https://web.archive.org/web/20210126065851/https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html

FireEye Responds to Wave of Destructive Cyber Attacks in Gulf Region

By by FireEye | Advanced Malware

Published: 2016-12-01 · Archived: 2026-04-05 16:44:45 UTC

Threat Research

In 2012, a suspected Iranian hacker group called the “Cutting Sword of Justice” used malware known as Shamoon – or Disttrack. In mid-November, Mandiant, a FireEye company, responded to the first Shamoon 2.0 incident against an organization located in the Gulf states. Since then, Mandiant has responded to multiple incidents at other organizations in the region.

Shamoon 2.0 is a reworked and updated version of the malware we saw in the 2012 incident. Analysis shows the malware contains embedded credentials, which suggests the attackers may have previously conducted targeted intrusions to harvest the necessary credentials before launching a subsequent attack.

FireEye HX and FireEye NX both detect Shamoon 2.0, and our Multi-Vector Virtual Execution (MVX) engine is also able to proactively detect this malware.

The following is a summary of what we know about Shamoon 2.0 based on the samples we’ve analyzed:

- The malware scans the C-class subnet of the IP it has assigned to every interface on the system for target systems.
- The malware then tries to access the ADMIN$, C$\Windows, D$\Windows, and E$\Windows shares on the target systems with current privileges.
- If current privileges aren’t enough to access the aforementioned shares, it uses hard coded, domain specific credentials (privileged credentials, likely Domain Administrator or local Administrator) gained during an earlier phase of the attack to attempt the same.
- Once it has access, it enables the Remote Registry service on the target device and sets HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy to 0 to enable share access.
- Once it has performed the earlier actions, it copies ntssrvr32.exe to the %WINDIR%\system32 of the target system and schedules an unnamed task (e.g. At1.job) to execute the malware.
- The identified malware had a hard coded date to launch the wiping. Systems infected with the malware scheduled the job to start the process shortly thereafter.
- The malware sets the system clock to a random date in August 2012. Analysis suggests this might be for the purposes of ensuring the component (a legitimate driver used maliciously) that wipes the Master Boot Record (MBR) and Volume Boot Record (VBR) is within its test license validity period.
- While the original Shamoon malware attempted to overwrite operating system files with an image of a burning U.S. flag, the recently discovered variant attempts to overwrite Windows operating system files,

although with a different image, a .JPG file depicting the death of Alan Kurdi, a Syrian child migrant who died while attempting to cross the Mediterranean Sea.

The following is guidance for detecting the malware, counteracting its activity, and attempting to prevent it from propagating in an environment. Please note that performing any of these actions could have a negative effect and should not be implemented without proper review and study of the impact of the environment.

- Monitor any events in the SIEM that show dates in August 2012.
- Monitor for system time change events that set the clock back to and from August 2012.
- Monitor for Remote Registry service starts.
- Monitor for changes to the aforementioned registry key value, if the value is currently non-zero.
- Prevent and limit access to the aforementioned shares, which could have significant impact based on setup.
- Prevent client-to-client communication to slow down the spread of the malware, which could also have a significant impact based on setup.
- Monitor filesystems for the creation of any of the filenames provided in the Indicators of Compromise list at the bottom of the post.
- Change the credentials of all privileged accounts and ensure local Administrator passwords are unique per system.

Indicators of Compromise

The following is a set of the Indicators of Compromise for the identified Shamoon variant. We recommend that critical infrastructure organizations and government agencies (especially those in the Gulf Cooperation Council region) check immediately for the presence or execution of these files within their Windows Server and Workstation environments. Additionally, we recommend that all customers continue to regularly review and test disaster recovery plans for critical systems within their environment.

File name: ntssrvr64.exe
Path: %SYSTEMROOT%\System32
Compile Time: 2009/02/15 12:32:19
File size:717,312

File name: ntssrvr32.exe
Path: %SYSTEMROOT%\System32 NA NA
File size: 1,349,632

File name: ntssrvr32.bat
Path: %SYSTEMROOT%\System32 NA
MD5: 10de241bb7028788a8f278e27a4e335f
File size: 160

File name: gpget.exe
Path: %SYSTEMROOT%\System32
PE compile time: 2009/02/15 12:30:41

MD5: c843046e54b755ec63ccb09d0a689674
File Size: 327,680

File name: drdisk.sys
Path: %SYSTEMROOT%\System32\Drivers
Compile time: 2011/12/28 16:51:29
MD5: 76c643ab29d497317085e5db8c799960
File Size: 31,632

File name: key8854321.pub
Path: %SYSTEMROOT%\System32
MD5: b5d2a4d8ba015f3e89ade820c5840639 782

File name: netinit.exe
Path: %SYSTEMROOT%\System32
MD5: ac4d91e919a3ef210a59acab0dbb9ab5
File Size: 183,808
Service Details
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"
Files created:

- %WINDIR%\inf\usbvideo324.pnf
- %WINDIR%\system32\netinit.exe

Dynamic Analysis Observables

RegistryItem HKLM\SYSTEM\CurrentControlSet\Services\NtsSrv\

RegistryItem HKLM\SYSTEM\ControlSet001\Services\NtsSrv\

RegistryItem HKLM\SYSTEM\CurrentControlSet\Services\wow32\

RegistryItem HKLM\SYSTEM\ControlSet001\Services\wow32\

RegistryItem HKLM\SYSTEM\CurrentControlSet\Services\drdisk\

RegistryItem HKLM\SYSTEM\ControlSet001\Services\drdisk\

FileItem C:\Windows\System32\caclsrv.exe

FileItem C:\Windows\System32\certutl.exe

FileItem C:\Windows\System32\clean.exe

FileItem C:\Windows\System32\ctrl.exe

FileItem C:\Windows\System32\dfrag.exe

FileItem C:\Windows\System32\dnslookup.exe

FileItem C:\Windows\System32\dvdquery.exe

FileItem C:\Windows\System32\event.exe

FileItem C:\Windows\System32\extract.exe

FileItem C:\Windows\System32\findfile.exe

FileItem C:\Windows\System32\fsutl.exe

FileItem C:\Windows\System32\gpget.exe

FileItem C:\Windows\System32\iissrv.exe

FileItem C:\Windows\System32\ipsecure.exe

FileItem C:\Windows\System32\msinit.exe

FileItem C:\Windows\System32\netx.exe

FileItem C:\Windows\System32\ntdsutl.exe

FileItem C:\Windows\System32\ntfrsutil.exe

FileItem C:\Windows\System32\ntnw.exe

FileItem C:\Windows\System32\power.exe

FileItem C:\Windows\System32\rdsadmin.exe

FileItem C:\Windows\System32\regsys.exe

FileItem C:\Windows\System32\routeman.exe

FileItem C:\Windows\System32\rrasrv.exe

FileItem C:\Windows\System32\sacses.exe

FileItem C:\Windows\System32\sfmsc.exe

FileItem C:\Windows\System32\sigver.exe

FileItem C:\Windows\System32\smbinit.exe

FileItem C:\Windows\System32\wcscript.exe

Source: https://web.archive.org/web/20210126065851/https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html