INNOVATIVE SOLUTIONS

Your Business. Secured!

New Shamoon Variant targeting **Middle East**

Shamoon was a destructive wiper which was used back in 2012 for attacks on Government and Oil & Gas entities in Saudi Arabia. Recently, another variant of Shamoon has been identified in the wild which is being named as “Shamoon 3’. This is really threatening and worrisome for the organizations since this could be as destructive as its variants found before.

Although this virus is being named “Shamoon 3”, however it is slightly different in behavior from its previous variations. Shamoon 2 would trigger at a certain time, already specified by the attackers and wipe all the files on the system and copying the picture all over the system’s filesystem. Behavioral analysis of Shamoon 3 shows that there are some significant differences from the previous variations. Trigger date for this virus is set in past date but this is not designed to travel within the network using pre-programmed credentials. Also, the command and control URL was missing which could be because either the attacker has complete control of the system, so they would manually install the Shamoon at some feasible time according to their motives.

Shamoon 3 is being noted as a testing malware since it doesn’t execute the malicious intent it is usually used for. It has all the code of malicious checks that were present in the previous variant’s code, however the execution steps and missing. Systems date and time is set to December 2017 at 11:51 pm, which is probably to ensure its instant execution. Service names that are generated by the dropper of these viruses are mentioned below:

Service name: **MaintenaceSvr**
Display name: **Maintenace Host Service Image**

Image path:

1. %System%\MaintenaceSvr32.exe LocalService
2. %System%\MaintenaceSvr64.exe LocalService

Drop paths have been mentioned below for the Shamoon 3

1. %System%\{random file name}.exe
2. %System%\Drivers\drdisk.sys, %Windows%\hdv_725x.sys

Shamoon 3 drops copies of itself in the following shared folders:

1. \\{IP address}\ADMIN$\system32\{random file name}.exe
2. \\{IP address}\C$\WINDOWS\system32\{random file name}.exe
3. \\{IP address}\D$\WINDOWS\system32\{random file name}.exe
4. \\{IP address}\E$\WINDOWS\system32\{random file name}.exe

Our offices
Riyadh | Jeddah | Al Khobar | Dubai | Abu Dhabi
info@is.com.sa | www.is.com.sa

INNOVATIVE SOLUTIONS

Innovative Solutions from its credible internal sources has obtained the IOCs which would assist the organizations in identifying the attacks. Furthermore, these have been shared below for public information. It is very important that along with securing environment in light of these IOCs, we should also take some pre-emptive measures to protect the organization.

Remedy Measures

1. All employees should be sent an advisory to be careful about opening any unsolicited emails which could contain malicious attachments.
2. Examine RDP & SSH connection, and block the unnecessary sessions.
3. Review the permissions granted to VPN users and all other remote access connections to your organization.
4. It's advised to force a full password-reset organization-wide of all accounts, and especially those with administrative privileges.
5. Patch and update the systems to prevent vulnerabilities from being exploited.
6. Enforce the principle of least privilege and network segmentation in your environment.
7. Ensure these hashes have been blocked in the endpoint security solutions and actively monitor the network for any signs of malicious traffic.

Indicators of Compromise (Hashes)

1. DE07C4AC94A50663851E5DABE6E50D1F
2. B41F586FC9C95C66F0967F1592641A85
3. 887C614608E7CD9A691858CAF468C28F
4. A4A9100413EBBA59CAB785D506448093
5. 001D216EE755F0BC96125892E2FB3E3A
6. 41953B002F779D43244E5D210504A102

Files

No record for the following hashes, but it's highly confirmed that it is used for such an attack.

1. 30825F6EF7B1BB5D3DE6640C2758FE68
2. ECDA82069D4349BF492404C369339F71

Our offices
Riyadh | Jeddah | Al Khobar | Dubai | Abu Dhabi
info@is.com.sa | www.is.com.sa

INNOVATIVE SOLUTIONS