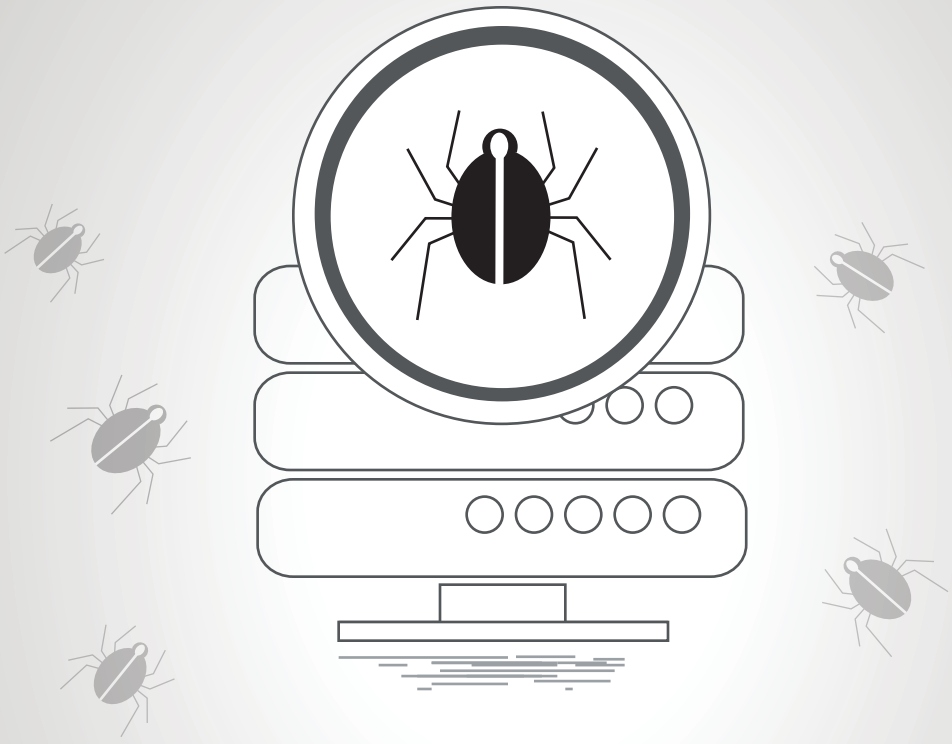
How to Protect Your Organization From The Shamoon Malware Attack



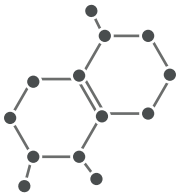
PALADION
HIGH SPEED CYBER DEFENSE

Background

In November of 2016, employees of Saudi Arabia civil aviation, among five other government organizations, returned to work after a long weekend to discover that they had been the victims of a large scale cyber-attack. The hackers optimized the destruction by beginning on a Thursday evening, to be sure that an entire weekend would pass before the infiltration was discovered. When all was said and done, 35,000 machines were compromised with data erased from more than 1000 computers. It was later determined that the hackers' motive was corporate espionage. It worked: customer data was exposed and trade secrets were lost. Although there are many theories as to the identity of the cyber terrorists, the one thing known for certain is that the ordeal was devastating to its victims.

> "When malware can attack 35,000 computers belonging to a government organization, we are talking about a very sophisticated, advanced cyber attack that everyone needs to be prepared for."

This massive attack, known as the Shamoon malware attack, was not the first time this method has been used. In 2012, a similar attack targeted the oil and energy sectors in Saudi Arabia. In 2012, workers were unable to reboot their computers and were instead welcomed with the image of a burning American flag. In the most recent attack, the image of a Syrian refugee child remained on the screens of infected computers. However, this wasn't the only difference. The 2016 version of the Shamoon malware employed an overall more sophisticated and advanced method of attack.



Anatomy of the Attack

For victims of the most recent Shamoon attack, an important element of this version was that it contained embedded user credentials harvested from previous attacks. This technique could be as simple as hackers accessing the passwords of former employees or it could suggest a long term, targeted attack involving phishing for passwords or quite possibly indicates the possibility of an inside job.

The attack itself is divided into three separate and distinct sections. The first phase is the dropper. In this phase, the malware persists into systems on the infected computer. It then attempts to spread across the local network making self-copies and dropping components. The malware is also advanced enough to detect both 32 bit and 64 bit architecture and drops the appropriate model depending on what it encounters.

In the next phase of the attack, the malware employs a wiper. Widely known as Disstrack, this is simply the name of the malware's specific wiper component. In this step, the malware uses already present EldoS driver software to override the hard disk. In addition, the malware ultimately has the ability to overwrite the master boot record making it impossible to reboot the infected computer.

> "The Shamoon malware is advanced enough to determine what architecture it Is encountering, use your existing software to override the hard disk and ultimately make it impossible to reboot your computer."

The final phase of the Shamoon attack is the reporter phase. This handles communication with the hacker controlling the server and transfers information back and forth. In addition, it wipes the driver and wipes the verification report sent to the central server concluding what is considered by many to be an expert kill chain.

In addition, there were credentials present to attack virtual desktop infrastructure (VDI), which represents an escalation that affects traditional recovery tactics. One of the benefits of the use of VDI in the workplace is the ability to take periodic snapshots of the virtual desktop, which allows for easy and quick restoration if there is a problem. The fact that the hackers took this into consideration means that they weren't content with just corporate espionage, they weren't satisfied until they had achieved total destruction.

Technical Specifications

In the latest Shamoon attack, one of the malware's more advanced techniques was its lateral movement capabilities. It attempts to access default shared folders like Admin$ shares to spread among the network. Admin$ are Administrative hidden network shares created by the Windows family of operating systems that allow system administrators to have remote access to every disk volume on a network-connected system. Currently, admin share gives access to C:\Windows or C:\Windows\System32. Shamoon copies the file to this location with various names like ntssrvr64.exe, gpget.exe, among others.

After the dropping phase is complete, the next phase is to remotely invoke the same by leveraging remote registry services to complete the job. Remote registry allows the malware the ability to create entry in the service manager which gives a hook attacker. The hackers will leverage RegConnectRegistryW kind of APIs to setup the dropped files in C:\Windows\System32 as windows services set to run during reboot. These services are created with various names like ntssrv etc.

In addition, Shamoon malware also leverages remote registries to disable UAC and enable shares. UAC can be disabled using the registry key:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy

Another tactic applied by the Shamoon malware is leveraging Net Schedule Job API (NetScheduleJobAdd) to schedule a job instead of creating a new service.

This API will in turn depend upon settings from this registry key:

HKLM\System\CurrentControlSet\Control\Lsa\SubmitControl

These APIs require authentication which it extracts from a local credential vault or by impersonating the currently logged in user.

This modus operandi can be disrupted if systems are hardened properly. Important things to check would be to:

- Disable admin shares. Move to powershell which is the next gen administration protocol for windows.
- Disable remote registry and start using powershell based registry APIs.
- Ensure UAC is enabled.

How to Prevent a Similar Attack

Knowing what is out there is the first step, and consistently checking a list of indicators to make sure you are not infected is an absolute necessity. Hiring professionals, such as Paladion's Threat Intel team, gives you access to a comprehensive list of Indicators of Compromise (IOCs) for Disttrack Droppers, Communication Components, Wiper Components, and EldoS RawDisk Samples for both 32-bit and 64-bit machines. We have provided these protections for all of our customers and we analyze historical data to detect any traces of Shamoon.

"The only way to be truly prepared for an attack like Shamoon is to remain continually aware of the latest threat intelligence and employ expert analysis to maintain your network security."

However, the best approach for any cyber-attack is proactive not reactive. Any organization at risk of hacking should employ a continuous application of threat intelligence, monitor for known patterns rather than putting something in place after an attack as well as seek out access to expert analysis. In addition, you should configure your SIEM with custom use cases for attacks of this nature.

It is also critical for every organization to continuously look out for attack patterns, fine-tune your SIEM and respond quickly to contain and prevent such attacks. Our threat intel team works non-stop to analyze new malware, develop IOCs and quickly roll it out across our customer environments. Our breach detection experts can detect any traces of IOCs in customer environments and help you implement preventive measures to detect and respond faster.

PALADION
HIGH SPEED CYBER DEFENSE

ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its semi-autonomous cyber platform and managed services with leading security technologies. Paladion is consistently rated and recognized by independent analyst firms and awarded by CRN, Asian Banker, Red Herring, amongst others.

For 17 years, Paladion has been actively managing cyber risk for over 700 customers from its six cyber operations centers placed across the globe. It houses 900+ cyber security professionals including security researchers, threat hunters, ethical hackers, incident responders, solution architects, consultants and more. Paladion is also actively involved in several information security research forums such as OWASP, and has authored several books on security monitoring, application security, and more.

WW Headquarters: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-844-507-7668

Bangalore: +91-80-42543444, Mumbai: +91-2233655151, Delhi: +91-9910301180, London: +44(0)2071487475, Dubai: +971-4-2595526, Sharjah: +971-50-8344863, Doha: +97433559018, Riyadh: +966(0)114725163, Muscat: +968 99383575, Kuala Lumpur: +60-3-7660-4988, Bangkok: +66 23093650-51, Jalan Kedoya Raya: +62-8111664399.

sales@paladion.net | www.paladion.net