



CASE STUDY

Reducing Fraud and Protecting Citizen Info

OVERVIEW

How Shape Stopped Targeted and Highly Sophisticated Attacks

The US Government serves over 100 million households and processes over \$2T in payment and benefits. Cyber criminals view government agencies as prime targets for large-scale automated attacks. Using credentials stolen from other websites, attackers use automation to test out large numbers of usernames and passwords with the aim of taking over citizen accounts and stealing valuable information and assets.

Cyber criminals using automated techniques and stolen credentials were able to take over half of the accounts they targeted at one US government agency. Even though the agency authenticated

website visitors by challenging them with a series of questions, based on information that was supposed to be only uniquely available to the agency, and that only the account holder should be able to answer, the cyber.

The government agency under attack needed a new approach to fight fraud and deployed the Shape Solution. Using Shape, the government agency stopped the account takeover attacks within 2 days of deploying Shape counter measures and going into full blocking mode thereby preventing hundreds of millions in cyber-fraud.

GOVERNMENT AGENCY

100M
households

300M+
citizens

\$2T
in benefits
and payments

**Loss of confidence
in ability to protect
citizen information**

ACCOUNT TAKEOVER ATTEMPTS

- Attackers compromised extensive multi-step authentication process.
- Stolen passwords and personal information combined with intelligent algorithms to guess answers to authentication questions.
- Millions of account takeovers attempted.

**Hundreds of thousands
of account takeovers**

SHAPE SOLUTION

- Eliminated all account hijacking and saved tens of millions of dollars.
- Blocked malicious bots & automated attacks.
- Protected citizen information.

**Millions of dollars in
cyber fraud avoided**

With full sets of stolen credentials available for purchase on darknets for as little as \$5, automation makes large-scale credential stuffing attacks economically feasible.

WHY SHAPE?

The US Government Agency evaluated anti-automation options and chose Shape Security for the company's ability to effectively and transparently stop unwanted automation at the agency's operational scale. The agency must meet citizen demands for technology that is backward compatible with legacy web applications and also comply with regulations related to accessibility. Shape's implementation team has deep skills in browser technologies and was able to work closely with the agency's security team to test and verify backward compatibility.

SHAPE DEPLOYMENT AND DEFENSE IMPLEMENTATION

Phase 1

Reconfigured application delivery controllers to route hardened pages through the ShapeShifter and validate traffic flows.

Phase 2

Began telemetry by Shape Security-as-a-Service and activated supervised and unsupervised learning by Shape Threat Intelligence team. Developed Shape countermeasures based on gathered data.

Phase 3

Activated Shape countermeasures in a non-blocking mode to verify countermeasure efficacy and browser compatibility.

Phase 4

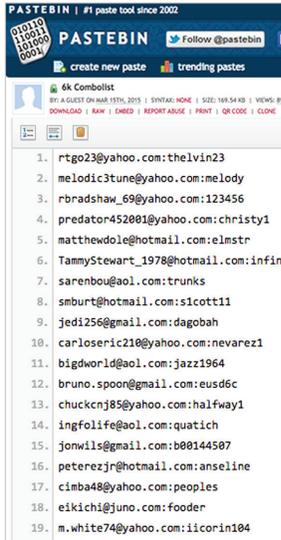
Put Shape service into production and began blocking unwanted automation.

SHAPE SOLUTION BENEFITS

- Dramatically reduced account takeovers and associated cyber-fraud.
- Reduced fraud losses as cyber-attackers abandoned account takeover attempts once Shape began blocking unwanted automated traffic.
- Met accessibility requirements (that precluded use of CAPTCHA) by delivering transparent access for human visitors.
- Provided comprehensive attack analytics to give a clear picture of all automation attacks.
- Enabled the agency to serve a broad population by offering backward compatibility with a wide variety of browsers.

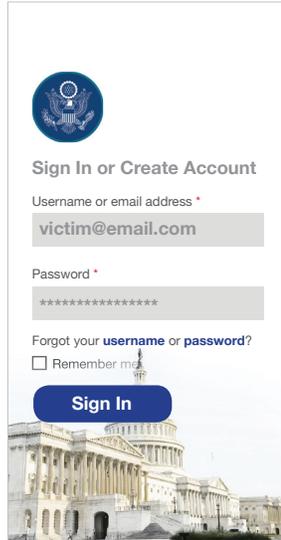
ANATOMY OF ATTACK

Stolen Credentials Combined with A.I.



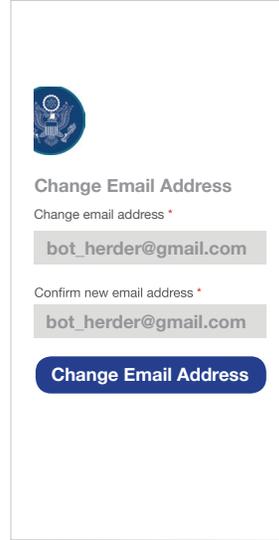
Stage 1

Attackers acquired spilled credentials from the open web of criminal marketplaces and password dump sites.



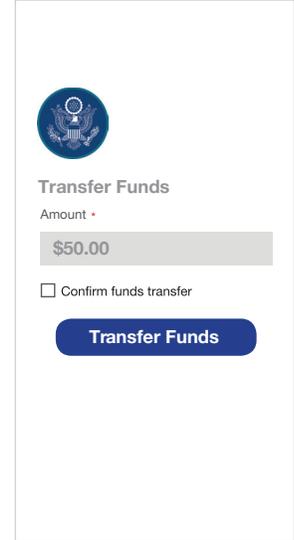
Stage 2

Attackers tested stolen passwords and personal information combined with intelligent algorithms to guess answers to authentication questions.



Stage 3

Attackers hijacked accounts when the credentials were valid.



Stage 4

Attackers then redirected payments and benefits.

CONCLUSION

This critical government agency was able to dramatically lower account takeover and associated fraud through the deployment of Shape. Working with the agency's web application and network technologists, Shape was able to successfully integrate Shape into the the agency's web application platform while meeting all compatibility and accessibility requirements. The agency continues to benefit on an ongoing basis from Shape threat intelligence, 24/7 monitoring, counter measure updates and threat research enabling the agency to stay ahead of cyber-criminals.



Part of F5

Shape Security defends the world's largest enterprises from sophisticated cyberattacks and fraud. Shape customers include three of the Top 5 US banks, five of the Top 10 global airlines, three of the Top 5 global hotels and two of the Top 5 US government agencies. The company has raised \$100M+ from Kleiner Perkins, Google Ventures, Eric Schmidt, and other leading investors to build an advanced web, mobile, artificial intelligence, and machine learning platform for global scale application defense. The Shape platform, covered by 50 issued patents and 100+ additional patent applications, prevented over \$1B in fraud in the last year. Shape was named by CNBC as one of the 50 most disruptive companies in the world. Today, the Shape Network defends 1.4 billion user accounts from account takeover and protects \$1B of in-store mobile payments worldwide.