WannaCry|WannaDecrypt0r NSA-Cyberweapon-Powered Ransomware Worm

- **Virus Name**: WannaCrypt, WannaCry, WanaCrypt0r, WCrypt, WCRY
- **Vector**: All Windows versions before Windows 10 are vulnerable if not patched for MS-17-010. It uses EternalBlue MS17-010 to propagate.
- **Ransom**: between $300 to $600. There is code to 'rm' (delete) files in the virus. Seems to reset if the virus crashes.
- **Backdooring**: The worm loops through every RDP session on a system to run the ransomware as that user. It also installs the DOUBLEPULSAR backdoor. It corrupts shadow volumes to make recovery harder. (source: malwarebytes)
- **Kill switch**: If the website `www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com` is up the virus exits instead of infecting the host. (source: malwarebytes). This domain has been sinkholed, stopping the spread of the worm. Will not work if proxied (source).

update: A minor variant of the virus has been found, it looks to have had the killswitch hexedited out. Not done by recompile so probably not done by the original malware author. On the other hand that is the only change: the encryption keys are the same, the bitcoin addresses are the same. On the other hand it is corrupt so the ransomware aspect of it doesn't work - it only propagates.

SECURITY BULLETIN AND UPDATES HERE: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Microsoft first patch for XP since 2014: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Killswitch source: https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/ https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

Exploit details: https://zerosum0x0.blogspot.com/2017/04/doublepulsar-initial-smb-backdoor-ring.html

Vulnerable/Not Vulnerable

To be infected requires the SMB port (445) to be open, or the machine already infected with DOUBLEPULSAR (and killswitch not registered or somehow blocked, or the network accessing it through a proxy).

The MS17-010 patch fixes the vulnerability.

- Windows XP: Doesn't spread. If run manually, can encrypt files.
- Windows 7,8,2008: can spread unpatched, can encrypt files.
- Windows 10: Doesn't spread. Even though Windows 10 does have the faulty SMB driver.
- Linux: Doesn't spread. If run manually with wine, can encrypt files.

Infections

- NHS (uk) turning away patients, unable to perform x-rays. (list of affected hospitals)
- Nissan (uk) http://www.chroniclelive.co.uk/news/north-east-news/cyber-attack-nhs-latest-news-13029913
- Telefonica (spain) (https://twitter.com/SkyNews/status/863044193727389696)
- power firm Iberdrola and Gas Natural (spain)
- FedEx (us) (https://twitter.com/jeancreed1/status/863089728253505539)
- University of Waterloo (ontario canada)
- Russia interior ministry & Megafon (russia) https://twitter.com/dabazdyrev/status/863034199460261890/photo/1
- VTB (russian bank) https://twitter.com/vassgatov/status/863175506790952962
- Russian Railroads (RZD) https://twitter.com/vassgatov/status/863175723846176768
- Portugal Telecom
- Сбербанк - Sberbank Russia (russia)
- Shaheen Airlines (pakistan, claimed on twitter)
- Train station in frankfurt (germany)
- Neustadt station (germany)
- the entire network of German Rail seems to be affected (@farbenstau)
- in China secondary schools and universities had been affected (source)
- A Library in Oman (@99arwan1)
- China Yanshui County Public Security Bureau (https://twitter.com/95cnsec/status/863292545278685184)
- Renault (France) (http://www.lepoint.fr/societe/renault-touche-par-la-vague-de-cyberattaques-internationales-13-05-2017-2127044_23.php) (http://www.lefigaro.fr/flash-eco/2017/05/13/97002-20170513FILWWW00031-renault-touche-par-la-vague-de-cyberattaques-internationales.php)
- Schools/Education (France) https://twitter.com/Damien_Bancal/status/863305670568837120
- University of Milano-Bicocca (italy)
- A mall in singapore https://twitter.com/nkl0x55/status/863340271391580161
- ATMs in china https://twitter.com/95cnsec/status/863382193615159296
- norwegian soccer team ticket sales https://www.nrk.no/telemark/eliteserieklubber-rammet-av-internasjonalt-dataangrep-1.13515245
- STC telecom (saudia arabia, more, more)
- All ATMs in india closed
- US radiology equipment https://twitter.com/Forbes/status/864850749225934852
- More at https://en.wikipedia.org/wiki/WannaCry_cyber_attack#List_of_affected_organizations they seem to be cataloguing the infections faster/better.

Informative Tweets

- Sample released by ens (thank you ens!): https://twitter.com/the_ens/status/863055007842750465
- Onion C&Cs extracted: https://twitter.com/the_ens/status/863069021398339584
- EternalBlue confirmed: https://twitter.com/kafeine/status/863049739583016960
- Shell commands: https://twitter.com/laurilove/status/863065599919915010
- Maps/stats: https://twitter.com/laurilove/status/863066699888824322
- Core DLL: https://twitter.com/laurilove/status/863072240123949059
- Hybrid-analysis: https://twitter.com/PayloadSecurity/status/863024514933956608
- Impact assessment: https://twitter.com/CTIN_Global/status/863095852113571840

- Uses DoublePulsar: https://twitter.com/laurilove/status/863107992425779202
- Your machine is attacking others: https://twitter.com/hackerfantastic/status/863105127196106757
- Tor hidden service C&C: https://twitter.com/hackerfantastic/status/863105031167504385
- FedEx infected via Telefonica? https://twitter.com/jeancreed1/status/863089728253505539
- HOW TO AVOID INFECTION: https://twitter.com/hackerfantastic/status/863070063536091137
- More of this to come: https://twitter.com/hackerfantastic/status/863069142273929217
- C&C hosts: https://twitter.com/hackerfantastic/status/863115568181850113
- Crypted files *will* be deleted after countdown: https://twitter.com/laurilove/status/863116900829724672
- Claim of attrib [take with salt]: https://twitter.com/0xSpamTech/status/863058605473509378
- Track the bitcoins: https://twitter.com/bl4sty/status/863143484919828481
- keys in pem format: https://twitter.com/e55db081d05f58a/status/863109716456747008
- neel points out a similarity with another virus https://twitter.com/neelmehta/status/864164081116225536
- shadowbrokers talk about responsible disclosure https://steemit.com/shadowbrokers/@theshadowbrokers/oh-lordy-comey-wanna-cry-edition
- another factsheet https://www.secureworks.com/research/wcry-ransomware-analysis

Cryptography details

- Each infection generates a new RSA-2048 keypair.
- The public key is exported as blob and saved to 00000000.pky
- The private key is encrypted with the ransomware public key and saved as 00000000.eky
- Each file is encrypted using AES-128-CBC, with a unique AES key per file.
- Each AES key is generated CryptGenRandom.
- The AES key is encrypted using the infection specific RSA keypair.

The RSA public key used to encrypt the infection specific RSA private key is embedded inside the DLL and owned by the ransomware authors.

- https://haxx.in/key1.bin (the ransomware pubkey, used to encrypt the users private key)
- https://haxx.in/key2.bin (the dll decryption privkey) the CryptImportKey() rsa key blob dumped from the DLL by blasty.

https://pastebin.com/aaW2Rfb6 even more in depth RE information by cyg_x1!!

Bitcoin ransom addresses

3 addresses hard coded into the malware.

- https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

C&C centers

- `gx7ekbenv2riucmf.onion`

- `57g7spgrzlojinas.onion`
- `xxlvbrloxvriy2c5.onion`
- `76jdd2ir2embyv47.onion`
- `cwwnhwhlz52maqm7.onion`

Languages

All language ransom messages available here: https://transfer.sh/y6qco/WANNACRYDECRYPTOR-Ransomware-Messages-all-langs.zip

m_bulgarian, m_chinese (simplified), m_chinese (traditional), m_croatian, m_czech, m_danish, m_dutch, m_english, m_filipino, m_finnish, m_french, m_german, m_greek, m_indonesian, m_italian, m_japanese, m_korean, m_latvian, m_norwegian, m_polish, m_portuguese, m_romanian, m_russian, m_slovak, m_spanish, m_swedish, m_turkish, m_vietnamese

File types

There are a number of files and folders wannacrypt will avoid. Some because it's entirely pointless and others because it might destabilize the system. During scans, it will search the path for the following strings and skip over if present:

- "Content.IE5"
- "Temporary Internet Files"
- " This folder protects against ransomware. Modifying it will reduce protection"
- "\Local Settings\Temp"
- "\AppData\Local\Temp"
- "\Program Files (x86)"
- "\Program Files"
- "\WINDOWS"
- "\ProgramData"
- "\Intel"
- "$"

The filetypes it looks for to encrypt are:

.doc, .docx, .xls, .xlsx, .ppt, .pptx, .pst, .ost, .msg, .eml, .vsd, .vsdx, .txt, .csv, .rtf, .123, .wks, .wk1, .pdf, .dwg, .onetoc2, .snt, .jpeg, .jpg, .docb, .docm, .dot, .dotm, .dotx, .xlsm, .xlsb, .xlw, .xlt, .xlm, .xlc, .xltx, .xltm, .pptm, .pot, .pps, .ppsm, .ppsx, .ppam, .potx, .potm, .edb, .hwp, .602, .sxi, .sti, .sldx, .sldm, .sldm, .vdi, .vmdk, .vmx, .gpg, .aes, .ARC, .PAQ, .bz2, .tbk, .bak, .tar, .tgz, .gz, .7z, .rar, .zip, .backup, .iso, .vcd, .bmp, .png, .gif, .raw, .cgm, .tif, .tiff, .nef, .psd, .ai, .svg, .djvu, .m4u, .m3u, .mid, .wma, .flv, .3g2, .mkv, .3gp, .mp4, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .mp3, .sh, .class, .jar, .java, .rb, .asp, .php, .jsp, .brd, .sch, .dch, .dip, .pl, .vb, .vbs, .ps1, .bat, .cmd, .js, .asm, .h, .pas, .cpp, .c, .cs, .suo, .sln, .ldf, .mdf, .ibd, .myi, .myd, .frm, .odb, .dbf, .db, .mdb, .accdb, .sql, .sqlitedb, .sqlite3, .asc, .lay6, .lay, .mml, .sxm, .otg, .odg, .uop, .std, .sxd, .otp, .odp, .wb2, .slk, .dif, .stc, .sxc, .ots, .ods, .3dm, .max, .3ds, .uot, .stw, .sxw, .ott, .odt, .pem, .p12, .csr, .crt, .key, .pfx, .der

credit herulume, thanks for extracting this list from the binary.

more details came from https://pastebin.com/xZKU7Ph1 thanks to cyg_x11

Some other interesting strings

- BAYEGANSRV\administrator
- Smile465666SA
- wanna18@hotmail.com

credit: nulldot https://pastebin.com/0LrH05y2

Encrypted file format

```
typedef struct _wc_file_t {
    char     sig[WC_SIG_LEN]     // 64 bit signature WANACRY!
    uint32_t keylen;             // length of encrypted key
    uint8_t  key[WC_ENCKEY_LEN]; // AES key encrypted with RSA
    uint32_t unknown;            // usually 3 or 4, unknown
    uint64_t datalen;            // length of file before encryption,
obtained from GetFileSizeEx
    uint8_t *data;               // Ciphertext Encrypted data using AES-128
in CBC mode
} wc_file_t;
```

credit for reversing this file format info: cyg_x11.

Vulnerability disclosure

The specific vulnerability that it uses to propagate is ETERNALBLUE.

This was developed by "equation group" an exploit developer group associated with the NSA and leaked to the public by "the shadow brokers". Microsoft fixed this vulnerability March 14, 2017. They were not 0 days at the time of release.

- https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/
- https://technet.microsoft.com/en-us/library/security/ms17-010.aspx