Executive Summary

On July 1, 2014, Department of Veterans Affairs ("VA") contracted Mandiant to conduct a Compromise Assessment within the VA environment. Mandiant executed the Compromise Assessment between July 1, 2014 and December 12, 2014. Mandiant's Compromise Assessment is designed to identify evidence of targeted threat groups in a client's environment. As part of the Compromise Assessment, Mandiant and VA deployed one Mandiant Intelligence Response (MIR) controller and MIR agent software to analyze domain controller systems in the environment. In addition, VA deployed 12 Mandiant network sensors to monitor network traffic.

Mandiant performed the following major steps for host-based analysis during the Compromise Assessment:

- Configured MIR hardware and software within the VA environment
- Assisted with the MIR agent deployment including troubleshooting and progress monitoring
- Searched the VA environment for Mandiant Indicators of Compromise (IOCs)
- Applied methodology-based analysis to identify suspicious activity that Mandiant had not previously described in IOCs
- Manually verified IOC search results
- Documented results of the host-based assessment

The host-based analysis included multiple approaches for identifying malicious activity. Mandiant used MIR to contact systems in the environment with nine separate data acquisitions, referred to as "sweeps". A list of the nine sweeps performed may be found in the section titled "Host-Based Compromise Assessment Details" and a detailed breakdown of the status of systems analyzed by each sweep is available in "Appendix D: MIR Sweep Status". On average for all 11 sweeps, Mandiant assessed approximately 96% of the 574 VA Domain Controllers with MIR agents. Typical coverage for an environment of this size is 80%.

Mandiant performed the following major steps for network analysis during the Compromise Assessment:

- Configured the network sensor for deployment
- Assisted with the deployment of the network sensor
- Reviewed ingress and egress network traffic for IOCs
- Reviewed all generated alerts
- Documented the results of the network-based assessment

During the Compromise Assessment, Mandiant used host-based IOCs, network-based IOCs, and manual review of information collected from VA systems to identify malicious activity.

Findings

During the Compromise Assessment, Mandiant did not identify evidence of compromise of the VA domain controllers by targeted threat actors. The Compromise Assessment also did not identify any evidence of data staging or theft (credentials, PII, PHI, and VA sensitive information).

Mandiant defined targeted threat groups as malicious actors that meet three criteria:

1. They have the ability to operate in the full spectrum of computer network intrusion
2. They display some element of tasking to accomplish a predefined mission
3. They show signs of organization, motivation, and funding towards a goal

Mandiant monitored live network traffic for all systems in the VA environment and identified evidence of compromise by an unknown threat group on one system. This system was later identified by VA staff as a non-VA desktop computer that a researcher had connected to the VA network. The VA staff removed the computer from the network and follow-up actions were undertaken to determine the details for how this unauthorized computer was connected to the VA network.