

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>

Ransomware

2016 in numbers

62 new ransomware families appeared

The number of new ransomware modifications increased **11 - FOLD**

2,900 Q1 → 32,091 Q3



An individual attacked

Q1 every 20 seconds | Q3 every 10 seconds

A business attacked

Q1 every 2 minutes | Q3 every 40 seconds



One in five SMBs who paid the ransom never got their data back

All the statistics were obtained using Kaspersky Security Network (KSN)
© 2016 AO Kaspersky Lab. All Rights Reserved.

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 /	25.32
2 Locky	Trojan-Ransom.Win32.Locky / Trojan-Dropper.JS.Locky	7.07
3 TeslaCrypt (active till May 2016)	Trojan-Ransom.Win32.Bitman / Trojan-Ransom.Win32.Scatter /	6.54
4 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:

- <https://securelist.com/analysis/kaspersky-security-bulletin/76757/kaspersky-security-bulletin-2016-story-of-the-year/>
- <https://blog.kaspersky.com/ransomware-in-targeted-attacks/6728/>
- https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf

CryptoLocker, Petya, Revenge

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted. More information about: <http://en.wikipedia.org>

Decrypting of your files. To receive your private key:

1. <http://twbers4hmi.com>
2. <http://twbers4hmi.com>
3. <http://twbers4hmi.com>

If all of this addresses are not working:

1. Download and install
2. After a successful
3. Type in the address
4. Follow the instructions

!!! Your personal identification

Your personal files are encrypted by CTB-Locker.

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.



WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

92 18 34

View

Next >>

© 2016 AO Kaspersky Lab. All Rights Reserved.

has been encrypted with an military grade encryption an special key. This page will help you decryption of your computer.

ed in: 10 seconds

CryptoLocker



Private key will be destroyed on 9/15/2013 8:44 PM

Time left 57 : 45 : 37

Next >>

Per omnia se che siamo in grado di recuperare il file, inviate un file di e-mail.

===GERMAN===
 Alle Dateien wurden mit REVENGE Ransomware verschlüsselt.
 Die notwendigen Schritte, um die Dateien wiederherzustellen.

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>
```

© 2016 AO Kaspersky Lab. All Rights Reserved.



Infección, secuencia de pasos:

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

Subject: Notice of court attendance

From: Court Agent <security@court.agents.com>
 Sunday, January 8, 2017 at 15:40 UTC
 To:

As a defendant you have been scheduled to attend the hearing in the court of your city.

Hearing date: 13 January 2017
 Hearing time: 9:00 a.m.
 Hearing subject: illegal use of software

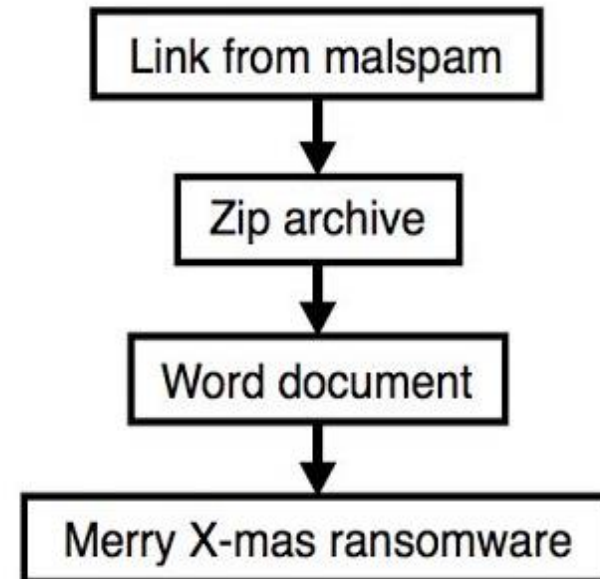
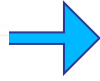
Prior to the court thoroughly study the plaint note in the attachment to this mail.

Sincerely,
 Court agent,
 Abigail Mason

http://neogenomes.com/court/PlaintNote_12545_copy.zip



PlaintNote_12545_copy.zip
 9K [View](#) [Download](#)



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/secreary>
- IDA PRO, Desensamblador Interactivo.
- Wireshark, Analizador de paquetes de Red.
- JPEXS Free Flash Decompiler, Descompilador.
- Pestudio, Analisis Estático de Malware, <https://www.winator.com/binaries.html>
- TCP View, Regshot, Process Explorer, SysInternals, <https://technet.microsoft.com/en-us/sysinternals>

- **Recursos:**

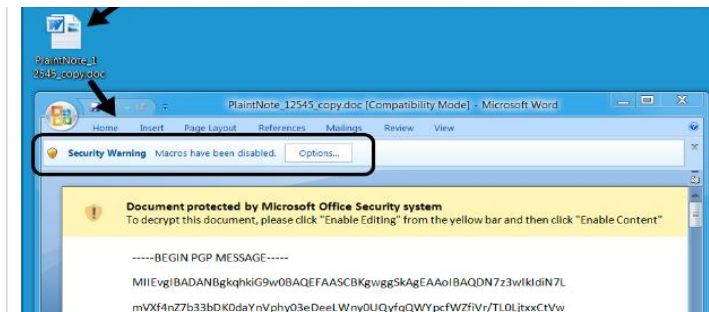
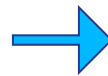
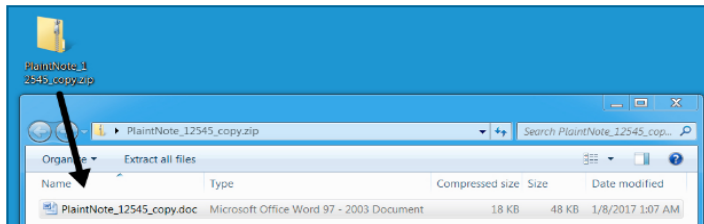
- <http://www.malware-traffic-analysis.net/>
- <https://www.virustotal.com/>
- <https://www.hybrid-analysis.com>
- <https://malwr.com/analysis/>
- <http://contagiodump.blogspot.pe/>
- <https://cartilha.cert.br/ransomware/>

- **Agradecimientos:**

- Lasha Khasaia, <https://secreary.com/SSMA>
- André R. Landim, CAIS/RNP, <https://www.rnp.br/servicos/seguranca>
- Geoffrey 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:



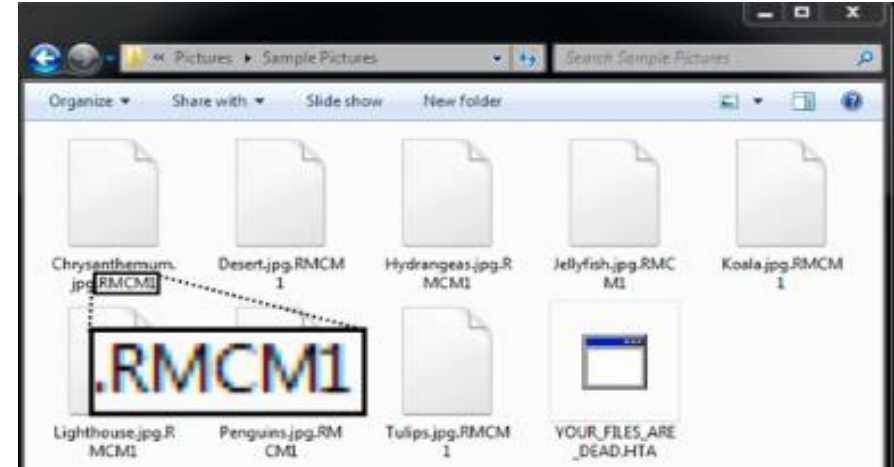
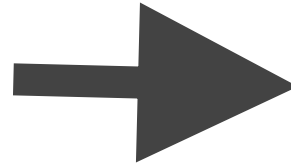
Fuentes:

- (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:

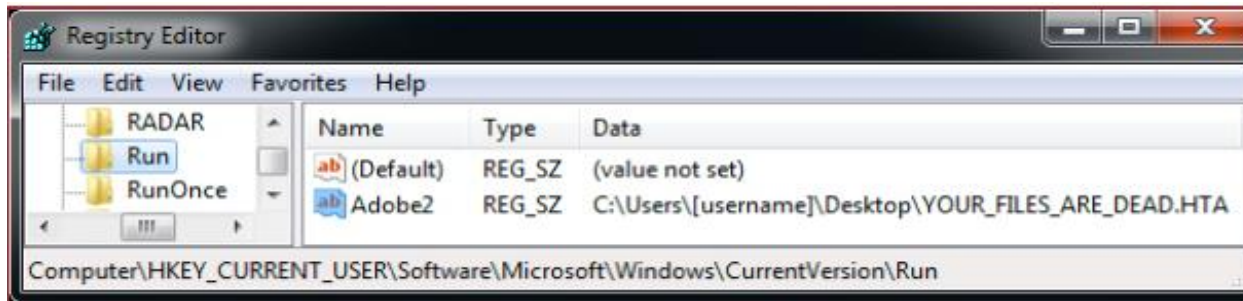
Archivos personales Cifrados:

- 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



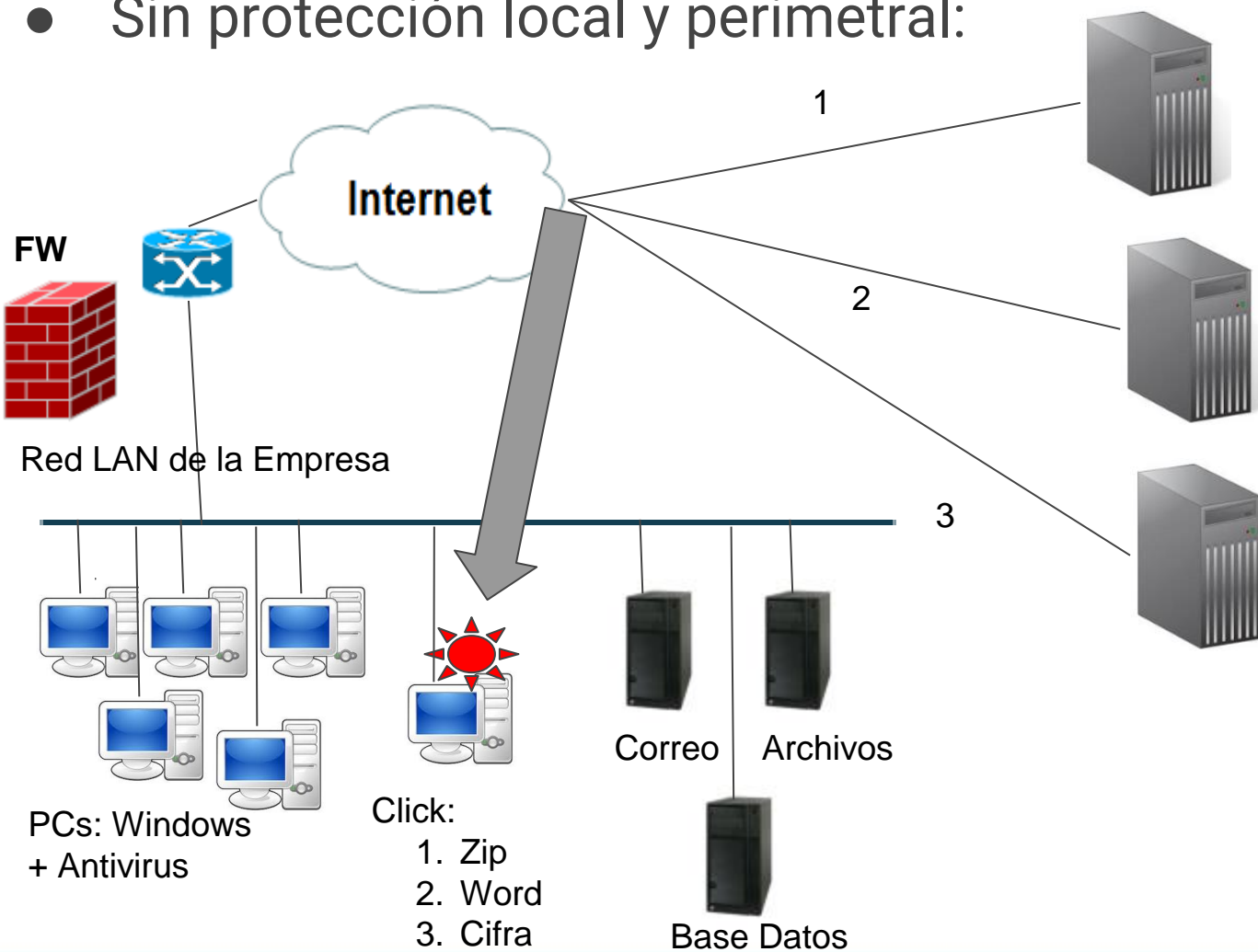
Date/Time	Dst	port	Host	Info
2017-01-08 15:57:48	192.185.18.204	80	neogenomes.com	GET /court/PlainNote_12545_copy.zip HTTP/1.1
2017-01-08 15:58:38	81.4.123.67	443	onion1.host:443	GET /temper/PGPClient.exe HTTP/1.1
2017-01-08 15:58:46	168.235.98.160	443	onion1.pw	POST /blog/index.php HTTP/1.1

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



Infección, Analizando:

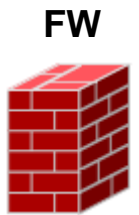
- Sin protección local y perimetral:



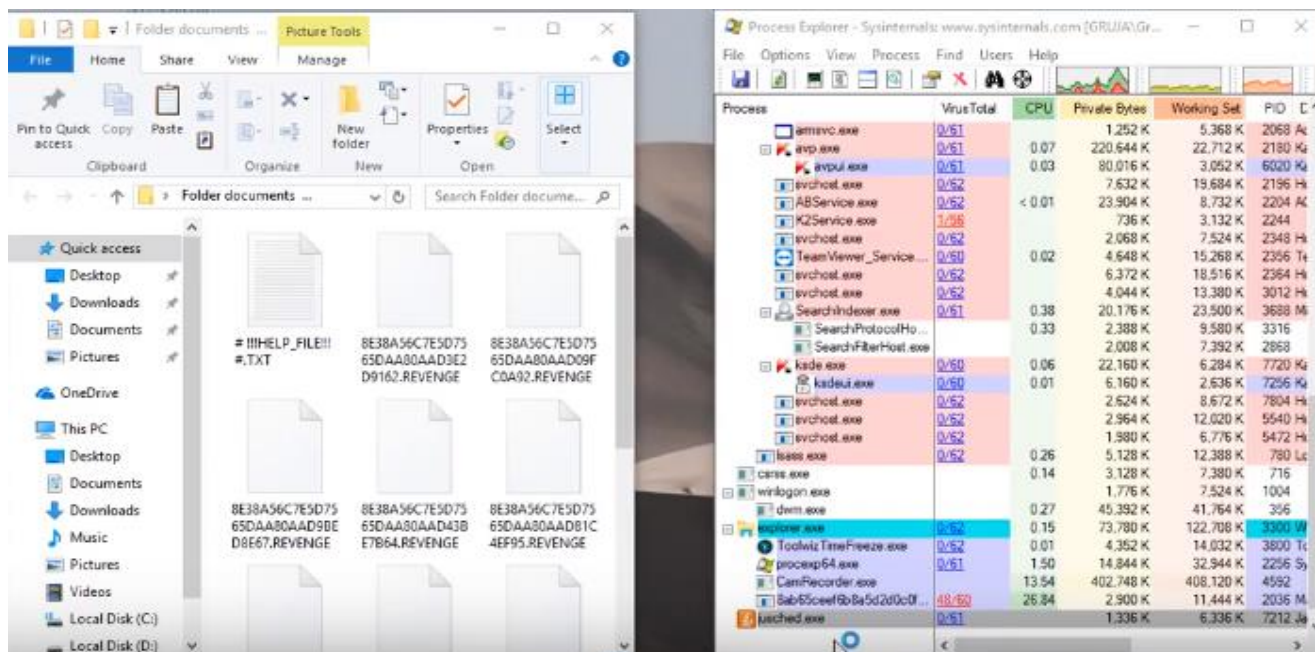
- **neogenomes.com** (Site Hackeado)
- 192.185.18.204:80:
- GET
- PlainNote_12545_copy.zip
- HTTP/1.1

- **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



Revenge Ramsoware: 2017-03-15



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-5uhcvesi.exe
 4. 2017-03-15-Revenge-Ransomware-decryption-instructions.txt
 5. 2017-03-15-page-from-activaclinics.com-with-injected-EITest-script.txt

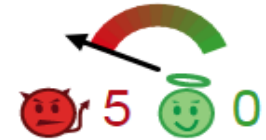
2017-03-15-Revenge-Ransomware-decryption-instructions: Bloc de notas

===ENGLISH===
 All of your files were encrypted using REVENGE Ransomware.
 The action required to restore the files.
 Your files are not lost, they can be returned to their normal state by decoding them.
 The only way to do this is to get the software and your personal decryption key.
 Using any other software that claims to be able to recover your files will result in corrupted files.
 You can purchase the software and the decryption key by sending us an email with your ID.
 And we send instructions for payment.
 After payment, you receive the software to return all files.
 For proof, we can decrypt one file for free. Attach it to an e-mail.



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

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




SHA256:	8ab65ceef6b8a5d2d0c0fb3ddb1c1756b5c224bafc8065c161424d63937721c
Nombre:	2017-03-15-EITest-Rig-EK-payload-Revenge-ransomware-5uhcvesi.exe
Detecciones:	51 / 60
Fecha de análisis:	2017-05-09 03:49:18 UTC (hace 3 días, 2 horas)

5uhcvesi.exe



Resources

Language TURKISH
Icon 

Fuentes:

- (1) <https://www.virustotal.com/es/file/8ab65ceef6b8a5d2d0c0fb3ddb1c1756b5c224bafc8065c161424d63937721c/analysis/1494301758/>
- (2) <https://malwr.com/analysis/YzE1ZmZlY2MxZjllNDNjM2FhNzA1YWU2ZTk3N2JhOTg/>
- (3) <https://www.hybrid-analysis.com/sample/8ab65ceef6b8a5d2d0c0fb3ddb1c1756b5c224bafc8065c161424d63937721c?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](https://secreary.com/SSMA)

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



Ukraine

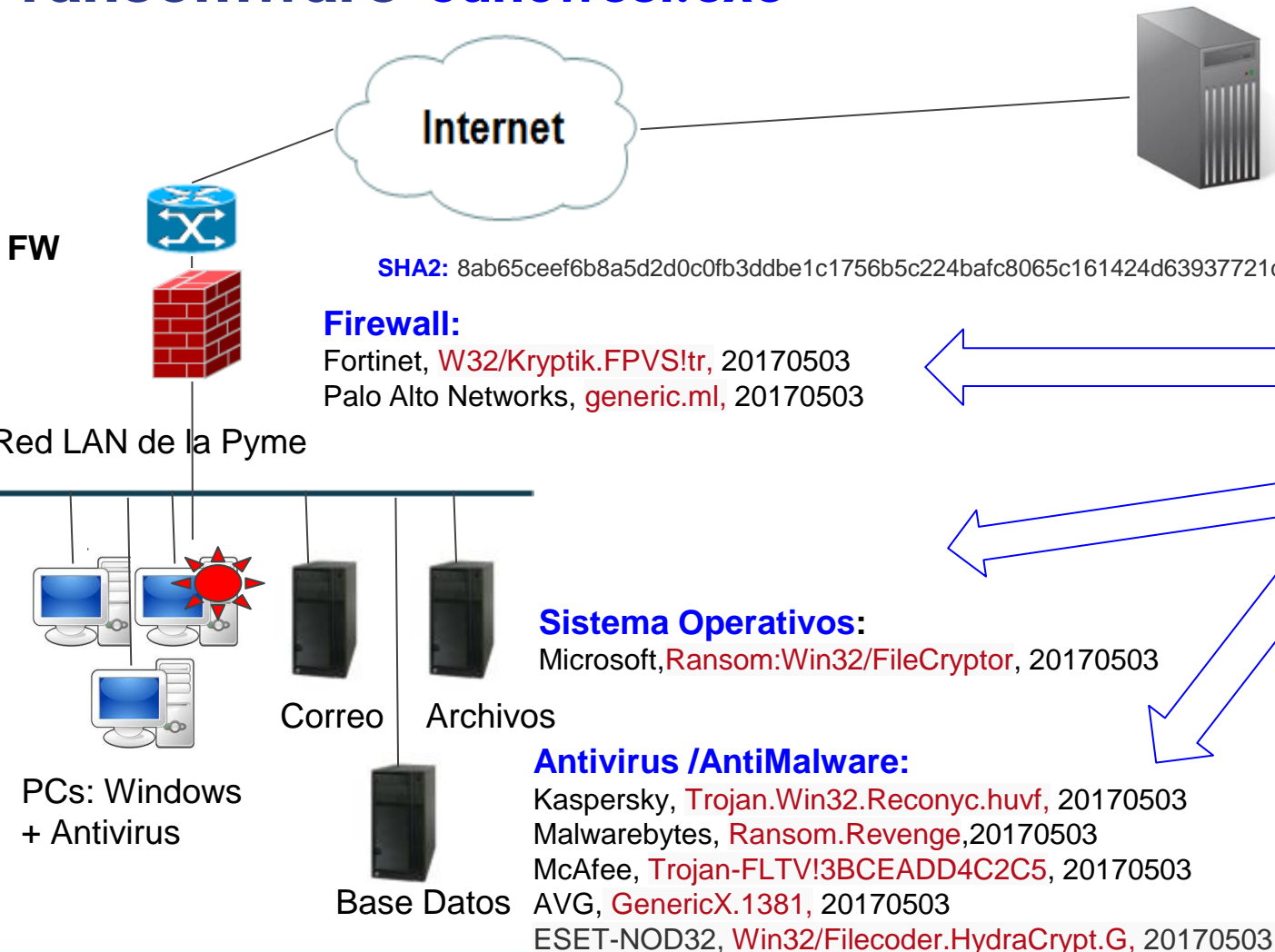
HTTP Traffic

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://secreary.com/SSMA>

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




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




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

Iniciativas:


NO MORE RANSOM!



CRYPTO SHERIFF




RANSOMWARE: Q&A



DECRYPTION TOOLS



REPORT A CRIME



PREVENTION ADVICE

▼ Merry X-Mas Decryptor

Merry X-Mas Decryptor can decrypt files encrypted by the Merry X-Mas ransomware

DOWNLOAD

Tool made by Check Point

DOWNLOAD

Tool made by Emsisoft

▼ Teslacrpt Decryptor

TeslaDecryptor can decrypt files encrypted by TeslaCrypt v3 and v4

For more information, please see this [how-to guide](#)

DOWNLOAD

Tool made by Kaspersky Lab

DOWNLOAD

Tool made by Intel Security

▼ Popcorn Decryptor

The tool is designed to decrypt files encrypted by the Popcorn Ransomware. This zip file is encrypted with password: "elevenpaths"

Please note that this zip file is encrypted with password: "elevenpaths". For more information please see this [how-to guide](#)

DOWNLOAD

Tool made by Elevenpaths

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/tesldecrypt.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/>



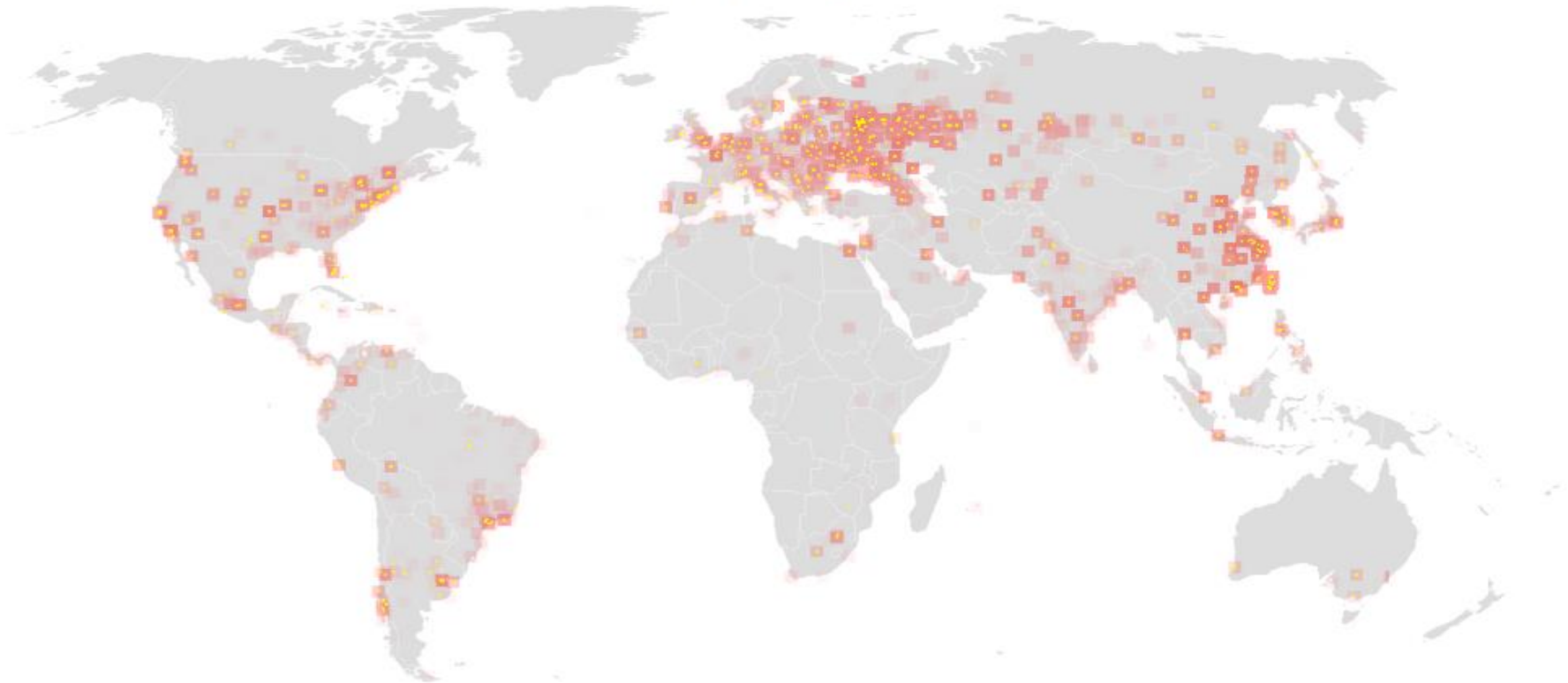
Antes del 12 de Mayo

¿Estábamos listos para lo que venía?



WannaCry - Viernes 12 de Mayo

6:25 PM Eastern ↻



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

WannaCry - Países y Entidades Afectadas



Countries hit in initial hours of cyber-attack

US: Delivery company FedEx affected

UK: 61 NHS organisations disrupted

Russia: Country's interior ministry reported 1,000 of its computers infected



Abfahrt	Linie	Ziel	Gleis
22:10	Pölla - Pölla/Lengfeld	Oiberröhen	8
22:30	Pölla - Pölla/Lengfeld	(S) Hbf	11
22:31	Wolfsgraben	g-B. Süd	10
22:38	Pölla - Zettl	Hbf	8
22:41		Hbf	9
22:36	Itzschitz	Hbf	5
22:44	Göhring - B.	Aue (Sachs)	14
22:45	Erzgebirg - Thauritz (Erzgeb)	Dresden Hbf	11
22:30	Pölla - Freiberg (Sachs) - Thauritz		

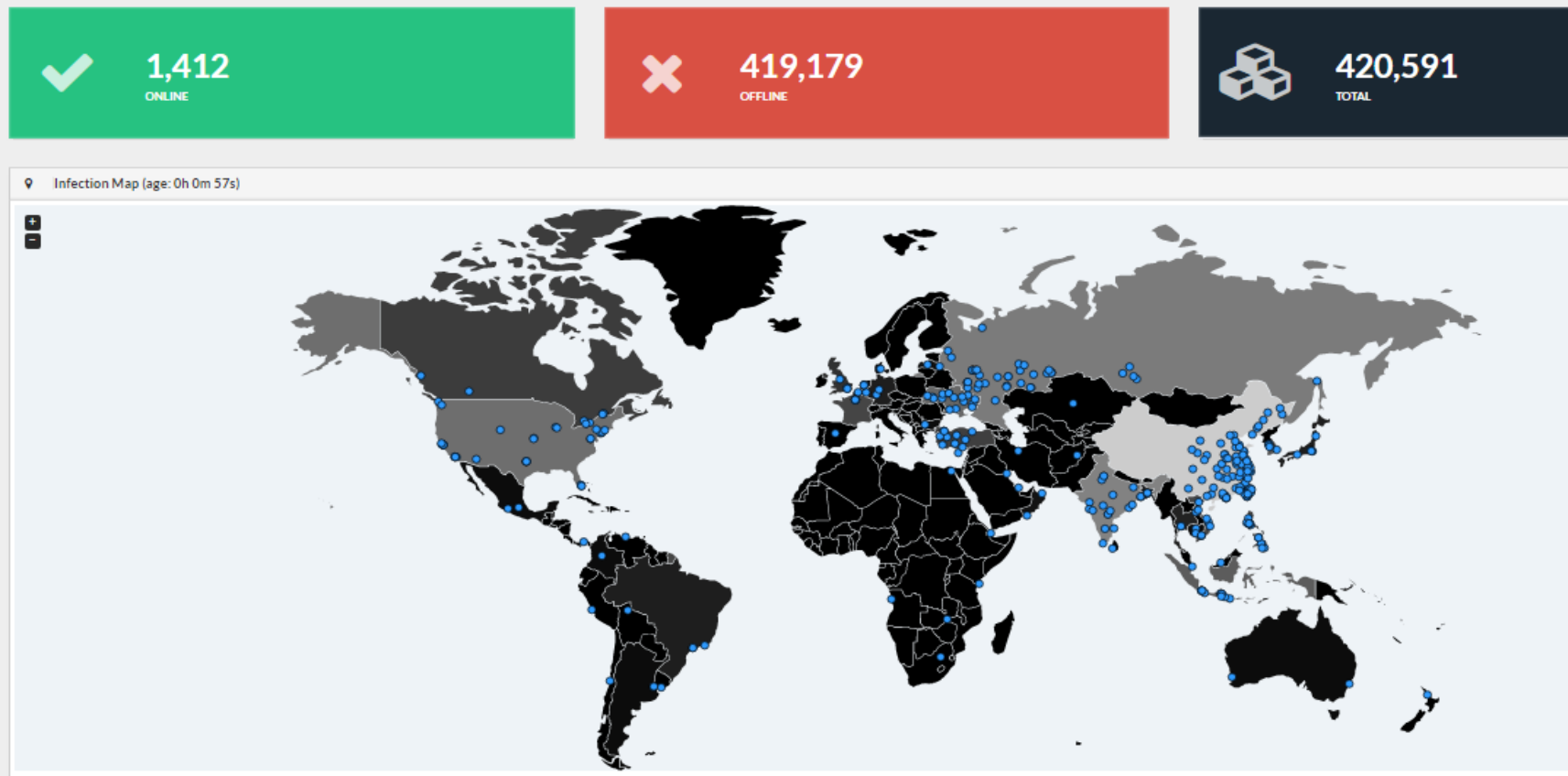


*Map shows countries affected in first few hours of cyber-attack, according to Kaspersky Lab research, as well as Australia, Sweden and Norway, where incidents have been reported since

Source: Kaspersky Lab's Global Research & Analysis Team



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 víctimas, + 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	
<p>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.</p>	
References	
<p>Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p> <ul style="list-style-type: none"> • 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
- ENGLISHMANDENTIST 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
- ETCETERABLU 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

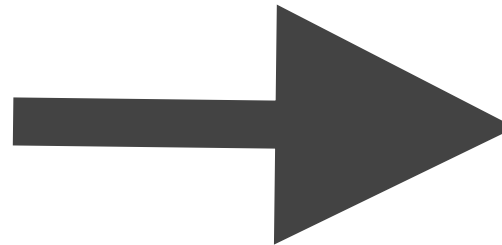


[Equation Group.](#)

Fuente:

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

theshadowbrokers @shadowbrokerss · 13 ago. 2016
 @RT_com @cnnbrk @time @breakingnews @bbcbreaking @wsj @nytimes
 Equation Group - Cyber Weapons Auction #EQGRP_AUCTION

Traducir del inglés

e	Size	Type
BANANAGLEE	6 items	Folde
BARGLEE	1 item	Folde
BLATSTING	7 items	Folde
BUZZDIRECTION	2 items	Folde
EXPLOITS	8 items	Folde
OPS	6 items	Folde
SCRIPTS	33 items	Folde
TOOLS	15 items	Folde
TURBO	2 items	Folde

Equation Group - Cyber Weapons Auction
 Imgur: The most awesome images on the Internet.
 imgur.com

4 34 34

theshadowbrokers @shadowbrokerss · 14 abr.
 @hackerfantastic Lost in Translation — Steemit [steemit.com/shadowbrokers/...](https://steemit.com/shadowbrokers/)
 enjoy!

Traducir del inglés



Lost in Translation — Steemit
 KEK...last week theshadowbrokers be trying to help peoples. This week theshadowbrokers be thinking fuck peoples. Any... by theshadowbrokers
 steemit.com

11 40 45

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 `Reeeeeeeeeeeeeeeee`.

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>

<https://github.com/misterch0c/shadowbroker/>

This repository Search Pull requests

misterch0c / shadowbroker

Code Issues 6 Pull requests 1 Projects 0 Wiki Insights

The Shadow Brokers "Lost In Translation" leak

21 commits 1 branch

Branch: master New pull request

- misterch0c committed on GitHub Merge pull request #19 from keep...
- oddjob oddjob
- swift decrypted files https://steemit.com/shadow...
- windows Merge branch 'master' of https://github.com...
- README.md Update README.md
- file-listing oddjob

README.md

<https://steemit.com/shadowbrokers/@the...>

Exploits

misterch0c / shadowbroker

Watch 353 Unstar 2,724 Fork 1,881

Code Issues 6 Pull requests 1 Projects 0 Wiki Insights

Branch: master shadowbroker / windows / specials /

Create new file Upload files Find file History

File	Description	Time
..	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	Latest commit bc8ff5f on 14 Apr
Eternalblue-2.2.0.xml	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
Eternalblue-2.2.0.exe	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
Eternalblue-2.2.0.fb	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
Eternalchampion-2.0.0.0.xml	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
Eternalchampion-2.0.0.exe	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
Eternalchampion-2.0.0.fb	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
etch-0.dll	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
etchCore-0.x64.dll	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
etchCore-0.x86.dll	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
eteb-2.dll	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago

Watch 353 Unstar 2,724 Fork 1,881

misterch0c / shadowbroker

Code Issues 6 Pull requests 1 Projects 0 Wiki Insights

Branch: master shadowbroker / windows / implants /

Create new file Upload files Find file History

File	Description	Time
..	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	Latest commit bc8ff5f on 14 Apr
Darkpulsar-1.1.0.9.xml	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
Darkpulsar-1.1.0.exe	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
Darkpulsar-1.1.0.fb	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
Mofconfig-1.0.0.0.fb	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
Mofconfig-1.0.0.0.xml	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
Mofconfig-1.0.0.exe	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago
pluginhelper.py	decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/L...	3 months ago

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

TOP SECRET//SI//NOFORN

TOP SECRET//SI//NOFORN



00566_2_FW1-Configuration: Bloc de notas

- Target: East
- Country: Du
Belgium, Eg
- Quad: 2
- Collection
 - 9 SAA
 - Admin

```

Archivo Edición Formato Ver Ayuda
ENSBPASA1# show run
: Saved
:
ASA Version 7.0(6)
!
hostname ENSBPASA1
domain-name sag
enable password PVSASRJovmamnVkD encrypted
names
name 192.168.202.25 sag-srv1|
name 192.168.202.20 sag-srv2
name 192.168.246.7 vpn1-2-nsrp
name 192.168.246.6 vpn2-int
name 192.168.246.5 vpn1-int
    
```

Al Quds Bank for
 Development &
 Investment

4 Shared, multi-bank
 SAA servers

ENSBDMGMT2

Middleware

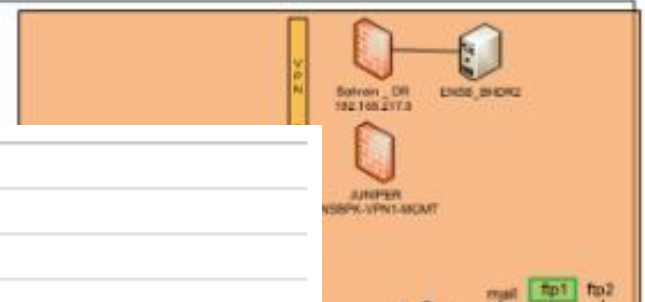
Back End

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



Employee Network

Financial Network



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	Host	I	K	L
		operatingSystemVersion	operatingSystem	name
192.168.200.33	ENSBDFIIV1	5.0 (2195)	Windows 2000 Server	QASERVER
192.168.200.34	fiiv-srv2	5.0 (2195)	Windows 2000 Server	QASERVER2
192.168.200.35	fiiv-srv3	5.1 (2600)	Windows XP Professional	QATEST
192.168.200.41	ENSBDKFAE1	5.1 (2600)	Windows XP Professional	QA
192.168.200.42	kfae-srv2	5.0 (2195)	Windows 2000 Server	QIIB
192.168.200.45	difx-srv1	5.0 (2195)	Windows 2000 Server	QIIB2K
192.168.200.46	difx-srv2	5.1 (2600)	Windows XP Professional	QAIS
192.168.200.47	ENSBDIFX1	5.0 (2195)	Windows 2000 Server	QIIB-CC
192.168.200.50	sharesaa-srv	5.0 (2195)	Windows 2000 Server	QIIB-CC
192.168.200.51	ENSBDL1 N	5.1 (2600)	Windows XP Professional	QIDRISI
192.168.200.52	ENSBDL2	5.2 (3790)	Windows Server 2003	QAHOST1
192.168.200.53	sharesaa-srv	5.2 (3790)	Windows Server 2003	QNBVM
192.168.200.56	pmap-srv1	6.1 (7600)	Windows Server 2008 R2 Enterprise	QAHOST3
192.168.200.57	pmap-srv2	5.2 (3790)	Windows Server 2003	QTEL
192.168.200.58	pmap-srv3	5.2 (3790)	Windows Server 2003	QTEL
192.168.200.59	dgcx-srv1	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

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](https://support.microsoft.com/es-co/help/4013389).

On this page

[Executive Summary](#)

[Affected Software and Vulnerability Severity Ratings](#)

[Vulnerability Information](#)

[Security Update Deployment](#)

[Acknowledgments](#)

[Disclaimer](#)

[Revisions](#)

<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 compañía, dejó 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**, **ExclusionEngine**, and **ExclusionEngine**.

Microsoft Security Advisory 4025685

Guidance related to June 2017 security update release

Published: June 13, 2017

Version: 1.0

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](#).

On this page

[Executive Summary](#)

[Advisory FAQ](#)

[Other Information](#)

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



The screenshot shows the main interface of the WannaCry ransomware. At the top, a red banner reads "Oops, your files have been encrypted!". Below this, a large padlock icon is displayed. The interface is divided into several sections:

- Payment timer:** A red box on the left indicates "Payment will be raised on 5/15/2017 16:50:06" with a "Time Left" of 02:23:34:22. Below it, another box states "Your files will be lost on 5/19/2017 16:50:06" with a "Time Left" of 06:23:34:22.
- Message:** A central text area explains the encryption and demands payment in Bitcoin. It includes a "What Happened to My Computer?" section and a "How Do I Pay?" section.
- Bitcoin Payment:** A section titled "Send \$300 worth of bitcoin to this address:" provides a Bitcoin address: `115p7UMMngo1pMvkpHjicRdfJNXj6LrLn`. A "Copy" button is next to the address.
- Navigation:** At the bottom, there are two buttons: "Check Payment" and "Decrypt".

Overlaid on the interface is a Windows-style message box titled "You have a new message:" from "@WanaDecryptor@". The message reads: "I have already sent decryption keys to many customers who had sent me the correct amounts of bitcoin, and I guarantee the decryptions for such honest customers. Send me a message with your unique bitcoin wallet address an hour before your payment. Then you will receive the decryption key more quickly." The message box has an "OK" button.

WannaCry - Bitcoins

The screenshot shows a forum post on BitcoinTalk.org. The post title is "Re: Monitoring WannaCry hackers' bitcoin addresses in real time" and it was posted on May 13, 2017, at 05:13:35 PM. A quote from a user named "coinits" on May 13, 2017, at 04:13:09 PM states: "For a global attack they have not collected a lot of bitcoin yet. Results as of 16:00 GMT". The main content of the post is a list of Bitcoin addresses associated with the WannaCry ransomware, highlighted in a green box:

- WANNACRY
- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- 115p7UMMngo1pMvkpHijcRdfJNXj6LrLn

Below the addresses, the post provides further details for "Wallet 3":

- Wallet 3: 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- live link: <https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94>
- 36 transactions = 6.53259945 BTC
- ~ 14.28 BTC x \$1735.35 per BTC = \$24,781 ransom paid thus far.

The post concludes with the instruction: "Add more addresses as you find them."

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

Resumen

Dirección: 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Hash 160: 17b4bd9a139158614e8f54c6b800a1822609436a




Herramientas: [Etiquetas Relacionadas](#) - Las salidas no utilizadas

Resumen

Dirección: 115p7UMMngo1pMvvpHijcRdfJNXj6LrLn

Hash 160: 00e8fd98ca34f195b020af4a8b1c7238663d4212

Herramientas: [Etiquetas Relacionadas](#) - Las salidas no utilizadas

Actas	WANNACRY	BTC 50.77421
Número		
total rec		
Balanc		
Actas	WANNACRY	USD 130,302.37
Número		
total rec		
Balanc		
Actas	WANNACRY	BRL 417,274.24
Número de transacciones	108	
total recibida	14.08097351 BTC	
Balace final	14.08097351 BTC	

Solicitud de Pago Botón de Donación

Fuente: <https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw>

Fuente: <https://blockchain.info/address/115p7UMMngo1pMvvpHijcRdfJNXj6LrLn>

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.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.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 .bzz .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 .cert .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

1. Aplicar el Parche MS17-010
2. Aislar los equipos Infeccionados
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 **políticas 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>



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Recomendaciones:

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>