Seguridad-Análisis de Ransomware

Ciberataque GLOBAL: Ramsoware WannaCry

Cesar Farro

https://medium.com/@cesarfarro

cesar.farro@gmail.com

Who am I:

Más (17) años en Seguridad de la Información en los últimos cinco (05) años en el área de Producto. Ingeniero Electrónico por la Universidad Privada del Norte y ha finalizado una maestría en Marketing en la Universidad del Pacífico del Perú. Certificación de Seguridad SANS GIAC Firewall Analyst, SANS GIAC Auditor, Lead Auditor ISO 27001, CheckPoint Administrator, ISS/IBM Security Analyst.

Fuentes:
(1) https://www.linkedin.com/in/cesar-farro-flores/

Índice:

- Definición
- Ramsoware antes de Mayo 2017
- Impacto Global
- Timeline
- Sistema Afectados
- Bitcoins
- Métodos de infección
- Recomendaciones
- Prevención
- Herramienta y Recursos Usados

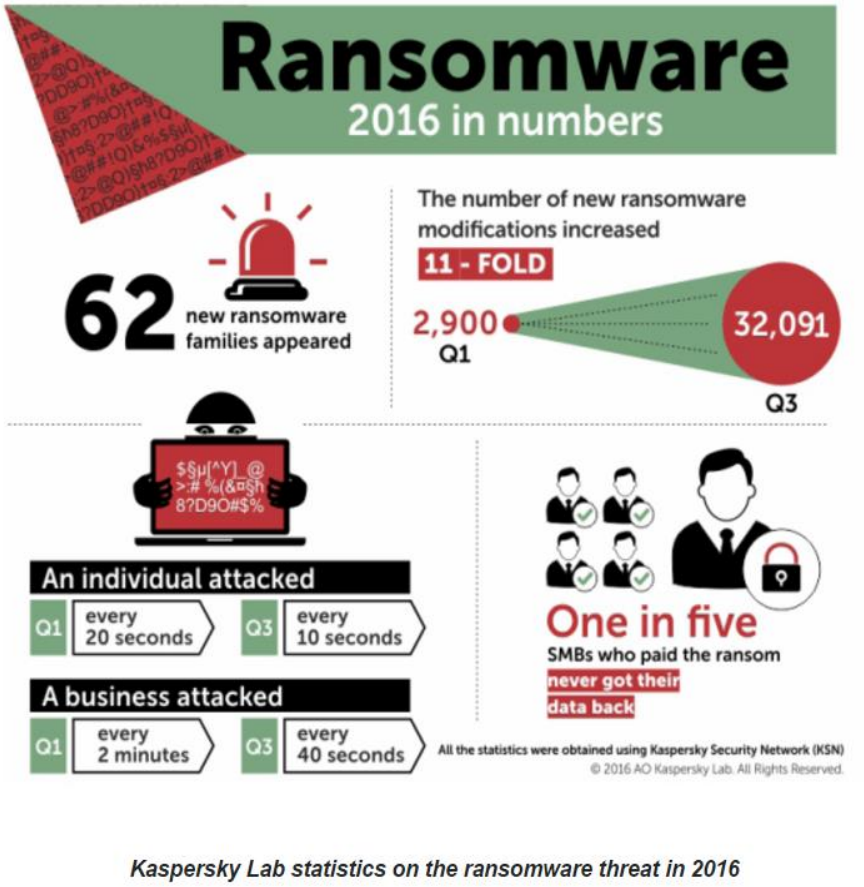
Definición:

Ransomware es un tipo de programa que restringe el acceso a determinados archivos y pide un rescate Bitcoins a cambio de quitar esta restricción.

Se hicieron populares en Rusia y su uso creció internacionalmente en junio del **2013**.

El método de propagación más común es mediante el envío de *correos electrónicos* maliciosos *(1)* .

Fuentes:
(1) https://www.incibe.es/protege-tu-empresa/avisos-seguridad/oleada-ransomware-correos-electronicosc



Kaspersky Lab statistics on the ransomware threat in 2016

Locky ransomware has so far been spread across 114 countries #KLReport

	Name	Verdicts*	percentage of users**
1	CTB-Locker	Trojan-Ransom.Win32.Onion / Trojan-Ransom.NSIS.Onion	25.32
2	Locky	Trojan-Ransom.Win32.Locky / Trojan-Dropper.JS.Locky	7.07
3	TeslaCrypt (active till May 2016)	Trojan-Ransom.Win32.Bitman	6.54
4	Scatter	Trojan-Ransom.Win32.Scatter / Trojan-Ransom.BAT.Scatter / Trojan-Downloader.JS.Scatter / Trojan-Dropper.JS.Scatter	2.85
5	Cryakl	Trojan-Ransom.Win32.Cryakl	2.79
6	CryptoWall	Trojan-Ransom.Win32.Cryptodef	2.36

Fuentes:
(1) https://securelist.com/analysis/kaspersky-security-bulletin/76757/kaspersky-security-bulletin-2016-story-of-the-year/
(2) https://blog.kaspersky.com/ransomware-in-targeted-attacks/6728/
(3) https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf

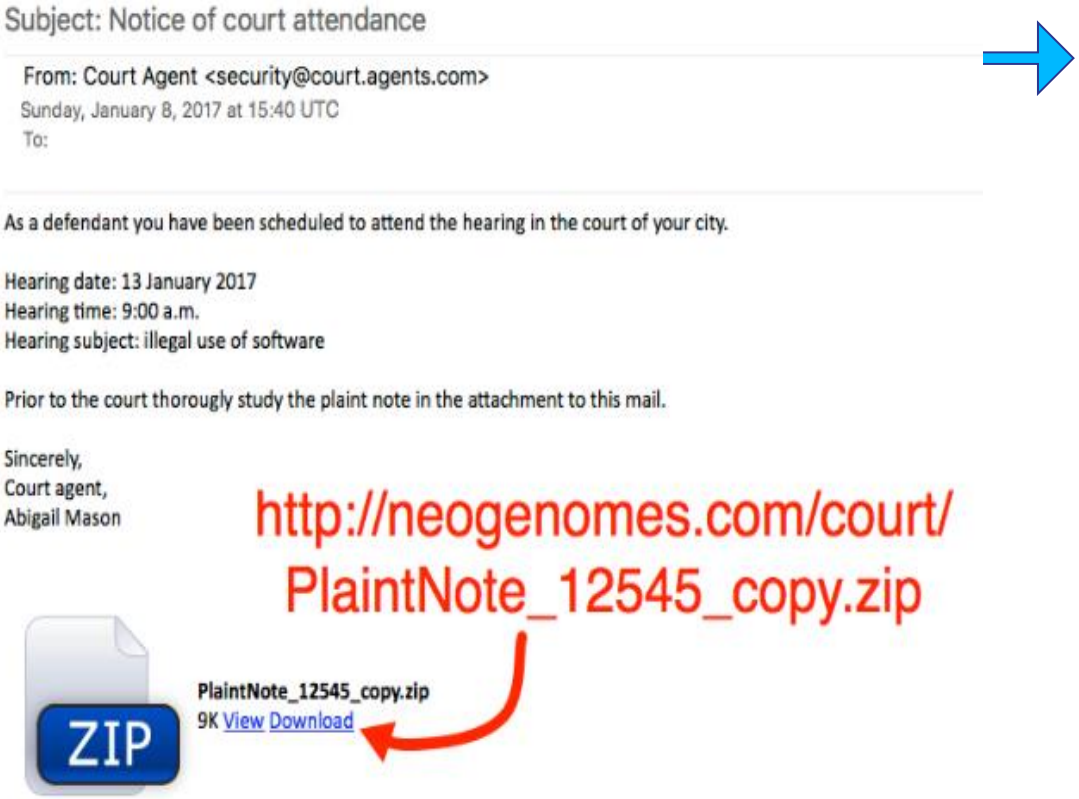
CryptoLocker, Petya,Revenge

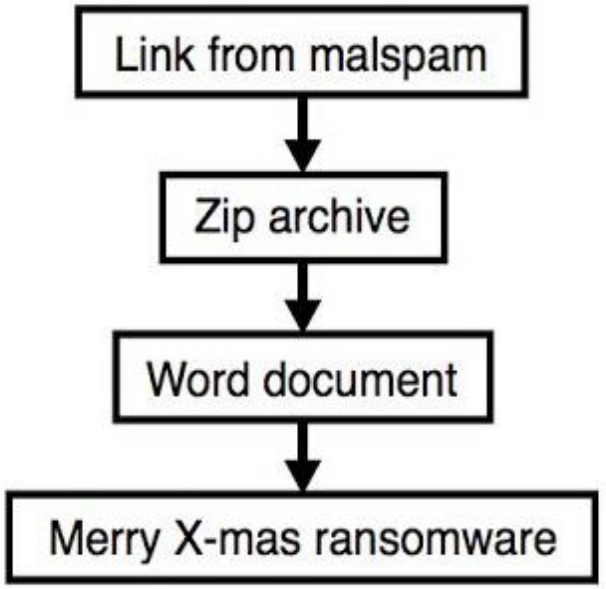
Web Server, Android, blocjed:

```
<?php
if ($_GET["page"] == "index") echo <<<ENDECHO
    <h2>Attention! What happened?</h2>

    <p>Your personal files are encrypted by <font color="red"><b>CTB-Locker</b></font>.<br>
    Your scripts, documents, photos, databases and other important files have been encrypted with strongest
        encryption algorithm AES-256 and unique key, generated for this site.</p>

    <p>Decryption key is stored on a secret Internet server and <b>nobody</b> can decrypt your files until you pay
        and obtain the decryption key.</p>
```


Infección, secuencia de pasos:

Método de Infección más común utilizando un correo electrónico, ejemplo:





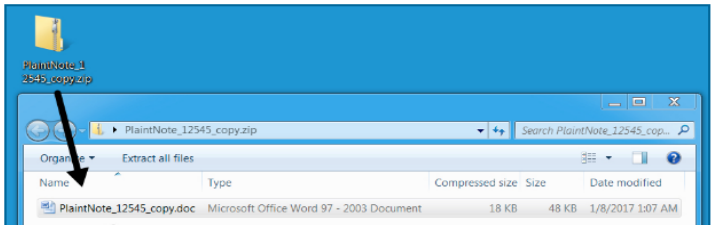
Fuentes: (1) https://isc.sans.edu/forums/diary/Merry+XMas+ransomware+from+Sunday+20170108/21905

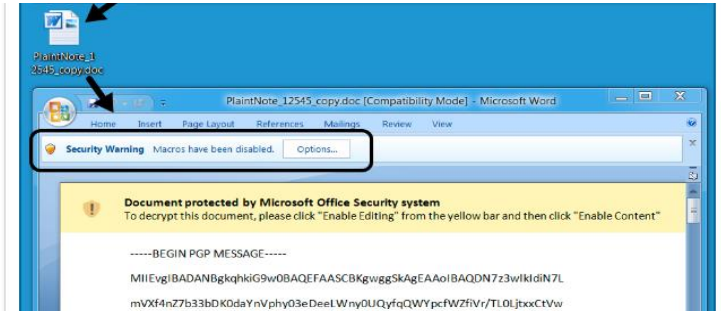
Herramientas y Recursos usados:

- **Herramientas:**
  - SSMA, Simple Static Malware Analyzer, Autor: Lasha Khasaia, https://github.com/secrary
  - IDA PRO, Desensamblador Interactivo.
  - Wireshark, Analizador de paquetes de Red.
  - JPEXS Free Flash Decompiler, Descompilador.
  - Pestudio, Analisis Estático de Malware, https://www.winitor.com/binaries.html
  - TCP View, Regshot, Process Explorer, SysInternals, https://technet.microsoft.com/en-us/sysinternals
- **Recursos:**
  - http://www.malware-traffic-analysis.net/
  - https://www.virustotal.com/
  - https://www.hybrid-analysis.com
  - https://malwr.com/analysis/
  - http://contagiodump.blogspot.pe/
  - https://cartilha.cert.br/ransomware/
- **Agradecimientos:**
  - Lasha Khasaia, https://secrary.com/SSMA
  - André R. Landim, CAIS/RNP, https://www.rnp.br/servicos/seguranca
  - Geffrey Velasquez, https://pe.linkedin.com/in/geffreyvelasquez
  - Carlos Toledo, https://www.linkedin.com/in/cftoledo/
  - Sergio de lo Santos, https://www.elevenpaths.com/es/index.html

Infección, secuencia de pasos:

Próximos pasos:



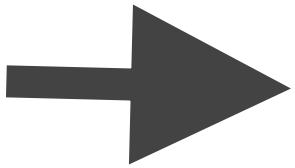


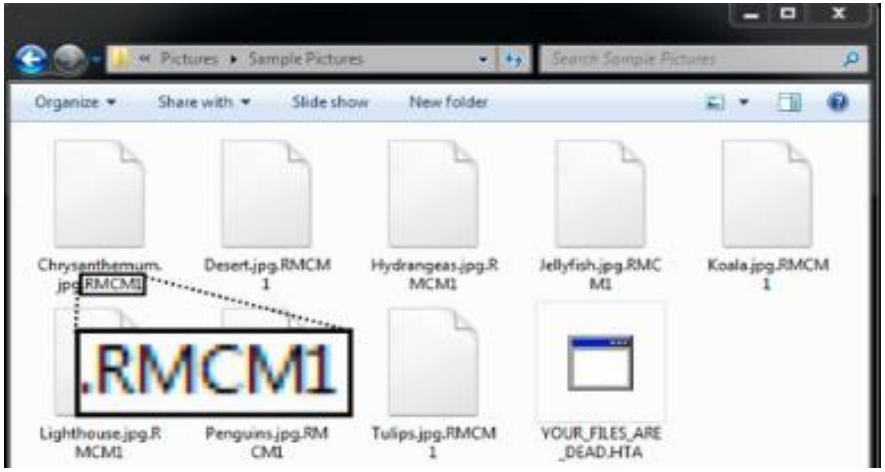
Fuentes:
(1) https://www.bleepingcomputer.com/news/security/-merry-christmas-ransomware-now-steals-user-private-data-via-diamondfox-malware/
(2) https://isc.sans.edu/forums/diary/Merry+XMas+ransomware+from+Sunday+20170108/21905

Infección, Analizando:

Archivos personales Cifrados:

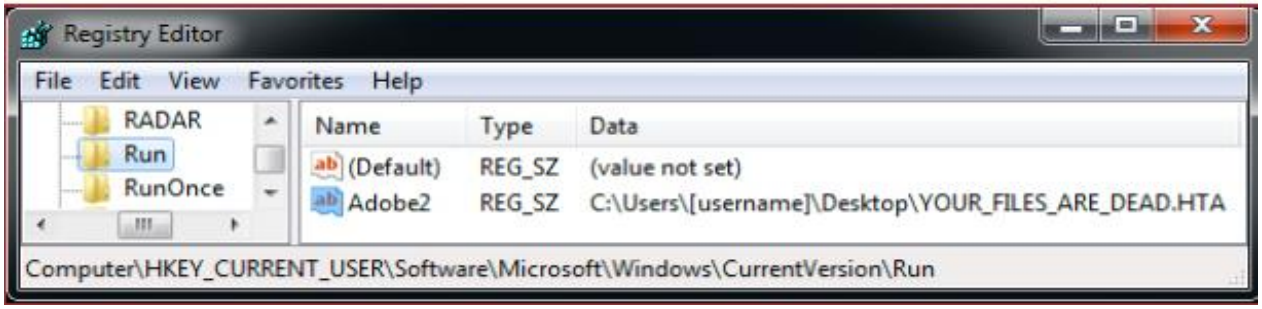
- Chrysanthemum.RMCM1
- Desert.jpg.RMCM1
- Hydranfeas.jpg.RMCM1
- Jellyfish.jpg.RMCM1
- Koala.jpg.RMCM1





Registros en Windows:

- Entrada Registry,Notificación Ramsoware aparesca al momento de logearse: YOUR_FILES_ARE_DEAD.HTA



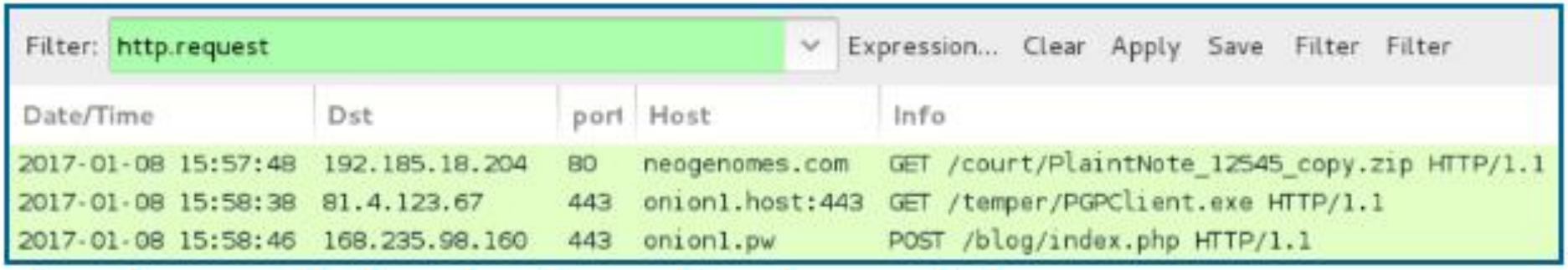
Fuentes:
(1) https://isc.sans.edu/forums/diary/Merry+XMas+ransomware+from+Sunday+20170108/21905

Infección, Analizando:

Actividad a nivel de conexiones:

- IP LAN -> 192.185.18.204:80: neogenomes.com
  - GET /court/**PlainNote_12545_copy.zip** HTTP/1.1
- IP LAN -> 81.4.123.67:443:onion1.host
  - GET /temper/PGPClient.exe HTTP/1.1
- IP LAN -> 168.235.98.160:443: onion1.pw
  - GET/blog/index.php HTTP/1.1

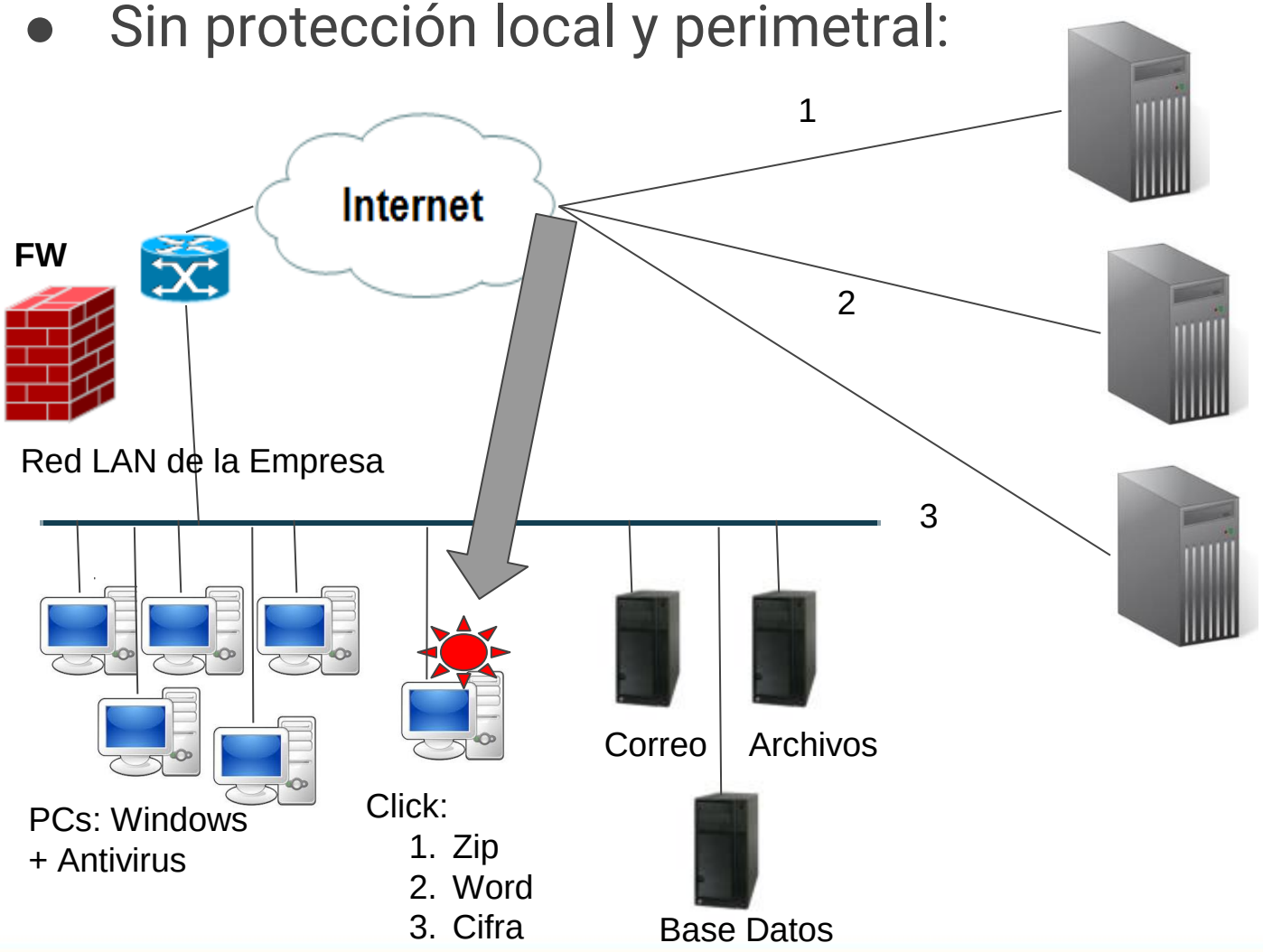
443, pero HTTP/1.1



Fuentes: (1) https://isc.sans.edu/forums/diary/Merry+XMas+ransomware+from+Sunday+20170108/21905

Infección, Analizando:

- Sin protección local y perimetral:



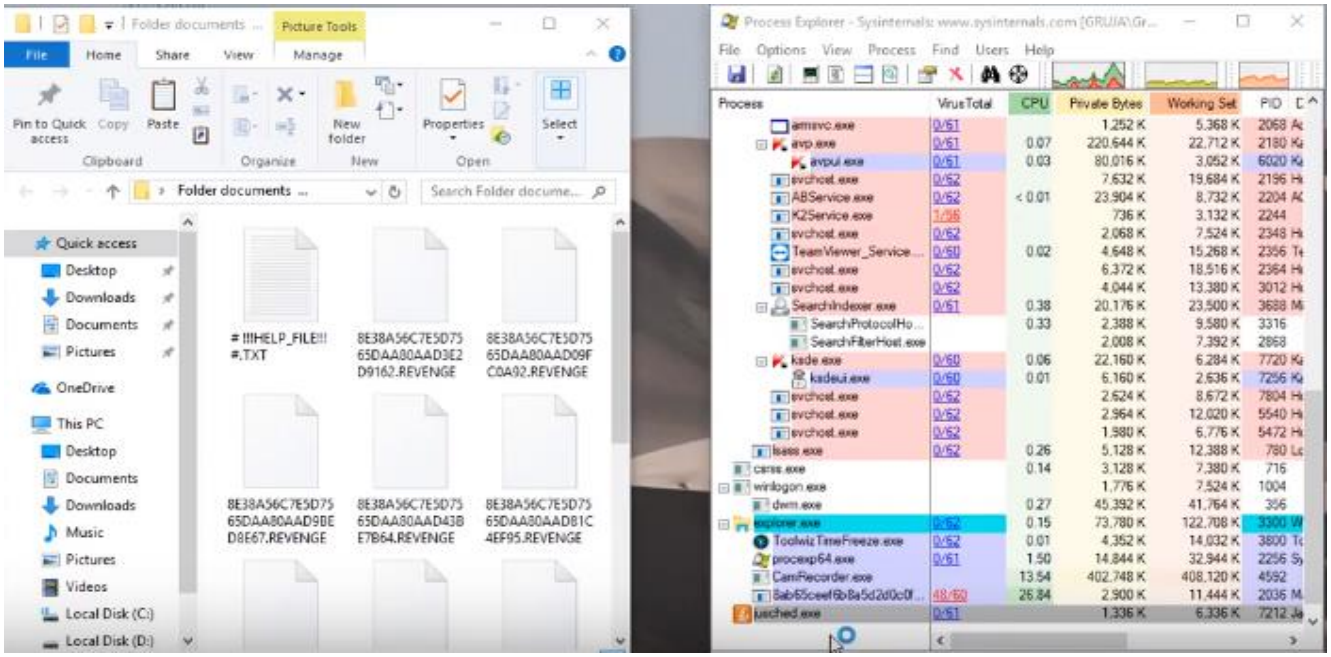
- **neogenomes.com** (Site Hackeado)
- 192.185.18.204:80:
- GET
- PlainNote_12545_copy.zip
- HTTP/1.1

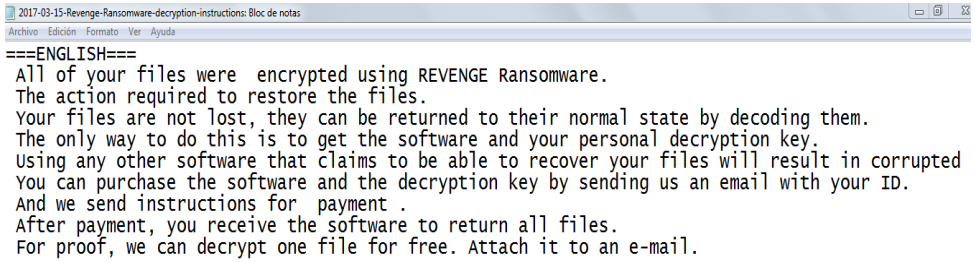
- **onion1.host**
- 81.4.123.67:443:
- GET
- temper/**PGPClient.exe**
- HTTP/1.1

- **onion1.pw**
- 168.235.98.160:443
- GET/blog/index.php
- HTTP/1.1

FW

Revenge Ramsoware: 2017-03-15





Fuentes:
(1) http://www.malware-traffic-analysis.net/2017/03/15/index3.html
(2) https://www.youtube.com/watch?v=x6bfGzo1HYI&t=43s

CONTACT E-MAILS:
EMAIL: rev00@india.com
EMAIL: revenge00@writeme.com
EMAIL: rev_reserv@india.com
ID (PERSONAL IDENTIFICATION):
0123456789ABCDEF

- ZIP archive of the pcap: **2017-03-15-EITest-Rig-EK-sends-Revenge-ransomware.pcap.zip**
  1. 2017-03-15-EITest-Rig-EK-sends-Revenge-ransomware.pcap
- ZIP archive of the malware: **2017-03-15-EITest-Rig-EK-sends-Revenge-ransomware-malware-and-artifacts.zip**
  1. 2017-03-15-EITest-Rig-EK-flash-exploit.swf
  2. 2017-03-15-EITest-Rig-EK-landing-page.txt
  3. 2017-03-15-EITest-Rig-EK-payload-Revenge-ransomware-5uhcwesi.exe
  4. 2017-03-15-Revenge-Ransomware-decryption-instructions.txt
  5. 2017-03-15-page-from-activaclinics.com-with-injected-EITest-script.txt

Analizando:2017-05-03 payload-Revenge-ransomware-5uhcwesi.exe

virustotal

PAYLOAD SECURITY

malwr

MALWARE-TRAFFIC-ANALYSIS.NET

SHA256:	8ab65ceef6b8a5d2d0c0fb3ddbe1c1756b5c224bafc8065c161424d63937721c
Nombre:	2017-03-15-ElTest-Rig-EK-payload-Revenge-ransomware-5uhcwesi.exe
Detecciones:	51 / 60
Fecha de análisis:	2017-05-09 03:49:18 UTC (hace 3 días, 2 horas)

5uhcwesi.exe

Filename	5uhcwesi.exe
Size	114KiB (116224 bytes)
Type	peexe
Description	PE32 executable (GUI) Intel 80386, for MS Windows
Architecture	32 Bit
SHA256	8ab65ceef6b8a5d2d0c0fb3ddbe1c1756b5c224bafc8065c161424d63937721c
Compiler/Packer	Microsoft visual C++ 8

Resources

Language	TURKISH
Icon	

Fuentes:
(1) https://www.virustotal.com/es/file/8ab65ceef6b8a5d2d0c0fb3ddbe1c1756b5c224bafc8065c161424d63937721c/analysis/1494301758/
(2) https://malwr.com/analysis/YzE1ZmZlY2MxZjllNDNjM2FhNzA1YWU2ZTk3N2JhOTg/
(3) https://www.hybrid-analysis.com/sample/8ab65ceef6b8a5d2d0c0fb3ddbe1c1756b5c224bafc8065c161424d63937721c?environmentId=100

Revenge Ramsoware, 5uhcwesi.exe

- **Filename:** 5uhcwesi.exe
- **Size:** 114KiB (116224 bytes)
- **Type:** peexe
- **Description:** PE32 executable (GUI) Intel 80386, for MS Windows
- **Architecture:** 32 Bit
- **SHA256:** 8ab65cecc161424d63937721c
- **Compiler/Packer:** Microsoft visual C++ 8
- **Rources, Language:** Turkish (1)

```
Number of Sections: 4

Section VirtualAddress VirtualSize SizeofRawData Entropy
.text   0x1000                27925         28160 6.46280371170478
.rdata  0x8000                23720         24064 4.857779619442116
.data   0xe000                11348          3584 2.202884041705499
.rsrc   0x11000               59184         59392 7.117123971032891
```

(2) SSMA Simple Static Malware Analyzer

- **IP: 91.207.7.77** , TCP Port 80, 5uhcwesi.exe PID Asociado: 3620, ASN: 47142 (PP Andrey Kiselev)

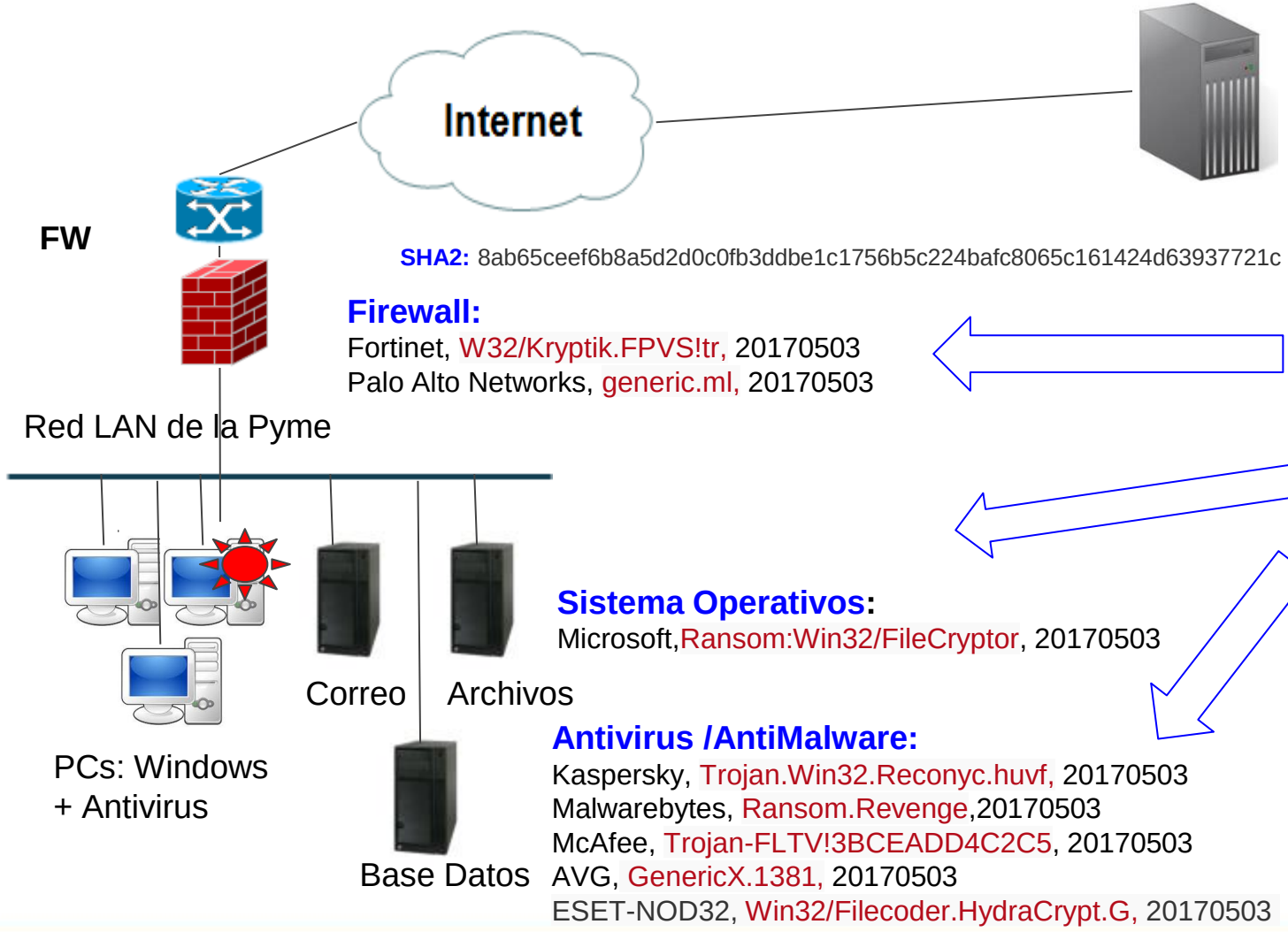
Ukraine

HTTP Traffic

Endpoint	Request	URL	Data
91.207.7.77:80	POST	/images/temp/4gallery/temp_reserv/gallery.php	POST /images/temp/4gallery/temp_reserv/gallery.php HTTP/1.1 Content-Type: application/x-www-form-urlencoded Host: 91.207.7.77 Content-Length: 26 Cache-Control: no-cache ⇄ 200 OK More Details
91.207.7.77:80	POST	/images/temp/4gallery/temp_reserv/gallery.php	POST /images/temp/4gallery/temp_reserv/gallery.php HTTP/1.1 Content-Type: application/x-www-form-urlencoded Host: 91.207.7.77 Content-Length: 29 Cache-Control: no-cache ⇄ 200 OK More Details

Fuentes:
(1) http://www.malware-traffic-analysis.net/2017/03/15/index3.html
(2) https://secrary.com/SSMA

Analizando en la Red: 2017-05-03 payload-Revenge-ransomware-5uhcwesi.exe



- 5uhcwesi.exe
- 191.207.7.77:80
- POST /imagenes/temp/4gallery/temp/_reserv/gallery.php

SHA2: 8ab65ceef6b8a5d2d0c0fb3ddbe1c1756b5c224bafc8065c161424d63937721c

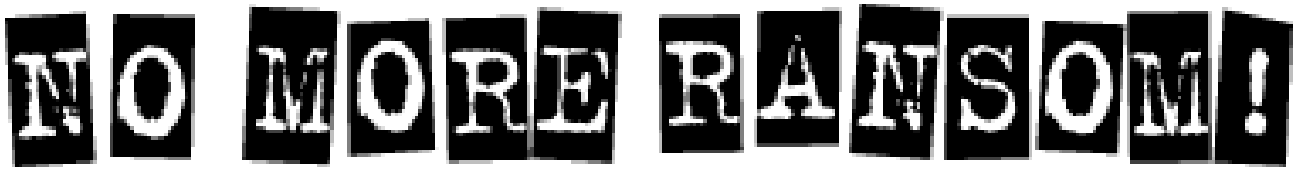
Firewall:
Fortinet, W32/Kryptik.FPVS!tr, 20170503
Palo Alto Networks, generic.ml, 20170503

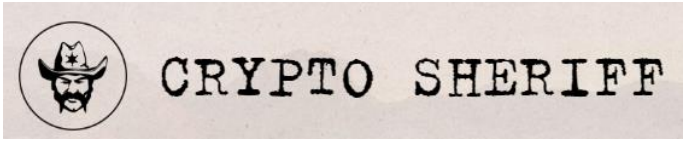
Sistema Operativos:
Microsoft,Ransom:Win32/FileCryptor, 20170503

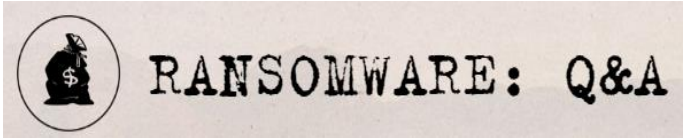
Antivirus /AntiMalware:
Kaspersky, Trojan.Win32.Reconyc.huvf, 20170503
Malwarebytes, Ransom.Revenge,20170503
McAfee, Trojan-FLTV!3BCEADD4C2C5, 20170503
AVG, GenericX.1381, 20170503
ESET-NOD32, Win32/Filecoder.HydraCrypt.G, 20170503

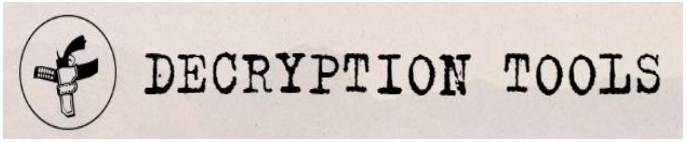
¿ Cómo se da cuenta el Administrador de Seguridad que se trata del mismo ramsoware, sí se están reportando con diferentes nombres?

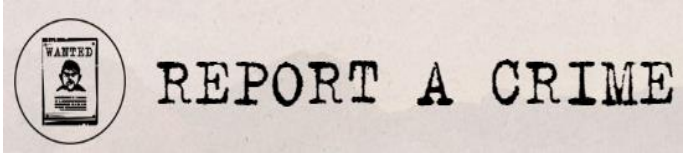
Iniciativas:

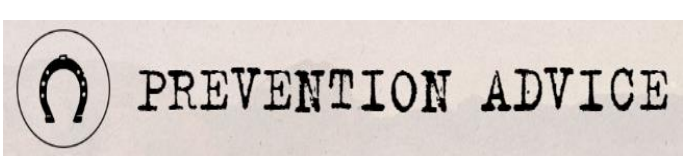


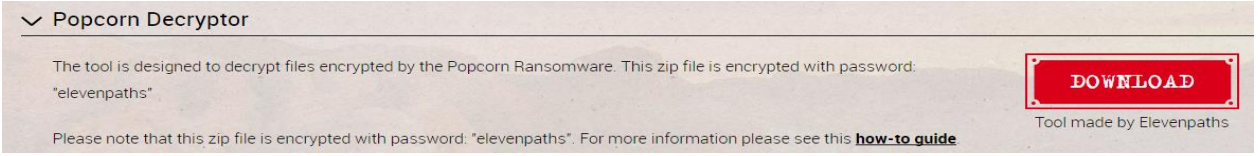












1. **Back-up!Back-up!Back-up!**
2. **Use robust antivirus software**
3. **Keep all the software on your computer up to date**
4. **Trust no one. Literally, Never open attachments in emails from someone you dont know.**
5. **Enable the "Show file extentions" option in the windows settings on your computer.**
6. **Disconnect immediately from the internet (such as home Wi-Fi)**

Fuentes:
https://www.nomoreransom.org/decryption-tools.html/
http://www.mcafee.com/us/downloads/free-tools/tesladecrypt.aspx

Recomendaciones:

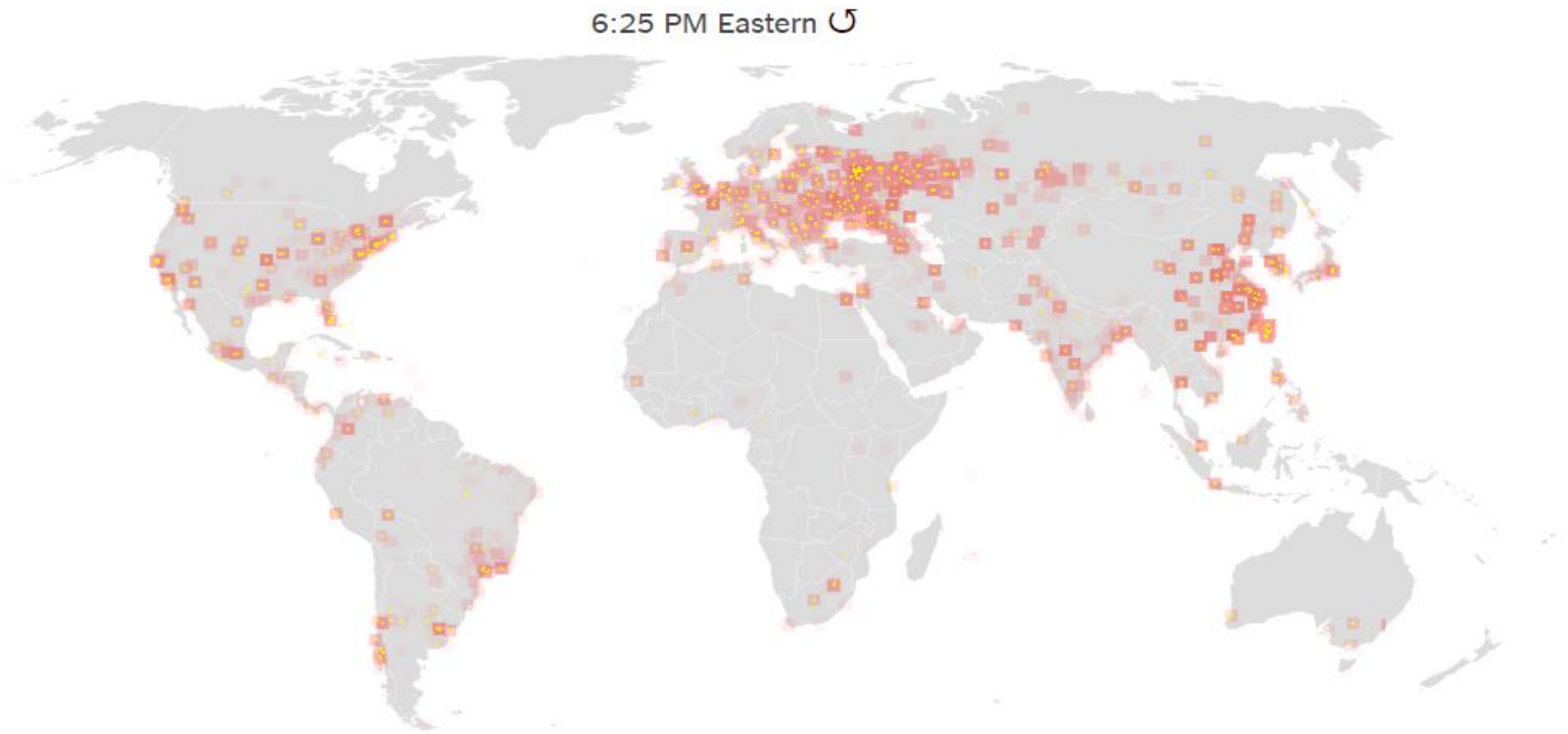
- **Cuidado-** Concientizar a tus empleados.
- **No pagar por el rescate.**
- **Backup** es la solución más efectiva.
- **Backup** automáticos de acuerdo a la alteración de los datos.
- Tenga **actualizado** las versiones del Sistema Operativo, Aplicaciones, Base de Datos.
- Tener versiones desactualizadas son potenciales vulnerables.
- Desistale los programas que no usa.
- Use programas originales.
- Instale un **Antivirus (Anti Malware)** mantenga actualizado de preferencia diariamente.
- **Antivirus** para validar discos duros y unidades removibles.
- Instale un **AntiSpam** y configure para verificar archivos adjuntos en correo electrónico,
- **Firewall** personal y actualizado

Fuentes:
(1) https://cartilha.cert.br/ransomware/

Antes del 12 de Mayo

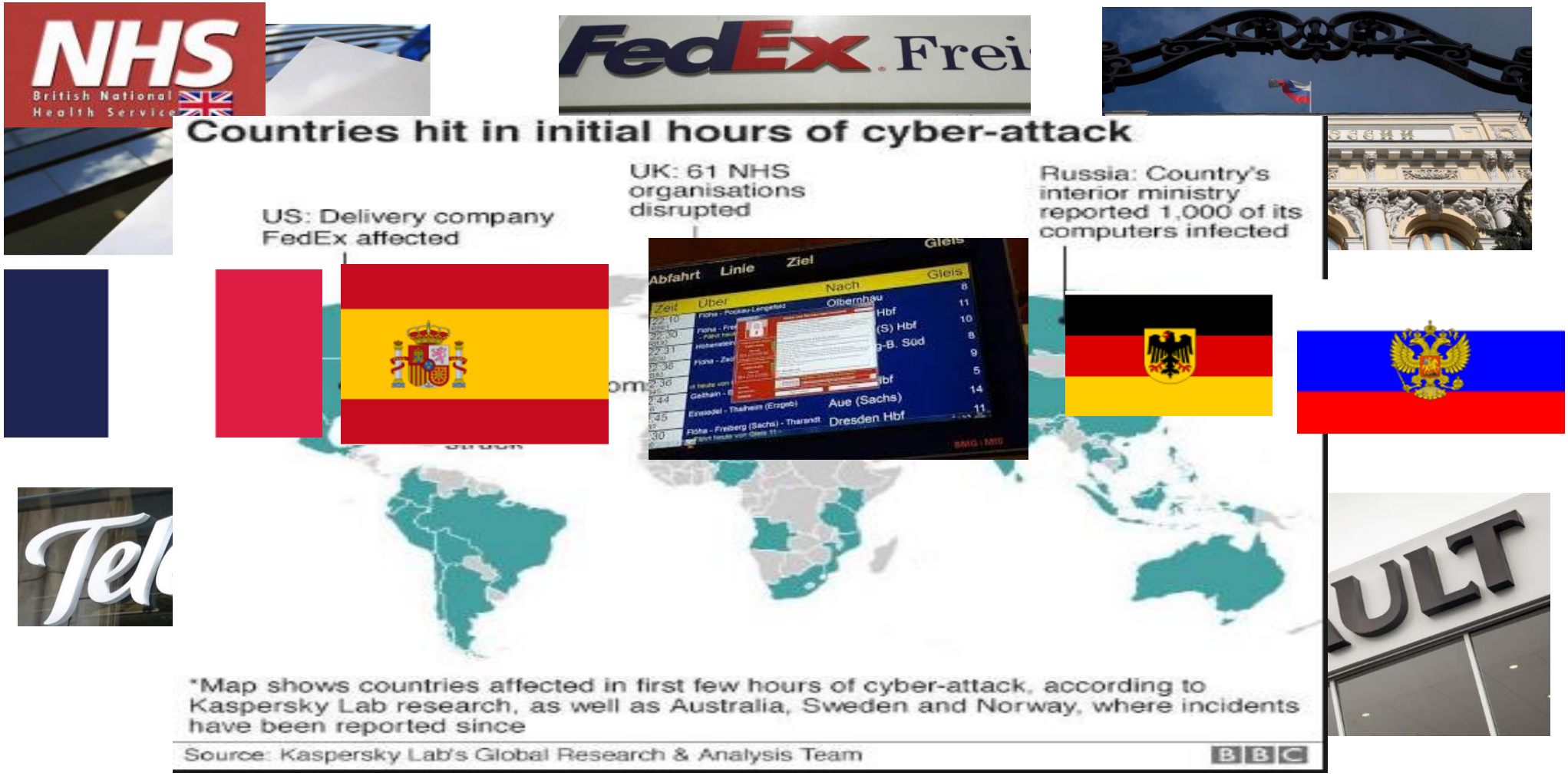
¿Estábamos listos para lo que venía?

WannaCry - Viernes 12 de Mayo

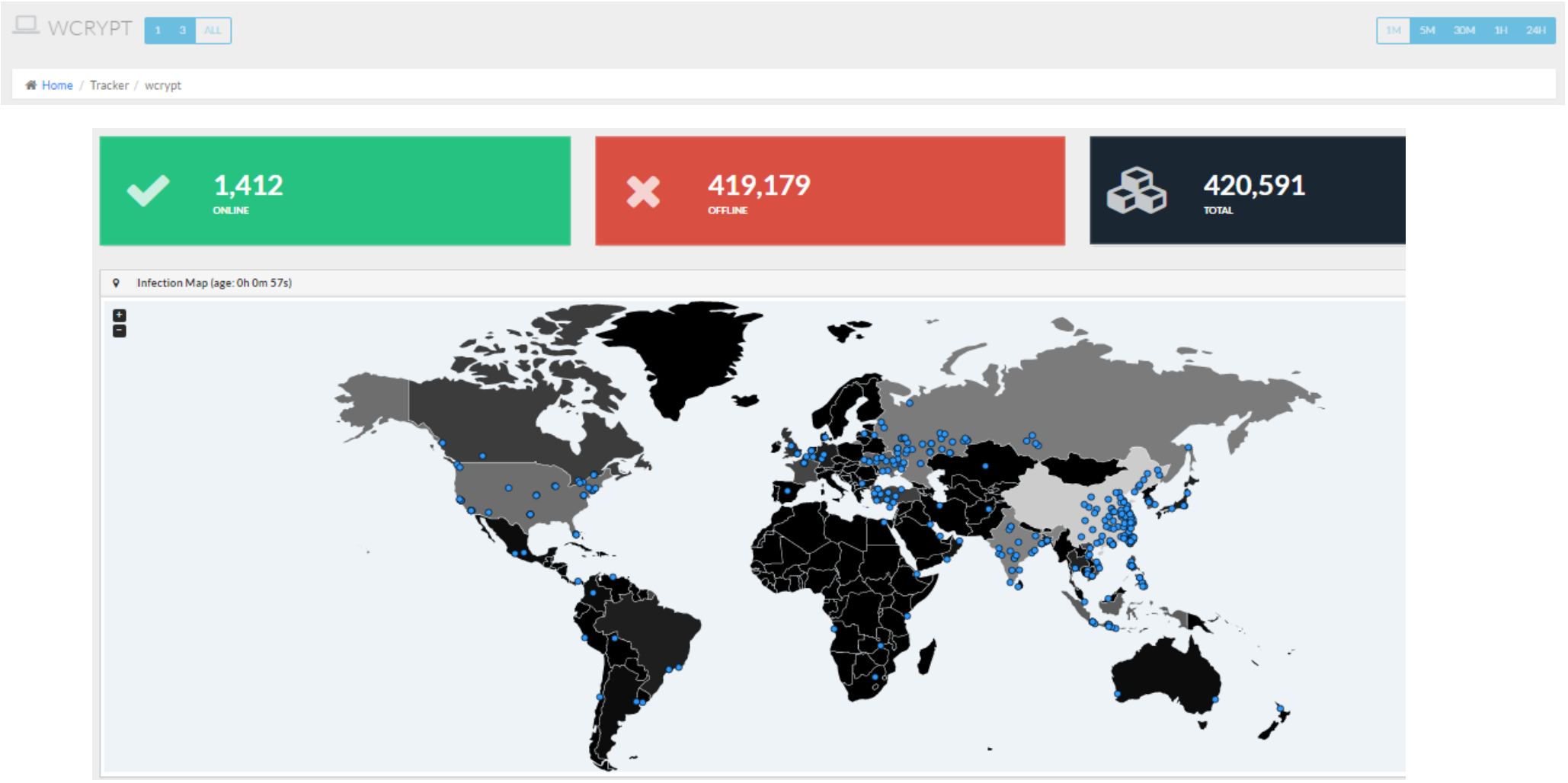


Fuente: https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html?_r=0

WannaCry - Países y Entidades Afectadas



Fuente: http://www.laprensa.hn/mundo/1070719-410/empresas-malware-wannacry-ciberataque-global



Fuente: https://intel.malwaretech.com/botnet/wcrypt/?t=1m&bid=all

WannaCry - Ramsoware

- Es un malware que afecta Windows el cual cifra archivos y solicita un pago en Bitcoins, este ataque empezó el viernes 12 de mayo, +200,000 victimas, + 150 países, se propaga por medio del puerto 445/TCP (SMB).
- Aprovecha una Vulnerabilidad: **CVE-2017–0145**
- Permite que atacantes remotos ejecuten código arbitrario vía paquetes creados con mala intención aprovechando una vulnerabilidad en el servicio SMB de Microsoft.

Fuente: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0145
Fuente: https://www.thesun.co.uk/tech/3562470/wannacry-ransomware-nhs-cyber-attack-hackers/

WannaCry - Ramsoware

CVE-ID	
CVE-2017-0145	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0144, CVE-2017-0146, and CVE-2017-0148.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0145
- BID:96705
- URL:http://www.securityfocus.com/bid/96705

Date Entry Created

20160909	Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Fuente: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0145
Fuente: https://www.thesun.co.uk/tech/3562470/wannacry-ransomware-nhs-cyber-attack-hackers/

NSA desarrollaba Exploits: “Cyber Weapons”

Exploits

- **EARLYSHOVEL** RedHat 7.0 - 7.1 Sendmail 8.11.x exploit
- **EBBISLAND (EBBSHAVE)** root RCE via RPC XDR overflow in Solaris 6, 7, 8, 9 & 10 (possibly newer) both SPARC and x86.
- **ECHOWRECKER** remote Samba 3.0.x Linux exploit.
- **EASYBEE** appears to be an MDaemon email server vulnerability
- **EASYFUN** EasyFun 2.2.0 Exploit for WDaemon / IIS MDaemon/WorldClient pre 9.5.6
- **EASYPI** is an IBM Lotus Notes exploit that gets detected as Stuxnet
- **EWOKFRENZY** is an exploit for IBM Lotus Domino 6.5.4 & 7.0.2
- **EXPLODINGCAN** is an IIS 6.0 exploit that creates a remote backdoor
- **ETERNALROMANCE** is a SMB1 exploit over TCP port 445 which targets XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2, and gives SYSTEM privileges (MS17-010)
- **EDUCATEDSCHOLAR** is a SMB exploit (MS09-050)
- **EMERALDTHREAD** is a SMB exploit for Windows XP and Server 2003 (MS10-061)
- **EMPHASISMINE** is a remote IMAP exploit for IBM Lotus Domino 6.6.4 to 8.5.2
- **ENGLISHMANSDENTIST** sets Outlook Exchange WebAccess rules to trigger executable code on the client's side to send an email to other users
- **EPICHERO** 0-day exploit (RCE) for Avaya Call Server
- **ERRATICGOPHER** is a SMBv1 exploit targeting Windows XP and Server 2003
- **ETERNALSYNERGY** is a SMBv3 remote code execution flaw for Windows 8 and Server 2012 SP0 (MS17-010)
- **ETERNALBLUE** is a SMBv2 exploit for Windows 7 SP1 (MS17-010)
- **ETERNALCHAMPION** is a SMBv1 exploit
- **ESKIMOROLL** is a Kerberos exploit targeting 2000, 2003, 2008 and 2008 R2 domain controllers
- **ESTEEMAUDIT** is an RDP exploit and backdoor for Windows Server 2003
- **ECLIPSEDWING** is an RCE exploit for the Server service in Windows Server 2008 and later (MS08-067)
- **ETRE** is an exploit for IMail 8.10 to 8.22
- **ETCETERABLUE** is an exploit for IMail 7.04 to 8.05
- **FUZZBUNCH** is an exploit framework, similar to MetaSploit
- **ODDJOB** is an implant builder and C&C server that can deliver exploits for Windows 2000 and later, also not detected by any AV vendors

Equation Group.

Fuente: GitHub, Inc. [US] | https://github.com/misterch0c/shadowbroker/

ShadowBrokers hacks NSA

Fuente:https://en.wikipedia.org/wiki/Equation_Group

WannaCry - Timeline, resumen

Agosto 2016
ShadowBrokers

14 de Marzo
Microsoft publica
18 Boletines, MS17-010,
ejecución remota de código
Server Message Block 1.0.

14 de Abril
Shadow Brokers
Publica Exploits

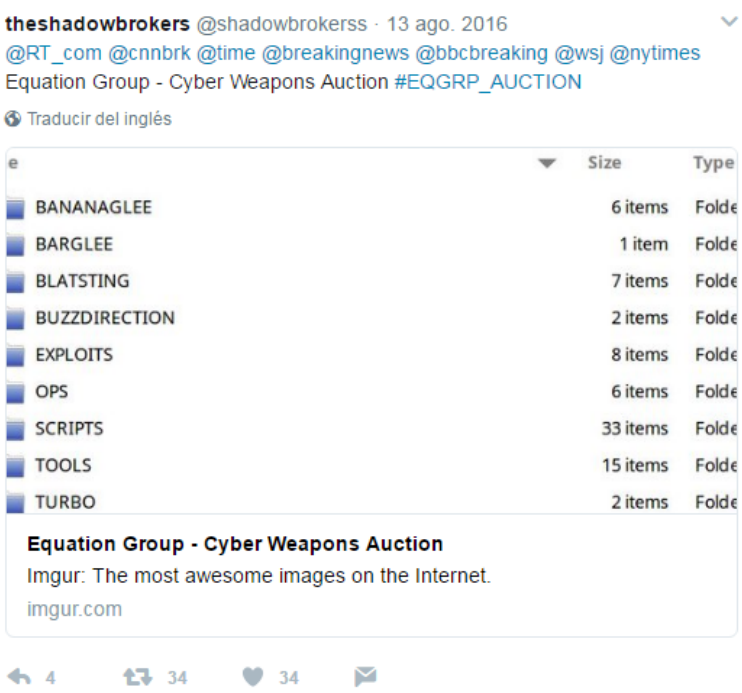
12 de Mayo
WannaCry,
afecto
+200k Pcs,
+150 Paises
aprovecha:
CVE-2017–0145

13 de Mayo
Microsoft publica
parches
Windows XP
Windows 8
Winsows Server
2003

13 de Junio
Microsoft Security
Advisory 4025685
Adobe Security Bulletin
APSB17-17

27 de Junio
Peyta Ramsoware
usa exploit SMS/Eternalblue
cifrados con AES-128bits.
Modifica MBR(Master Boot Record) y
habilita la encriptación de
MFT(Master File Table), Luego
reinicia la máquina.

Fuente: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
Fuente: https://github.com/misterchoc/shadowbroker/
Fuente: https://twitter.com/shadowbrokerss/with_replies



Fifth leak: "Lost in Translation" [edit]

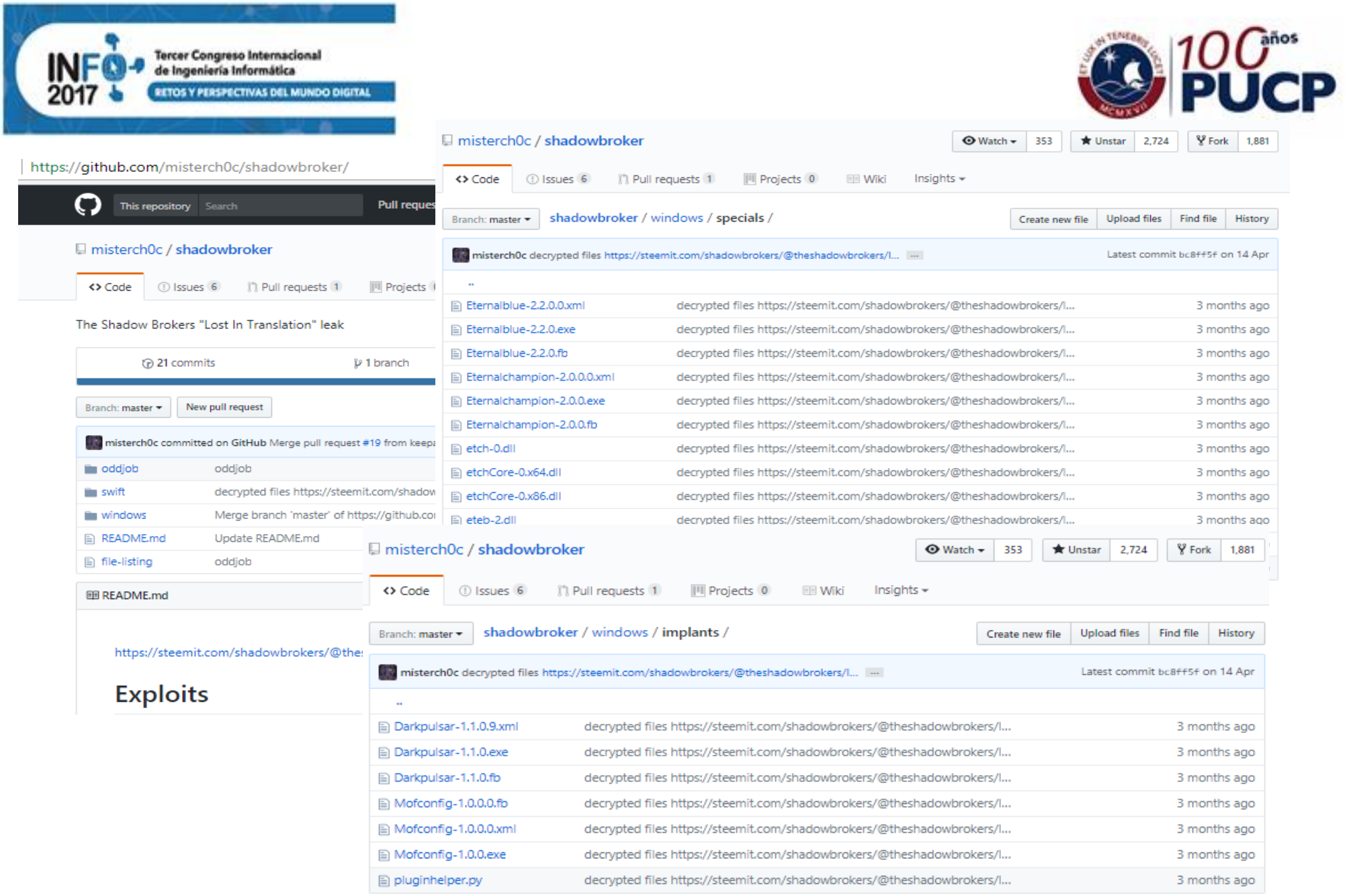
On April 14, 2017, the Twitter account used by The Shadow Brokers posted a tweet with a link[20] to a Steemit story. Herein, a message with a link to the leak files, encrypted with the password `Reeeeeeeeeeeeee`.

The overall content is based around three folders: "oddjob", "swift" and "windows".[21] The fifth leak is suggested to be the "...most damaging release yet"[22] and CNN quoted Matthew Hickey saying, "This is quite possibly the most damaging thing I've seen in the last several years,".[23]

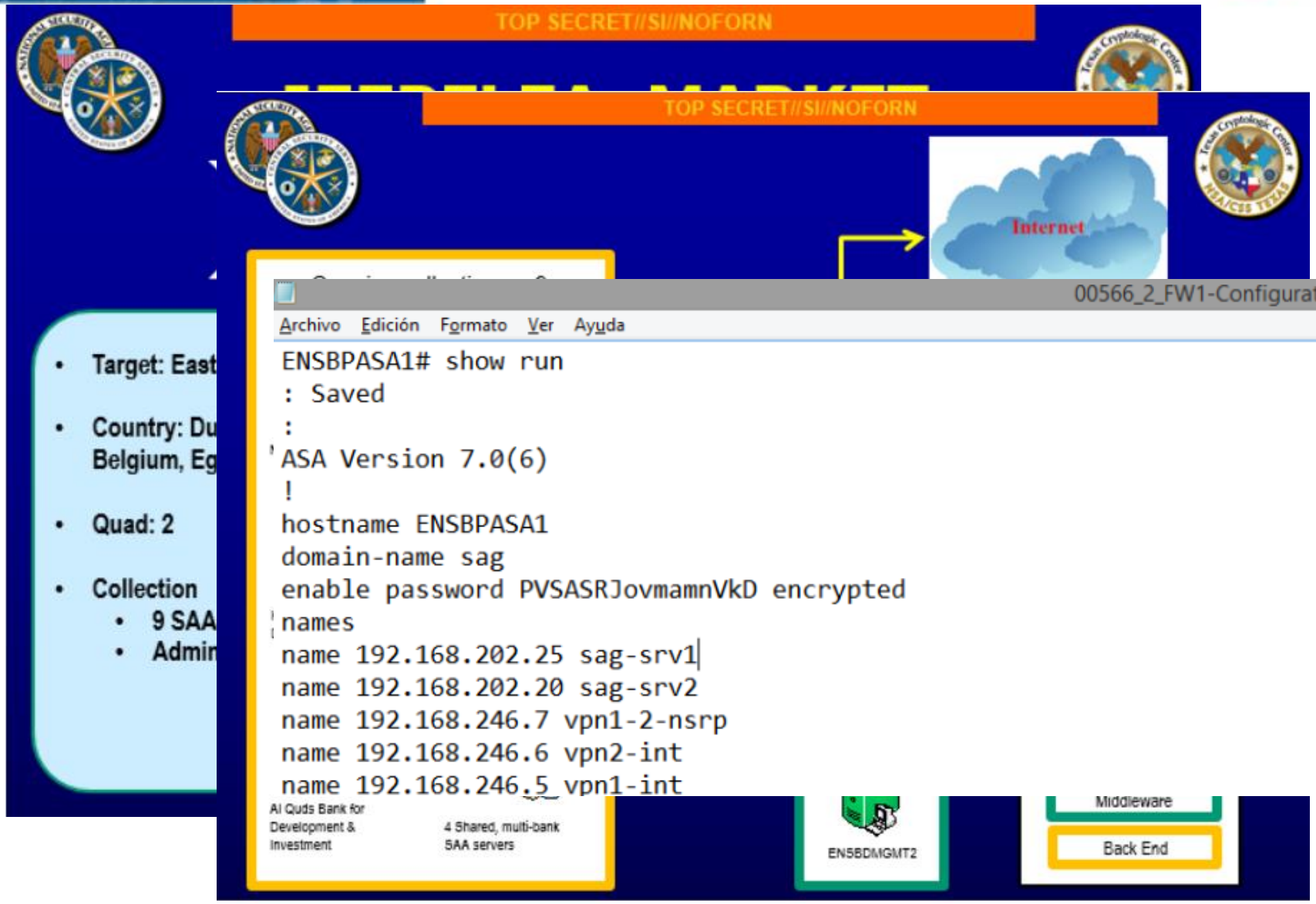
The leak includes, amongst other things, the tools and exploits codenamed: DANDERSPIRITZ, ODDJOB, FUZZBUNCH, DARKPULSAR, ETERNALSYNERGY, ETERNALROMANCE, ETERNALBLUE, EXPLODINGCAN and EWOKFRENZY.[22][24][25]

Some of the exploits targeting the Windows operating system, had been patched in a Microsoft Security Bulletin on March 14, 2017, one month before the leak occurred.[26][27] Some speculated that Microsoft may have been tipped off about the release of the exploits.[28]

Fuente: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx



Fuente: https://github.com/misterch0c/shadowbroker/



Fente: https://github.com/misterchoc/shadowbroker/

LEGEND:

Box has been implanted and we are collecting

This mean the bank is of interest

BOLD means the box has been scanned and is UP

RED means the box has been s

IP	H
192.168.200.33	ENSBDFIIV1
192.168.200.34	fiiv-srv2
192.168.200.35	fiiv-srv3
192.168.200.41	ENSBDKFAE1
192.168.200.42	kfae-srv2
192.168.200.45	difx-srv1
192.168.200.46	difx-srv2
192.168.200.47	ENSBDDIFX1
192.168.200.50	sharedsaa-srv
192.168.200.51	ENSBDSL1 N
192.168.200.52	ENSBDSL2
192.168.200.53	sharedsaa-srv
192.168.200.56	pmap-srv1
192.168.200.57	pmap-srv2
192.168.200.58	pmap-srv3
192.168.200.59	dgcx-srv1

I	K	L
operatingSystemVersion	operatingSystem	name
5.0 (2195)	Windows 2000 Server	QASERVER
5.0 (2195)	Windows 2000 Server	QASERVER2
5.1 (2600)	Windows XP Professional	QATEST
5.1 (2600)	Windows XP Professional	QA
5.0 (2195)	Windows 2000 Server	QIIB
5.0 (2195)	Windows 2000 Server	QIIB2K
5.1 (2600)	Windows XP Professional	QAIS
5.0 (2195)	Windows 2000 Server	QIIB-CC
5.1 (2600)	Windows XP Professional	QIDRISI
5.2 (3790)	Windows Server 2003	QAHOST1
5.2 (3790)	Windows Server 2003	QNBVM
6.1 (7600)	Windows Server 2008 R2 Enterprise	QAHOST3
5.2 (3790)	Windows Server 2003	QTEL
6.1 (7600)	Windows 7 Enterprise	QUENTIN-ENLA
5.2 (3790)	Windows Server 2003	QNBPH1
5.2 (3790)	Windows Server 2003	QNBPH2
5.2 (3790)	Windows Server 2003	QNBPH1-DEV
6.1 (7600)	Windows Server 2008 R2 Enterprise	QASAA7
6.1 (7600)	Windows Server 2008 R2 Enterprise	QAREPORTING2-5

Fonte: https://github.com/misterch0c/shadowbroker/

Microsoft Security Bulletin MS17-010 - Critical

Security Update for Microsoft Windows SMB Server (4013389)

Published: March 14, 2017

Version: 1.0

Executive Summary

This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

This security update is rated Critical for all supported releases of Microsoft Windows. For more information, see the **Affected Software and Vulnerability Severity Ratings** section.

The security update addresses the vulnerabilities by correcting how SMBv1 handles specially crafted requests.

For more information about the vulnerabilities, see the **Vulnerability Information** section.

For more information about this update, see Microsoft Knowledge Base Article 4013389.

On this page

https://support.microsoft.com/es-co/help/4013389/title

MS17-010: Actualización de seguridad para Windows Server de SMB: 14 de marzo de 2017

Correo electrónico
Imprimir

Resumen

Esta actualización resuelve vulnerabilidades en Microsoft Windows. La más grave de estas vulnerabilidades podría permitir la ejecución remota de código si un atacante envía mensajes especialmente diseñados a un servidor de Microsoft Server Message Block 1.0 (SMBv1).
Para obtener más información acerca de la vulnerabilidad, consulte el boletín de seguridad de Microsoft MS17-010.

Fuente: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Exploits - -> Microsoft

13 de Junio, 2017

- **EternalBlue SMB exploit** → WannaCry ransomware attack, para diferente versiones de Windows.
- Pero la compañia, dejo tres Windows zero-day exploits unpatched?, Windows Hacking Tools:
  - "EsteemAudit,"
  - "ExplodingCan,"
  - "EnglishmanDentist,"
- **EsteemAudit**, peligroso Windows Hacking tool, RDP Microsoft Windows Server 2003 and Windows XP machines,
- **ExplodingCan,** explota un bug de IIS 6.0.
- **EnglishmanDentist,** explota Microsoft Exchange servers.

Fuente: http://thehackernews.com/2017/06/important-windows-updates.html

Microsoft,publica:

13 de Junio, 2017

- Microsoft blog post, the critical down-level patches for three Windows exploits were prompted by an "elevated risk of destructive cyberattacks" by government organizations, referred to as "nation-state actors or other copycat organizations.
- patches for Windows XP, Vista, and Server 2003 contain fixes or mitigations for three alleged **NSA-developed exploits — EsteemAudit,**

Microsoft Security Advisory 4025685

Guidance related to June 2017 security update release

Published: June 13, 2017

Version: 1.0

On this page
Executive Summary
Advisory FAQ
Other Information

Executive Summary

Microsoft is announcing the availability of additional guidance for critical security updates, that are at heightened risk of exploitation due to past and threatened nation-state attacks and disclosures. Some of the releases are new, and some are for older platforms that we are making publicly available today.

Consumers who have automatic updates enabled through Windows Update are already protected and have no action to take. Windows 10 has automatic updates enabled. To check if automatic updates are enabled see Windows Update: FAQ.

Which Windows version are you running?	
For customers using **Windows Server 2008**, **Windows 7**, **Windows Server 2008 R2**, **Windows Server 2012**, **Windows 8.1**, **Windows 8.1 RT**, **Windows Server 2012 R2**, **Windows 10**, or **Windows Server 2016** see Microsoft Knowledge Base Article 4025686 for guidance.	For customers using **Windows XP**, **Windows Vista**, **Windows 8**, **Windows Server 2003**, or **Windows Server 2003 R2** see Microsoft Knowledge Base article 4025687 for guidance.

Fuente: https://technet.microsoft.com/en-us/library/security/4025685.aspx

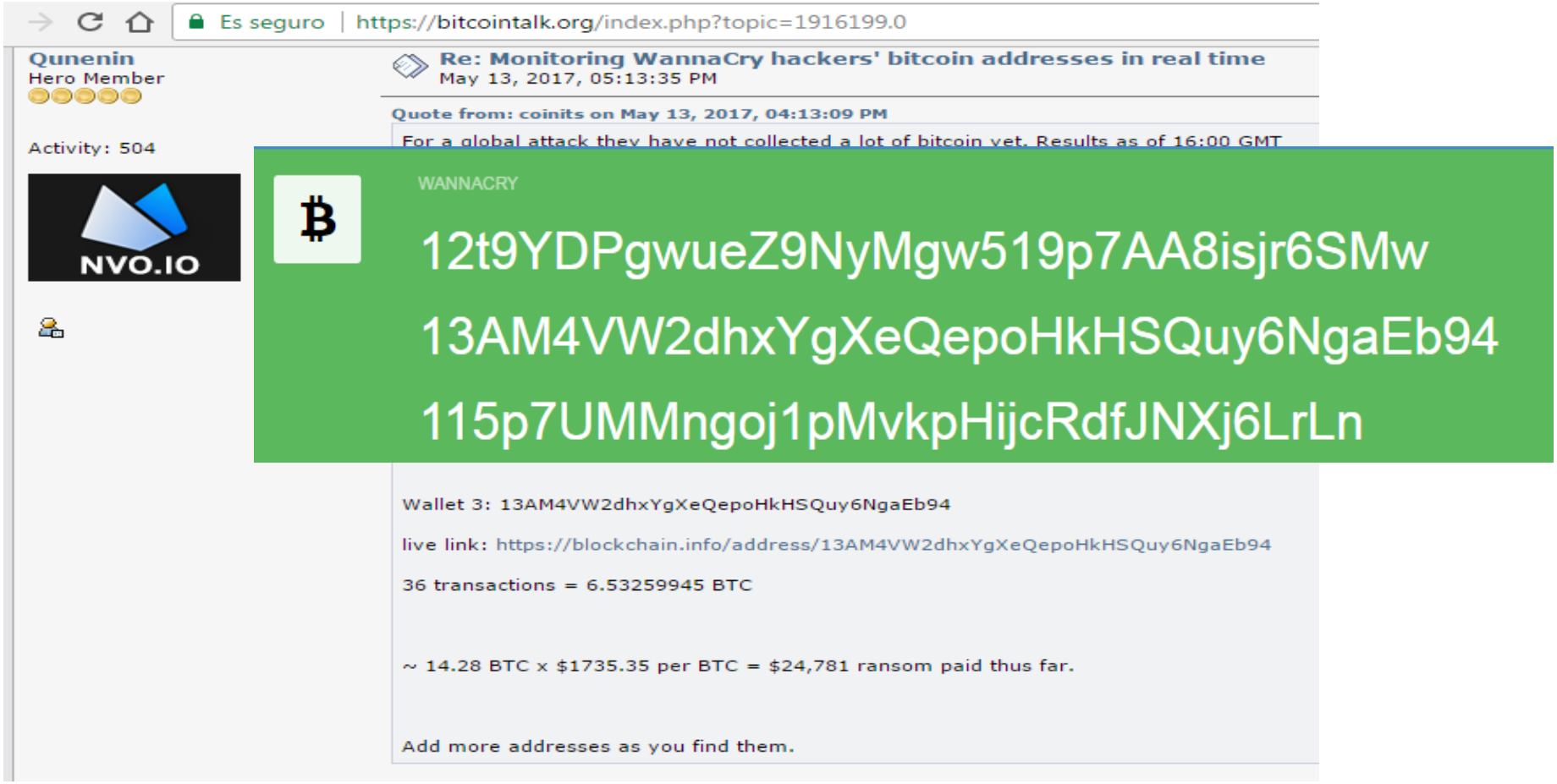
WannaCry - Sistemas afectados

1. Windows Vista
2. Windows Server 2008
3. Windows 7
4. Windows Server 2008 R2
5. Windows 8.1
6. Windows Server 2012
7. Windows Server 2012 R2
8. Windows RT 8.1
9. Windows 10
10. Windows Server 2016

Fuente: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

WannaCry - ScreenShots

WannaCry - Bitcoins



Fuente: https://bitcointalk.org/index.php?topic=1916199.0
Fuente: http://howmuchwannacrypaidthehacker.com/index.php

WannaCry - Bitcoins

1	BTC	↔	2522.71	USD

Resumen	
Dirección	12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Hash 160	14a477964ed719135d1598da348a858b18b44fd5
Herramientas	Etiquetas Relacionadas - Las salidas no utilizadas

Actas	
Número	
total re	
Balanc	

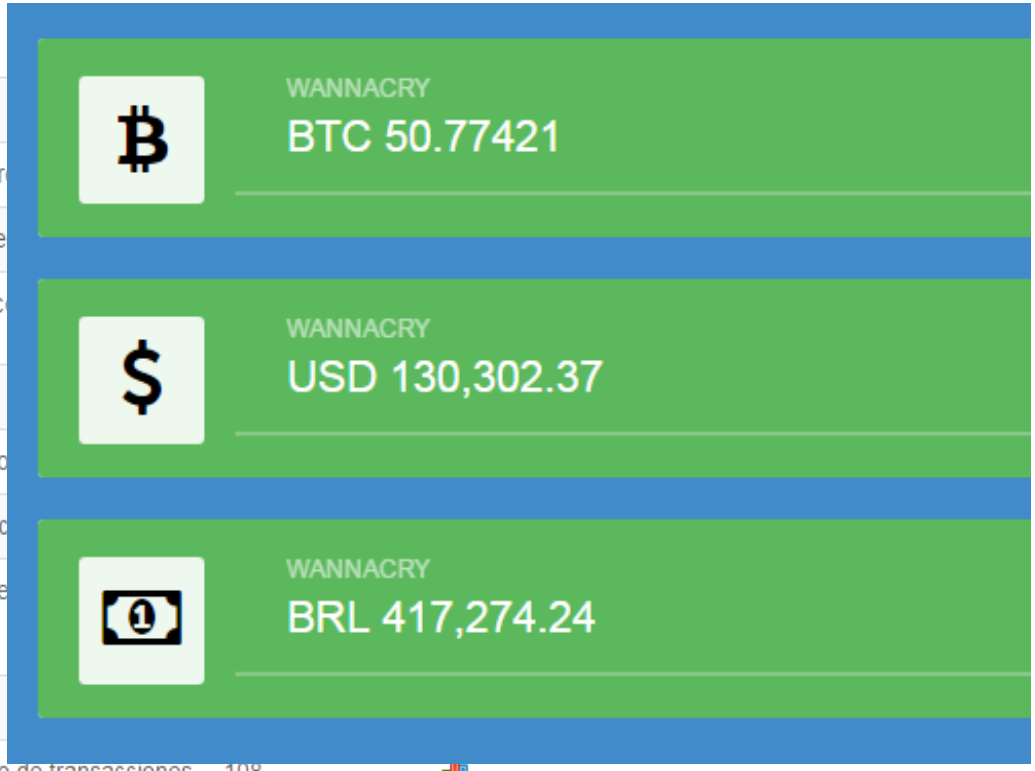
Resumen	
Dirección	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Hash 160	17b4bd9a139158614e8f54c6b800a1822609436a
Herramientas	Etiquetas Relacionadas - Las salidas no utilizadas

Actas	
Número	
total rec	
Balance	

Resumen	
Dirección	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Hash 160	00e8fd98ca34f195b020af4a8b1c7238663d4212
Herramientas	Etiquetas Relacionadas - Las salidas no utilizadas

Actas		
Número de transacciones	108	
total recibida	14.08097351 BTC	
Balance final	14.08097351 BTC	

Solicitud de Pago | Botón de Donación



Fuente: https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Fuente: https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Fuente: http://howmuchwannacrypaidthehacker.com/index.php

WannaCry - Método de Infección

- Se está realizando por medio de **SPAM masivo**, correo electrónico o a través de una **memoria USB** de manera directa a tu computadora.
- Una vez que abres el archivo adjunto, automáticamente ejecuta el malware el cual genera dos acciones:
- **Busca otras computadoras** con el sistema operativo Windows que están vulnerables **y ya no sería necesario enviar un correo** o hacer otra acción adicional para su ejecución.
- Desde la computadora windows infectada realiza una conexión hacia servidores que están en Internet llamados **C&C (Command & Control)** estos servidores sirven para descargarse otros componentes/payload.

Fuente: https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Ransom:Win32/WannaCrypt

WannaCry - Instalación

Una vez que tu computadora está infectado se intentará conectar a Internet hacia:

"xxx.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" al puerto 80.

Luego crea el siguiente archivo y servicio:

- %SystemRoot% \tasksche.exe
- mssecsvc2.0

Fuente: https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Ransom:Win32/WannaCrypt

WannaCry - Files

123 .jpeg .rb .cs .odt .tiff .602 .jpg .rtf .csr .onetoc2 .txt .doc .js .sch .csv .ost .uop

.3dm .jsp .sh .db .otg .uot .3ds .key .sldm .dbf .otp .vb .3g2 .lay .sldm .dch .ots

.vbs .3gp .lay6 .sldx .der" .ott .vcd .7z .ldf .slk .dif .p12 .vdi .accdb .m3u .sln .dip

.PAQ .vmdk .aes .m4u .snt .djvu .pas .vmx .ai .max .sql .docb .pdf .vob .ARC

.mdb .sqlite3 .docm .pem .vsd .asc .mdf .sqlitedb .docx .pfx .vsdx .asf .mid .stc

.dot .php .wav .asm .mkv .std .dotm .pl .wb2 .asp .mml .sti .dotx

.png .wk1 .avi .mov .stw .dwg .pot .wks .backup .mp3 .suo .edb .potm .wma .bak

.mp4 .svg .eml .potx .wmv .bat .mpeg .swf .fla .ppam .xlc .bmp .mpg .sxc .flv .pps

.xlm .brd .msg .sxd .frm .ppsm .xls .bz2 .myd .sxi .gif .ppsx .xlsb .c .myi .sxm .gpg

.ppt .xlsm .cgm .nef .sxw .gz .pptm .xlsx .class .odb .tar .h .pptx .xlt .cmd .odg

.tbk .hwp .ps1 .xltm .cpp .odp .tgz .ibd .psd .xltx .crt .ods .tif .iso .pst .xlw .jar .rar

.zip .java .raw

Fuente: https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Ransom:Win32/WannaCrypt

WannaCry - Prevención

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

1. Aplicar el Parche MS17-010
2. Aislar los equipos Infectados
3. Desactivar el servicio SMBv1.
4. Bloquear la comunicación de los puertos 137/UDP y 138/UDP así como los puertos 139/TCP y 445/TCP en las redes de las organizaciones.
5. Bloquear los puertos Netbios desde Internet
6. Bloquear el acceso a la red TOR

Fuente: https://www.incibe.es/protege-tu-empresa/avisos-seguridad/importante-oleada-ransomware-afecta-multitud-equipos

Recomendaciones:

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

1. Aplicar el **Parche MS17–010** para mitigar la vulnerabilidad SMB del 14 de Mayo en sistemas operativos Windows.
2. Afinar las p**olíticas del Antispam** (instalado localmente o como servicio) para ayude a identificar y bloquear malware, phishing sobre correo electrónico.
3. Escanear correo electrónico de entrada, salida para detectar y bloquear archivos ejecutables con destino usuarios finales a nivel de Gateway y usuario final.
4. Habilitar un Scan automático Antivirus, Antimalware a nivel de PC, Servidor, UTM (Scan Antivirus para Trafico de Navegación HTTP, HTTPS, DNS), etc.
5. Implementar el principio: **“Mínimo Privilegio/Menor Autoridad”**. Los usuarios no debería tener acceso como Super usuario (Administrador/Windows, root/Unix, Linux, sa,admin/Cisco/Huawei) para sistemas operativos, Aplicaciones, Dispositivos de red, Firewalls, etc.
6. Deshabilitar Macros/Scripts en Microsoft Office.
7. Desarrollar un programa de Concientización en los usuarios finales para que noingresen en links maliciosos, no abran adjuntos con archivos de dudosa procedencia..

Fuente: https://www.us-cert.gov/ncas/alerts/TA17-181A

Recomendaciones:

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

8. Los usuarios finales deben tener un canal “Oficial” de reporte ante un Incidente de Seguridad 24x7 debería existir punto de contacto oficial: repore.Incidente@empresa.com y número de teléfono.
9. Regularmente realizar un **Pentesting a tus servicios públicos**, red LAN/WAN por lo menos 1 vez al año.
10. **Probar tus Backups**, y asegura que estén trabajando adecuadamente, los backups desarrollarlos en dispositivos que no estén conectados a la red.
11. Utilizar Firewalls o IDS Host a nivel de Servidores para protección de un ataque desde Internet y desde la red Interna por un empleado.
12. **Deshabilitar servicios innecesarios** en tus sistemas que no usas, para el caso de Ramsoware WannaCry y Petya desabilitar SMBv1.

Fuente: https://www.us-cert.gov/ncas/alerts/TA17-181A

Recomendaciones:

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

13. En tu firewall perimetral, bloquea TCP 445, TCP/UDP 137,138, y TCP 339 tráfico de Internet hacia la red de la empresa.
14. **Segmentar la red de usuarios** con la red de los servidores de la empresa, tratando de que si hay una intrusión este aislado el incidente.
15. **Hardenización de PCs, Servidores Críticos, Red Switches de Core**, Switches de Distribución, apoyarse del fabricante, soporte del integrador para mejorar la seguridad de cada sistema y mejores practicas de la Industria por ejemplo SANS Reading Room, Grupos de Usuarios de los sistemas que usan en tu empresa.
16. **Realizar administración de los equipos críticos fuera de banda**, por si se cae la comunicación principal se cae.
17. **Contar con herramientas de Monitoreo de los fabricantes** y Open Source que permitan ver el Trafico, Conexiones, Intentos de Ataques de Red, Falsos Positivos, Logs de los Servidores, Firewall, IPS/IDS, PCs, etc, Es decir tener un Panel de Control con la Visibilidad de la red de la Empresa.

Fuente: https://www.us-cert.gov/ncas/alerts/TA17-181A