Fileless Malware Campaigns Tied to Same Attacker

Two recent fileless malware campaigns targeting financial institutions, government agencies and other enterprises have been linked to the same attack group.

Two recent fileless malware campaigns targeting financial institutions, government agencies and other enterprises have been linked to the same attack group.

The campaigns, disclosed by Kaspersky Lab and Cisco's Talos research outfit in the last five weeks, made extensive use of fileless malware and known penetration testing tools and utilities to spy on organizations and move data and money off of networks.

Researchers at Israeli security company Morphisec said today that in investigating a recent campaign, they discovered the framework used to deliver the DNS PowerShell Messenger attacks reported by Cisco and a similar attack uncovered by Kaspersky Lab that used Meterpreter and other known utilities against 140 banks worldwide. The Meterpreter attacks, Kaspersky Lab said, could be connected to the GCMAN and Carbanak groups, which were responsible for $1 billion in thefts from financial institutions, according to a 2015 report. FireEye calls this group FIN7 and said it was targeting individuals involved in SEC filings.

The framework has since disappeared online following a brief interaction with the attacker and Morphisec researchers. Omri Dotan of Morphisec said the researchers attempted to build some trust with the attacker and tried to communicate in Russian before he disabled the command and control infrastructure and removed the framework.

"There is a high level of probability that we have attributed a whole bunch of attacks across the globe to one actor and this platform," Dotan said. "Through this [interaction] we had with them, they took it down and quite likely disrupted any ongoing attacks. Now they are going to have to rebuild it and do this stuff over from scratch."

Morphisec said in an analysis published today that on March 8 during an investigation into an attack against several high-profile enterprises, it found the framework used to deliver a number of variations of attacks, all of which leave no artifacts on the compromised machines. These artifacts either match, or are similar to, others used in the attacks described by Kaspersky and Cisco, they said.

The attacks begin with phishing emails targeting organizations using a Word document that is protected, which urges the user to enable the content. By doing so, the victim executes a macro embedded in the document that executes a PowerShell command using Windows Management Instrumentation, infrastructure used to automate tasks on remote machines.

A PowerShell script called Updater.ps1 is enabled that opens a backdoor and grabs commands from the command and control server. It also lowers security restrictions around macros so that more macro-based documents can be sent and will execute without user interaction. Morphisec said it found additional scripts on the command and control server that execute Mimikatz, which is used to extract passwords and hashes from memory, LaZagne, a open source application used to retrieve credentials stored on a local hard drive, and DNS Messenger.

Dotan said Morphisec was on the command and control server for three days and was able fingerprint a number of artifacts on the framework, encryption routines and IP addresses that led them to conclude the likely connection with other similar attacks.

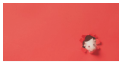
"At some point toward the end of our investigation the attacker contacted our people through the shellcode. We had a brief interaction where our folks tried to lure the hacker to reveal part of his identity," Dotan said. "At some point, we tried to talk to them in Russian, but at that point, he asked for 'English, please.' He then started to shut down the command and control server and completely took down the platform."

Dotan said that Morphisec has made all of the artifacts it recovered public but has shared them with Israel's cybersecurity administration.

Share this article:

Malware

SUGGESTED ARTICLES



APT36 Taps Coronavirus as 'Golden Opportunity' to Spread Crimson RAT

The Pakistani-linked APT has been spotted infecting victims with data exfiltration malware.

March 27, 2020

Activities of a Nigerian Cybercriminal Uncovered

Rise and fall of a Nigerian cybercriminal called 'Dtom,' who made hundreds of thousands of dollars in a 7-year campaign, outlined in new report.

March 27, 2020

Coronavirus-Themed APT Attack Spreads Malware

The APT group was spotted sending spear-phishing emails that purport to detail information about coronavirus – but they actually infect victims with a custom RAT.

March 13, 2020

DISCUSSION

INFOSEC INSIDER

A Practical Guide to Zero-Trust Security

January 13, 2020

7 Tips for Maximizing Your SOC

December 31, 2019

Mean Time to Hardening: The Next-Gen Security Metric

December 30, 2019

Combining AI and Playbooks to Predict Cyberattacks

December 26, 2019

The Case for Cyber-Risk Prospectuses

December 24, 2019

Newsletter

Subscribe to Threatpost Today

Join thousands of people who receive the latest breaking cybersecurity news every day.

Subscribe now

Twitter

A new Mirai botnet variant is exploiting a critical #security flaw in Zyxel network-attached storage devices, accor... https://t.co/dVEJvNNzmw

2 hours ago

Follow @threatpost

Subscribe to our newsletter, Threatpost Today! Get the latest breaking news delivered daily to your inbox.

Subscribe now

Copyright © 2020 Threatpost - Privacy Policy - Terms and Conditions - Advertise