Endpoint Protection

symantec.com/connect/blogs/shamoon-multi-staged-destructive-attacks-limited-specific-targets

Feb 27, 2017 09:11 AM

A L Johnson

Recent attacks involving the destructive malware Shamoon (W32.Disttrack.B) were launched by attackers conducting a much wider campaign in the Middle East. While the attackers have compromised multiple targets in the region, only selected targets in Saudi Arabia were infected with Shamoon.

On February 15, publications from IBM (The Full Shamoon) and Palo Alto (Magic Hound) separately discussed a persistent attack campaign operating primarily in the Middle East with links to Shamoon. This campaign was conducted by a group we identify as Timberworm. The group appears to have facilitated the third wave of destructive attacks involving Shamoon in January 2017. Timberworm operates in the Middle East and beyond. Only specific organizations affiliated with Saudi Arabia appear to have been earmarked for destructive wiping attacks.

During the January attacks, Symantec discovered a high correlation between Timberworm and the presence of Shamoon in a number of organizations in Saudi Arabia. Timberworm appears to have gained access to these organizations' networks weeks and, in some cases, months before the Shamoon attacks occurred. Once on the network, the attackers' primary goal appeared to be similar to Greenbug (an actor previously discussed in relation to the November 17 wave of attacks): detailed network reconnaissance, credential harvesting, and persistent remote access.

When Timberworm had sufficient access to a number of high value organizations, Shamoon was then preconfigured with a wipe date and the necessary credentials to maximize the overall impact during a coordinated attack. This procedure is consistent with what was observed during Greenbug operations prior to the November 17 attacks, which may indicate that multiple groups are cooperating to facilitate these destructive attacks, possibly at the direction of a single entity.

Stage 1: Timberworm recon

Timberworm's carefully planned operation saw the attackers send spear phishing emails to individuals at targeted organizations. In some cases, the emails contained Microsoft Word or Excel files as attachments. In others, the emails contained malicious links, which if clicked, downloaded similar Word or Excel files.

Computer network exploitation

Opening the document invoked PowerShell from a malicious macro, which provided the attackers with remote access to the compromised computer. Some basic reconnaissance was then performed using existing system tools to determine if the target was of interest. Once Timberworm was satisfied, it then deployed custom malware, hacktools, and software traditionally used in system/network administration. Some of the tools deployed during these attacks included:

- PsExec, a tool for executing processes on other systems from Microsoft Sysinternals
- PAExec, a free re-implementation of PsExec from Poweradmin
- Netscan, a multipurpose IPv4/IPv6 network scanner
- Samdump, a hacking tool that dumps Windows password hashes
- Mimikatz (Hacktool.Mimikatz), a hacking tool to harvest credentials
- TightVNC, an open-source remote desktop access application
- Plink, a command line network connection tool supporting encrypted communications
- Rar, archiving utility for compressing files before ex-filtration.

During this phase, once the attacker appeared to have achieved the desired level of network access, Plink was executed to provide an additional avenue of remote access (Fex reverse RDP over SSH connections). This pattern of activity is also consistent with what was observed during Greenbug operations in 2016, before the eventual deployment of Shamoon.

Stage 2: Shamoon destruction

At this point the attackers configured the Shamoon payloads per organization and then coordinated the attacks on a pre-determined date. In the January 23 attacks Symantec observed consistent usage of PAExec across numerous organizations to initially deploy W32.Disttrack.B. After it was deployed, it would self-propagate and wipe accessible computers across the network.

Multiple teams cooperating?

Timberworm appears to be a much larger operation, infiltrating a much broader range of organizations beyond those affected by the recent Shamoon attacks. Similarly, Greenbug targeted a range of organizations in the Middle East beyond those affected by Shamoon, including companies in the aviation, energy, government, investment, and education sectors. While both groups leveraged two distinct toolsets, their targets, tactics, and procedures align very well and in close proximity to the coordinated wiping events.

"Living off the land"

The Shamoon attacks illustrate how a growing number of targeted attack groups are relying on common-off-the-shelf tools to compromise targets. The Shamoon attackers managed to get access to targets' networks using socially engineered spear-phishing emails and abusing Office macros and PowerShell to gain initial footholds. In particular, the use of PowerShell has been a popular tactic of late. Recent Symantec research found a total of 111 malware families that use the PowerShell command line. More than 95 percent of the PowerShell scripts analyzed through the BlueCoat Malware Analysis sandbox were found to be malicious.

The appeal of "living off the land" is obvious. Attackers believe malicious activity will be more difficult to detect if legitimate tools are involved and malware use is kept to a minimum. The use of legitimate tools may also serve to thwart attribution to specific actors.

Protection

Symantec and Norton products protect against Shamoon with the following detections:

Antivirus:

- W32.Disttrack
- W32.Disttrack!gen1
- W32.Disttrack!gen4
- W32.Disttrack!gen6
- W32.Disttrack!gen7
- W32.Disttrack!gen8
- W32.Disttrack.B
- Backdoor.Mhretriev
- Hacktool.Mimikatz

Intrusion prevention system:

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

Indicators of compromise

Netscan

MD5

1ef78a72e4957c04197992bab2f86335

SHA256

63d51bc3e5cf4068ff04bd3d665c101a003f1d6f52de7366f5a2d9ef5cc041a7

TightVNC

MD5

a2ff24322c12558eb1f29aea3ca6f24a

SHA256

1ba26bcd857944b0486a76928f41f74d91dad492b46ea93c4ca246a0503cdaae

Hacktool.Mimikatz

MD5

a9ae14b298fb12fad76347ff8f61dd40 (x86)

27552cd0d24cb1eb59259d2acd7181bf (x64)

SHA256

0de2b74ff045f7c1af2d42aaf00aa98d44351850a968faf7b37bfa650684003c (x86)

28290b9475c62039dda26b64e45f3e14815b6acd9ed49156a14e361df0524af8 (x64)

PAExec

MD5

22e9853298c96b1ab89d8f71c4e82302

SHA256

01a461ad68d11b5b5096f45eb54df9ba62c5af413fa9eb544eacb598373a26bc