Wave of Ransomware attacks

How to safe guard your technology assets

Building a better working world

What is Ransomware?

Ransomware is a type of computer malware that encrypts files, disks and locks computers. The hacker then demands a ransom for decryption tool which has to be paid within a stipulated time in the form of bitcoins.

ShadowBrokers Exploit Release

ShadowBrokers, as part of the set of exploits it collected and last month it released a number of Windows-related exploits. In that, EternalBlue exploit using SMB for Windows hosts up to Windows 8 and Windows Server 2012. Security researchers reported that massive number of ransomware attack using ShadowBrokers exploits, EternalBlue. These exploits were used by malware authors especially ransomware authors in wild. In UK, almost 40 hospitals were running limited operations due to the ransomware attack, WannaCry ransomware variant.

What is Wanna Decryptor Ransomware?

Wanna Decrypter 2.0 ransomware is a fast spreading ransomware that started its assault against hospitals across the UK before spilling across the globe. The first infections were reported around afternoon UK time on Friday 12th May 2017.

This ransomware appears to have exploited a Windows vulnerability for which Microsoft released a patch for in March called MS17-010. That flaw was in the Windows Server Message Block (SMB) service, which Windows computers use to share files and printers across local networks.

Wanna Decryptor is also known as WannaCry, WCry, WanaCrypt and WanaCrypt0r – encrypted files extension are changed to .wnry, .wcry, .wncry and .wncrypt. And we also seen another ransomware variant called AES-Ni ransomware which will comes with note as it used NSA tools/ShadowBroker leak.

This ransomware leverages the AES-128 cryptosystem to lock data down, therefore any further manipulations are only efficient as long as the secret AES key is at the victim's disposal.

Known Victims around the Globe

- NHS (uk) turning away patients, unable to perform x-rays.
- Telefonica (spain)
- FedEx (us)
- University of Waterloo (us)
- Russia interior ministry & Megafon (russia)
- Сбера bank (russia)
- Shaheen Airlines (india, claimed on twitter)
- Train station in frankfurt (germany)
- Neustadt station (germany)
- the entire network of German Rail seems to be affected (@farbenstau)
- Russian Railroads (RZD), VTB russian bank
- Portugal Telecom

What should be done if you are not a victim of this ransomware?

There are multiple preventive steps that could be taken to safeguard your IT assets against this fast spreading infection.

1. Company level

a. Block SMB port access and RDP (Remote Desktop Protocol) to all computers from the internet. Port 445 and 139 for SMB and 3389 for RDP should be blocked.

b. Block SMB for the time being within the company through a group policy or other endpoint security solution.

c. Stop granting any privilege escalation requests to users who want to run an unknown program as an administrator.

d. Ensure all windows OS and Microsoft software are patched especially the MS17-010. Any unsupported or outdated operating systems should either be upgraded or re-configured to stop SMB and RDP.

e. Issue a notice to all employees to not open unknown attachments and emails and if in doubt read emails on their mobile devices without opening the attachments.

f. Disable office macros through a group policy.

g. Make sure all backup solutions are safe guarded. Encourage users to backup their data immediately on a removable and encrypted hard drive and keep it in a safe place and not connected to the computer. No IT administrator or employees should have backup drives mapped to their computers with write access. Only the backup software should have a unique user account with write access to the backup media and users should only have read access to backup media.

h. Make sure each endpoint and server has latest version of a reputable endpoint security solution with latest definition updates.

i. Enable scanning of all attachments at your endpoints and email gateways. See a list of file hashes and IP addresses to block and observe at the end of this advisory.

j. Disable uPNP on all your gateways, firewalls, routers and proxy servers.

2. Employees

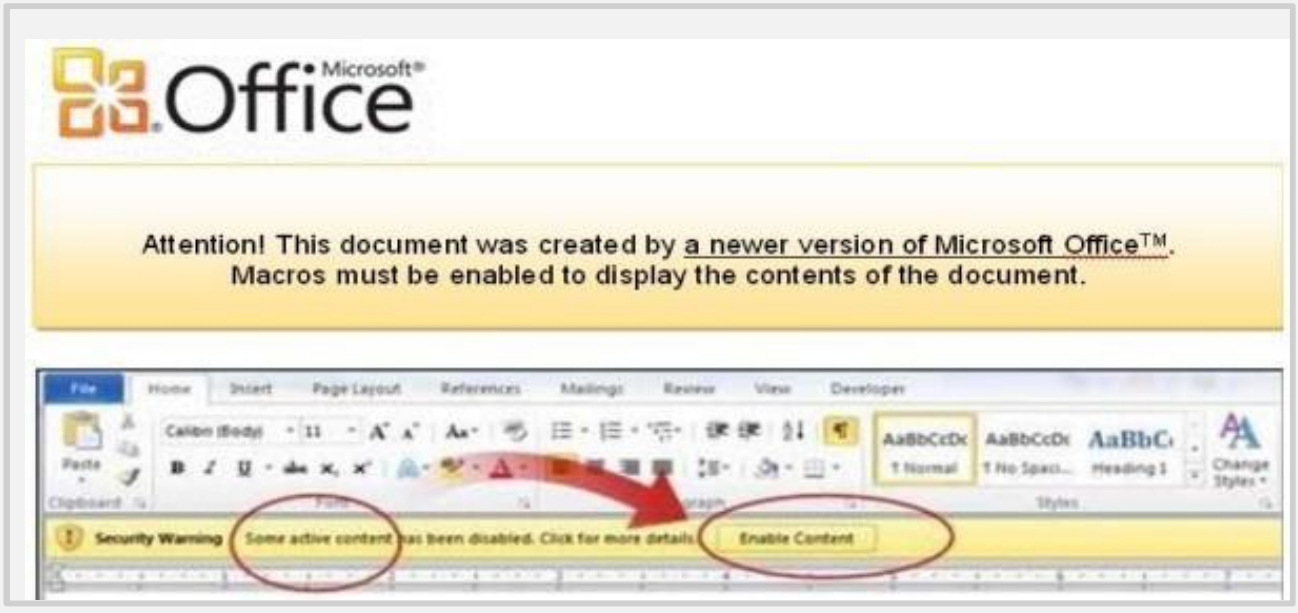
a. Disconnect from the internet and take a backup of all your data on an encrypted, removable hard drive. Disconnect the hard drive and keep it at a secure location after the backup is completed.

b. Do not open attachments from unknown sources and do not download or open unauthorized software.

c. Do not check your personal email on company computer as most free email services will not have advanced security scanning of attachments.

d. If you suspect any unusual hard drive activity on your computer, immediately shut it down and notify your IT administrator.

e. Do not enable macros on office documents and watch out for warnings and alerts such as these:



3. IT Administrators

a. Disconnect all network shares from idle computers and servers.

b. Recheck network shares with write permissions.

c. Change passwords of and safeguard all common domain administrator accounts and refrain from logging in using these accounts. Use these accounts to only authorize specific actions as per standard operating procedures.

d. Make sure backup solutions provide write access to only accounts that are hard configured in the backup solution.

e. User accounts should only have read access.

f. Enable volume shadow copy if possible through group policy and enforce it.

g. Update the endpoint security solution and enable anti-malware or anti-ransomware modules.

h. Prevent privilege escalation of unknown programs and processes.

i. Create a manual signature on your endpoint security solution and monitor for file hashes and extensions specific in this advisory. In case of any such findings on a user computer, disconnect it from the network and shut it down.

j. Call for the incident response team to deal with the situation and plan for a procedural approach before applying an unverified solution from the internet.

What if you are already infected?

If you notice the following screen on your computer or the file extensions of important files have changed to one of those specified at the end of this advisory then unfortunately you are a victim of this ransomware. Follow these steps immediately to reduce the impact:

1. Disconnect all network connections and external storage immediately.
2. Shutdown the computer and inform your IT teams.
3. Do not pay any ransom to the hacker as this fuels the illegal ecosystem and there is no guarantee that you will get the data back.
4. Safeguard and keep your backups ready before experts assist you.

Key signatures associated with the Wanna Decryptor ransomware

1. Ransomware activation notice:

2. Indicators of compromise (IOCs)

File Names:

- @Please_Read_Me@.txt
- @WanaDecryptor@.exe
- @WanaDecryptor@.exe.lnk
- Please Read Me!.txt (Older variant)
- C:\WINDOWS\tasksche.exe
- C:\WINDOWS\qeriuwjhrf
- 131181494299235.bat
- 176641494574290.bat
- 217201494590800.bat
- [0-9]{15}.bat #regex
- !WannaDecryptor!.exe.lnk
- 00000000.pky
- 00000000.eky
- 00000000.res
- C:\WINDOWS\system32\taskdl.exe

Known CnC IP addresses

- 188.166.23.127:443
- 193.23.244.244:443
- 2.3.69.209:9001
- 146.0.32.144:9001
- 50.7.161.218:9001
- 217.79.179.77
- 128.31.0.39
- 213.61.66.116
- 212.47.232.237
- 81.30.158.223
- 79.172.193.32
- 89.45.235.21
- 38.229.72.16
- 188.138.33.220

Domains

- gx7ekbenv2riucmf(.)onion
- 57g7spgrzlojinas(.)onion
- xxlvbrloxvriy2c5(.)onion
- 76jdd2ir2embyv47(.)onion
- cwwnhwhlz52maqm7(.)onion
- sqjolphimrr7jqw6(.)onion
- hxxp://iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea(.)com
- easysupport.us
- fkksjobnn43.org
- trialinsider.com
- ecoland.pro
- holdingair.top
- palindromus.top
- serionbrasil.com.br

- Known hash values
  - ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
  - c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
  - 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
  - 0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
  - 428f22a9afd2797ede7c0583d34a052c32693cbb55f567a60298587b6e675c6f
  - 5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
  - 62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d1b1
  - 72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b033dd
  - 85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
  - a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f78594906b
  - a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
  - b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
  - eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42bcd4
  - 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
  - 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
  - 2c2d8bc91564050cf073745f1b117f4ffdd6470e87166abdfcd10ecdff040a2e
  - 7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
  - a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
  - fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
  - 9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf967
  - b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
  - 4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
  - 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
  - d41d8cd98f00b204e9800998ecf8427e
  - 666c806b76568adb5a6c3d34c434820e
  - a8d30fd8ffd02886818a89ebdd8e7502
  - 6faeaf98d0eaf6671d74bc8e468bddc8ed1e0597
  - 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
  - 11d0f63c06263f50b972287b4bbd1abe0089bc993f73d75768b6b41e3d6f6d49
  - 149601e15002f78866ab73033eb8577f11bd489a4cea87b10c52a70fdf78d9ff
  - 16493ecc4c4bc5746acbe96bd8af001f733114070d694db76ea7b5a0de7ad0ab
  - 190d9c3e071a38cb26211bfffeb6c4bb88bd74c6bf99db9bb1f084c6a7e1df4e
  - 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
  - 2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd
  - 4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
  - 593bbcc8f34047da9960b8456094c0eaf69caaf16f1626b813484207df8bd8af

Known hash values

- 5ad4efd90dcde01d26cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acaec
- 6bf1839a7e72a92a2bb18fbedf1873e4892b00ea4b122e48ae80fac5048db1a7
- 7c465ea7bcccf4f94147add808f24629644be11c0ba4823f16e8c19e0090f0ff
- 9b60c622546dc45cca64df935b71c26dcf4886d6fa811944dbc4e23db9335640
- 9fb39f162c1e1eb55fbf38e670d5e329d84542d3dfcdc341a99f5d07c4b50977
- b3c39aeb14425f137b5bd0fd7654f1d6a45c0e8518ef7e209ad63d8dc6d0bac7
- b47e281bfbeeb0758f8c625bed5c5a0d27ee8e0065ceeadd76b0010d226206f0
- b66db13d17ae8bcaf586180e3dcd1e2e0a084b6bc987ac829bbff18c3be7f8b4
- c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
- d8a9879a99ac7b12e63e6bcae7f965fbf1b63d892a8649ab1d6b08ce711f7127
- e14f1a655d54254d06d51cd23a2fa57b6ffdf371cf6b828ee483b1b1d6d21079
- e8450dd6f908b23c9cbd6011fe3d940b24c0420a208d6924e2d920f92c894a96
- ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
- f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
- F01644082db3fa50ba9f4773f11f062ab785c9db02a3a3cfe022cc69763f631d

URL's

http://146.0.32.144:9001

http://188.166.23.127:443

http://193.23.244.244:443

http://2.3.69.209:9001

http://50.7.161.218:9001

- List of file extensions
  - der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .sxw, .stw, .3ds, .max, .3dm, .ods, .sxc, .stc, .dif, .slk, .wb2, .odp, .sxd, .std, .sxm, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .mdf, .ldf, .cpp, .pas, .asm, .cmd, .bat, .vbs, .sch, .jsp, .php, .asp, .java, .jar, .class, .mp3, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mp4, .mkv, .flv, .wma, .mid, .m3u, .m4u, .svg, .psd, .tiff, .tif, .raw, .gif, .png, .bmp, .jpg, .jpeg, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .ARC, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .dwg, .pdf, .wk1, .wks, .rtf, .csv, .txt, .msg, .pst, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm, .xlsx, .xls, .dotm, .dot, .docm, .docx, .doc,

SNORT Rules and Yara Rules for detection

Snort Rules for EternalBlue Detection:

```
alert tcp $HOME_NET 445 -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response"; flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218; rev:2;)

alert smb any any -> $HOME_NET any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Request (set)"; flow:to_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 18 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:set,ETPRO.ETERNALBLUE; flowbits:noalert; classtype:trojan-activity; sid:2024220; rev:1;)

alert smb $HOME_NET any -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response"; flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218; rev:1;)
```

Yara Rules to Detect

Yara:

```
rule wannacry_1 : ransom
{
meta:
date = "2017-05-12"

Strings:
$s1 = "Ooops, your files have been encrypted!" wide ascii nocase
$s2 = "Wanna Decryptor" wide ascii nocase
$s3 = ".wcry" wide ascii nocase
$s4 = "WANNACRY" wide ascii nocase
$s5 = "WANACRY!" wide ascii nocase
$s7 = "icacls . /grant Everyone:F /T /C /Q" wide ascii nocase

Condition:
any of them
}

rule wannacry_2{
meta:
weight = 100
strings:
$string1 = "msg/m_bulgarian.wnry"
$string2 = "msg/m_chinese (simplified).wnry"
$string3 = "msg/m_chinese (traditional).wnry"
$string4 = "msg/m_croatian.wnry"
$string5 = "msg/m_czech.wnry"
$string6 = "msg/m_danish.wnry"
$string7 = "msg/m_dutch.wnry"
$string8 = "msg/m_english.wnry"
$string9 = "msg/m_filipino.wnry"
$string10 = "msg/m_finnish.wnry"
$string11 = "msg/m_french.wnry"
$string12 = "msg/m_german.wnry"
$string13 = "msg/m_greek.wnry"
$string14 = "msg/m_indonesian.wnry"
$string15 = "msg/m_italian.wnry"
$string16 = "msg/m_japanese.wnry"
$string17 = "msg/m_korean.wnry"
$string18 = "msg/m_latvian.wnry"
$string19 = "msg/m_norwegian.wnry"
$string20 = "msg/m_polish.wnry"
$string21 = "msg/m_portuguese.wnry"
$string22 = "msg/m_romanian.wnry"
$string23 = "msg/m_russian.wnry"
$string24 = "msg/m_slovak.wnry"
$string25 = "msg/m_spanish.wnry"
$string26 = "msg/m_swedish.wnry"
$string27 = "msg/m_turkish.wnry"
$string28 = "msg/m_vietnamese.wnry"
condition:
any of ($string*)
}
```

References

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0147

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0147

https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168

https://github.com/countercept/doublepulsar-detection-script

https://www.bleepingcomputer.com/forums/t/635140/aes-ransomware-aes256-aes-ni-read-this-importanttxt-support-topic/

https://isc.sans.edu/forums/diary/ETERNALBLUE+Windows+SMBv1+Exploit+Patched/22304/

https://kc.mcafee.com/corporate/index?page=content&id=KB89335&elqTrackId=080d6d6426f34a2fb9b7fae0ca16d59a&elq=4afc2fce2f364fe681380f6b3e722410&elqaid=7257&elqat=1&elqCampaignId=4054

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

ED None

Contact:

Rahul Rishi

Partner, Advisory

Email : Rahul.Rishi@in.ey.com

Phone: +91 9811999050

Vidur Gupta

Director, Cyber Security

Ernst & Young - EY

Email: Vidur.gupta@in.ey.com

Phone: +91 9650711300