Malware: EternalRocks

EternalRocks is a new Network Worm which is the successor to the WannaCry ransomware. EternalRocks leverages some of the same vulnerabilities and exploit tools as WannaCry but is potentially more dangerous because it exploits seven NSA tools that were released as part of the ShadowBrokers dump for infection instead of two used by WannaCry.

So EternalRocks has the potential to spread faster and infect more systems. EternalRocks is currently dormant and isn't doing anything nefarious such as encrypting hard drives. But EternalRocks could be easily weaponized in an instant, making the need for preventive action urgent.

Discovery Credit

Miroslav Stampar, a security researcher who created famous 'sqlmap' tool and a member of the Croatian Government CERT. Stampar learned of EternalRocks after it infected his SMB honeypot. Stampar found that EternalRocks disguises itself as WannaCry to fool security researchers, but instead of dropping ransomware, it gains unauthorized control on the affected computer to launch future cyber attacks.

WannaCry used only two of the SMB exploit tools:

1. EternalBlue — SMBv1 exploit tool
2. DoublePulsar — Backdoor Trojan

EternalRocks leverages seven NSA SMB exploit tools to locate vulnerable systems:

1. EternalBlue — SMBv1 exploit tool
2. EternalRomance — SMBv1 exploit tool
3. EternalChampion — SMBv2 exploit tool
4. EternalSynergy — SMBv3 exploit tool
5. SMBTouch — SMB reconnaissance tool
6. ArchTouch — SMB reconnaissance tool
7. DoublePulsar — Backdoor Trojan

EternalRocks does not have a kill-switch which helped curtail WannaCry and mitigate the ransomware damages. One of the things EternalRocks does is that it leaves the DOUBLEPULSAR implant unprotected, which means other threat actors could leverage EternalRocks infected machines for their own intents and purposes.

Working of EternalRocks Attack

EternalRocks installation takes place in a two-stage process.

During the first stage, EternalRocks downloads the Tor web browser on the affected computers, which is then used to connect to its command-and-control (C&C) server located on the Tor network on the Dark Web.

First stage malware UpdateInstaller.exe (got through remote exploitation with second stage malware) downloads necessary .NET components (for later stages) TaskScheduler and SharpZLib from the Internet, while dropping svchost.exe and taskhost.exe.

According to Stampar, the second stage comes with a delay of 24 hours in an attempt to avoid sandboxing techniques, making the worm infection undetectable. After 24 hours, EternalRocks responds to the C&C server with an archive containing the seven Windows SMB exploits mentioned above.

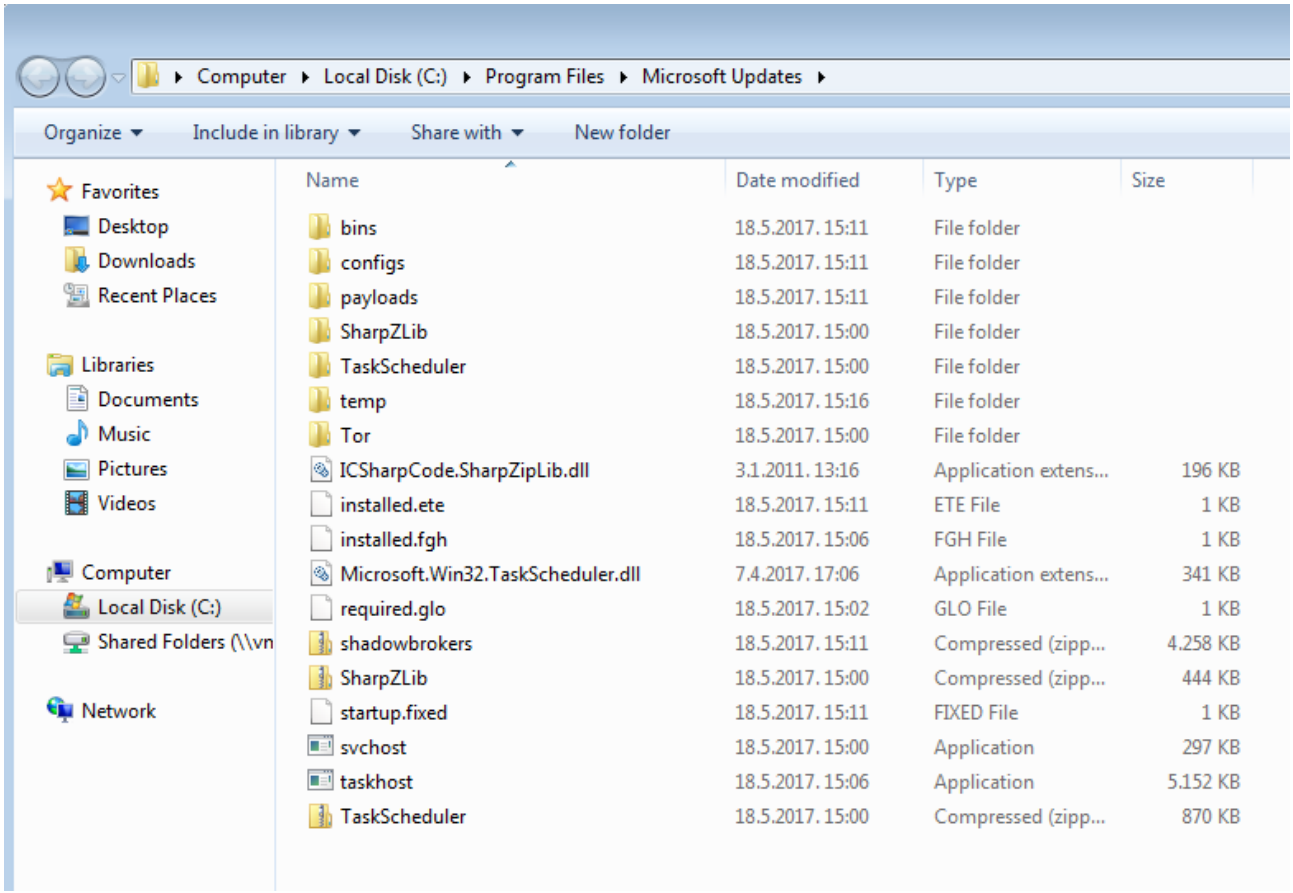
Component ***svchost.exe*** is used for downloading, unpacking and running Tor from archive.torproject.org along with C&C (ubgdgno5eswkhmpy.onion) communication requesting further instructions (e.g. installation of new components).

After initial run it drops the exploit pack shadowbrokers.zip containing all the seven SMB exploits and unpacks contained directories payloads/, configs/ and bins/. After that, starts a random scan of opened 445 (SMB) ports on Internet, while running contained exploits (inside directory bins/) and pushing the first stage malware through payloads (inside directory payloads/). Also, it expects running Tor process from first stage to get further instructions from C&C.

Host Based Indicators

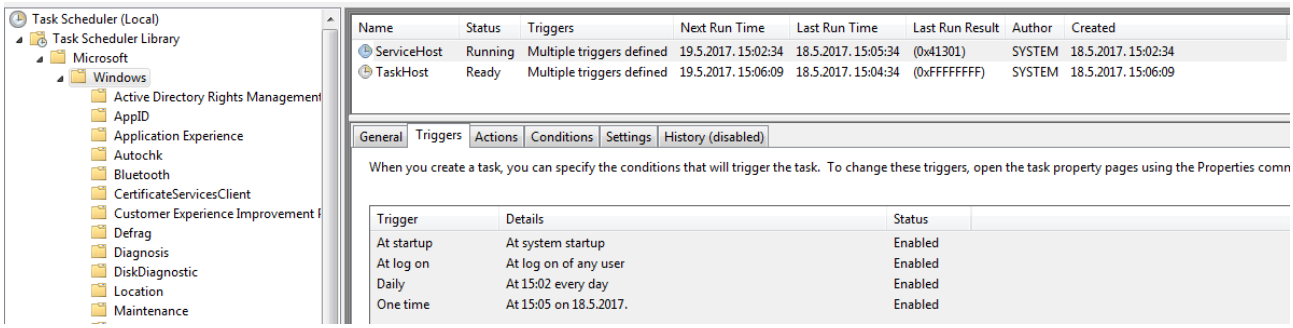
Paths

- c:\Program Files\Microsoft Updates\SharpZLib.zip # in newer variants
- c:\Program Files\Microsoft Updates\svchost.exe
- c:\Program Files\Microsoft Updates\installed.fgh
- c:\Program Files\Microsoft Updates\ICSharpCode.SharpZipLib.dll # in newer variants
- c:\Program Files\Microsoft Updates\Microsoft.Win32.TaskScheduler.dll
- c:\Program Files\Microsoft Updates\SharpZLib\ # in newer variants
- c:\Program Files\Microsoft Updates\temp\tor.zip
- c:\Program Files\Microsoft Updates\temp\Tor\
- c:\Program Files\Microsoft Updates\required.glo
- c:\Program Files\Microsoft Updates\taskhost.exe
- c:\Program Files\Microsoft Updates\TaskScheduler.zip
- c:\Program Files\Microsoft Updates\TaskScheduler\
- c:\Program Files\Microsoft Updates\torunzip.exe # in older variants



Persistence

- Two scheduled tasks ServiceHost and TaskHost having multiple triggers



Mutexes

- {8F6F00C4-B901-45fd-08CF-72FDEFF}
- {8F6F0AC4-B9A1-45fd-A8CF-72FDEFF}
- {8F6F0AC4-B9A1-45fd-A8CF-727220DE8F}
- 20b70e57-1c2e-4de9-99e5-69f369006912

Network indicators

C&C server(s)

- ubgdgno5eswkhmpy.onion

Downloading required .NET components (first stage)

- http://api.nuget.org/packages/taskscheduler.2.5.23.nupkg
- http://api.nuget.org/packages/sharpziplib.0.86.0.nupkg # in newer variants

Comparison between WannaCry, UIWIX and EternalRocks

	WannaCry	UIWIX	EternalRocks
Attack Vectors	SMB vulnerabilities (MS17-010), TCP port 445	SMB vulnerabilities (MS17-010), TCP port 445	SMB vulnerabilities (MS17-010), five vulnerabilities and two tools, TCP port 445
File Type	Executable (EXE)	Dynamic-link Library (DLL)	Executable (EXE)
Appended extension	{original filename}.WNCRY	._{unique id}.UIWIX	N/A
Autostart and persistence mechanisms	Registry	None	Scheduled Tasks
Anti-VM, VM check, or anti-sandbox routines	None	Checks presence of VM and sandbox-related files or folders	None
Network activity	On the internet, scans for random IP addresses to check if it has an open port 445 (Propagation); connects to .onion site using Tor browser (C&C Communication)	Uses mini-tor.dll to connect to .onion site (its C&C) to send encrypted information and gathered information (C&C communication)	On the internet, scans for random IP addresses to check if it has an open port 445 (Propagation) ; connects to .onion site using Tor browser (C&C communication)
Exceptions (doesn't execute if it detects certain system components)	None	Terminates itself if found running in Russia, Kazakhstan, and Belarus	N/A
Exclusions (directories or file types it doesn't encrypt)	Avoids encrypting files in certain directories	Avoids encrypting files in two directories, and files with certain strings in their file name	N/A
Network scanning and propagation	Yes (worm-like propagation)	No	Yes (worm-like propagation)
Kill switch	Yes	No	N/A
Number of targeted file types	176	All files in the affected system except those in its exclusion list	N/A
Shadow copies deletion	Yes	No	N/A
Ransom Notes	Multilingual (27)	English only	N/A

Protection from ransomware

1. Regular Data backup: This helps restore the last saved data and minimise data loss. Keep the back up on a disconnected hard drive or external device on pre-defined regular basis.
2. Prevention: To prevent infiltration of malware, having password protected tools to identify and filter certain file extensions like ".exe" or ". Zip", are essential. Emails that appear suspicious should also be filtered at exchange level. Users need to ensure that hidden file extension is displayed, since it becomes easier to filter them.
3. User awareness: Awareness among users needs to be created to avoid opening unsolicited attachment. Malwares are typically designed to mimic identities of people that users interact with on a regular basis either on a personal or professional level.
4. Rules in IPS: It's necessary to create rules in the Intrusion Prevention Software (IPS) to discard or disallow the opening of files with extension ".exe" from local App data folders or Appdata. Yara rules set has been provided below.
5. Regular patch and upgrades: To prevent leaks or vulnerabilities in software, ensure to regularly update the software versions and apply patches released by vendor.
6. Enable the Windows Firewall: Disallow Tor
7. Randomize the Local Administrator Password Immediately: The malware after infection owns the local SAM database. It may get the local Administrator account password in clear text, or it may only get the hash. Either one can be used to connect to other machines on your network. If all of your computers have the same local user/password combo, the attacker owns all of them.

Yara Rules for EternalRocks detection:

```
rule EternalRocks_UpdateInstaller
{
strings:
$s0 = "C:\\Users\\tmc\\Documents\\" ascii
$s1 = "C:\\Users\\tmc\\Documents\\" wide
$s2 = "20b70e57-1c2e-4de9-99e5-69f369006912" fullword wide
$s3 = "{8F6F0AC4-B9A1-45fd-A8CF-727220DE8F}" fullword wide
$s4 = "ubgdgno5eswkhmpy.onion" fullword wide
$s5 = "Wrote SVCHOST to File System" fullword wide
$s6 = "Going to copy SharpZLib now" fullword wide
$s7 = "Already Copied Task Scheduler" fullword wide
$s8 = "required.glo" fullword wide
$s9 = "\\Tor\\tor.exe \"Microsoft Update Installer\" ENABLE" fullword wide
$s10 = "C:\\Program Files\\Microsoft Updates" fullword wide
$s11 = "MicroBotMassiveNet" fullword ascii

condition:
uint16(0) == 0x5a4d and 2 of them
}

rule EternalRocks_TorUnzip
{
strings:
$s0 = "c:\\Program Files\\Microsoft Updates\\temp\\tor.zip" wide
$s1 = "C:\\Users\\tmc\\Documents\\TorUnzip\\Project1.vbp" wide
$s2 = "TorUnzip" fullword ascii
$s3 = "WindowsUnZip" fullword ascii

condition:
uint16(0) == 0x5a4d and 3 of them
}

rule EternalRocks_svchost
{
strings:
$s0 = "Microsoft.Win32.TaskScheduler" fullword ascii
$s1 = "svchost.exe" fullword ascii
$s2 = "svchost.exe" fullword wide
$s3 = "ConfusedByAttribute" fullword ascii
$s4 = "ICSharpCode.SharpZipLib" fullword ascii
$s5 = "Microsoft 2017" fullword ascii
condition:
uint16(0) == 0x5a4d and all of them
}

rule EternalRocks_taskhost_final
{
strings:
$s0 = "EternalRocks" fullword wide
$s1 = "EternalRocks" fullword ascii
```

```
$s2 = "20D5CCEE9C91A1E61F72F46FA117B93FB006DB51" fullword ascii
$s5 = "4086658a-cbbb-11cf-b604-00c04fd8d565" fullword ascii

condition:
uint16(0) == 0x5a4d and 3 of them
}

rule EternalRocks_shadowbrokers
{
strings:
$s0 = "eternalblue" fullword ascii
$s1 = "eternalchampion" fullword ascii
$s2 = "eternalromance" fullword ascii
$s3 = "eternalsynergy" fullword ascii
$s4 = "shellcode" ascii
$s5 = ".inconfig.xml" ascii

condition:
uint16(0) == 0x4b50 and all of them
}
```

References:

1. https://github.com/stamparm/EternalRocks/
2. http://www.tenable.com/blog/wannacry-2-0-detect-and-patch-eternalrocks-vulnerabilities-now
3. http://thehackernews.com/2017/05/smb-windows-hacking-tools.html
4. http://blog.trendmicro.com/latest-wannacry-uiwix-eternalrocks-shadowbrokers/