WannaCry ?

Autore: **Pasquale Scola**

License Information

To cite this work: "*Analisi del Malware WannaCry, 2017, Pasquale Scola*"

WannaPay or not ?

WannaCry ?

WannaCry, noto anche come WanaCrypt0r 2.0, Wanna Decryptor 2.0, WCry 2, WannaCry 2 e Wanna Decryptor 2, è un malware informatico che il 12 Maggio 2017 ha infettato i sistemi informatici di numerose organizzazioni a livello mondiale tra cui: Deutsche Bahn, Portugal Telecom, FedEx, Telefónica, Renault, l'Università degli Studi di Milano-Bicocca, il National Health Service (NHS) britannico, il Ministero dell'interno russo.

Al 22 maggio risultano colpiti più di duecentomila computer in almeno 150 paesi, rendendolo uno dei maggiori virus informatici mai avvenuti nella storia digitale.

Informazioni generali sul Malware

WannaCry sfrutta una vulnerabilità di **SMB** (Server Message Block), un protocollo Windows utilizzato nelle reti locali, e non solo, per condividere file, stampanti ecc. La vulnerabilità viene sfruttata tramite un exploit chiamato **EternalBlue** sviluppato dalla **National Security Agency (NSA)** statunitense per attaccare piattaforme informatiche basate sul sistema operativo Microsoft Windows. **EternalBlue** è stato rubato da un gruppo di hacker chiamati «**The Shadow Brokers»** e pubblicato in rete il 14 aprile 2017. Tale vulnerabilità permette di lanciare payload remoto sul computer della vittima.

Oltre a EternalBlue, WannaCry utilizza **DoublePulsar**, una backdoor persistente per sistemi Windows, sempre realizzata dalla National Security Agency(NSA) statunitense. **DoublePulsar**, come EternalBlue, è stat**a** rubat**a** dal gruppo di hacker «The Shadow Brokers» agli inizi del 2017 e pubblicat**a** in rete. Tale Backdoor viene installata sul computer della vittima dopo aver sfruttato la vulnerabilità del protocollo SMB che permette di lanciare eseguibili da remoto sul computer infetto. La backdoor viene successivamente utilizzata per installare tutte le componenti del Malware WannaCry utili per la sua riproduzione all'interno della LAN di appartenenza, e non solo, e per la cifratura dei file. Allo stesso tempo, viene utilizzata dal team WannaCry per controllare la macchina, lanciare eventuali comandi remoti e avere un feedback del numero di macchine infette.

Oltre al contagio continuo, è stato ipotizzato che WannaCry sia partito da eventuali mail di Phishing. Attualmente (22 Maggio), non vi è alcuna evidenza di ciò.

Informazioni generali sul Malware

La vulnerabilità del protocollo SMB versione 1 di Microsoft era nota sin dagli inizi del 2017. Il 14 marzo 2017 Microsoft ha rilasciato una patch (MS17-010) esclusivamente per i sistemi operativi sotto assistenza.

I computer vulnerabili, dunque, risultano essere quelli con vecchie versioni di Windows (ad esempio Windows XP) e quelli che non hanno installato la patch. Tutte le versioni di Windows 8 e 10 (client e Server) risultano immuni a tale attacco, utilizzando di default nuove versioni del protocollo SMB. Microsoft, con la patch di marzo, ha coperto anche Windows 8 e 10 dato che comunque contenevano SMBv1 (anche se non utilizzato di Default).

Considerata la portata dell'attacco, dopo il 12 maggio 2017, Microsoft ha rilasciato delle patch anche per i sistemi operativi non più sotto la propria assistenza, consigliando comunque di aggiornare il sistema operativo a una versione più recente.

Analisi tecnica del Malware

Principali sistemi operativi target del malware:

- Windows XP (all services pack) (x86) (x64)
- Windows Server 2003 SP0 (x86)
- Windows Server 2003 SP1/SP2 (x86)
- Windows Server 2003 (x64)
- Windows Vista (x86)
- Windows Vista (x64)
- Windows Server 2008 (x86)
- Windows Server 2008 R2 (x86) (x64)
- Windows 7 (all services pack) (x86) (x64)

Architettura altamente modulare

- **EternalBlue**: SMB PROTOCOL EXPLOIT

- **DoublePulsar**: Persistent Backdoor Windows System (Molto potente, lavora a livello kernel)

- **WannaCry:** Logica di funzionamento, crittografia dei file utente basata su algoritmo RSA 2048 BIT.

Scopo del Malware

Malware appartenente alla famiglia dei ransom (riscatto). Chiede alle vittime infette una certa somma di denaro e, in cambio, promette di eliminare il problema creato.

Gli scopi principali sono:

- **Economico;**
- **Politico-sociale;**
- **Fama internazionale;**
- **Divertimento.**

Funzionamento Tecnico del Malware

- Due file iniziali, «mssecsvc.exe» e «tasksche.exe», vengono rilasciati sulla macchina.
- Il file «tasksche.exe» viene eseguito e crea il servizio «mssecsvc2.0». Tale servizio contiene la backdoor persistente. Il servizio esegue vari task (tra cui taskdl.exe e taskse.exe) in background e crea una cartella «Tor/» con nove dll, cioè tutto il necessario per connettersi ad alcuni server della TOR network (rete che garantisce l'anonimato) gestiti dal team WannaCry; cancella tutti i file temporanei ed eventuali copie di backup trovate sulla macchina e si mette in attesa silente fintantoché non riceve l'OK dal Server per far partire l'attacco crittografico; allo stesso tempo lancia l'eseguibile «mssecsvc.exe», utile per la riproduzione.
- L'eseguibile «mssecsvc.exe» fa partire due thread: il primo esegue uno scan di tutta la rete locale della macchina e cerca di infettare il maggior numero di computer possibile, sfruttando la vulnerabilità del protocollo SMB (porte 135, 445); il secondo spara IP pubblici randomici, cercando di infettare eventuali server remoti che hanno porte SMB pubbliche in ascolto.

Funzionamento Tecnico del Malware

Prima di far partire il processo di contagio, l'eseguibile «tasksche.exe» va a fare una richiesta HTTP di tipo GET verso uno strano domino. Se tale dominio **risulta NON raggiungibile**, parte l'infezione, altrimenti il malware si ferma, non continua più a infettare altre macchine né cifra i file della macchina dove risiede.

Una sorta di kill switch, impostato dagli autori di WannaCry per bloccare l'infezione e la propagazione del virus informatico, allo scopo, sostanzialmente, di avere la possibilità di bloccarlo in un dato momento.

Tale kill switch è stato casualmente scoperto da un giovane analista di malware, **Marcus Hutchins**, noto su Twitter con il nome di MalwareTech. Dopo aver fatto un'analisi dei flussi di rete generati dal malware, il ventiduenne inglese ha notato una strana richiesta HTTP verso il seguente il link:

- http://iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/ **(Non accedere a questo link sotto eventuali reti aziendali, potrebbe far partire dei falsi alert impostati dagli amministratori della rete dopo gli attacchi avvenuti il 12 Maggio)**

Successivamente, con circa 10 dollari ha registrato il dominio come pubblico e ha bloccato la diffusione della versione attuale di WannaCry. Al link troverete la frase seguente: «*where the bots party hard and the researchers harder*»

Ovviamente i computer che avevano già ricevuto la cifratura dei file non hanno potuto beneficiare di questa scoperta.

Funzionamento tecnico

Durante il processo di cifratura dei file, il malware procede innanzitutto ad individuare le directory principali sulla macchina (C:\, D:\, E:\ ecc..), successivamente applica la crittografia tramite algoritmo RSA a 2048 bit. I file all'interno della macchina risultano tutti oscurati e in alcuni casi viene anche cambiato il formato in «.wannacry/wanadecritptor ecc..».

Dopo il processo di crittografia appare la schermata del malware, con tutte le informazioni utili e la richiesta di pagamento basato su BitCoin. Il BitCoin è una moneta elettronica che garantisce la totale anonimità del mittente e del destinatario. Il concetto di banca (quale ente centrale) sparisce totalmente. Tutti i pagamenti sono decentralizzati, basandosi sulla Blockchain Technology.

È presente anche la possibilità di decriptare alcuni file prima del pagamento in modo da mostrare all'utente che il malware è in grado di decifrare i file. Ovviamente, questo non assicura che dopo il pagamento i file vengano ripristinati.

Funzionamento tecnico

Ci sono vari tipi di file e cartelle che WannaCry non attacca per evitare la destabilizzazione del sistema operativo:

- "Content.IE5"
- "Temporary Internet Files"
- "\Local Settings\Temp"
- "\AppData\Local\Temp"
- "\Program Files (x86)"
- "\Program Files"
- "\WINDOWS"
- "\ProgramData"
- "\Intel"
- "$"

Funzionamento tecnico

I seguenti formati di file vengono attaccati da WannaCry:

.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

Portafogli BitCoin utilizzati dagli Hacker

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

Dettagli della crittografia

- WannaCry genera una coppia di chiavi RSA-2048.
- La chiave pubblica è salvata in 00000000.pky
- La chiave privata viene cifrata con una chiave pubblica di WannaCry (differente dalla precedente) nel file 00000000.eky
- Ciascun file viene cifrato tramite AES-128-CBC, con unico AES key per file.
- La AES key viene generata tramite CryptGenRandom.
- La AES key viene criptata usando la chiave pubblica RSA creata in precedenza.

Chiavi note

Public Key note utilizzate dal Malware:

- https://haxx.in/key1.bin (**download diretto del file bin**)
- https://haxx.in/key2.bin (**download diretto del file bin**)
- https://pastebin.com/aaW2Rfb6

Funzionamento tecnico

Macchina con Windows 7:

Funzionamento tecnico

Esecuzione del Malware:

Funzionamento tecnico

Finestra di richiesta del pagamento:

Recupero File

Se l'utente non dispone di una copia di backup dei file, il recupero di questi ultimi è molto difficile.

Altre caratteristiche sul Malware

- Come descritto in precedenza, il malware utilizza la rete TOR per comunicare con i server di WannaCry. La TOR network (conosciuta anche come Deep Web) è una rete nata per scopi di ricerca. Successivamente, sono stati fatti diversi abusi su questa rete ed è stata utilizzata per scopi illegali.

- **I flussi verso questa rete non possono essere bloccati del tutto dalle organizzazioni. Utilizzando dei flussi https su porta 443, questi ultimi non possono essere bloccati da eventuali firewall dato che sono protocolli e porte lecite. E' possibile inserire i nodi più conosciuti della rete TOR in una blacklist, ma questo va solo a minimizzare il problema, poiché tale rete è in continua espansione.**

- Si ipotizza che il periodo di attività del malware sia durato qualche settimana, ovvero che in tale periodo siano state infettate il maggior numero di macchine, e che, successivamente, dall' 11/12 Maggio 2017, l'attacco sia partito. Si presume che il WannaCry team abbia fatto partire l'attacco (ovvero che i server abbiano comunicato ai client sulle macchine di far partire il processo di cifratura), in **un momento di picco online di computer infetti nel mondo**.

Domini e IP Tor utilizzati

(Lista non esaustiva)

- 188.166.23.127:443 - Tor Exit Node
- 193.23.244.244:443 - Tor Exit Node
- 2.3.69.209:9001 - Tor Exit Node
- 146.0.32.144:9001 – Tor Exit Node
- 50.7.161.218:9001 - Tor Exit Node
- 128.31.0.39 - Tor Exit Node
- 213.61.66.116 - Tor Exit Node
- 212.47.232.237 - Tor Exit Node
- 81.30.158.223 - Tor Exit Node
- 79.172.193.32 - Tor Exit Node

Domini e IP Tor utilizzati

Tor C2s (lista non esaustiva)

- xxlvbrloxvriy2c5.onion
- cwwnhwhlz52maqm7.onion
- gx7ekbenv2riucmf.onion
- 57g7spgrzlojinas.onion
- 76jdd2ir2embyv47.onion

Hash Values dei file WannaCry

hash values osservati

- c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
- 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
- 0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
- 428f22a9afd2797ede7c0583d34a052c32693cbb55f567a60298587b6e675c6f
- 5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
- 62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d1b1
- 72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b033dd
- 85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
- a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f78594906b
- a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
- b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
- eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42bcd4
- 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
- 2c2d8bc91564050cf073745f1b117f4ffdd6470e87166abdfcd10ecdff040a2e
- 7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
- a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
- fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
- 9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf967
- b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
- 4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
- 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
- ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

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;
```

Cosa fare per difendersi

- Per i normali utenti è conveniente seguire ed installare le nuove patch rilasciate dalla casa madre (nel caso di WannaCry, Microsoft Windows) del sistema operativo (magari con l'opzione di aggiornamento automatico). E' conveniente avere sempre una nuova versione del sistema operativo sotto assistenza della casa costruttrice.
- Le grosse aziende non possono limitarsi ad installare le nuove patch in tempo (accorgimento, questo, comunque spesso non rispettato), ma devono fare grosse attività di prevenzione: avere settori di ricerca applicata nell'ambito della Computer Security è un must. È necessario collaborare con i gruppi di ricerca universitari a livello mondiale e seguire community internazionali nell'ambito delle quali vengono pubblicate quasi in real-time le nuove vulnerabilità scoperte.
- Attività quotidiana alla scoperta di nuove vulnerabilità.
- Occorre essere attivi, e non passivi (la vulnerabilità del protocollo SMBv1 era nota da inizio 2017)!!!
- Inoltre, tutti i colossi digitali hanno aperto dei programmi denominati «Bug Bounty», attraverso i quali coloro che hanno scoperto eventuali vulnerabilità nei loro sistemi, vengono invitati alla segnalazione in cambio di un compenso in denaro. Grosse vulnerabilità prevedono compensi milionari, soprattutto se trattasi di quei programmi di grosso uso di massa (es. Windows, Google Chrome ecc..). Ovviamente, non sempre tali vulnerabilità vengono segnalate al vendor, ma sono invece talvolta utilizzate nel mercato dell'illegalità.
- In generale, il «Bug Bounty» ha avuto un grosso successo in questi ultimi anni: Facebook, ad esempio, ha dichiarato di ricevere molte segnalazioni (in molti casi anche gravi) e, grazie a questo, ha potuto sanare molti problemi di sicurezza. La spesa totale sostenuta da Facebook per il Bug Bounty dal 2011 ad oggi risulta essere superiore ai 5 milioni di dollari (source: https://www.facebook.com/notes/facebook-bug-bounty/facebook-bug-bounty-5-million-paid-in-5-years/1419385021409053/), somma sicuramente inferiore rispetto al caso in cui tali vulnerabilità fossero state utilizzate contro l'azienda: avrebbero portato innumerevoli danni ai sistema oltre al conseguente danno di immagine.

Impatto Sociale

Giornali di tutto il mondo hanno parlato di questo attacco.

Heat Map

Mappa di diffusione del malware WannaCry nel mondo (source: https://twitter.com/joetidy/status/863121806626095105/photo/1):

Organizzazioni colpite(lista non esaustiva)

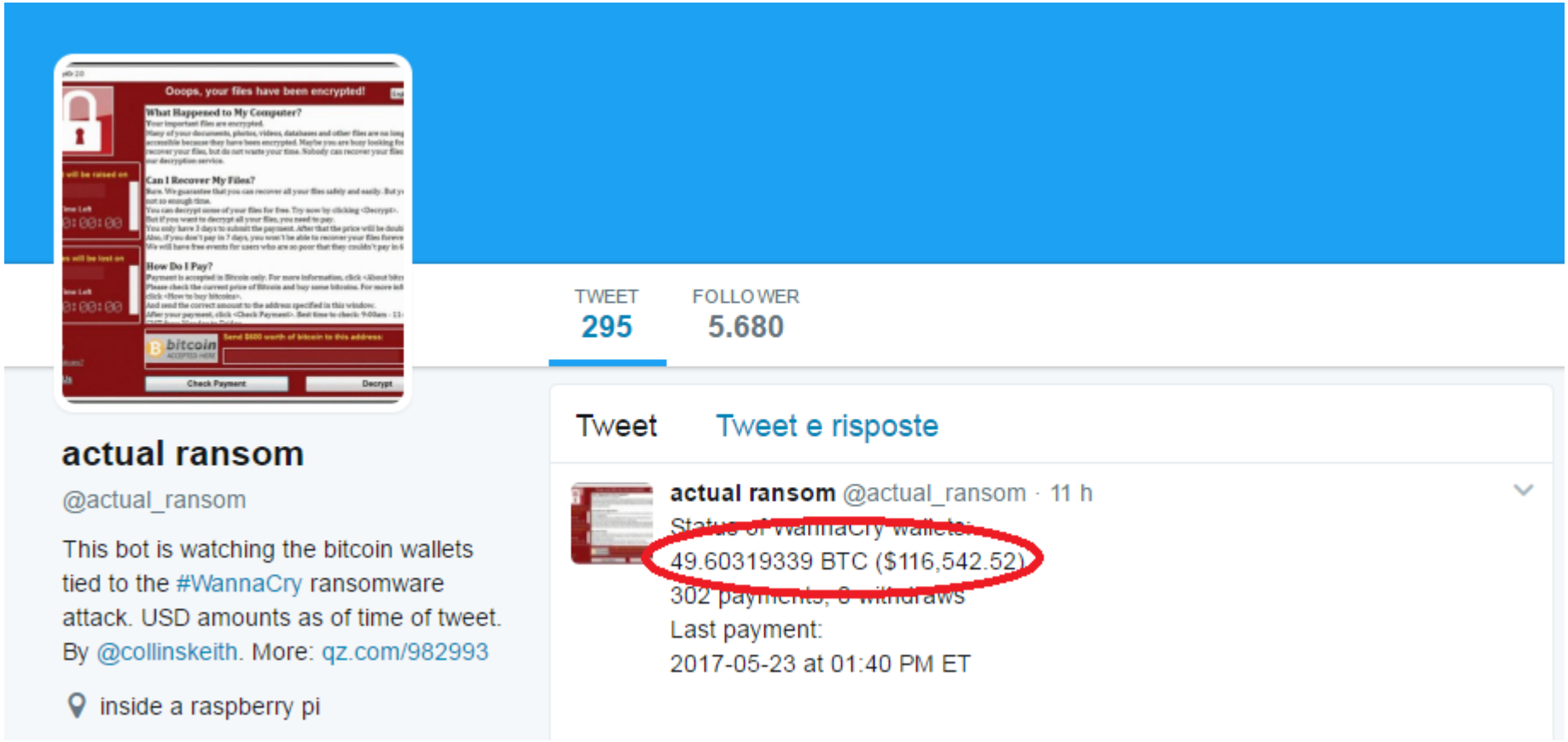
- NHS (uk) turning away patients, unable to perform x-rays. (list of affected hospitals)
- Nissan (uk) http://www.chroniclelive.co.uk/news/north-east-news/cyber-attack-nhs-latest-news-13029913
- Telefonica (spain) (https://twitter.com/SkyNews/status/863044193727389696)
- power firm Iberdrola and Gas 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.

Portafoglio BitCoin

- Un utente Twitter ha creato un Twitter bot che legge in tempo reale il portafoglio bitcoin utilizzato dagli hacker: ogni tre ore comunica la somma totale raggiunta e ogniqualvolta viene eseguito un pagamento , esso viene segnalato.

- Al 24 Maggio, il numero di pagamenti ricevuti dagli hacker risulta essere 302 per un totale di 49.60319339 BTC ($116,542.52)

Portafoglio BitCoin



Source: https://twitter.com/actual_ransom

Modello di Business di WannaCry

Apparentemente, il modello di business di questo malware si basa su una richiesta di riscatto di circa 300-600 dollari per vittima.

Il business maggiore scatenato , tuttavia, è stato di tutt'altra natura:

- **Business sociale**, scatenato dai vari social network e quotidiani mondiali: tale business sociale supera di gran lunga l'irrisoria somma intascata finora (18 Maggio, 116,542.52 dollari) dagli autori del malware.

- Crescita di importanza delle aziende che svolgono ruoli di sicurezza informatica nel mondo.

Lo scopo reale di tale malware risulta ancora ignoto.

Link Utili

WannaCry Real time Map:
https://intel.malwaretech.com/botnet/wcrypt

Esecuzione del malware (video)
https://www.youtube.com/watch?v=4MMeSneDBNs

Altri Link
http://www.news.com.au/technology/online/hacking/massive-cyber-attack-creates-chaos-around-the-world/news-story/b248da44b753489a3f207dfee2ce78a9

https://steemit.com/shadowbrokers/@theshadowbrokers/oh-lordy-comey-wanna-cry-edition

https://www.thesun.co.uk/tech/3562470/wannacry-ransomware-nhs-cyber-attack/

https://krebsonsecurity.com/tag/wanna-cry-ransomware/

https://bitcoin.org/it/

https://twitter.com/malwaretechblog

https://steemit.com/news/@mariaalmeida/hackers-threaten-to-sell-malicious-code-used-in-ransomware-attacks

https://en.wikipedia.org/wiki/DoublePulsar

NEWS

- Sample released by 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