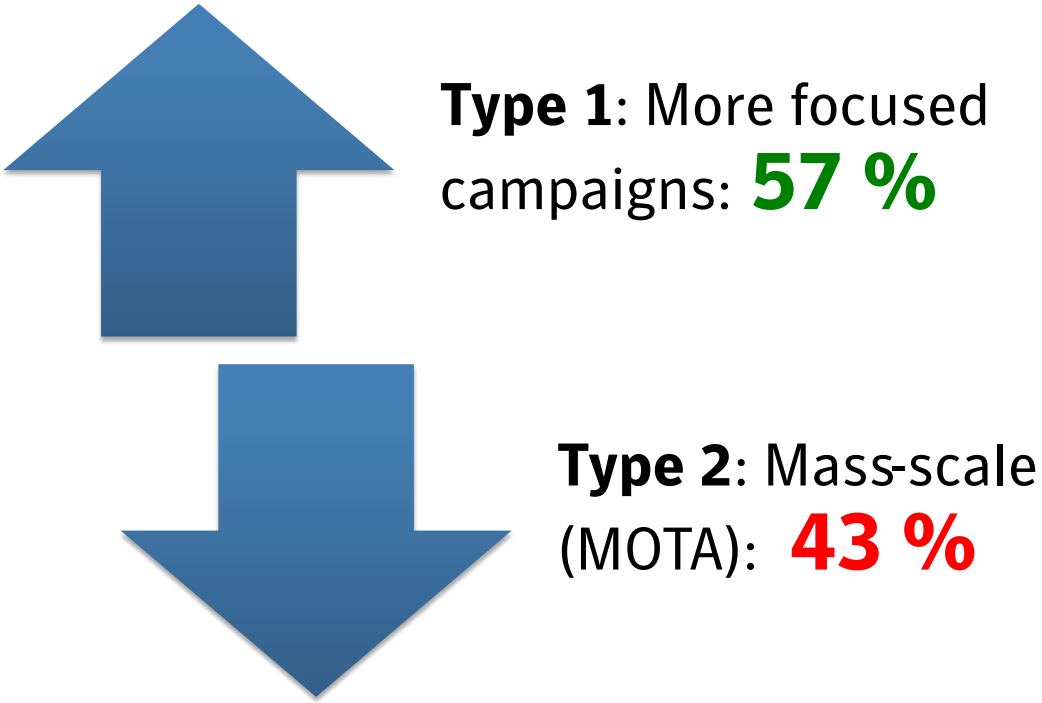


Figure 7: Types of campaigns

Type 1 – highly targeted campaigns

Campaign against an intergovernmental organization on October 8, 2014

As we have seen, 57 percent of spear phishing attacks are forming rather small campaigns, meaning they are organized on a relatively small scale and tend to focus on specific targets. A first example of such a campaign took place on October 8, 2014, and targeted an intergovernmental organization. As illustrated in Figure 8, spear phishing emails were sent to nine different recipients within the organization but from only three different email addresses. All emails had the same subject line—"Situation Report about Afghan"—a topic relevant to the targeted recipients and that turns out to also be the name of the attached file. The attached file ("Situation Report about Afghan.doc"; md5=ed9f9814a9fd661ec00392171133a4cc) was carrying a malicious payload exploiting an old vulnerability in Microsoft Office (CVE-2012-1058), allowing arbitrary code, such as code to install a back door or any other piece of malicious code, to be executed by the attacker. Although the vulnerability was patched shortly after it was disclosed (CVE-2012-1058), in February 2012, it seemed to have been widely used by cybercriminals in numerous targeted attack campaigns. Evidence also shows the attacks likely originated from Russia (domain names in source email addresses ended with .ru top-level domain and were hosted in Russia).

As far as we know, Symantec customers have been protected against the exploitation of the CVE-2012-1058 vulnerability since its disclosure.[17]

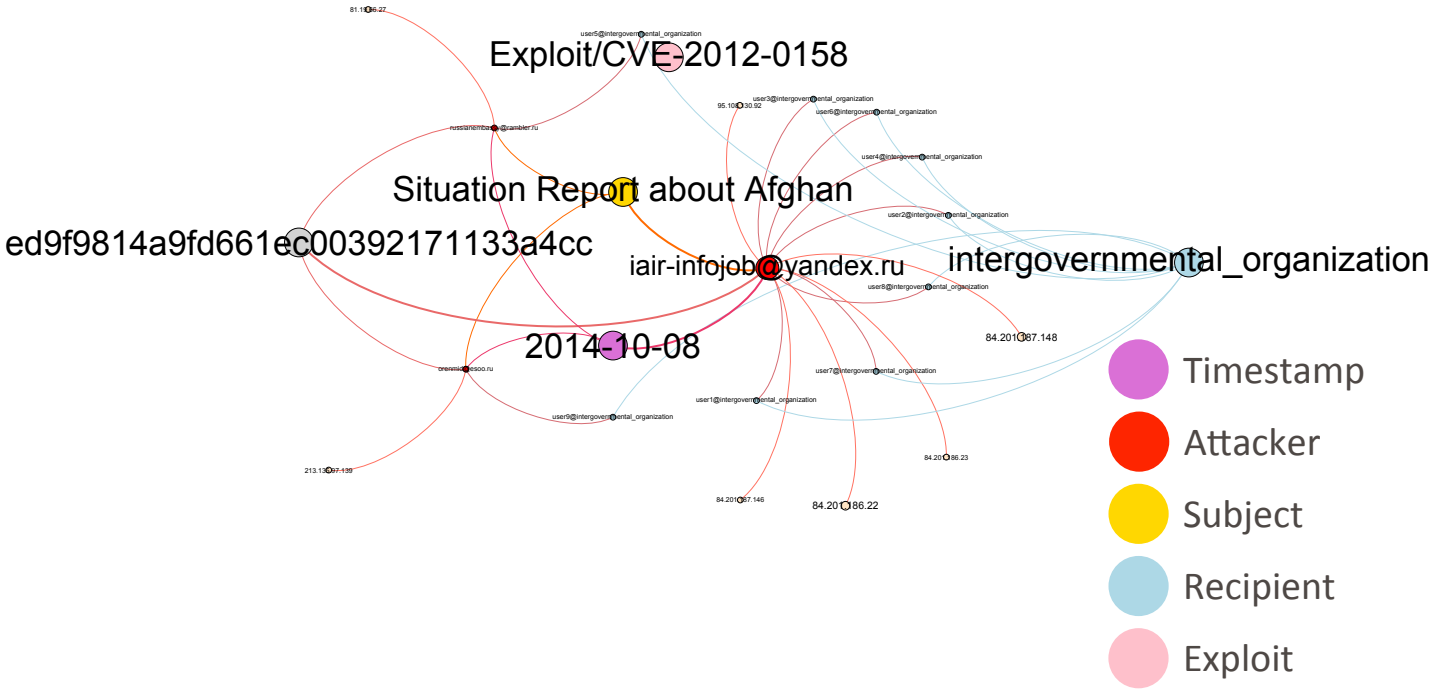


Figure 8: Spear phishing email campaign against an intergovernmental organization

Campaign against a major energy company between February 8, 2014, and February 22, 2014

Another highly targeted spear phishing email campaign took place between February 8, 2014, and February 22, 2014, and targeted an American company active in the energy sector. During this campaign, nine spear phishing emails were sent to a single recipient in the company but from eight different email addresses. On some days and during the 15 days this campaign lasted, up to two emails per day were sent. This campaign is illustrated in Figure 8. All emails included a different subject line (such as "Fortune 100 Loyalty Incentives Program," "Trade Monitoring Report as at 14th February"). While the name of the attached file remained the same throughout the campaign ("script.au3"), the content of the file varied a lot, possibly due to a single piece of malware repacked several times, thus producing apparently different files. We do not know whether the attacks were successful or what the objective of the attacker(s) was, for instance, using the infected system as a pivot to infiltrate other systems in the corporate network, stealing sensitive information from the infected system directly). We believe the attacks all originated from within the United States (domain names in source email addresses were hosted in the United States). Finally, the duration and highly targeted aspect of this campaign show that attackers nowadays can be perseverant and determined to attack a given company or, in this case, a given individual within that company.

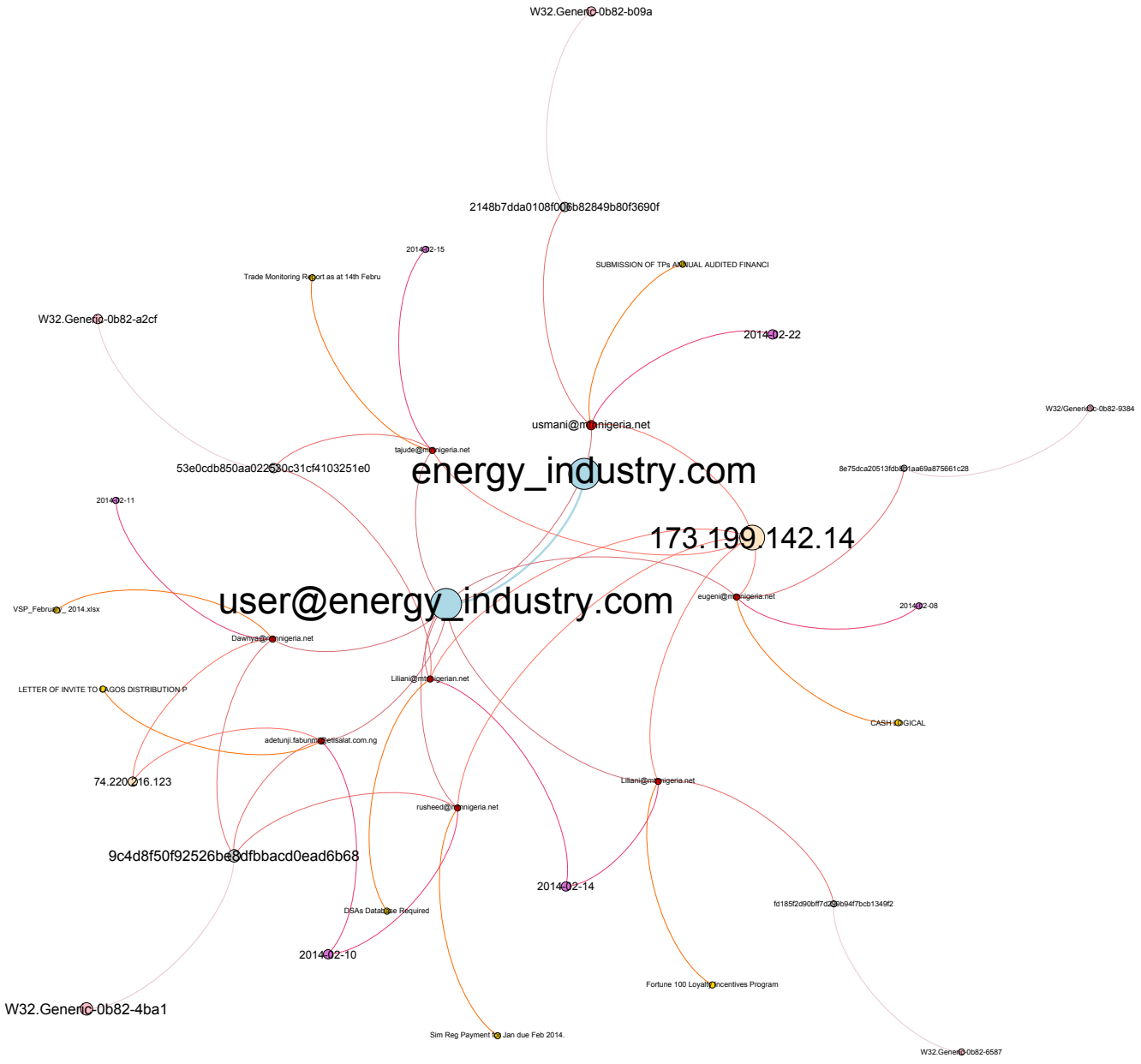


Figure 9: Spear phishing email campaign against a major energy company

Type 2: Mass-scale Organizational Targeted Attacks (MOTAs)

About two-fifths of targeted attacks identified in 2014 were organized on a larger scale and fit the profile of a MOTA. MOTAs target a large number of people in multiple organizations, working in different sectors, over multiple days. As described earlier, we used a threshold of five different companies, active in five completely different sectors, to classify attack campaigns and label them as MOTA versus highly focused. Most of the large-scale campaigns are quite well resourced, with up to 17 different exploits used during the same campaign.

The Bagle mass-mailer worm campaign between January 1, 2014, and April 29, 2014

A first example of such a campaign, illustrated in Figure 10, took place between January 1, 2014, and April 29, 2014; targeted no less than 12 companies located in Europe, Asia, and Australia; and was active in seven different industry sectors, including public administration, finance and insurance, and transportation. A total of 155 emails were sent over a period of about four months. This campaign thus appears loosely focused.

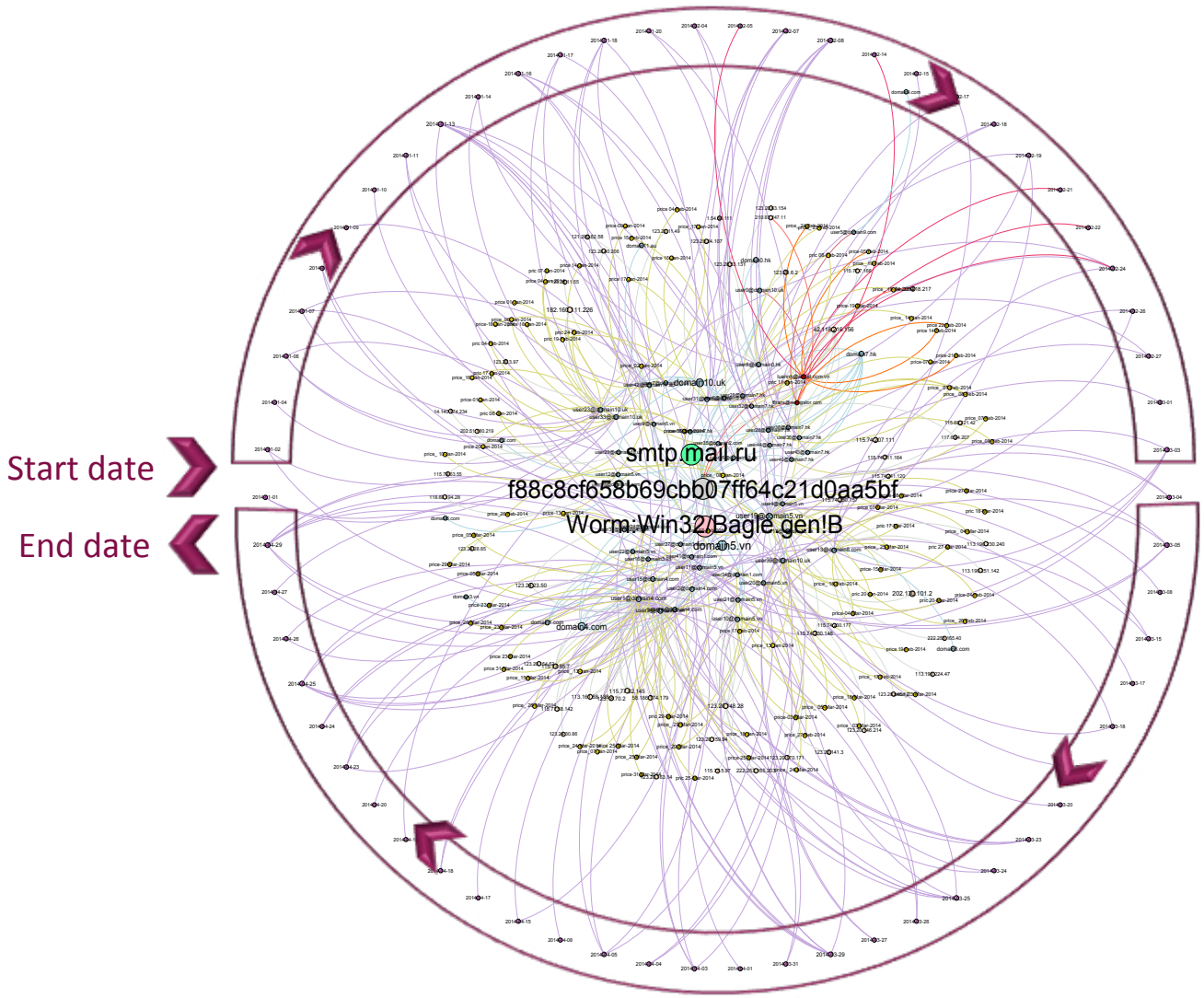


Figure 10: The Bagle mass-mailer worm campaign

When looking at the file attached to the emails, we can see that all emails were carrying a variant of the Bagle worm (Worm:Win32/Bagle.gen!B), which is a piece of code that replicates itself automatically by sending copies of itself via an attached file in an email.[18] Although the attached file name (pattern: "[8-12 characters].exe") was different in almost every spear phishing email, the content of the file was identical throughout the campaign (md5=f88c8cf658b69cbb07ff64c-21d0aa5bf). Moreover, the subject line included in the emails varied with the attachment file name and always followed the pattern "price[-_][date in the format dd-mm-yyyy]." Also, we found that the instance of the Bagle worm observed in this campaign used the free Russian mail service mail.ru to send the emails through which it replicated itself.

As far as we know, Symantec customers were protected against these attacks.

The Ebola campaign on October 27–28, 2014

Another interesting example of a mass-scale spear phishing email campaign took place on October 27–28, 2014, and consisted of 80 emails that targeted about 50 different companies active in 10 different industry sectors around the world. All emails included a subject line referring to the Ebola virus that dominated the news headlines in 2014.

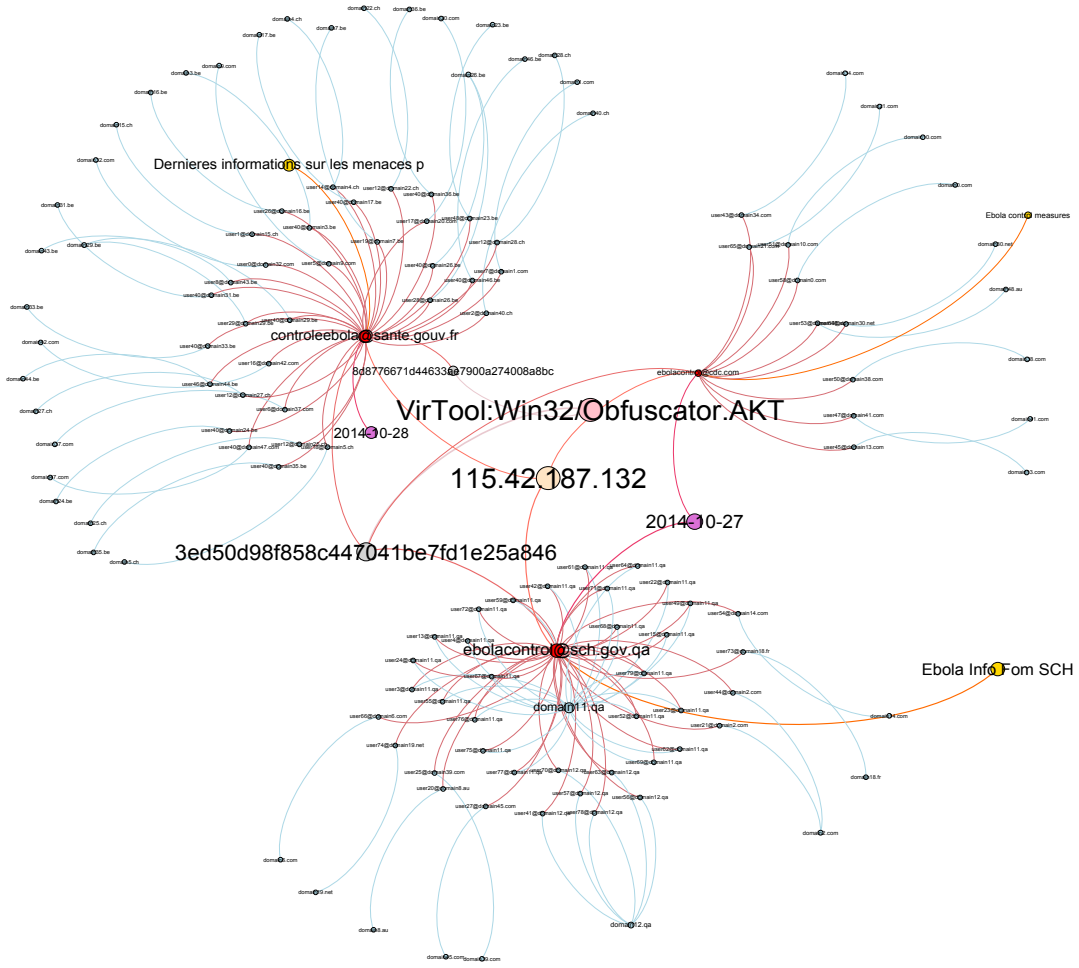


Figure 11: The Ebola campaign

In this campaign, illustrated in Figure 11, all emails were carrying two apparently different instances of an obfuscated piece of malware (VirTool:Win32/Obfuscator.AKT, md5=3ed50d98f-858c447041be7fd1e25a846; 8d8776671d44633ae7900a274008a8bc). The obfuscation of the attached malware hindered the detection and identification of the underlying piece of malicious code. However, the attached piece of code was apparently dropping a Trojan. All emails were sent using only three different source email addresses, but all three could be tracked to a single source IP address (115[.]42[.]187[.]132). We identified two waves in the campaign: (1) one taking place on October 27 and (2) one taking place on October 28.

1. In the first wave, emails were sent from two source email addresses. Two different subject lines—one for each source address—were used for the emails. The set of recipients varied with the source email address used.
2. In the second wave, emails were sent from a single source email address. A singular aspect of this wave is that it appeared to target a French-speaking audience, with emails (including the subject line) translated into French and apparently originating from the French Ministry of Health (@sante.gouv.fr source email address). Of course, the source email address was likely spoofed by the attacker(s). Email recipients were also mostly located in France, Belgium, and Switzerland.

APPENDIX C: SPAM & FRAUD ACTIVITY TRENDS

Appendix C: Spam & Fraud Activity Trends

Spam and Fraud Activity Trends

This section covers phishing and spam trends. It also discusses activities observed on underground economy-type servers, as this is where much of the profit is made from phishing and spam attacks.

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking (or spoofing) a specific, usually well-known brand. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they can then use to commit fraudulent acts. Phishing generally requires victims to provide their credentials, often by duping them into filling out an online form. This is one of the characteristics that distinguish phishing from spam-based scams (such as the widely disseminated "419 scam"[19] and other social engineering scams).

Spam is usually defined as junk or unsolicited email sent by a third party. While it is certainly an annoyance to users and administrators, spam is also a serious security concern because it can be used to deliver Trojans, viruses, and phishing attacks. Spam can also include URLs that link to malicious sites that, without the user's being aware of it, attack a user's system upon visitation. Large volumes of spam could also cause a loss of service or degradation in the performance of network resources and email services.

This section includes the following metrics:

- Analysis of Spam Activity Trends
- Analysis of Spam Activity by Geography, Industry Sector, and Company Size
- Analysis of Spam Delivered by Botnets
- Analysis of Phishing Activity by Geography, Industry Sector, and Company Size
- Whois attacking you? Beware of malicious BGP hijacks!

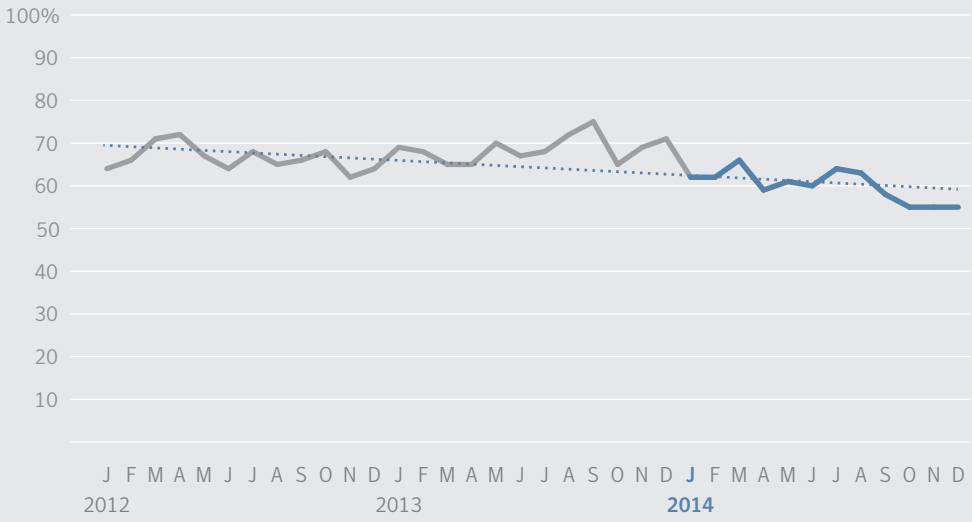
Analysis of Spam Activity Trends

Background

This section discusses the patterns and trends relating to spam message volumes and the proportion of email traffic identified as spam during 2014.

Methodology

The analysis for this section is based on global spam and overall email volumes for 2014. Global values are determined based on the statistically representative sample provided by Symantec Messaging Gateway[20] operations, and the spam rates include spam blocked by Symantec.cloud.



Global Spam Rate, 2012–2014

Source: Symantec

Commentary

- Approximately 28 billion spam emails were in circulation worldwide each day in 2014, compared with 29 billion in 2013, representing a decrease of 3.3 percent in global spam volume.
- Overall for 2014, 60 percent of email traffic was identified as spam, compared with 66.4 percent in 2013, representing a decrease of 6.4 percentage points.

Analysis of Spam Activity by Geography, Industry Sector, and Company Size

Background

Spam activity trends can also reveal patterns that may be associated with particular geographical locations or hotspots. This may be a consequence of social and political changes in the region, such as increased broadband penetration and increased competition in the marketplace, which can drive down prices, thereby increasing adoption rates. There may also be other factors at work based on the local economic conditions. Similarly, the industry sector may also have an influence on an organization's risk factor; certain industries may be exposed to different levels of threat by the nature of their business.

Moreover, the size of an organization can also play a part in determining its exposure to risk. Small and medium businesses (SMBs) may find themselves the targets of spam attacks because they are perceived to be softer targets than larger organizations. They are likely to have less stringent security countermeasures than larger organizations, which can apply greater resources to their antispam and security countermeasures.

Methodology

Analysis of spam activity based on geography, industry sector, and company size is based on the patterns of spam activity for Symantec.cloud clients for threats during 2014.

Industry	2014	2013
Mining	56.8%	60.0%
Manufacturing	56.2%	66.0%
Construction	56.2%	60.5%
Services – Non-Traditional	55.6%	60.4%
Services – Professional	55.5%	65.2%
Finance, Insurance & Real Estate	55.4%	73.0%
Agriculture, Forestry & Fishing	55.3%	65.4%
Public Administration	55.0%	65.5%
Wholesale	54.8%	65.1%
Nonclassifiable Establishments	54.5%	65.4%

Proportion of Email Traffic Identified as Spam by Industry Sector, 2014

Source: Symantec.cloud

Company Size	2014	2013
1–250	55.2%	70.4%
251–500	55.5%	65.4%
501–1000	55.2%	65.2%
1001–1500	54.9%	65.6%
1501–2500	55.4%	65.6%
2501+	55.4%	65.6%

Proportion of Email Traffic Identified as Spam by Organization Size, 2014

Source: Symantec.cloud

Country/Region	2014	2013
Serbia	90.3%	65.8%
Ukraine	89.0%	65.3%
Burundi	79.3%	61.3%
Chile	76.6%	61.1%
Bulgaria	73.2%	62.9%
Zimbabwe	72.5%	63.7%
Sri Lanka	68.6%	75.7%
Northern Mariana Islands	66.3%	61.9%
Bahamas	66.3%	61.6%
Azerbaijan	64.4%	61.5%

Proportion of Email Traffic Identified as Spam by Geographic Location, 2014

Source: Symantec.cloud

Commentary

- The spam rate decreased across all top 10 geographies in 2014. The highest rate of spam was for organizations in Serbia, with an overall average spam rate of 90.3 percent.
- The spam rate decreased across all top 10 industry sectors in 2014, with mining on the top, with 56.8 percent. But in 2013, finance was subjected to the highest spam rate, with 73.0 percent.
- The spam rate decreased for all sizes of organizations in 2014.
- Of all emails sent to large enterprises with more than 2,500 employees in 2014, 55.4 percent were identified as spam, compared with 65.6 percent in 2013.

Analysis of Spam Delivered by Botnets

Background

This section discusses botnets and their use in sending spam. Similar to how ballistic analysis can reveal the gun used to fire a bullet, botnets can be identified by common features within the structure of email headers and corresponding patterns during the Simple Mail Transfer Protocol (SMTP) transactions. Spam emails are classified for further analysis according to the originating botnet during the SMTP transaction phase. This analysis reviews only botnets involved in sending spam and does not look at botnets used for other purposes, such as financial fraud or distributed denial-of-service attacks.

Methodology

Symantec.cloud spam honeypots collects millions of spam emails each day. These were classified according to a series of heuristic rules applied to the SMTP conversation and the email header information.

A variety of internal and external IP reputation lists were also used in order to classify known botnet traffic based on the source IP address of the sending machine. Information is shared with other security experts to ensure the data is up to date and accurate.

Location of Botnet Activity	% of Botnet Spam
United States	7.7%
Spain	6.9%
Argentina	5.2%
Germany	4.9%
Italy	4.5%
Vietnam	4.3%
Russia	4.0%
Brazil	3.5%
India	2.7%
Romania	2.7%

Top Sources of Botnet Spam by Location, 2014

Source: Symantec.cloud

Commentary

- In 2014, approximately 74 percent of spam email was distributed by spam-sending botnets, compared with 76 percent in 2013. Ongoing actions to disrupt a number of botnet activities during the year contributed to this gradual decline.
- The top spam botnet, Kelihos, was responsible for 51.6 percent of spam, generating an estimated 1 billion spam emails each day, compared with 10 billion in 2013.
- The United States was at the top of the spam-sending botnet table in 2014 and was the source of approximately 7.7 percent of global botnet spam, 0.8 percentage point higher than Spain, in second place.

Analysis of Phishing Activity by Geography, Industry Sector, and Company Size

Background

Phishing activity trends can also reveal patterns that may be associated with particular geographical locations or hotspots. For example, the industry sector may also have an influence on an organization's risk factor; certain industries may be exposed to different levels of threat by the nature of their business.

Moreover, the size of an organization can also play a part in determining its exposure to risk. SMBs may find themselves the targets of spam attacks because SMBs are perceived to be softer targets, as they are less likely to have the same levels of defense in depth as larger organizations, which tend to have greater budgetary expenditure applied to antispam and security countermeasures.

Methodology

Analysis of phishing activity based on geography, industry sector, and company size is based on the patterns of spam activity for Symantec.cloud clients for threats during 2014.

Industry	2014	2013
Agriculture, Forestry & Fishing	1 in 833.4	1 in 1,173.6
Public Administration	1 in 838.9	1 in 216.4
Nonclassifiable Establishments	1 in 946.2	1 in 1,294.5
Services – Professional	1 in 1,193.2	1 in 1,155.4
Services – Non-Traditional	1 in 1,554.8	1 in 1,567.7
Construction	1 in 1,625.6	1 in 1,368.8
Finance, Insurance & Real Estate	1 in 1,630.5	1 in 767.7
Mining	1 in 1,931.6	1 in 1,355.4
Wholesale	1 in 2,074.0	1 in 1,533.1
Transportation, Communications, Electric, Gas & Sanitary Services	1 in 2,172.9	1 in 2,226.1

Proportion of Email Traffic Identified as Phishing by Industry Sector, 2014

Source: Symantec.cloud

Company Size	2014	2013
1–250	1 in 1,401.5	1 in 689.5
251–500	1 in 1,253.5	1 in 1,075.9
501–1000	1 in 1,248.4	1 in 1,574.6
1001–1500	1 in 1,639.6	1 in 1,309.8
1501–2500	1 in 1,621.2	1 in 1,709.3
2501+	1 in 1,685.4	1 in 844.7

Proportion of Email Traffic Identified as Phishing by Organization Size, 2014

Source: Symantec.cloud

Country/Region	2014	2013
South Africa	1 in 568.0	1 in 419.8
Canada	1 in 765.6	1 in 1,059.3
Austria	1 in 805.8	1 in 1,049.0
New Zealand	1 in 961.5	1 in 1,784.7
United Kingdom	1 in 1,072.4	1 in 454.1
Netherlands	1 in 1,162.5	1 in 1,115.9
Belgium	1 in 1,312.2	1 in 1,935.4
Switzerland	1 in 1,462.6	1 in 1,917.7
Germany	1 in 1,472.7	1 in 1,901.1
Singapore	1 in 1,521.9	1 in 2,600.7

Proportion of Email Traffic Identified as Phishing by Geographic Location, 2014

Source: Symantec.cloud

Commentary

- The highest average rate for phishing activity in 2014 was for organizations in South Africa, with an overall average phishing rate of 1 in 568.0, compared with 1 in 419.8 in 2013.
- Organizations in the agriculture sector were subjected to the highest level of phishing activity in 2014, with 1 in 833.4 emails identified and blocked as a phishing attack. In 2013 the sector with the highest average phishing rate was government and public sector, with a phishing rate of 1 in 216.4.
- The phishing rate decreased for all sizes of organization in 2014. Of all emails sent to large enterprises with more than 2,500 employees in 2014, 1 in 1,685.4 was identified and blocked as a phishing attack, compared with 1 in 844.7 in 2013.
- Of all emails sent to businesses with up to 250 employees in 2014, 1 in 1,401.5 was identified and blocked as a phishing attack, compared with 1 in 689.5 in 2013.

"Whois" attacking you? Beware of malicious BGP hijacks!

Background

What is BGP hijacking?

The Internet is divided into thousands of smaller networks called autonomous systems (ASes), each of them belonging to a single entity (for example, an Internet service provider, a company, a university). Routing between ASes is achieved using the Border Gateway Protocol (BGP), which allows ASes to advertise to others the addresses of their network and receive the routes to reach other ASes.

Each AS implicitly trusts the peer ASes it exchanges routing information with. BGP hijacking is an attack against the routing protocol that consists of taking control of blocks of IP addresses owned by a given organization, without its authorization. This enables the attacker to perform other malicious activities (for example, spamming, phishing, malware hosting) using hijacked IP addresses belonging to somebody else.

In the volumes 17 and 19 of the Symantec Internet Security Threat Report we highlighted a phenomenon where so-called fly-by spammers temporarily steal (or hijack) blocks of network IP addresses and use them to send spam and hinder their traceability. We presented several real-world case studies involving very sophisticated spammers who briefly hijacked other people's networks in order to originate spam from them and successfully circumvented traditional spam IP blacklists. Although at the time we presented a limited number of cases of spammers behaving this way, we envision that such a phenomenon will become more prevalent.

Why is it important to detect BGP hijacking attacks?

It is important to detect and mitigate malicious BGP hijacks for the following reasons:

- Oftentimes when facing an attack, network operators use services such as whois to determine the individual or organization responsible for the offending IP address(es). However, BGP hijack attacks can lead to misattributing other attacks, such as denial-of-service attacks or spam, launched from hijacked networks due to hijackers' stealing the IP identity of the victim network owner. Correctly attributing attacks is critical when responding with possible legal actions.
- Many security systems protecting networks and systems rely on IP reputation as a first layer of defense. For example, spam filters heavily use IP blacklists to filter out emails coming from known spam senders. An attacker can thus defeat such protections by hijacking a network with a good reputation and then using the available IP addresses to launch devious attacks.

Methodology

How is Symantec able to identify malicious BGP hijacks using SpamTracer[21] technology?

Identifying malicious BGP hijacks involves (i) identifying networks originating nefarious network traffic, such as spam; and (ii) determining whether these networks have been stolen (or hijacked) from their legitimate owner. A tool called SpamTracer has been developed within Symantec Research Labs to track such attacks. SpamTracer monitors the routes toward networks seen originating cyberattacks to detect when the attackers manipulate the Internet routing to steal (or hijack) IP addresses used in these cyberattacks.

Data and commentary

In 2014, Symantec research identified, using SpamTracer, no less than 2,655 network IP address blocks that were hijacked from their legitimate owner. While hijacked, networks were used to send spam and host scam websites.

Malicious BGP hijack signature?

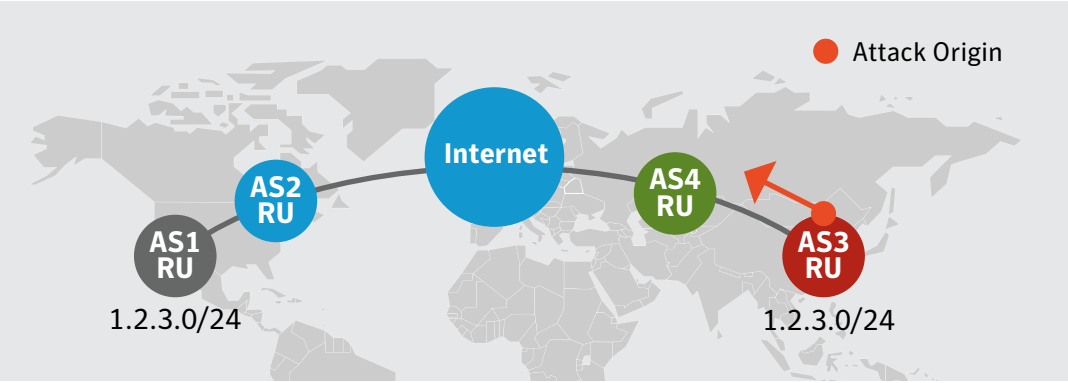
Looking at how the network IP address blocks were announced in BGP by the attackers, we were able to determine the modus operandi used to abuse the Internet routing and hijack the networks.

Hijacked network IP address blocks were:

- Not announced/used by their legitimate owner prior to being hijacked (that is, they were "dormant")
- Advertised by the attackers either (i) by a rogue origin AS (prefix hijack) or (ii) by the valid origin AS but via a rogue upstream provider (AS hijack)

In a prefix hijack, illustrated in Figure 1, the attacker (AS3) typically advertises the hijacked IP prefix (for example, 1.2.3.0/24, normally owned by AS1) using a rogue origin AS number (AS3). In our example, AS3 is said to be a rogue origin AS because the address block 1.2.3.0/24 is normally advertised by AS1, not AS3.

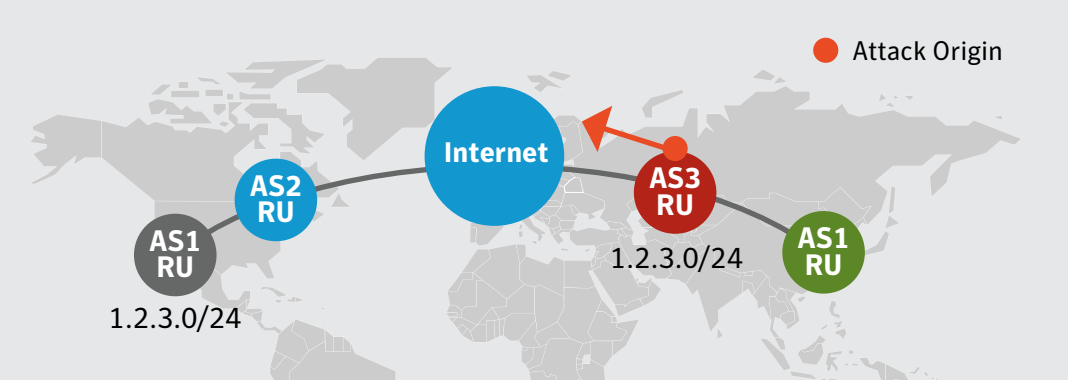
Prefix hijacks accounted for 92 percent (2,443 out of 2,655) of hijacks identified by Symantec in 2014.



- *Figure 1: Prefix hijack*

In an AS hijack, illustrated in Figure 2, the attacker (AS3) typically advertises the hijacked IP prefix (for example, 1.2.3.0/24, normally owned by AS1) using the AS number of the legitimate owner (AS1) but via a rogue upstream provider (AS3). In our example, AS3 is said to be a rogue upstream provider for AS1 because AS1 is normally connected (or a peer) with AS2, not AS3.

AS hijacks accounted for 8 percent (212 out of 2,655) of hijacks identified by Symantec in 2014.



- *Figure 2: AS hijack*

How long do hijacks last?

An important aspect of hijacks is their duration. The shorter a hijack attack lasts, the harder it is to detect and mitigate it. Attackers are more likely to be successful and evade protections, such as spam IP blacklists, if they use hijacked networks for a short period of time, because by the time a network is identified as "bad" by these protections, the attacker has already moved to another network. We identified two main hijack phenomena: short lived (from a few minutes to one week) and long lived (from one week to several months).

Out of the 2,655 hijacks uncovered during 2014, 98.7 percent were short lived (that is, they lasted at most one week). Moreover, 85.5 percent lasted less than 24 hours. Such short-lived hijacks clearly show that attackers are willing to remain as stealthy as possible and raise as little attention as possible.

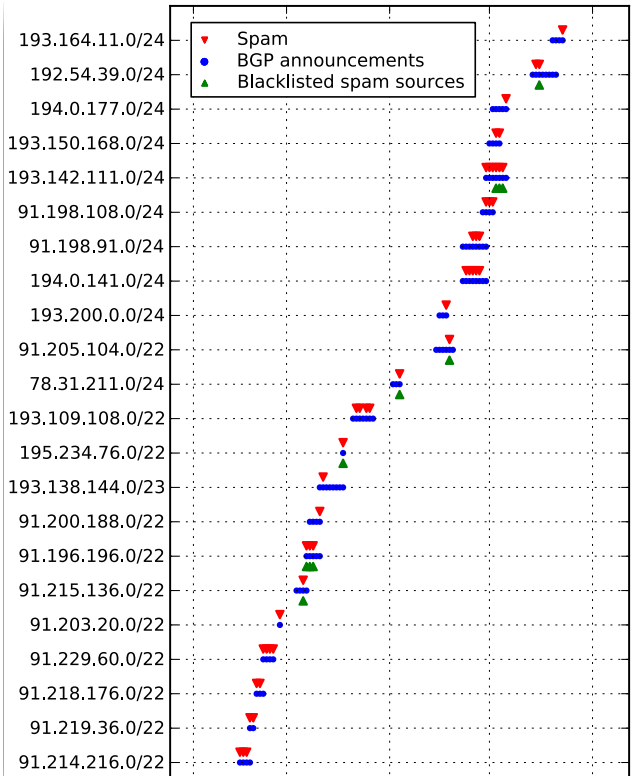
How effective is this spamming technique?

In the volumes 17 and 19 of the Symantec Internet Security Threat Report we reported evidence of spammers abusing the Internet routing to send spam in a stealthy way and prevent any traceback. The main objective of these sophisticated spammers is to circumvent spam IP black-lists by sending spam from a clean, "reputable" network until it starts appearing on blacklists and its reputation is degraded.

Out of the 2,655 IP address blocks identified as having been hijacked during 2014, 64 of them sent spam to spam traps set up by Symantec.cloud. Spam traps are decoy domains or email accounts used for the sole purpose of collecting all emails addressed to them since they are all spam. Out of these 64 hijacked networks that we know have been used for spamming, only 13 ended up being blacklisted by Spamhaus (SBL), Uceprotect, or Manitu. The remaining 51 network blocks never appeared to be blacklisted even though we observed spam emails sent from them. Figure 3 shows the BGP announcements, spam, and blacklisted spam sources related to a sample of 25 out of 64 short-lived hijacked IP prefixes. The figure highlights:

- The strong temporal correlation between BGP announcements and spam
- The low number of IP address blocks (7 out of 64) blacklisted before the end of the hijack

A total of 4,149 spam emails were received from these 64 hijacked IP address blocks. We extracted from this spam all advertised URLs that were pointing to 1,174 unique domain names, resolving to IP addresses belonging to the same hijacked IP address blocks, showing that some IP addresses were used in parallel to send spam and host the advertised scam websites. From whois information, we observed that these domain names were usually created within a few days before the networks were hijacked. This shows that attackers, very likely, control the entire IP address blocks and take full advantage of them.



- *Figure 3: Correlation between BGP announcements, spam emails, and blacklisted spam sources related to hijacked IP address ranges*

What about those not used for sending spam?

While examining hijacks that did not send spam to Symantec.cloud, we uncovered an intriguing phenomenon. This phenomenon is significant since it includes 2,562 short-lived hijacks, representing 97.8 percent of all short-lived hijacks identified. Figure 4 depicts a sample of 87 (out of 2,562) hijacks that occurred in June 2014 and shows that:

- All hijacks are actually performed by groups of two to four prefixes, starting and ending at the same time.
- During the 13-month period there were always, at any point in time, at least two IP prefixes hijacked.

Although only part of the phenomenon is depicted, it is recurrent and persistent over the complete year of 2014. This strongly indicates that the hijacks may have been performed with the same modus operandi. The fact that some groups of hijacks start only seconds after the end of previous groups further suggests that they might be carried out in an automated way, possibly also relying on some automated process to find target network address blocks to hijack.

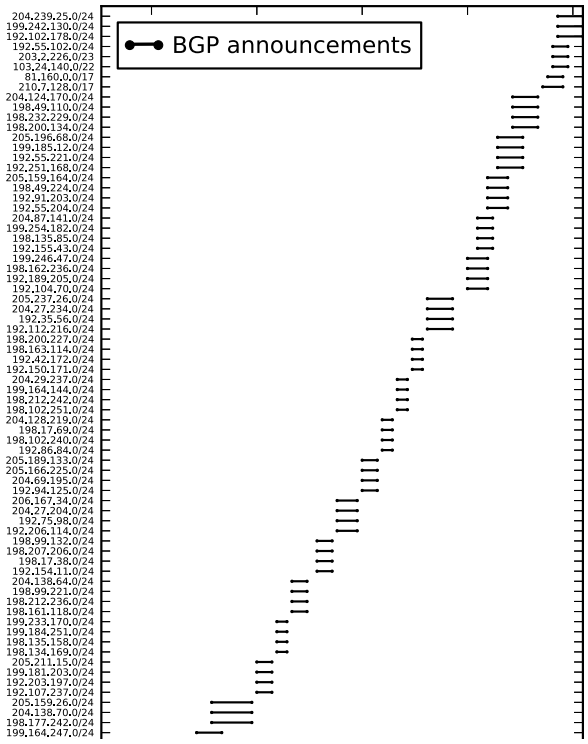


Figure 4: Intriguing hijack phenomenon in which hijacks are performed by groups of at least two IP prefixes (for the sake of conciseness, only a sample of 87 [out of 2,562] IP address ranges hijacked in June 2014 are depicted)

How many attackers are we facing?

While identifying malicious BGP hijacks is an important first step in the mitigation of these attacks, we wanted to gain more insight into the cybercriminal organizations behind such sophisticated attacks. In particular, we wanted to determine whether we could observe spammers repeatedly hijacking blocks of IP addresses for a short period of time to send spam using these hijacked (or stolen) IP addresses. We leveraged Symantec's advanced TRIAGE data analytics technology to identify spam campaigns launched from the 64 hijacked networks that sent spam to Symantec. cloud spam traps. We applied TRIAGE to the approximately 5,000 spam emails sent from hijacked networks. TRIAGE identified 30 different spam campaigns, from which we uncovered three key modi operandi of hijacking spammers: (i) 10 campaigns (out of 30) involved a single hijacked IP prefix that was not abused elsewhere in any other campaign; (ii) 17 campaigns involved a single hijacked IP prefix, yet the hijacked prefix was abused concurrently in different spam campaigns; and (iii) three campaigns were observed abusing multiple hijacked IP prefixes sequentially over a longer period of time. While the first two phenomena actually confirmed our intuition about the behavior of this class of spammers, the latter phenomenon is the most interesting, as it confirms the existence of BGP spectrum agility in the form of campaigns of BGP hijacks orchestrated by the same spammers. Indeed, it highlights the existence of a more agile and sophisticated modus operandi of spammers capable of hijacking and abusing multiple IP prefixes, and subsequently hopping from one hijacked IP prefix to another to distribute spam. This agility enables them to send spam in a stealthier manner and thus stay undetected "under the radar."

The graph in Figure 5 describes a campaign of spam emails sent from network IP address blocks that have been hijacked (or stolen) from their legitimate owner.[22] It illustrates the BGP spectrum agility phenomenon,[23] in which spammers temporarily hijack blocks of IP addresses to send spam. By repeatedly hijacking new blocks of IP addresses and sending spam from them for a short period of time, they manage to circumvent IP blacklists. We can distinguish in the figure below the 12 different hijacked IP address blocks (yellow nodes) involved in this spam campaign. Over 660 spam emails were sent from these network blocks. Each of them was used to distribute spam using a large number of one-time URLs, with most of them including domain names (blue nodes) registered at ENOM (large pink node) and using privacy-protected email addresses provided by whoisprivacyprotect.com (red nodes). The spam-advertised content (domain URLs) was hosted on one of the six shared server IP addresses (light gray nodes). The campaign had a lifetime of 84 days, with only 24 active days (purple nodes laid out in a clockwise fashion) during which spammers were hopping from one hijacked IP prefix to another, in an effort to circumvent IP-based spam filters and reputation systems.

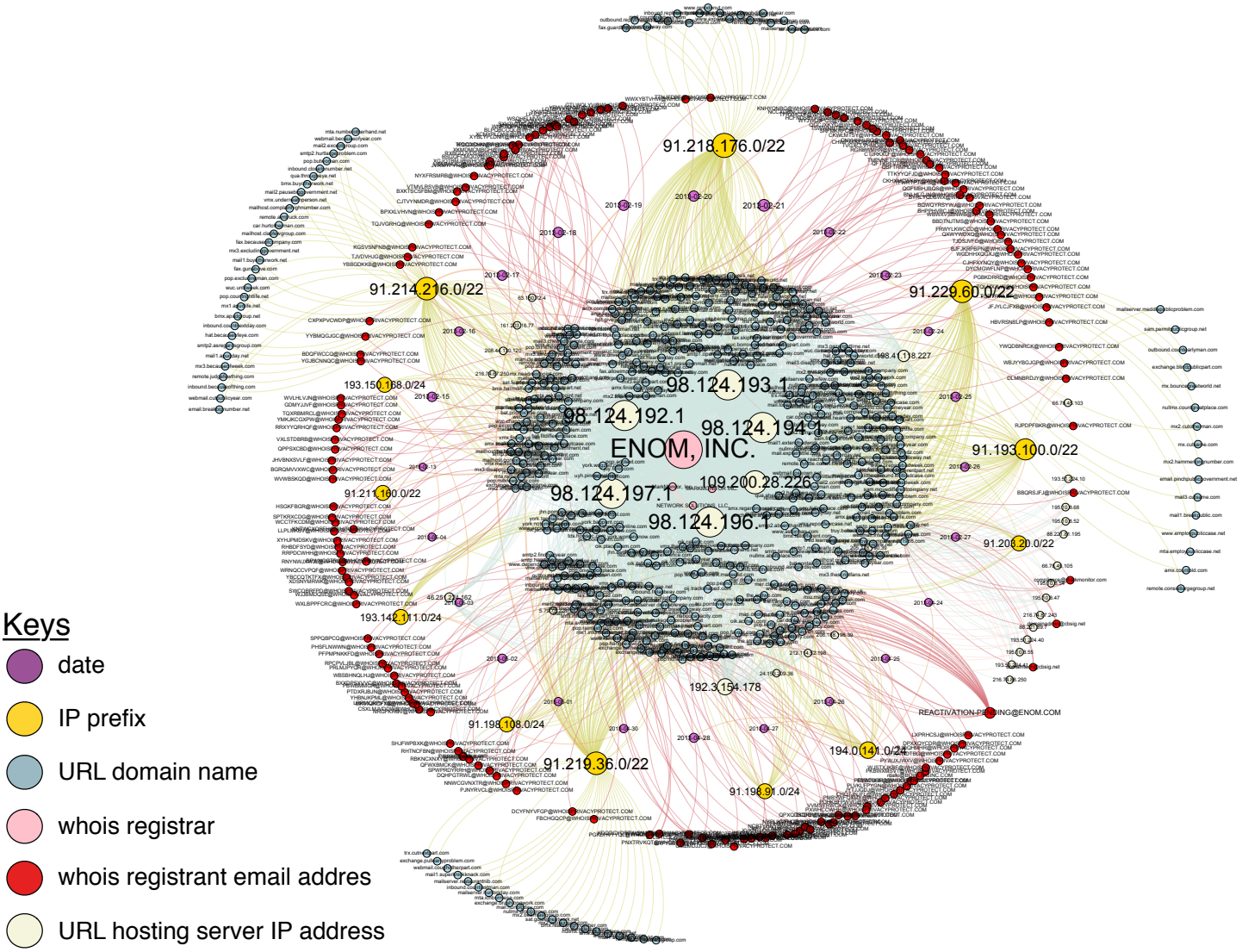


Figure 5: An example of a large-scale spam campaign involving multiple hijacked IP prefixes (the nodes are laid out in a clockwise fashion to reflect the timeline of the campaign)

Effectiveness of countermeasures?

BGP hijacking is a well-known attack against the Internet routing infrastructure. Recently, network operators have started to adopt and deploy a framework, commonly referred to as RPKI, meant to secure BGP and prevent address hijacking. RPKI works as a security extension to the routing protocol (BGP) by ensuring the authenticity and integrity of the messages exchanged between networks (ASes) using cryptography. The framework is divided into two modules that would prevent any hijacking attack. However, the first module protects BGP against prefix hijacks only, which accounted for 92 percent of the hijacks identified by Symantec in 2014. While the first module is already being deployed, it has been adopted by only about 4 percent of the Internet. The second module (BGPsec), which is required to mitigate AS hijacks (8 percent of the identified hijacks in 2014), is not yet being deployed and has not even been standardized yet.

Interestingly we found that none of the 2,655 hijacks we identified were detected by the RPKI system. The adoption and deployment of the first RPKI module by all networks on the Internet could have prevented no less than 2,442 (92 percent) hijacks.

Conclusion

It has been more than two years since our first report of malicious BGP hijacking attacks being carried out by cybercriminals on the Internet. In 2014 the scale and prevalence of these attacks reached unprecedented levels, with more than 2,000 confirmed attacks (up 875 percent compared with 2013). Using SpamTracer, a system developed within Symantec Research Labs, we have documented the existence of persistent and stealthy campaigns of malicious BGP hijacks. We have also shown that today's BGP hijack mitigation systems, such as the RPKI system, are easily defeated by the sophisticated hijack attacks we've observed. By identifying confirmed cases of spammers performing BGP hijacks to send spam from stolen networks, we also confirmed the increased prevalence of sophisticated spammers willing to remain stealthy and hinder their traceability. We found that all network IP address blocks we identified as having been hijacked were dormant blocks (that is, they were not publicly announced by their legitimate owner when they were hijacked). As of today, as much as 20 percent of the all the available IPv4 addresses are currently allocated to some organization but not publicly announced, which makes them potentially vulnerable to such malicious BGP hijacks.

Disclaimer

In this article, for the sake of conciseness, we discuss hijacks and attackers instead of candidate hijacks and likely attackers even though we have no bulletproof evidence of their wrongdoing. IP address blocks and ASes were likely abused in hijacks between January 2014 and December 2014 and, therefore, might now be legitimately used.

APPENDIX D: VULNERABILITY TRENDS

Appendix D: Vulnerability Trends

Vulnerability Trends

A vulnerability is a weakness that allows an attacker to compromise the availability, confidentiality, or integrity of a computer system. Vulnerabilities may be the result of a programming error or a flaw in the design that will affect security.

Vulnerabilities can affect both software and hardware. It is important to stay abreast of new vulnerabilities being identified in the threat landscape because early detection and patching will minimize the chances of being exploited. This section discusses selected vulnerability trends, providing analysis and discussion of the trends indicated by the data.

The following metrics are included:

- Total Number of Vulnerabilities
- Zero-Day Vulnerabilities
- Web Browser Vulnerabilities
- Web Browser Plug-In Vulnerabilities
- ICS Vulnerabilities

Total Number of Vulnerabilities

Background

The total number of vulnerabilities for 2014 is based on research from independent security experts and vendors of affected products. The yearly total also includes zero-day vulnerabilities that attackers uncovered and that were subsequently identified post-exploitation. The Symantec DeepSight Intelligence vulnerability database tracks vulnerabilities reported in major, well-known applications that are in common business use and in applications that customers have specifically requested be tracked. For example, DeepSight does not track vulnerabilities in all open-source projects and consumer products, such as video games.

Symantec gathers information on all of these vulnerabilities as part of its DeepSight vulnerability database and alerting services. Examining these trends also provides further insight into other topics discussed in this report. Calculating the total number of vulnerabilities provides insight into vulnerability research being conducted in the threat landscape. There are many motivations for conducting vulnerability research, including security, academic, promotional, and software quality assurance, as well as, of course, the malicious motivations that drive attackers.

Discovering vulnerabilities can be advantageous to both sides of the security equation. Legitimate researchers may learn how better to defend against attacks by analyzing the work of attackers who uncover vulnerabilities; conversely, cybercriminals can capitalize on the published work of legitimate researchers to advance their attack capabilities. The vast majority of vulnerabilities that are exploited by attack toolkits are publicly known by the time they are exploited.

Methodology

Information about vulnerabilities is made public through a number of sources. These include mailing lists, vendor advisories, and detection in the wild. Symantec gathers this information and analyzes various characteristics of the vulnerabilities, including technical information and ratings, in order to determine the severity and impact of the vulnerabilities. This information is stored in the DeepSight vulnerability database, which houses approximately 66,400 distinct vulnerabilities spanning a period of over 20 years, from more than 21,300 vendors representing over 62,300 products.

As part of the data gathering process, Symantec scores the vulnerabilities according to version 2.0 of the community-based Common Vulnerability Scoring System (CVSS).[24] Symantec adopted version 2.0 of the scoring system in 2008. The total number of vulnerabilities is determined by counting all of the vulnerabilities published during the reporting period.

All vulnerabilities are included, regardless of severity or whether or not the vendor that produced the vulnerable product confirmed them.

Year	Total Number of Vulnerabilities
2014	6,549
2013	6,787
2012	5,291
2011	4,989
2010	6,253
2009	4,814
2008	5,562
2007	4,644
2006	4,842

Total Vulnerabilities Identified, 2006–2014

Source: Symantec

Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2014	591	556	568	528	601	445	447	625	619	471	617	481	6,549
2013	565	515	695	481	582	547	607	493	598	658	579	467	6,787

Total Vulnerabilities Month by Month, 2013–2014

Source: Symantec

Commentary

- The actual number of new vulnerabilities reported is down, and the trend is still up: The total number of new vulnerabilities reported in 2014 stood at 6,549. This figure amounts to approximately 126 new vulnerabilities a week. Compared with the 6,787 new vulnerabilities reported in 2013, it represents a decrease of 4 percent, yet the overall trend is still on an upward trajectory.
- One thing to note is that websites hosting malicious toolkits often contain multiple exploits that can be tried against the visitor. In some cases, the kit will attempt to use all exploits at its disposal in a non-intelligent fashion, whereas in more modern advanced kits, the website code will attempt to fingerprint the software installed on the computer before deciding which exploit(s) to send to maximize the success rate.

Zero-Day Vulnerabilities

Background

Zero-day vulnerabilities are vulnerabilities against which the vendor has not released a patch. The absence of a patch for a zero-day vulnerability presents a threat to organizations and consumers alike, because in many cases this type of threat can evade purely signature-based detection until a patch is released. The unexpected nature of zero-day threats is a serious concern, especially because they may be used in targeted attacks and in the propagation of malicious code.

Methodology

Zero-day vulnerabilities are a subset of the total number of vulnerabilities documented over the reporting period. A zero-day vulnerability is one that appears to have been exploited in the wild prior to being publicly known. It may not have been known to the affected vendor prior to exploitation, and at the time of the exploit activity, the vendor had not released a patch. The data for this section consists of the vulnerabilities that Symantec has identified that meet the above criteria.

Year	Count
2014	24
2013	23
2012	14
2011	8
2010	14
2009	12
2008	9
2007	15
2006	13

Volume of Zero-Day Vulnerabilities, 2006–2014

Source: Symantec

CVE Identifier	Description
CVE-2014-0493	Adobe Acrobat And Reader CVE-2014-0493 Remote Code Execution Vulnerability
CVE-2014-0495	Adobe Acrobat and Reader CVE-2014-0495 Remote Code Execution Vulnerability
CVE-2014-0496	Adobe Acrobat And Reader CVE-2014-0496 Remote Code Execution Vulnerability
CVE-2014-0491	Adobe Flash Player And AIR CVE-2014-0491 Remote Security Bypass Vulnerability
CVE-2014-0492	Adobe Flash Player and AIR CVE-2014-0492 Information Disclosure Vulnerability
CVE-2014-0497	Adobe Flash Player CVE-2014-0497 Remote Code Execution Vulnerability
CVE-2014-0322	Microsoft Internet Explorer CVE-2014-0322 Use-After-Free Remote Code Execution Vulnerability
CVE-2013-7331	Microsoft XMLDOM ActiveX Control Multiple Information Disclosure Vulnerabilities
CVE-2014-0502	Adobe Flash Player and AIR CVE-2014-0502 Remote Code Execution Vulnerability
CVE-2014-0502	Adobe Flash Player and AIR CVE-2014-0502 Remote Code Execution Vulnerability
CVE-2014-0498	Adobe Flash Player and AIR CVE-2014-0498 Remote Stack Overflow Vulnerability
CVE-2014-0324	Microsoft Internet Explorer CVE-2014-0324 Memory Corruption Vulnerability
CVE-2014-1761	Microsoft Word CVE-2014-1761 Remote Memory Corruption Vulnerability
CVE-2014-1776	Microsoft Internet Explorer CVE-2014-1776 Remote Code Execution Vulnerability
CVE-2014-0515	Adobe Flash Player CVE-2014-0515 Buffer Overflow Vulnerability
CVE-2014-0517	Adobe Flash Player and AIR CVE-2014-0517 Unspecified Remote Security Bypass Vulnerability
CVE-2014-0518	Adobe Flash Player and AIR CVE-2014-0518 Unspecified Remote Security Bypass Vulnerability
CVE-2014-0520	Adobe Flash Player and AIR CVE-2014-0520 Unspecified Remote Security Bypass Vulnerability
CVE-2014-0519	Adobe Flash Player and AIR CVE-2014-0519 Unspecified Remote Security Bypass Vulnerability
CVE-MAP-NOMATCH	Linux Kernel 'ptrace' Function Call Local Privilege Escalation Vulnerability
CVE-2014-0546	Adobe Acrobat and Reader CVE-2014-0546 Unspecified Security Bypass Vulnerability
CVE-2014-4114	Microsoft Windows CVE-2014-4114 OLE Package Manager Remote Code Execution Vulnerability
CVE-2014-6352	Microsoft Windows CVE-2014-6352 OLE Remote Code Execution Vulnerability
CVE-2014-9163	Adobe Flash Player CVE-2014-9163 Unspecified Stack Based Buffer Overflow Vulnerability

Zero-Day Vulnerabilities Identified in 2014

Source: Symantec

Commentary

With 24 new zero-day vulnerabilities disclosed in 2014, this represents the highest number since 2006.

- There was a 4 percent increase in vulnerabilities in 2014 compared with 2013. However, the number of vulnerabilities in 2014 was magnified due to an increase in the number of published vulnerabilities for Adobe products. In 2014 there were 14 Adobe-related vulnerabilities, compared with seven in 2013.
- As the number of zero-day vulnerabilities increased, attacks using these vulnerabilities were also on the rise. Some of these vulnerabilities were leveraged in targeted attacks, through the use of watering-hole-based attacks. Adobe Flash Player and Microsoft Windows ActiveX Control vulnerabilities were widely used in such targeted attacks, and Microsoft-related products and technologies accounted for more than a third of the zero-day vulnerabilities disclosed in 2014.
- Many attack scenarios were planned in such a way that an attacker would craft a malicious webpage to exploit the vulnerability, and email or other similar means would be used to entice unsuspecting users to visit it. Once the page was viewed, the attacker-supplied malicious code would potentially be run undetected.

Web Browser Vulnerabilities

Background

Web browsers are ubiquitous components for both enterprise and individual users on desktop and mobile devices. Vulnerabilities in web browser are a serious security concern due to their role in online fraud and in the propagation of malicious code, spyware, and adware. In addition, web browsers are exposed to a greater amount of potentially untrusted or hostile content than are most other applications and are particularly targeted by multi-exploit attack kits.

Web-based attacks can originate from malicious websites and from legitimate websites that have been compromised to serve malicious content. Some content, such as media files or documents, are often presented in browsers via browser plug-in technologies. While browser functionality is extended by the inclusion of various plug-ins, the addition of a plug-in component also results in a wider potential attack surface for client-side attacks.

Methodology

Browser vulnerabilities are a subset of the total number of vulnerabilities cataloged by Symantec throughout the year. To determine the number of vulnerabilities affecting browsers, Symantec considers all vulnerabilities that have been publicly reported, regardless of whether they have been confirmed by the vendor. While vendors do confirm the majority of browser vulnerabilities that are published, not all vulnerabilities may have been confirmed at the time of writing. Vulnerabilities that are not confirmed by a vendor may still pose a threat to browser users and are therefore included in this study.

This metric examines the total number of vulnerabilities affecting the following popular web browsers:

- Apple Safari
- Google Chrome
- Microsoft Internet Explorer
- Mozilla Firefox
- Opera

Year	Apple Safari	Google Chrome	Microsoft Internet Explorer	Mozilla Firefox	Opera	Total
2014	86	155	282	109	7	639
2013	54	219	148	157	13	591
2012	343	268	60	186	34	891

Browser Vulnerabilities, 2012–2014

Source: Symantec

Commentary

- Five popular browsers had 639 reported vulnerabilities in total in 2014, which is a slight increase from 591 in 2013. This is due to a reduction in the number of disclosed vulnerabilities for Chrome, Firefox, and Opera.

Web Browser Plug-In Vulnerabilities

Background

This metric examines the number of vulnerabilities affecting plug-ins for web browsers. Browser plug-ins are technologies that run inside the web browser and extend its features, such as allowing additional multimedia content from webpages to be rendered. Although plug-ins are often run inside the browser, some vendors have started to use sandbox containers to execute plug-ins in order to limit the potential harm of vulnerabilities. Unfortunately, web browser plug-ins continue to be one of the most exploited vectors for web-based attacks and drive-by downloads that silently infect consumer and enterprise users.

Many browsers now include various plug-ins in their default installation and also provide a framework to ease the installation of additional plug-ins. Plug-ins now provide much of the expected or desired functionality of web browsers and are often required in order to use many commercial sites. Vulnerabilities affecting plug-ins are an increasingly favored vector for a range of client-side attacks, and the exploits targeting these vulnerabilities are commonly included in attack kits. Web attack kits can exploit many different browser and browser plug-in vulnerabilities at one time, enabling full access to download any malware to affected computers.

Some plug-in technologies include automatic update mechanisms that aid in keeping software up to date, which may aid in limiting exposure to certain vulnerabilities. Enterprises that choose to disable these updating mechanisms, or continue to use vulnerable out-of-date versions, will continue to put their organizations at considerable risk of silent infection and exploitation. Through a variety of drive-by web attacks, exploits against browser plug-in vulnerabilities continue to be a favored infection vector for hackers and malware authors to breach enterprises and consumer systems. To help mitigate the risk, some browsers have started to check for the version of installed third-party plug-ins and inform the user if there are any updates available for install. Enterprises should also check to determine whether every browser plug-in is needed and consider removing or disabling potentially vulnerable software.

Methodology

Web browser plug-in vulnerabilities comprise a subset of the total number of vulnerabilities cataloged by Symantec over the reporting period. The vulnerabilities in this section cover the entire range of possible severity ratings and include those that are both unconfirmed and confirmed by the affected product's vendor. Confirmed vulnerabilities consist of security issues that the vendor has publicly acknowledged, either by releasing an advisory or otherwise making a public statement to concur that the vulnerability exists. Unconfirmed vulnerabilities are vulnerabilities that are reported by third parties—usually security researchers—and have not been publicly confirmed by the vendor. That a vulnerability is unconfirmed does not mean that the vulnerability report is not legitimate but only that the vendor has not released a public statement confirming the existence of the vulnerability.

Symantec identified the following popular browser plug-ins as having the most reported vulnerabilities in 2014:

- Adobe Reader
- Adobe Flash Player
- Apple QuickTime
- Microsoft ActiveX
- Mozilla Firefox extensions
- Oracle Sun Java Platform, Standard Edition (Java SE)

Year	Adobe Acrobat Reader	Adobe Flash	Active X	Apple QuickTime	Firefox Extension	Oracle Sun Java	Total
2014	46	76	72	23	0	119	**336**
2013	68	56	54	13	0	184	375

Browser Plug-In Vulnerabilities, 2013–2014

Source: Symantec

Commentary

- In 2014, 336 vulnerabilities affecting browser plug-ins were documented by Symantec, a decrease compared with the 375 vulnerabilities in 2013.
- The number of published Java vulnerabilities decreased significantly in 2014. This caused the reduction seen in the total count for 2014.

ICS Vulnerabilities

Background

This metric examines all the vulnerabilities with industrial control systems (ICS) technologies. ICS is a general term that encompasses several types of control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and other smaller control system configurations such as programmable logic controllers (PLCs) often found in the industrial sectors and in critical infrastructure. ICSs are typically used in industries such as electrical, water, oil, and gas. Based on data received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices.

SCADA represents a wide range of protocols and technologies for monitoring and managing equipment and machinery in various sectors of critical infrastructure and industry. This includes, but is not limited to, power generation, manufacturing, oil and gas, water treatment, and waste management. The security of SCADA technologies and protocols is a national security concern because the disruption of related services can result in, among other things, the failure of infrastructure and potential loss of life.

Methodology

This discussion is based on data surrounding publicly known vulnerabilities affecting ICS technologies. Due to the potential for disruption of critical infrastructure services, these vulnerabilities may be associated with politically motivated or state-sponsored attacks, representing a concern for both governments and enterprises involved in the sector. While this metric provides insight into public ICS/SCADA vulnerability disclosures, due to the sensitive nature of vulnerabilities affecting critical infrastructure it is likely that private security research is conducted by ICS technology and security vendors. Symantec does not have insight into any private research because the results of such research are not publicly disclosed.

BID	Title	Published
64941	Multiple WellinTech Products ActiveX Remote Code Execution Vulnerability	January 14, 2014
64938	Multiple WellinTech Products Information Disclosure Vulnerability	January 14, 2014
64972	Ecava IntegraXor Stack Buffer Overflow Vulnerability	January 16, 2014
65262	Schneider Electric Telvent SAGE 3030 RTUs Remote Denial of Service Vulnerability	January 30, 2014
65337	Rockwell Automation RSLogix 5000 CVE-2014-0755 Security Bypass Vulnerability	February 4, 2014
65635	Multiple Schneider Electric Products Remote Denial of Service Vulnerability	February 18, 2014
65706	Iconics GENESIS32 ActiveX Control CVE-2014-0758 Remote Code Execution Vulnerability	February 20, 2014
66500	Multiple Schneider Electric Products Stack Buffer Overflow Vulnerability	March 27, 2014
66554	Ecava IntegraXor Account Information Disclosure Vulnerability	April 1, 2014
66709	WellinTech KingSCADA CVE-2014-0787 Stack-Based Buffer Overflow Vulnerability	April 8, 2014
66732	Advantech WebAccess CVE-2014-0768 Stack-Based Buffer Overflow Vulnerability	April 8, 2014
66742	Advantech WebAccess CVE-2014-0773 Security Bypass Vulnerability	April 8, 2014
66722	Advantech WebAccess CVE-2014-0765 Stack Based Buffer Overflow Vulnerability	April 8, 2014
66740	Advantech WebAccess CVE-2014-0763 SQL Injection Vulnerability	April 8, 2014
66725	Advantech WebAccess CVE-2014-0766 Stack-Based Buffer Overflow Vulnerability	April 8, 2014
66728	Advantech WebAccess CVE-2014-0767 Stack-Based Buffer Overflow Vulnerability	April 8, 2014
66750	Advantech WebAccess CVE-2014-0771 Information Disclosure Vulnerability	April 8, 2014
66718	Advantech WebAccess CVE-2014-0764 Stack-Based Buffer Overflow Vulnerability	April 8, 2014
66733	Advantech WebAccess CVE-2014-0770 Stack-Based Buffer Overflow Vulnerability	April 8, 2014
66749	Advantech WebAccess CVE-2014-0772 Information Disclosure Vulnerability	April 8, 2014
66934	Progea Movicon CVE-2014-0778 Information Disclosure Vulnerability	April 15, 2014
67056	InduSoft Web Studio CVE-2014-0780 Directory Traversal Vulnerability	April 24, 2014
68717	Advantech WebAccess CVE-2014-2366 Remote Information Disclosure Vulnerability	July 15, 2014
68716	Advantech WebAccess CVE-2014-2367 Remote Authentication Bypass Vulnerability	July 15, 2014
68718	Advantech WebAccess CVE-2014-2365 Remote Code Execution Vulnerability	July 18, 2014
68715	Advantech WebAccess CVE-2014-2368 Unsafe ActiveX Control Remote Security Weakness	July 18, 2014
68714	Advantech WebAccess CVE-2014-2364 Multiple Remote Stack Based Buffer Overflow Vulnerabilities	July 18, 2014
68872	Siemens SIMATIC WinCC and PCS 7 CVE-2014-4685 Local Privilege Escalation Vulnerability	July 23, 2014
68880	Siemens SIMATIC WinCC and PCS7 Database Server Remote Privilege Escalation Vulnerability	July 23, 2014
68875	Siemens SIMATIC WinCC and PCS7 CVE-2014-4686 Privilege Escalation Vulnerability	July 23, 2014
68879	Siemens SIMATIC WinCC And PCS7 CVE-2014-4683 Remote Privilege Escalation Vulnerability	July 23, 2014
68876	Siemens SIMATIC WinCC And PCS7 WebNavigator Server Information Disclosure Vulnerability	July 24, 2014
70193	Multiple Schneider Electric Products CVE-2014-2732 Directory Traversal Vulnerability	September 30, 2014
71239	Multiple Siemens Products CVE-2014-8551 Remote Code Execution Vulnerability	November 21, 2014
71240	Multiple Siemens SIMATIC Products CVE-2014-8552 Information Disclosure Vulnerability	November 21, 2014

ICS Vulnerabilities, 2014

Source: Symantec

Commentary

- The number of ICS vulnerabilities increased slightly in 2014, with 35 publicly disclosed vulnerabilities, compared with the 39 vulnerabilities disclosed in 2013.

APPENDIX E: GOVERNMENT THREAT ACTIVITY TRENDS

Appendix E: Government Threat Activity Trends

Government Threat Activity Trends

The following section of the Symantec Internet Security Threat Report for Government provides an analysis of threat activity trends relating to government and critical infrastructure protection (CIP), including malicious activity that Symantec observed in 2014.

Attacks are defined as any malicious activities carried out over a network that has been detected by an intrusion detection system (IDS) or firewall. Definitions for the other types of malicious activities can be found in their respective sections within this report.

This section will discuss the following metrics, providing analysis and discussion of the trends indicated by the data:

- Malicious Activity by Critical Infrastructure Sector
- Sources of Origin for Government-Targeted Attacks
- Attacks by Type—Notable Critical Infrastructure Sectors

Malicious Activity by Critical Infrastructure Sector

Background

This metric indicates the level to which government and critical infrastructure organizations may have been compromised and are being used by attackers as launching pads for malicious activity. These attacks could potentially expose sensitive and confidential information, which could have serious ramifications for government and critical infrastructure organizations. Such information could be used for strategic purposes in the case of state- or group-sponsored attacks, especially since attackers who use compromised computers for malicious activity can mask their actual location.

Methodology

This metric evaluates the amount of malicious activity originating from computers and networks that are known to belong to government and critical infrastructure sectors. To measure this, Symantec cross-referenced the IP addresses of known malicious computers with Standard Industrial Classification (SIC) codes[25] that are assigned to each industry and provided by a third-party service.[26] Symantec has compiled data on numerous malicious activities that were detected originating from the IP address space of these organizations. These activities include bot-infected computers, phishing hosts, spam zombies, and network attack origins.

Industry Sector	% of CIP Source Activity	% of CIP Source IP Addresses
Financial Services	52.8%	1.9%
Manufacturing	45.1%	96.3%
Government	0.6%	0.6%
Government–State	0.6%	0.6%
Internet Service Provider	0.5%	0.6%
Utilities/Energy	0.2%	0.01%
Telecommunications	0.1%	0.01%
Transportation	0.1%	0.0002%
Health Care	0.07%	0.02%
Government–National	0.01%	0.02%
Government–Local	0.000005%	0.00001%

Malicious Activity by Critical Infrastructure Sector
Source: Symantec

Commentary

- Financial services was the top sector for malicious activity: The financial services sector was the origin of the most malicious activity in 2014, accounting for 52.8 percent of attacks and 1.9 percent of source IP addresses originating from CIP networks.

Sources of Origin for Government-Targeted Attacks

Background

Attacks targeting government organizations may serve as a means of expressing disagreement with policies and programs that the government has developed and implemented. Such attacks are likely to be carried out for a variety of purposes, including blocking access to government Internet-based resources, gaining access to potentially sensitive information, and discrediting the government itself. In addition, attacks may be motivated by espionage and attempts to steal government-classified information. These attacks may result in the disruption of critical services, as with denial-of-service (DoS) attacks, or the exposure of highly sensitive information. An attack that disrupts the availability of a high-profile government organization website will get much wider notice than one that takes a single user offline. In addition, malicious code attacks targeting governments can be motivated by profit because governments store considerable amounts of personal identification data that could be used for fraudulent purposes, such as identity theft. Personal data can include names, addresses, government-issued identification numbers, and bank account credentials, all of which can be effectively exploited for fraud by attackers. Government databases also store information that could attract politically motivated attacks, including critical infrastructure information and other sensitive intelligence.

Methodology

This metric will assess the top sources of origin of government-targeted attacks by determining the location of computers from which the attacks occurred. It should be noted that attackers often attempt to obscure their tracks by redirecting attacks through one or more servers that may be located anywhere in the world; thus, the attacker may be located somewhere other than where the attacks appear to originate.

Geography	% of Source Activity	% of Source IP Addresses
United States	61.19%	18.70%
China	19.94%	60.91%
Netherlands	8.20%	4.09%
Germany	1.92%	1.24%
France	1.72%	1.04%
Korea, South	1.50%	3.83%
United Kingdom	1.45%	1.28%
Russia	1.40%	4.03%
Australia	1.38%	1.48%
Taiwan	1.31%	3.40%

Sources of Origin of Government-Targeted Attacks

Source: Symantec

Commentary

- The United States and China remained the top two sources of origin of attacks that targeted the government sector in 2014.
- The high ranking in this metric of these two countries reflects the fact that they were also the top two sources of origin of all Internet-wide network attacks globally, with the highest populations of Internet-connected users worldwide.

Attacks by Type—Notable Critical Infrastructure Sectors

Background

This section of the Symantec Internet Security Threat Report for Government focuses on the types of attacks detected by sensors deployed in notable critical infrastructure sectors. Government and critical infrastructure organizations are the target of a wide variety of attack types. The ability to identify attacks by type assists security administrators in evaluating which assets may be targeted and may assist them in ensuring that assets receiving a disproportionate number of attacks are made secure.

The following sectors will be discussed in detail:

- Government
- Biotech/pharmaceutical
- Healthcare
- Financial services
- Transportation
- Telecommunications
- Utilities

Methodology

The following types of attacks are considered for this metric:

- Attacks on web servers: Web servers facilitate a variety of services for government and critical infrastructure sectors, such as hosting publicly available information, customer support portals, and online stores. Some web servers also host remotely accessible interfaces that employees use to perform routine, job-related tasks from remote locations. Furthermore, a web server may be a portal to an organization's internal network and database systems.
- Attacks on web browsers: Web browsers are exposed to a greater amount of potentially untrusted or hostile content than most other applications are. As the Internet has become commonplace for business and leisure activities, there is an increased reliance on browsers and their plug-ins. Attacks on web browsers can originate from not only malicious websites but also legitimate websites that have been compromised to serve malicious content. Browsers can also facilitate client-side attacks because of their use of plug-ins and other applications in handling potentially malicious content served from the web, such as compromised documents and media files.
- Attacks on SMTP (Simple Mail Transfer Protocol): SMTP is designed to facilitate the delivery of email messages across the Internet. Email servers using SMTP as a service are likely to be targeted by attackers because external access is required to deliver email. While most services can be blocked by a firewall to protect against external attacks and allow access only to trusted users and entities, for email to function effectively for organizations, it has to be available both internally and externally to other email servers. The necessity of allowing both internal and external access increases the probability that a successful attack will improve attackers' chances of gaining access to the network.

- DoS attacks: DoS attacks are a threat to government and critical infrastructures because the purpose of such attacks is to disrupt the availability of high-profile websites or other network services and thus make them inaccessible to users and employees. A successful DoS attack could result in the disruption of internal and external communications, making it practically impossible for employees and users to access potentially critical information. Because these attacks often receive greater exposure than those that take a single user offline, especially for high-profile government websites, they could also result in damage to the organization's reputation. A successful DoS attack on a government network could also severely undermine confidence in government competence and impair the defense and protection of government networks.
- Backscatter: Generally, backscatter is considered to be a type of Internet background noise, which is typically ignored. While not a direct attack, backscatter is evidence that a DoS attack against another server on the Internet is taking place and is making use of spoofed IP addresses. When one of these spoofed IP addresses matches the address of a Symantec sensor, any error messages that the attacked server sends to the spoofed address will be detected by a Symantec sensor as backscatter.
- Shellcode/exploit attacks: Shellcode is a small piece of code used as the payload in the exploitation of a vulnerability. An attacker can exploit a vulnerability to gain access to a system, inject this code, and use a command shell to take control of a compromised machine. By remotely controlling a compromised system, an attacker can gain access to an organization's network and, from there, perpetrate additional attacks. Moreover, this type of attack can monopolize valuable resources that may be critical to government operations.

Top-10 Attacks	Percent
Web (server)	95.7%
P2P	3.7%
Shellcode/Exploit	0.14%
DoS	0.11%
SMTP (Email)	0.06%
Misc	0.04%
Web (browser)	0.04%
Brute force	0.02%
DNS	0.01%
Backscatter	0.01%

Attacks by Type—Overall Government and Critical Infrastructure Organizations

Source: Symantec

- Web server attacks were the most common type of attack for government and critical infrastructure: In 2014, the most common attack type seen by all sensors in the government and critical infrastructure sectors related to attacks on web servers and accounted for 95.1 percent of all attacks.
- Peer-to-peer (P2P) attacks were the second most common type of attack for government and critical infrastructure, accounting for 2.3 percent of attacks. P2P attacks consist of general ones like DoS, man-in-the-middle, and worm propagation attacks, and specific ones like rational attacks, file poisoning, and so on.
- DoS attacks are often associated with social and political protests since they are intended to render a site inaccessible to legitimate users of those services. Man-in-the-middle attacks are where the attacker inserts himself or herself undetected between two nodes. He can then choose to stay undetected and spy on the communication, or more actively manipulate the communication.
- Shellcode is a small piece of code used as the payload in the exploitation of a software vulnerability. It is called shellcode because it typically starts a command shell from which the attacker can control the compromised machine. Shellcode can either be local or remote, depending on whether it gives an attacker control over the machine it runs on (local) or over another machine through a network (remote).

Top-5 Attacks	Percent
P2P	94.4%
Shellcode/Exploit	1.5%
Web (server)	0.7%
SMTP (Email)	0.6%
Web (browser)	0.3%

Attacks by Type—Government

Source: Symantec

Top-5 Attacks	Percent
P2P	83.7%
Shellcode/Exploit	4.1%
Web (server)	2.7%
DoS	1.6%
SMTP (Email)	1.5%

Attacks by Type—Financial Services

Source: Symantec

Top-5 Attacks	Percent
P2P	71.3%
Brute force	12.9%
Web (server)	3.2%
Shellcode/Exploit	1.6%
DoS	0.4%

Attacks by Type—Healthcare

Source: Symantec

Top-3 Attacks	Percent
Web (server)	53.8%
Brute force	10.3%
DoS	7.7%

Attacks by Type—Transportation

Source: Symantec

Top-4 Attacks	Percent
DoS	56.3%
Web (server)	36.5%
Shellcode/Exploit	7.0%
Web (browser)	0.1%

Attacks by Type—Telecommunications

Source: Symantec

Top-5 Attacks	Percent
DoS	56.6%
Web (browser)	23.8%
Shellcode/Exploit	13.0%
Web (server)	5.4%
SMTP (Email)	0.9%

Attacks by Type—Utilities

Source: Symantec

Top-5 Attacks	Percent
Web (server)	99.9%
Shellcode/Exploit	0.04%
DoS	0.04%
Web (browser)	0.0004%
SMTP (Email)	0.0002%

Attacks by Type—Manufacturing

Source: Symantec

Top-5 Attacks	Percent
Web (server)	46.2%
DNS	20.2%
Web (browser)	13.9%
Shellcode/Exploit	9.5%
SMTP (Email)	6.1%

Attacks by Type—Internet Service Provider

Source: Symantec

- The financial services sector was predominantly targeted by P2P attacks and secondly by shellcode/exploit attacks, whereas the transportation sector was primarily targeted by web server and brute force attacks in 2014.
- P2P attacks became most common in the government and healthcare sectors in 2014, whereas shellcode/exploit attacks were most prevalent in these sectors in 2013.
- DoS attacks dominate the telecommunications and utilities sectors, attempting to disrupt services and communications within them.

Footnotes

01 For more details about Norton Safe Web, please visit http://safeweb.norton.com

02 For more details about Symantec RuleSpace, please visit http://www.symantec.com/theme.jsp?themeid=rulespace

03 http://www.idanalytics.com

04 For example, the Fair and Accurate Credit Transactions Act of 2003 (FACTA) of California. For more on this act, please see: http://www.privacyrights.org/fs/fs6a-facta.htm. Another example is the Health Insurance Portability and Accountability Act of 1996. For more information, see http://www.cms.hhs.gov/HIPAAGenInfo/.

05 http://www.symantec.com/security_response/writeup.jsp?docid=2010-011922-2056-99

06 http://www.symantec.com/security_response/writeup.jsp?docid=2006-011714-3948-99

07 http://www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99

08 CIFS is a file-sharing protocol that allows files and other resources on a computer to be shared with other computers across the Internet. One or more directories on a computer can be shared to allow other computers to access the files within.

09 Because malicious code samples often use more than one mechanism to propagate, cumulative percentages may exceed 100 percent.

10 http://www.vis-sense.eu/

11 Marco Cova, Corrado Leita, Olivier Thonnard, Angelos D. Keromytis, and Marc Dacier. An Analysis of Rogue AV Campaigns. In Proc. of the 13th International Conference on Recent Advances in Intrusion Detection (RAID), 2010.

12 O. Thonnard, M. Dacier. A Strategic Analysis of Spam Botnets Operations. CEAS'11, Perth, WA, Australia, Sep 2011.

13 Jelena Isacenkova, Olivier Thonnard, Andrei Costin, Davide Balzarotti, Aurelien Francillon. Inside the SCAM Jungle: A Closer Look at 419 Scam Email Operations. International Workshop on Cyber Crime (IWCC 2013), IEEE S&P Workshops, 2013.

14 P.-A. Vervier, O. Thonnard, and M. Dacier. Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks. In Proc. of the Network and Distributed System Security (NDSS) Symposium. IEEE, 2015.

15 Olivier Thonnard, Leyla Bilge, Gavin O'Gorman, Seán Kiernan, Martin Lee. Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat. In Proc. of the 15th International Conference on Research in Attacks, Intrusions, and Defenses (RAID), 2012.

16 Symantec Internet Security Threat Report (ISTR), Volume 17, April 2012.

17 Symantec product detections for Microsoft monthly Security Advisories—February 2012. http://www.symantec.com/business/support/index?page=content&id=TECH181344

18 Worm:Win32/Bagle.gen!B. http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=Worm%3aWin32%2fBagle.gen%21C#tab=1

19 http://www.symantec.com/connect/blogs/419-oldest-trick-book-and-yet-another-scam

20 http://www.symantec.com/messaging-gateway/

21 P.-A. Vervier and O. Thonnard. Spamtracer: How Stealthy Are Spammers? In IEEE International TMA Workshop, pages 453–458, 2013.

22 P.-A. Vervier, O. Thonnard, and M. Dacier. Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks. In Network and Distributed System Security (NDSS) Symposium, 2015.

23 A. Ramachandran and N. Feamster. Understanding the Network-Level Behavior of Spammers. In SIGCOMM, pages 291–302, 2006.

24 http://www.first.org/cvss/cvss-guide.html

25 SIC codes are the standard industry codes that are used by the United States Securities and Exchange Commission to identify organizations belonging to each industry. For more on this, please see http://www.sec.gov/

26 http://www.digitalenvoy.net/

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings – anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenues of $6.7 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

More Information

- Symantec Worldwide: http://www.symantec.com/
- ISTR and Symantec Intelligence Resources: http://www.symantec.com/threatreport/
- Symantec Security Response: http://www.symantec.com/security_response/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/
- Norton Cybercrime Index: http://us.norton.com/cybercrimeindex/

Symantec Corporation World Headquarters

350 Ellis Street

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com

For specific country offices
and contact numbers,
please visit our website.
For product information in the U.S.,
call toll-free 1 (800) 745 6054.

04/15 21347926