TATA CONSULTANCY SERVICES
Experience certainty.

Malware Advisory

Shamoon Malware:Re-emerges

12th December, 2018

Table of Contents

Overview

Shamoon, the rarely seen but destructive malware that was used to wipe Saudi Aramco's servers in 2012, may be back in play, according to Chronicle, Alphabet's cybersecurity arm. Shamoon, an information-stealing malware that also includes a destructive module, renders infected systems useless by overwriting the Master Boot Record (MBR), the partition tables, and most of the files with random data. Once overwritten, the data are not recoverable. There are only three known times Shamoon variants have been used in the wild with the Saudi incident the most famous.The Shamoon disk-wiping malware has received a major upgrade and now features a ransomware module, along with support for both 32-bit and 64-bit architectures according to researchers. Shamoon, also known as Disttrack, first spotted in 2012, is one of today's most notorious malware families, even if one of the rarest. Because of the highly destructive functionality of the Shamoon “Wiper” module, an organization infected with the malware could experience operational impacts including loss of intellectual property (IP) and disruption of critical systems. Actual impact to organizations vary, depending on the type and number of systems impacted.

Severity: Severe
Release Date: 12th December, 2018
Target OS: Windows 98, Windows 95, Windows XP, Windows Server 2008, Windows 7, Windows Me, Windows Vista, Windows NT, Windows Server 2003, Windows 2000
Distribution Method: Via Trojan installation and password stealing.
Discovered By: Chronicle, Alphabet's cybersecurity arm

Technical detail

a) How does it enters to the system

The attackers appear to have done a significant amount of preparatory work for the operation. The malware was configured with passwords that appear to have been stolen from the targeted organizations and were likely used to allow the threat to spread across a targeted organization's network. How the attackers obtained the stolen credentials is unknown. e.g Disttrack is a Trojan horse that attempts to steal confidential information from the compromised computer. It may also download configuration files and updates from the Internet.

Shamoon has three primary functional components:

- Dropper—the main component and source of the original infection. It installs a number of other modules.
- Wiper—this module is responsible for the destructive functionality of the malware.
- Reporter—this module is responsible for reporting infection information back to the attacker.

Lets look at one of the scenario where the malware had a default configuration that triggered the disk-wiping payload at 8:45pm local time on Thursday. The Saudi Arabian working week runs from Sunday to Thursday. It would appear that the attack was timed to occur after most staff had gone home for the weekend in the hope of reducing the chance of discovery before maximum damage could be caused.

b) How this Ransomware infects to your system

Pattern of Disttrack malware used by Shamoon in Past:

Shamoon uses a number of components to infect computers. The first component is a dropper, which creates a service with the name 'NtsSrv' to remain persistent on the infected computer. It spreads across a local network by copying itself on to other computers and will drop additional components to infected computers. The dropper comes in 32-bit and 64-bit versions. If the 32-bit dropper detects a 64-bit architecture, it will drop the 64-bit version.

The second component is the wiper, which drops a third component, known as the Eldos driver. This enables access to the hard disk directly from user-mode without the need of Windows APIs. The wiper uses the Eldos driver to overwrite the hard disk with the aforementioned photos of the Syrian boy.

The final component is the reporter. This is responsible for handling communications with a command and control (C&C) server operated by the attackers. It can download additional binaries from the C&C server and change the pre-configured disk-wiping time if instructed by the C&C server. It is also configured to send a report verifying that a disk has been wiped to the C&C server.

3. Indicators Of Compromise:

MD5:

- 7145d303065760829ad66887b8feabad
- 27d18ff26f88d0f78c5d00138208686a
- a7deb28a52521e5782d5ec367ae20afc
- 887c614608e7cd9a691858caf468c28f
- de07c4ac94a50663851e5dabe6e50d1f
- b51fdec78474c52378e9d565b4e5f343
- 41953b002f779d43244e5d210504a102
- b41f586fc9c95c66f0967f1592641a85
- 6018e0c533ff120e77e11f37d978f109
- c9e5f8c371d3973385157ffeb8feb0fc
- c7880a6c02a0d6081a656a46ab934264

SHA-1:

- d71e15e07a9a2cc22fd2fc97e30eebca632fa799
- 5879bb68735654a1c54264b9e345fa493a3f1b24
- 07e88dd71e64cad117522620e446be92971746d7
- ceb7876c01c75673699c74ff7fac64a5ca0e67a1
- df177772518a8fcedbbc805ceed8daecc0f42fed
- 73450de5821a8041404b1217c8b91b15583239bf
- 940237503152ac0bf65df0af40e99b04f0870106
- 10411f07640edcaa6104f078af09e2543aa0ca07
- 7962032804226cbf1291620cb0f2ee828b340476
- 99ca7f540bdedeb7169ed23ebd87fe9f8e9cb729
- b7208deee0110c5979a39b3fb2b66d3411dc9bab

SHA-256

- ee084f2c6fd2cc16f613fadd712641b5742489ca87851739dc868b976867858f
- 36414012564b88b5a2dcded39fc5ed22301ea2ef2f455bf697fa97a5925cb721
- 101e74ef7a18d3a790f1d30edc7bd9f4ebf0afb2cb85cffcd5710d0a53df77a6
- 391e7b90bf3f0bfeb2c2602cc65aa6be4dd1c01374b89c4a48425f2d22fe231c
- c3ab58b3154e5f5101ba74fccfd27a9ab445e41262cdf47e8cc3be7416a5904f
- 4d4531f0372d4364e3d9b7e6ea13abf241bbc4a4b761f8a2aea67428d0de8d83
- 0c0b31af92df5ff10d4c1f4d8c45a6a03ad8357db73abf0380ef84e21c464d37

- 0694bdf9f08e4f4a09d13b7b5a68c0148ceb3fcc79442f4db2aa19dd23681afe
- 5cccd1282cd2149ff3860dcbbbc9eafa05a8b72db6c2bd26ac98b0d5cf1a8b44
- 3c6d46c5fecab7cfe2fb8e1002d62735701af80ec67566d4bf95c257de353034
- c684009768a0f7401b85291b4ef0d9719b05f2db0bf083c2148e368b11f02dbd

Import files:

- HAL.dll
- msrpc.sys
- ntoskrnl.exe
- NETIO.SYS
- ADVAPI32.dll
- GDI32.dll
- KERNEL32.dll
- SHELL32.dll
- USER32.dll
- WINMM.dll
- ADVAPI32.dll
- GDI32.dll
- KERNEL32.dll
- NETAPI32.dll
- SHELL32.dll
- USER32.dll
- WINMM.dll
- WS2_32.dll

File names:

- ksecdd.sys
- P6_ImportClient.exe
- ndis.sy_
- prnlx00ctl.ex_
- MaintenaceSrv32.ex_
- P7ReportEngineClient.exe
- gsusp_DEA704283226_081312_1554
- kscaptur_ibv32.ex_
- QReportHKeeperClient.exe
- P7EntSchedulerClient.exe
- pacer.sys

Mitigation measures

System owners and administrators should review any configuration changes before implementation to avoid unwanted impacts.

- Malware is stealing the credential of administrator's account and then use the credentials to drop the payload. Hence it is required to maintain the strong passwords.
- Disable credential caching for all desktop devices with particular importance on critical systems such as servers and restrict the number of cached credential for all portable devices to no more than three if possible. This can occur through a Group Policy Object (GPO).
- Consider restricting account privileges. It is our recommendation all daily operations should be executed using standard user accounts unless administrative privileges are required for that specific function. Configure all standard user accounts to prevent the execution and installation of any unknown or unauthorized software. Both standard and administrative accounts should have access only to services required for nominal daily duties, enforcing the concept of separation of duties. Lastly, disable Web and email capabilities on administrative accounts. Compromise of admin accounts is one vector that allows malicious activity to become truly persistent in a network environment.
- Ensure password policy rules are enforced and Admin password values are changed periodically.
- Consider prohibiting hosts within the production environment or DMZ from sharing an Active Directory enterprise with hosts on other networks. Each environment should have separate forests within Active Directory, with no trust relationships allowed between the forests if at all possible. If necessary, the trust relationships should be one-way with the low integrity environment trusting the higher integrity environment.
- Minimize network exposure for all control system devices. Where possible, disable RDP on critical devices.
- Ensure all network operating systems, web browsers, and other related network hardware and software remain updated with all current patches and fixes.
- Audit your network for systems that use RDP for remote communication. Disable the service if unneeded or install available patches. Users may need to work with their technology venders to confirm that patches will not affect system processes.
- Maintain a good back-up strategy.
- Enable logging and ensure that logging mechanisms capture RDP logins. Keep logs for a minimum of 90 days and review them regularly to detect intrusion attempts.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.

Preventive Measures

- Always keep your patch levels up to date, especially on computers that host public services accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- Build host systems, especially critical systems such as servers, with only essential applications and components required to perform the intended function. Any unused applications or functions should be removed or disabled, if possible, to limit the attack surface of the host.
- Implement network segmentation through V-LANs to limit the spread of malware.
- Consider the deployment of Software Restriction Policy set to only allow the execution of approved software (application whitelisting).
- Recommend the whitelisting of legitimate executable directories to prevent the execution of potentially malicious binaries.
- Consider the use of two-factor authentication methods for accessing privileged root level accounts or systems.
- Consider deploying a two-factor authentication through a hardened IPsec/VPN gateway with split-tunneling prohibited for secure remote access.
- Deny direct Internet access, except through the use of proxies for Enterprise servers and workstations. Perform regular content filtering at the proxies or external firewall points of presence. Also consider the deployment of an explicit versus transparent proxy policy.
- Implement a Secure Socket Layer (SSL) inspection capability to inspect both ingress and egress encrypted network traffic for potential malicious activity.
- Isolate network services, such as email and Web application servers by utilizing a secure multi-tenant virtualization technology. This will limit the damage sustained from a compromise or attack of a single network component.
- Implement best practice guidance and policy to restrict the use of non-Foundation assets for processing or accessing Foundation-controlled data or systems (e.g., working from home, or using a personal device while at the office). It is difficult to enforce corporate policies, detect intrusions, and conduct forensic analysis or remediate compromises on non-corporate owned devices.
- Implement best practice guidance and policy to limit the use of social networking services at work, such as personal email, instant messaging, Facebook, Twitter, except where there is a valid business case for use, and this business case has been approved by the organization Chief IT Security Officer. If a valid business case exists for use, implement a guidance/policy that reduces the risk of data loss and malware threats.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Place control system networks behind firewalls, and isolate or air gap them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

References

- https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever
- https://www.isssource.com/shamoon-mitigation-strategies/
- https://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B
- https://www.bleepingcomputer.com/news/security/shamoon-disk-wiping-malware-upgraded-with-ransomware-module/
- https://virustotal.com/