Shamoon: Destructive Threat Re-Emerges with New Sting in its Tail

symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail

Threat Hunter TeamSymantec

Organizations in Saudi Arabia and the UAE have been hit in latest attacks that involve new wiper malware.

After a two-year absence, the destructive malware Shamoon (W32.Disttrack.B) re-emerged on December 10 in a new wave of attacks against targets in the Middle East. These latest Shamoon attacks are doubly destructive, since they involve a new wiper (Trojan.Filerase) that deletes files from infected computers before the Shamoon malware wipes the master boot record.

News of the attacks first emerged on December 10 when Italian oil services firm Saipem said that it had been hit by a cyber attack against its servers in the Middle East. Two days later, the company said that Shamoon had been used in the attack, which affected between 300 and 400 servers and up to 100 personal computers.

Symantec has found evidence of attacks against two other organizations during the same week, in Saudi Arabia and the United Arab Emirates. Both organizations are involved in the oil and gas industry.

New wiper deployed

Unlike previous Shamoon attacks, these latest attacks involve a new, second piece of wiping malware (Trojan.Filerase). This malware will delete and overwrite files on the infected computer. Shamoon itself will meanwhile erase the master boot record of the computer, rendering it unusable.

The addition of the Filerase wiper makes these attacks more destructive than use of the Shamoon malware alone. While a computer infected by Shamoon could be unusable, files on the hard disk may be forensically recoverable. However, if the files are first wiped by the Filerase malware, recovery becomes impossible.

Filerase is spread across the victim's network from one initial computer using a list of remote computers. This list is in the form of a text file and is unique to each victim, meaning the attackers likely gathered this information during an earlier reconnaissance phase of the intrusion. This list is first copied by a component called OCLC.exe and passed on to another tool called Spreader.exe. The Spreader component will then copy Filerase to all the computers listed. It will then simultaneously trigger the Filerase malware on all infected machines.

It is possible that the Shamoon malware itself was spread via these same tools, but this is unknown. In at least one instance, Shamoon was executed using PsExec, indicating that the attackers had access to credentials for the network.

Possible link to Elfin

One of the new Shamoon victims Symantec observed the organization in Saudi Arabia had recently also been attacked by another group Symantec calls Elfin (aka APT33) and had been infected with the Stonedrill malware (Trojan.Stonedrill). There were additional attacks against this organization in 2018 that may have been related to Elfin or could have been the work of yet another group.

The proximity of the Elfin and the Shamoon attacks against this organization means it is possible that the two incidents are linked.

A history of destructive attacks

Shamoon (W32.Disttrack) first emerged in 2012 when it was used in a series of disruptive attacks against the Saudi energy sector.

Activity then ceased until it made a surprise comeback in late 2016. A slightly modified version of the malware (W32.Disttrack.B) was used in attacks against a range of targets, again in Saudi Arabia. The attacks appeared timed to cause maximum destruction. The malware was configured to trigger at 8:45pm local time on Thursday, November 17, 2016. The Saudi working week runs from Sunday to Thursday, meaning computers were wiped after most staff had left for the weekend, minimizing the chance of discovery before the attack was complete.

Recurring menace

Why Shamoon has suddenly been deployed again remains unknown. However, the fact that the malware seems to be taken out of retirement every few years means that organizations need to remain vigilant and ensure that all data is properly backed up and a robust security strategy is in place.

Protection

Symantec has the following protections in place against the Shamoon attacks:

File-based protections

- W32.Disttrack
- W32.Disttrack!gen1
- W32.Disttrack!gen4
- W32.Disttrack!gen6

- W32.Disttrack!gen7
- W32.Disttrack!gen8
- W32.Disttrack.B
- Trojan.Filerase

Network-based protections (Intrusion Prevention System)

- System Infected: Disttrack Trojan Activity 2
- System Infected: Disttrack Trojan Activity 3

Indicators of Compromise

- d9e52663715902e9ec51a7dd2fea5241c9714976e9541c02df66d1a42a3a7d2a - Executes the Spreader.exe component
- 35ceb84403efa728950d2cc8acb571c61d3a90decaf8b1f2979eaf13811c146b - Spreader.exe, which spreads the Trojan.Filerase component across specified computers
- 5203628a89e0a7d9f27757b347118250f5aa6d0685d156e375b6945c8c05eb8a - Trojan.Filerase component
- 0266be9130bdf20976fc5490f9191edaafdae09ebe45e74cd97792412454bf0d - Trojan.Filerase component
- bd2097055380b96c62f39e1160d260122551fa50d1eccdc70390958af56ac003 - W32.Disttrack.B
- c3ab58b3154e5f5101ba74fccfd27a9ab445e41262cdf47e8cc3be7416a5904f - W32.Disttrack.B
- 0975eb436fb4adb9077c8e99ea6d34746807bc83a228b17d321d14dfbbe80b03 - W32.Disttrack.B
- 0694bdf9f08e4f4a09d13b7b5a68c0148ceb3fcc79442f4db2aa19dd23681afe - W32.Disttrack.B

Threat Intelligence

Customers of the DeepSight Intelligence Managed Adversary and Threat Intelligence (MATI) service have received reports on Shamoon which detail methods of detecting and thwarting activities of this adversary..

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?