Updated Shamoon Malware Profile

Security Advisory	AE-Advisory 17-02	**Criticality**	Critical	
Advisory Released On	29 January 2017			

Impact

- Destruction
- Inference with Industrial Control Systems
- Disruption
- Degradation

Solution

- Refer to the Solution section below

Affected Platforms

- Enterprise/Network Systems
- Users/Application and Software

Affected Industries

- Governments
- Basic Materials/Chemicals/Mining/Metals
- Energy & Utilities
- Transportation/Industrial Manufacturing/Automotive

Summary

aeCERT has researched and found out about new version of Shamoon that might be a threat to UAE government entities and Gulf region. The destructive computer virus that appeared four years ago crippled tens of thousands of computers at the Middle Eastern energy companies. These attacks has been reported as warning of the new attacks by Crowd Strike, Fire Eye, Intel Corp's McAfee security unit, Palo Alto Networks Inc and Symantec Corp.

Threat Details

Recently the newer version of Shamoon is striking again by targeting government entities.

Upon execution, Shamoon controls network credentials to spread a dropper to systems on the same network that contains multiple subcomponents. One of these components, the wiper and in some cases it is developed into a ransomware, the wiper is known to destroy data on the target system. The malware is capable of self-propagation via network shares, dropping secondary components, and destroying sensitive information contained on an affected system.

The below table is a reference to the hashes/File characteristics:

File Name	MD5	File Type	Compile Time	Size
gpget.exe	c843046e54b755ec63ccb09d0a689674	PE.EXE	2009-02-15T12:30:41	327680
ntssrvr64.exe	8fbe990c2d493f58a2afa2b746e49c86	NA	NA	NA
key8854321.pub	b5d2a4d8ba015f3e89ade820c5840639	NA	NA	782
netinit.exe	ac4d91e919a3ef210a59acab0dbb9ab5	PE.EXE	2009-02-15T12:29:41	183808
ntssrvr32.exe	5446f46d89124462ae7aca4fce420423	PE.EXE	2009-02-15T12:31:44	1349632
Drdisk.sys	76c643ab29d497317085e5db8c799960	NA	2011-12-28 16:51:29	31632

ntssrvr32.bat	10de241bb7028788a8f278e27a4e335f	NA	NA	160
msinit	3cbb119d282d77d86186b1679559cd6b	NA	NA	194048
netinit	6417c75c569312a7f46176260d08fa96	NA	NA	155136
drdisk	1493d342e7a36553c56b2adea150949e	NA	NA	27280
File Name	SHA256 Hash	File Type	Compile Time	Size
turkey.exe	31d3b2101c299bceee38847a3f4982d078e78f31980476189482c1ac5a8c6388	.EXE	1/18/2017 16:12	NA
cc2.exe	3a08840c9fd2181e8bb1a81f0ff4dd103cf973c0bf66a400c7ba59a1953c8f99	.EXE	1/18/2017 7:58:28 AM	NA
msword.exe	6f3c5b949b2fe529456e3d44fd9de723b9f105377f5452c048994066ccb2de30	.EXE	1/23/2017 5:48	NA
cc1.exe	9579a1746a0fb10faee52c5e0dd1d12a23648f0810a909a2beab6b2c1e58ef6c	.EXE	1/16/2017 12:04	NA
googleage.exe	714eb446753c85186b3836ead5824a36e118a77329fc98031ec99ef64ec1cf93	.EXE	1/8/2017 10:37:22 PM	NA
Gate Pass.doc	0219b27a87b08e261dd174e0259a36df073928e3159fe3e5b620cee622e53d8f	.EXE	NA	NA

The following file paths are located at which the various SHAMOON-involved components may be present.

Host-Based Signatures

Droppers:

- %WINDIR%\system32\ntssrv64.exe
- %WINDIR%\system32\ntssrv32.exe

ElDos Driver:

- %WINDIR%\system32\drdisk.sys

Downloader:

- %WINDIR%\system32\netinit.exe

Wipers:

- %WINDIR%\system32\caclsrv.exe
- %WINDIR%\system32\certutl.exe
- %WINDIR%\system32\clean.exe
- %WINDIR%\system32\ctrl.exe
- %WINDIR%\system32\dfrag.exe
- %WINDIR%\system32\dnslookup.exe
- %WINDIR%\system32\dvdquery.exe
- %WINDIR%\system32\event.exe
- %WINDIR%\system32\findfile.exe
- %WINDIR%\system32\gpget.exe
- %WINDIR%\system32\ipsecure.exe
- %WINDIR%\system32\iissrv.exe
- %WINDIR%\system32\msinit.exe
- %WINDIR%\system32\ntfrsutil.exe
- %WINDIR%\system32\ntdsutl.exe
- %WINDIR%\system32\power.exe
- %WINDIR%\system32\rdsadmin.exe
- %WINDIR%\system32\regsys.exe
- %WINDIR%\system32\sigver.exe
- %WINDIR%\system32\routeman.exe
- %WINDIR%\system32\rrasrv.exe
- %WINDIR%\system32\sacses.exe
- %WINDIR%\system32\sfmsc.exe
- %WINDIR%\system32\smbinit.exe
- %WINDIR%\system32\wcscript.exe
- %WINDIR%\system32\ntnw.exe
- %WINDIR%\system32\netx.exe
- %WINDIR%\system32\fsutl.exe
- %WINDIR%\system32\extract.exe

Affiliated configuration files:

- %WINDIR%\inf\usbvideo324.pnf
- %WINDIR%\inf\netimm173.pnf

Additionally created files:

- c:\windows\temp\key8854321.pub

Additionally observed files:

- %WINDIR%\system32\ntssrvr32.bat

Registry Keys Created

SHAMOON is known to create a service for the instantiation of related components.

- HKLM\SYSTEM\CurrentControlSet\Services\NtsSrv
- HKLM\SYSTEM\CurrentControlSet\Services\wow32
- HKLM\SYSTEM\CurrentControlSet\Services\drdisk

Service Configuration:

- Display name: "Microsoft Network Realtime Inspection Service"
- Service name: "NtsSrv"
- Description: "Helps guard against time change attempts targeting known and newly discovered vulnerabilities in network time protocols"

Network-Based Indicators

Network communications of the downloader components have been known to generate the following HTTP traffic patterns:

- http://[HOST]/category/page.php?shinu=

Historical reporter modules have been known to generate traffic with the following HTTP patterns:

- http://[HOST]/ajax_modal/modal/data.asp?mydata=[MYDATA]&uid=[UID]&state=[STATE]

Solution

As of now, individuals and organizations that wish to avoid being compromised by the before mentioned virus should adhere to the following practices:

- Ensure that software on computers, servers and web applications is being regularly updated to prevent known vulnerabilities from being exploited
- Treat unsolicited emails with suspicion. Targeted attacks frequently distribute malware through malicious links and attachments in emails.
- Keep security software up-to-date with the latest definitions

Finally, you need to ensure that the backups are functioning. We also recommend that you have your backup files stored in an offline DR site to avoid a complete data loss in case of any virus in the future.

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae