# *cert.to* Advisory 2017

## *EternalRock Malware*

### *(1) Short Background*

- EternalRocks is a network worm emerged in first half of May 2017. Originally named as **MicroBotMassiveNet .** EternalRock was discovered when it infected Miroslav Stampars honeypot. Stampar is the creator of sqlmap tool, which is used to detect and exploit SQL injection flaws.

- And discovered that it uses 7 NSA tools via SMB to perform attack:
    1. EternalBlue
    2. EternalChampion
    3. EternalRomance
    4. EternalSynergy
    5. DoublePulsar
    6. ArchiTouch
    7. SmbTouch.

- Once this worm has obtained this initial foothold, it then uses another NSA tool, DOUBLEPULSAR, to propagate to new vulnerable machines.

### *(2) Affected Systems*

- EternalRocks disguises itself as WannaCry to fool researchers. It doesn't appear to be dropping ransomware at the moment, but it leaves PC vulnerable to remote commands for future attacks.

### *(3) What does it do?*

- 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. According to what Stampar said:

  *"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 (e.g. sample) and taskhost.exe (e.g. sample),"*

- 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)," Stampar adds.

- All the seven SMB (Server Message Block) exploits are then downloaded to the infected computer. EternalRocks then scans the internet for open SMB ports to spread itself to other vulnerable systems as well.

## *(4) How to avoid?*

- To make sure that you remain protected, you’re advised
  1. Apply all the security patches
  2. Always make sure to do a back-up for your system and ensure that your system have a fully tested back-up solution in place.
  3. Have a training on how the users can safely use there email in a safe way and protecting its data and personal information.
  4. Also to upgrade to a newer version of Windows.

- For more information you can contact the CERT team

  **CERT-TO**

  Phone: +676 2378 / +676 20100

  Enquiries. : *enquiries@cert.to*

  Report Info: report@cert.to

  Website: http://www.cert.to