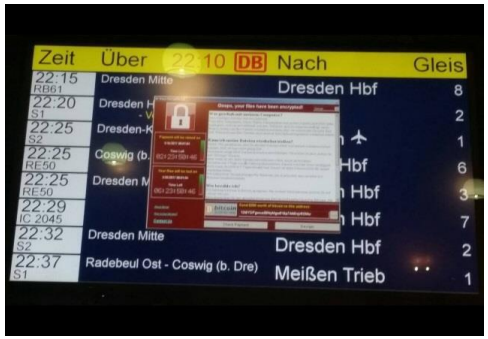
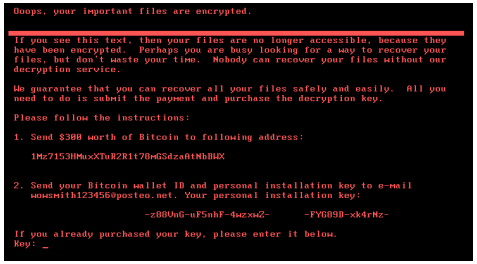
CENTRO CRIPTOLÓGICO NACIONAL

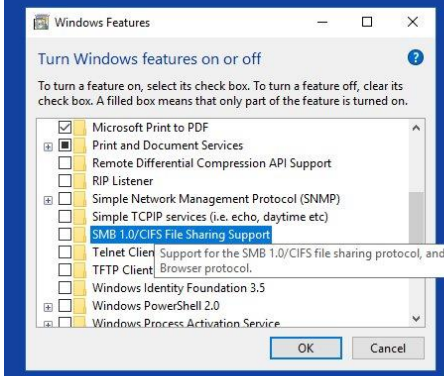
CAMPAÑA DE CIBERATAQUES CON RANSOMWARE WANNACRY / PETYA





USO OFICIAL

INDICE



Security TIP

Just Disable SMB to Prevent Against WannaCry Attacks

SMB comes enabled by default on Windows, which users are advised to disable immediately.

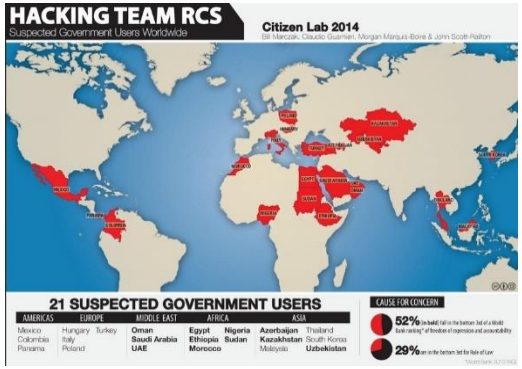
Method 1: Search "Windows features," open above shown settings, Uncheck SMB > click OK and restart your PC.

Method 2: One-line PowerShell command to disable SMB v1:

"Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol"

Vulnerabilidades en el dominio público

- El 05.07.2015 **Hacking Team** fue comprometido (400 GB datos) permitiendo que se hicieran **públicos exploits de día cero (sin parche de seguridad)**.
- **The Shadow Brokers**, grupo de hackers que apareció por primera vez en el verano de 2016. Publicaron varias filtraciones que contenían **herramientas de hacking de la NSA** (Equation Group), incluyendo varios exploits de día cero.
- La serie **"Vault 7"**, se estrenó el 07.03.2017 con el capítulo "Year Zero". Es la **filtración de datos de inteligencia más extensa** hasta la fecha, superando a "ShadowBrokers".
- Se revelan **capacidades de ataque significativas**, con múltiples herramientas disponibles para varias plataformas como Linux, Windows, Android, iOS, macOS y otros.



Ciberamenaza. Ransomware en AAPP

2015

Tipo	Nº incidentes
Cryptowall	109
Cryptolocker	93
Torrentlocker	89
Teslacrypt	73
Otros	73

Total: 427

2016

Tipo	Nº incidentes
Locky	785
Teslacrypt	319
Torrentlocker	308
Cryptowall	278
Otros	340

Total: 2.030

CORREOS

Su paquete ha llegado a **20 de marzo**. Courier no pudo entregar una carta certificada a usted. Imprima la informaci'on de env'io y mostrarla en la oficina de correos para recibir la carta certificada.

CD 438685108339

Descargar informaci'on sobre su env'io

Si la carta certificada no se recibe dentro de los 30 d'ias laborables Correos tendr'a derecho a reclamar una indemnizaci'on a usted para 'el est'a manteniendo en la cantidad de 7,55 euros por cada d'ia de cumplir. Usted puede encontrar la informaci'on sobre el procedimiento y las condiciones de la carta de mantener en la oficina m'as cercana. Este es un mensaje generado autom'aticamente.

Condiciones y T'erminos del Servicio de localizaci'on de env'ios

La consulta del estado detallado para env'ios individuales y del estado final para env'ios masivos es un servicio gratuito que Correos le ofrece para sus env'ios remitidos con car'acter registrado. Este servicio es de car'acter informativo sin que en ning'un caso sustituya la informaci'on que ud. puede obtener mediante acuse de recibo o certificaci'on de servicios postales. Correos no se responsabiliza de los errores u omisi'on de informaci'on, por lo que advierte que no se adopten decisiones o acciones derivadas de la informaci'on obtenida por este servicio.

Haga clic aqu'i para darse de baja.

@ Copyright 2014 Sociedad Estatal Correos y Tel'egrafos, S.A.

RESUMEN DE LA FACTURA
Fecha factura: 21 de junio de 2016
Periodo de facturación: del 20/05/2016 al 21/06/2016
Factura nº: LVP29664QL1292971
Ref.Factura: 08068237 1371 32810

Total Factura: 875,37 €

Datos del Cliente
código personal: 512462
Actividad económica (CNAE): 8577
CUPS: ES8748355 9JWCK
Potencia contratada: 26,3, 26,3 Y 26,3 kW
Tarifa de acceso: 3.0A
Contrato de acceso: 1186106947
Número de Contador: 4137696

CONSULTA TU FACTURA Y CONSUMO

Política de privacidad

Endesa se reserva el derecho de modificar, unilateralmente, en cualquier momento y sin previo aviso las presentes condiciones. En estos casos se procederá a su publicación y aviso con la máxima antelación posible. De igual modo, se reserva el derecho a modificar, unilateralmente, en cualquier momento y sin previo aviso, la presentación y configuración de la Web.

Con respecto a la cesión de datos personales a terceros, se comunica a los usuarios que con carácter general los datos personales no serán cedidos a terceras entidades, salvo en aquellos supuestos en los que la cesión responda al cumplimiento de una obligación legal o también en aquellos casos en los que exista una relación contractual de encargo de tratamiento para la prestación de un determinado servicio. En todo caso los usuarios deben saber que en el caso de producirse una cesión de este tipo, la misma únicamente se llevará a cabo cuando se haya obtenido el consentimiento expreso por parte del Usuario.

© Endesa S.A. 2016

El "ransomware" está contribuyendo a hacer la ciberamenaza real

Familia/Versión Ransomware: https://id-ransomware.malwarehunterteam.com/
Herramientas de descifrado: https://www.nomoreransom.org/decryption-tools.html

CRONOLOGIA

- **Febrero 2015**, Compañía KASPERSKY publica la existencia de EQUATION GROUP (Vinculado a NSA). Este grupo esta realizando ataques de gran complejidad desde 1996.
- **Agosto 2016** grupo SHADOWBROKERS comunica que dispone de las herramientas de la NSA y pide 500 millones de dólares (en bitcoins).
- **Enero 2017** NSA informa a MICROSOFT de ls vulnerabilidades DOUBLEPULSAR y EHERNALBLUE**.**
- **14 de marzo 2017** MICROSOFT publica parche de seguridad CRITICO que resuelve estas vulnerabilidades**.**
- **14 de abril 2017** SHADOWBROKER publica estas vulnerabilidades en INTERNET.
- **12 de mayo 2017** Se detecta ataque en TELFONICA.

WannaCry como caso de estudio para futuros ciberataques

Microsoft Security Bulletin MS17-010 - Critical

ShadowBrokers leak

WannaCry 2.0 ransomeware outbreak started appearing in the wild.

March 14 2017

April 14 2017

May 12 2017

May 15 2017

New variants of WannaCry appear in the wild

2 months interval

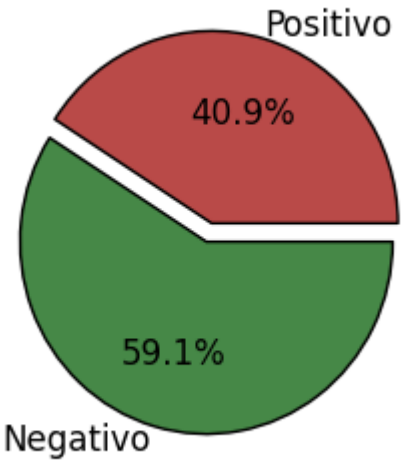
WannaCry CAPACIDADES

- **Vulnerabilidad ETERNALBLUE**. Permite la ejecución de código remoto.
- **Vulnerabilidad DOUBLEPULSAR.** Permite el despliegue por la red corporativa usando en puerto 445 y protocolo SMB (comunicación entre equipos Windows).
- Código dañino NO muy bien implementado. ***Motivo KILL-SWITCH????***
  - **http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com**
- Cifra muy bien implementada. Clave secreta (AES 128) para cada fichero. Doble empleo de Clave Pública para proteger este cifrado. Necesidad de la **clave PRIVADA** (dificultad computacional de romper la clave).
- Sistema de cobro deficiente. Rescate de 300$ (3 días para pagar / 6 días para perder los ficheros). **Ha recaudado + $ 70.000** .
- Atribución: LAZARUS Group (KN) ????

WannaCry .... Detección ANTIVIRUS

Análisis solicitado por info@ccn-cert.cni.es
Fecha: 2017-05-12 17:00:36
Nombre: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.bin
Tamaño: 3514368 bytes
Tipo de fichero: PE32 executable (GUI) Intel 80386, for MS Windows
Tipo MIME: application/x-dosexec
MD5: 84c82835a5d21bbcf75a61706d8ab549
SHA1: 5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA256: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

Resultado: POSITIVO



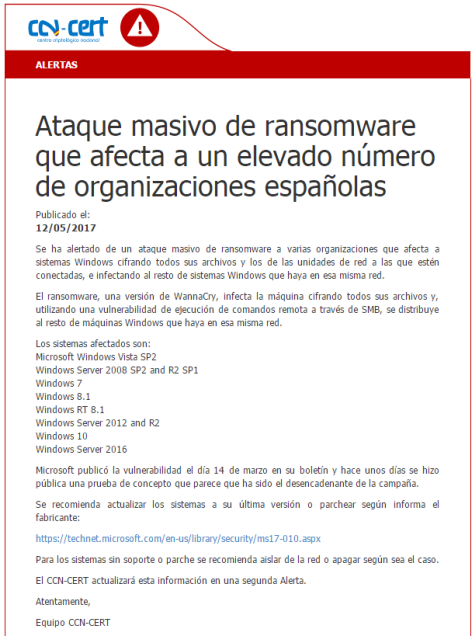
Antivirus	Resultado	Malware
NANO-Antivirus	NEGATIVO	
Symantec	NEGATIVO	
Zillya	NEGATIVO	
AVG	POSITIVO	Trojan horse Ransom_r.CFY
Arcabit	POSITIVO	Trojan.Graftor.D5A218
Quick Heal	NEGATIVO	
Avast	POSITIVO	OK
Ad-Aware	POSITIVO	Gen:Variant.Graftor.369176
Ikarus	NEGATIVO	
Nod32	POSITIVO	Win32/Filecoder.WannaCryptor.D trojan
Vba32	NEGATIVO	
Emsisoft	POSITIVO	Gen:Variant.Graftor.369176 (B)
Mcafee	NEGATIVO	
Kaspersky	NEGATIVO	
Sophos	NEGATIVO	
ClamAV	NEGATIVO	
Zoner	NEGATIVO	
F-Prot	NEGATIVO	
Dr.Web	POSITIVO	BACKDOOR.Trojan
BitDefender	POSITIVO	Gen:Variant.Graftor.369176
eScan	POSITIVO	Gen:Variant.Graftor.369176(DB)
ClamAV	NEGATIVO	

Campaña Wannacry (12.05)

- **12.05.2017** se tiene constancia de **ciberataque tipo ransomware** (WannaCry) en Telefónica.
- **12.05.2017 (13:40 / 16:30)** CCN-CERT difunde **primera alerta a su comunidad**,.
- **12.05.07 (19:30/19:54/21:50)** Primera versión vacuna **WannaCry Prevention**. Investigación del modo de proceder del código dañino.

CCN-CERT AL 07/17 Ataque masivo de ransomware

Detalles
Publicado: 12 Mayo 2017 13:49 h.



ALERTAS

Ataque masivo de ransomware que afecta a un elevado número de organizaciones españolas

Publicado el:
12/05/2017

Se ha alertado de un ataque masivo de ransomware a varias organizaciones que afecta a sistemas Windows cifrando todos sus archivos y los de las unidades de red a las que estén conectadas, e infectando al resto de sistemas Windows que haya en esa misma red.

El ransomware, una versión de WannaCry, infecta la máquina cifrando todos sus archivos y, utilizando una vulnerabilidad de ejecución de comandos remota a través de SMB, se distribuye al resto de máquinas Windows que haya en esa misma red.

Los sistemas afectados son:
Microsoft Windows Vista SP2
Windows Server 2008 SP2 and R2 SP1
Windows 7
Windows 8.1
Windows RT 8.1
Windows Server 2012 and R2
Windows 10
Windows Server 2016

Microsoft publicó la vulnerabilidad el día 14 de marzo en su boletín y hace unos días se hizo pública una prueba de concepto que parece que ha sido el desencadenante de la campaña.

Se recomienda actualizar los sistemas a su última versión o parchear según informa el fabricante:

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

Para los sistemas sin soporte o parche se recomienda aislar de la red o apagar según sea el caso.

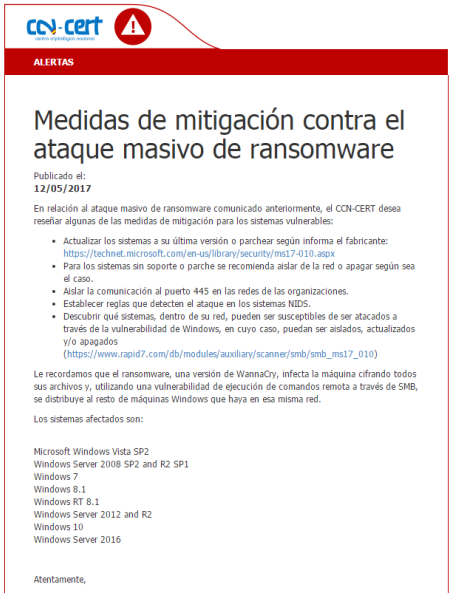
El CCN-CERT actualizará esta información en una segunda Alerta.

Atentamente,

Equipo CCN-CERT

CCN-CERT AL 08/17 Medidas de mitigación contra el ataque de ransomware (2)

16:30 h.



ALERTAS

Medidas de mitigación contra el ataque masivo de ransomware

Publicado el:
12/05/2017

En relación al ataque masivo de ransomware comunicado anteriormente, el CCN-CERT desea reseñar algunas de las medidas de mitigación para los sistemas vulnerables:

- Actualizar los sistemas a su última versión o parchear según informa el fabricante: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- Para los sistemas sin soporte o parche se recomienda aislar de la red o apagar según sea el caso.
- Aislar la comunicación al puerto 445 en las redes de las organizaciones.
- Establecer reglas que detecten el ataque en los sistemas NIDS.
- Descubrir qué sistemas, dentro de su red, pueden ser susceptibles de ser atacados a través de la vulnerabilidad de Windows, en cuyo caso, puedan ser aislados, actualizados y/o apagados (https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_ms17_010)

Le recordamos que el ransomware, una versión de WannaCry, infecta la máquina cifrando todos sus archivos y, utilizando una vulnerabilidad de ejecución de comandos remota a través de SMB, se distribuye al resto de máquinas Windows que haya en esa misma red.

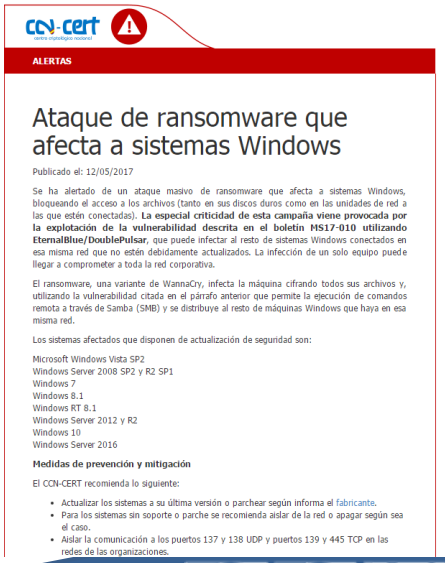
Los sistemas afectados son:

Microsoft Windows Vista SP2
Windows Server 2008 SP2 and R2 SP1
Windows 7
Windows 8.1
Windows RT 8.1
Windows Server 2012 and R2
Windows 10
Windows Server 2016

Atentamente,

CCN-CERT AL 09/17 Ataque de ransomware que afecta a sistemas Windows (3)

Detalles
Publicado: 12 Mayo 2017 19:30 h.



ALERTAS

Ataque de ransomware que afecta a sistemas Windows

Publicado el: 12/05/2017

Se ha alertado de un ataque masivo de ransomware que afecta a sistemas Windows, bloqueando el acceso a los archivos (tanto en sus discos duros como en las unidades de red a las que estén conectadas). **La especial criticidad de esta campaña viene provocada por la explotación de la vulnerabilidad descrita en el boletín MS17-010 utilizando EternalBlue/DoublePulsar**, que puede infectar al resto de sistemas Windows conectados en esa misma red que no estén debidamente actualizados. La infección de un solo equipo puede llegar a comprometer a toda la red corporativa.

El ransomware, una variante de WannaCry, infecta la máquina cifrando todos sus archivos y, utilizando la vulnerabilidad citada en el párrafo anterior que permite la ejecución de comandos remota a través de Samba (SMB) y se distribuye al resto de máquinas Windows que haya en esa misma red.

Los sistemas afectados que disponen de actualización de seguridad son:

Microsoft Windows Vista SP2
Windows Server 2008 SP2 y R2 SP1
Windows 7
Windows 8.1
Windows RT 8.1
Windows Server 2012 y R2
Windows 10
Windows Server 2016

Medidas de prevención y mitigación

El CCN-CERT recomienda lo siguiente:

- Actualizar los sistemas a su última versión o parchear según informa el fabricante.
- Para los sistemas sin soporte o parche se recomienda aislar de la red o apagar según sea el caso.
- Aislar la comunicación a los puertos 137 y 138 UDP y puertos 139 y 445 TCP en las redes de las organizaciones.

Publicado: 12 Mayo 2017 19:54 h. Listado SAT-SARA y SAT-INET

ALERTAS

Listado de ficheros, hash e IoCs del ataque de ransomware

Publicado el: 12/07/2017

Continuando con la información sobre el ataque de ransomware que afecta a sistemas Windows, el CCN-CERT informa sobre sus investigaciones y adjunta un listado de ficheros, hash e indicadores de compromisos (IoC) que tienen relación con el citado incidente de ransomware.

Ficheros creados por el programa

- **taskse.exe**
  MD5: 8495400f199ac77853c53b5a3f278f3e
  SHA1: be5d6279874da315e3080b06083757aad9b32c23
  SHA256:
  2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d

- **taskdl.exe**
  MD5: 4fef5e34143e646dbf9907c4374276f5
  SHA1: 47a9ad4125b6bd7c55e4e7da251e23f089407b8f
  SHA256:
  4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79

- **@WanaDecryptor@.exe**

Directorios creados o utilizados

C:\TaskData\Tor\

Claves de registro

reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "zvcytmeqpytz910" /t REG_SZ /d "\"C:\tasksche.exe\"" /f

Publicado 12 Mayo 2017 21:51 h. Listado SAT-SARA y SAT-INET

ALERTAS

Herramienta de prevención del ransomware WannaCry

Publicado el: 12/07/2017
Fecha alerta

En relación con el incidente de seguridad de la campaña del **ransomware,** de la variante de **WannaCry** notificada en los últimos boletines, el CCN-CERT pone a su disposición un script que permite **parar la ejecución** de este código dañino en equipos con **Microsoft Windows**, tanto en los idiomas español como en inglés.

Para ejecutar el script basta con copiarlo en el escritorio del equipo y ejecutarlo con privilegios de administrador.

El CCN-CERT quiere hacer notar que dicha herramienta no elimina el malware, ni permite el descifrado de los ficheros afectados por este ransomware. No obstante, y como se ha indicado, sí permite parar la actividad de cifrado de los ficheros del equipo.

Enlace a la herramienta

Atentamente,

Equipo CCN-CERT

//

Esta es una lista de notificaciones del CCN-CERT.

Por favor, no responda a este correo. Si necesita más información, póngase en contacto con nosotros a través del correo:

info@ccn-cert.cni.es

Campaña Wannacry (13.05)

- **13.05.2017 (13:00/18:40)**, se desarrolla vacuna, **herramienta CCN-CERT NoMoreCry v0.1**. Más de 50.000 descargas.

Publicado 13 Mayo 2017 13:05 h. Listado Alertas, SAT-SARA y SAT-INET

ALERTAS

NoMoreCry Tool, herramienta del CCN-CERT que impide la ejecución del ransomware WannaCry

Publicado el: 13/05/2017
Fecha alerta

En relación con el incidente de seguridad de la campaña del **ransomware WannaCry** notificada en los últimos boletines, el CCN-CERT informa sobre el desarrollo de la herramienta "***CCN-CERT NoMoreCry Tool***". Esta herramienta, disponible para todas las entidades que lo requieran, crea un mutex (algoritmo de exclusión mutua) en el equipo que previene la ejecución del código dañino WannaCry 2.0. Es importante reseñar que, en el caso de

ERT AL 12/17 CCN-CERT's tool to prevent the execution of the ransomware WannaCry

: 13 Mayo 2017 18:04 h.

Herramienta para prevenir la infección por el ransomware WannaCry

Detalles
Publicado: 13 Mayo 2017 16:03 h.

- herramienta
- rasnsomware
- wannacry
- NoMoreCry

El CCN-CERT ha desarrollado una herramienta para prevenir la infección por el malware WannaCry 2.0. Se trata de "*CCN-CERT NoMoreCry Tool*", una herramienta disponible para todas las entidades que lo requieran, que crea un mutex (algoritmo de exclusión mutua) en el equipo que previene la ejecución del código dañino WannaCry 2.0. Es importante reseñar que, en el caso de **máquinas infectadas, la ejecución de esta herramienta NO es de aplicación** al no actuar sobre la misma de la forma prevista.

El Equipo de Respuesta del Centro Criptológico Nacional hace notar que la herramienta deberá **ejecutarse tras cada reinicio**, debido a que no presenta persistencia en el equipo. Este proceso se puede automatizar mediante la modificación del registro de Windows o a través de la aplicación de políticas en el dominio.

Esta herramienta funciona en **sistemas operativos superiores a Windows XP**.

CCN-CERT NoMoreCry Tool se encuentra en la plataforma en la nube del CCN-CERT, LORETO. Junto a ella también está disponible el Script que evita la ejecución del código dañino en equipos Windows en inglés y en español.

Más información:

Enlace a la herramienta CCN-CERT NoMoreCry y script

Comunicado CCN-CERT

CCN-CERT IA-03/17 Medidas Seguridad ransomware

CCN-CERT BP-04/16 Buenas Prácticas frente al ransomware

ALERTAS

NoMoreCry Tool, CCN-CERT's tool to prevent the execution of the ransomware WannaCry

Publicado el: 13/07/2017
Fecha alerta
Concerning with the massive WannaCry ransomware campaign notified in the latest bulletins, CCN-CERT announces the development of the tool "***CCN-CERT NoMoreCry Tool***".

This tool is available to all organisations that need to use it. It creates a mutex (mutual exclusion algorithm) on the computer that prevents the execution of the malicious code WannaCry 2.0. It is important to note that **this tool is Not intended to clean compromised machines**.

CCN-CERT indicates that the tool should be run after each restart. This process can be automated by modifying the Windows registry or through the implementation of the proper policies in the domain

This tool works on operating systems v**ersions higher than Windows XP**.

CCN-CERT NoMoreCry Tool is located in CCN-CERT's cloud, LORETO. In this location there is also available a complementary Script that prevents the execution of the malware on Windows computers in English and Spanish.

Further information on:

CCN-CERT NoMoreCry and script

CCN-CERT Press Release

Campaña Wannacry (14.05)

- **14.05.2017 (18:00)**, se publica **informe de código dañino** (CCN-CERT ID 17/17 Ransom.WannaCry) Versión 0.2 NoMoreCry

Informe del ransomware WannaCry con vacuna y medidas para su detección y desinfección

Detalles
Publicado: 14 Mayo 2017 18:13 h.

- herramienta
- Ransomware
- vulnerabilidad
- Informe de Código Dañino
- Windows
- wannacry

- El CCN-CERT ha actualizado además la vacuna para impedir la ejecución del código dañino en todos los sistemas Windows
- El informe recoge el análisis preliminar de la campaña masiva que ha afectado a nivel global con varias muestras de ransomware de la familia WannaCry, que realizan un cifrado masivo de ficheros y solicitan un rescate para recuperarlos.

El CCN-CERT acaba de publicar en su portal el Informe de Código Dañino: CCN-CERT ID-17/17 Código Dañino. WannaCry, que recoge el análisis preliminar de la campaña de ransomware de la familia WannaCry, iniciada este viernes, 12 de mayo, y que realiza un cifrado masivo de ficheros para, después, solicitar un rescate para recuperarlos.

Esta variante de ransomware incorpora código para realizar la explotación de la vulnerabilidad publicada por Microsoft el día 14 de marzo descrita en el boletín MS17-010 y conocida como ETERNALBLUE. Hasta el momento todas las máquinas han sido atacadas mediante este exploit.

El ransomware WannaCry, escanea tanto la red interna como la externa, realizando conexiones al puerto 445 (SMB) en busca de equipos no actualizados, para propagarse a ellos e infectarlos, lo que le confiere a la muestra funcionalidad similar a la de un gusano. Este movimiento lateral dentro de la red utiliza una variante del payload DOUBLEPULSAR.

Campaña Wannacry (15/16.05)

- **15/16.05.2015** Vigilancia y coordinación con organismos. Se remiten **+90 alertas** de conexión a servidores. Versión 0.3 NoMoreCry

CCN-CERT AL 13/17 CCN-CERT NoMoreCry Tool V.0.3, actualizada la vacuna frente a WannaCry

Detalles
Publicado: 15 Mayo 2017 16:23 h.

ccn-cert
centro criptológico nacional

ALERTAS

CCN-CERT NoMoreCry Tool V.0.3, actualizada la vacuna frente a WannaCry

Publicado el: 15/05/2017
Fecha alerta

El CCN-CERT ha actualizado a una versión 3 su herramienta para prevenir la infección por el malware **WannaCry 2.0**. Se trata de ***NoMoreCry-v0.3*** (para Windows XP y superiores) y ***NoMoreCry2000-v0.3*** (para Windows 2000). En ambos casos se crea en el equipo los objetos de exclusión mutua que impiden la ejecución del código dañino. Esta nueva versión de la herramienta consta también de un fichero de texto (**NoMoreCry_mutex**) que obligatoriamente debe acompañar al ejecutable en la misma ruta. Dentro de este fichero se encuentran los nombres de los objetos de exclusión mutua que la herramienta creará.

Esta nueva versión admite la ejecución en modo silencioso mediante su ejecución desde linea de comandos mediante la opción "-s". Ej.: c:\NoMoreCry.exe -s

Es importante reseñar que, **en el caso de máquinas infectadas, la ejecución de esta herramienta NO es de aplicación.**

Asimismo, hay que tener en cuenta que la presente herramienta no presenta persistencia en el equipo, por lo que para la correcta protección frente a esta amenaza deberá **ejecutarse tras cada reinicio**. Esto se puede automatizar mediante la modificación del registro de Windows o mediante la aplicación de políticas de grupo en el dominio.

CCN-CERT NoMoreCry Tool V.0.3, actualizada la vacuna frente a WannaCry

Detalles
Publicado: 15 Mayo 2017 16:34 h.

- herramienta
- Ransomware
- wannacry
- NoMoreCry

El CCN-CERT ha actualizado a una versión 3 su herramienta para prevenir la infección por el malware **WannaCry 2.0**. Se trata de *NoMoreCry-v0.3* (para Windows XP y superiores) y *NoMoreCry2000-v0.3* (para Windows 2000). En ambos casos se crea en el equipo los objetos de exclusión mutua que impiden la ejecución del código dañino. Esta nueva versión de la herramienta consta también de un fichero de texto (NoMoreCry_mutex) que obligatoriamente debe acompañar al ejecutable en la misma ruta. Dentro de este fichero se encuentran los nombres de los objetos de exclusión mutua que la herramienta creará.

Esta nueva versión admite la ejecución en modo silencioso mediante su ejecución desde linea de comandos mediante la opción "-s". Ej.: c:\NoMoreCry.exe -s

Es importante reseñar que, **en el caso de máquinas infectadas, la ejecución de esta herramienta NO es de aplicación.**

Asimismo, hay que tener en cuenta que la presente herramienta no presenta persistencia en el equipo, por lo que para la correcta protección frente a esta amenaza deberá ejecutarse tras cada reinicio. Esto se puede automatizar mediante la modificación del registro de Windows o mediante la aplicación de políticas de grupo en el dominio.

Ambas herramientas se encuentran en la plataforma en la nube del CCN-CERT, LORETO. Es preciso acceder previamente a sus ficheros correspondientes: README_v0.3 (para Windows XP y superiores) y README_Win2000-v03 (para Windows 2000)

Más información:

Acceso a las herramientas (V.0.3)

Informe de Código Dañino. Ransom.WannaCry

Balance del Centro Criptológico Nacional frente a la campaña de ciberataques con ransomware

Detalles
Publicado: 15 Mayo 2017 19:35 h.

- herramienta
- Ransomware
- wannacry
- campaña

- Se han redoblado los esfuerzos para detectar y detener el código dañino, analizarlo y aplicar medidas que mitiguen el impacto en el sector público y empresas de interés estratégico para el país, en coordinación con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC).
- La colaboración con otras entidades, nacionales e internacionales, públicas y privadas, ha sido ejemplar y clave para evitar un mayor impacto del ataque y ofrecer una serie de medidas preventivas.
- Se recomienda aplicar a los sistemas las últimas actualizaciones de Microsoft Windows y la ejecución de la vacuna contra el ransomware desarrollada por el CCN-CERT.

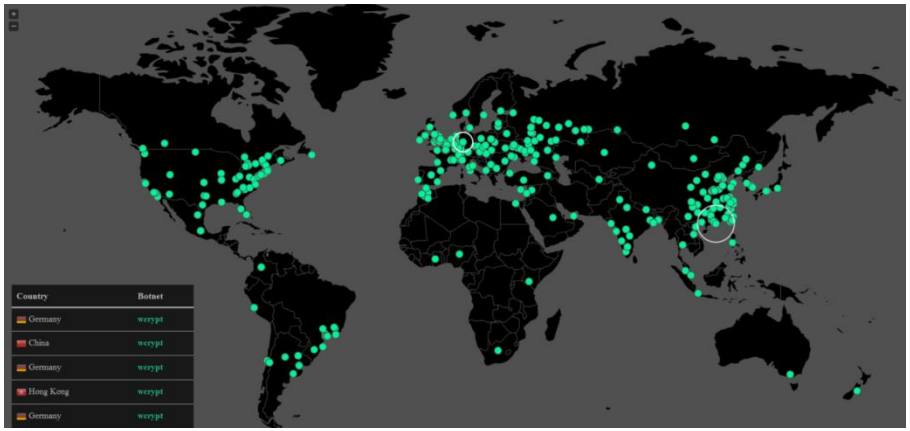
Desde que comenzaron a llegar al CCN-CERT los primeros incidentes del ransomware WannaCry, a primeras horas del viernes 12 de mayo, su equipo de expertos inició la tarea de contención, prevención y erradicación, con el fin mantener protegido el ciberespacio español y, muy especialmente, el sector público y las empresas de interés estratégico para el país.

Desde un primer momento se redobló el trabajo para conocer más información sobre el modo de proceder de este código dañino, sus características técnicas, la forma de cifrar y ocultar la información, su persistencia en el sistema, el modo de detenerlo, cómo desinfectarlo y, sobre todo, se desarrolló una vacuna con la que poder impedir que el virus se ejecutara. Así, en menos de 24 horas, el 14 de mayo, se contaba ya con una herramienta que impedía la ejecución del ransomware: CCN-CERT NoMoreCry; una aplicación desarrollada por el CERT Gubernamental Nacional y puesta a disposición de todas las entidades que así lo requieran y que continúa actualizándose en estos momentos.

Del mismo modo, el CCN-CERT ha publicado un Informe de Código Dañino (CCN-CERT ID 17-17 Ransom.WannaCry), en permanente actualización, que recoge todas las novedades que sus investigadores van recopilando. El informe pretende facilitar a todos los responsables de seguridad de una organización las principales pautas de actuación frente a este ciberataque. Desde las medidas preventivas, hasta las reactivas y de desinfección.

IMPACTO

- Más de 230.00 equipos infectados en un total de 179 países.
- Se han detectado 300 direcciones IP únicas infectadas al primer servidor en España, de acuerdo a la información compartida (EGC).
- **En España,**
  - Impacto en diferentes operadores de servicios esenciales (6).
  - Otros SIN CONFIRMAR
  - AAPP (2 CCAA. Impacto leve).



CCN-CERT:
12 Técnicos
10 operadores 1º
4 expertos externos

Conclusiones / Juicio Crítico

- **Mecanismo ALERTA funcionó**. AAPP y sector público actuaron todo el fin de semana.
  - Sistemas NO ACTUALIZADOS / Sistemas Operativos fuera de soporte.
  - Buena coordinación AGE (SGAD-CNPIC-MCCD) / CAAA (Menos con EELL)
  - Coordinación externa PARCIAL
  - Coordinación internacional **EGC / NCIRC-OTAN/ NCSC (UK)** / CERT-PT
  - Coordinación con empresas seguridad

- **HA FUNCIONADO EL ENS ?????**
- Canales de comunicación con SECTOR PRIVADO.
  - Se desconoce impacto real.
  - Descarga masiva de NoMoreCry.

- **Incrementar y ampliar las capacidades de vigilancia**. **MÁS POSIBILIDAD DE ACTUACIÓN ANTE ATAQUE EN CURSO (SOC AGE)**
  - **Mejorar el intercambio**.

4.3.5 Gestión de cambios [op.exp.5]

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se mantendrá un control continuo de cambios realizados en el sistema, de forma que:

a) Todos los cambios anunciados por el fabricante o proveedor serán analizados para determinar su conveniencia para ser incorporados, o no.
b) Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un equipo que no esté en producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario. El equipo de pruebas será equivalente al de producción en los aspectos que se comprueban.
c) Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados.
d) Mediante análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen una situación de riesgo de nivel alto serán aprobados explícitamente de forma previa a su implantación.

4.3.4 Mantenimiento [op.exp.4]

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas.
b) Se efectuará un seguimiento continuo de los anuncios de defectos.
c) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

RESULTADOS INES 2016 – PROCESOS CRÍTICOS

CCN-STIC 824

Procesos críticos	AGE	CC.AA.	EE.LL.	UNIV.	Global 2016	Global 2015
Proceso de Autorización (org.4)	50	80	50	42,5	**50**	**44**
Análisis de Riesgos (op.pl.1)	50	80	50	50	**50**	**46**
Gestión de derechos de acceso (op.acc.4)	75	80	75	52	**78,5**	**65**
Incidentes (op.ext.7)	62	80	50	67	**50**	**57**
Concienciación	50	61,8	35,8	45	**46,5**	**18**
Gestión de la configuración (op.exp.2 +op.exp.3)	60	70	50	50	**50**	**26**
Mantenimiento y Gestión de cambios (op.exp.4+op.exp.5)	58	79	50	50	**50**	**26**
Continuidad de operaciones (op.cont.1/2/3 y medios alternativos.9)	50	54	34,7	33,7	**40,1**	**3**

4.3.5 Gestión de cambios [op.exp.5]

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se mantendrá un control continuo de cambios realizados en el sistema, de forma que:

a) Todos los cambios anunciados por el fabricante o proveedor serán analizados para determinar su conveniencia para ser incorporados, o no.
b) Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un equipo que no esté en producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario. El equipo de pruebas será equivalente al de producción en los aspectos que se comprueban.
c) Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados.
d) Mediante análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen una situación de riesgo de nivel alto serán aprobados explícitamente de forma previa a su implantación.

Ciberseguridad. Decálogo

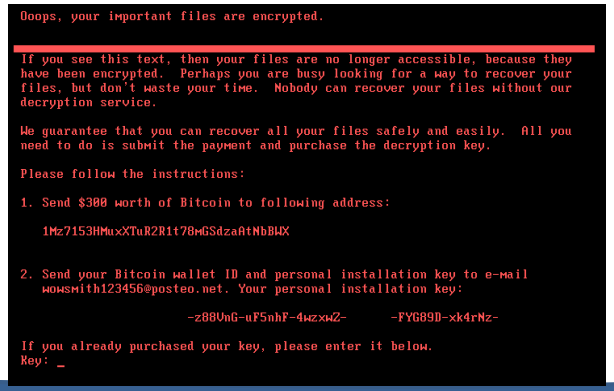
1. Aumentar la capacidad de Vigilancia.
2. Herramientas de Gestión Centralizada.
3. Política de seguridad.
4. **Aplicar configuraciones de seguridad y actualizaciones de seguridad.**
5. Empleo de productos confiables y certificados.
6. Concienciación de usuarios.
7. Compromiso de dirección (Aceptación Riesgo)
8. Legislación y Buenas Prácticas.
9. Intercambio de Información.
10. Trabajar como si se estuviera comprometido.

Petya

- Comenzó a propagarse en Ucrania el 27.06.2017, para poco después extenderse por todo el mundo.
- Contrariamente a WannaCry, Petya permanece en la red local y no intenta expandirse para infectar Internet.

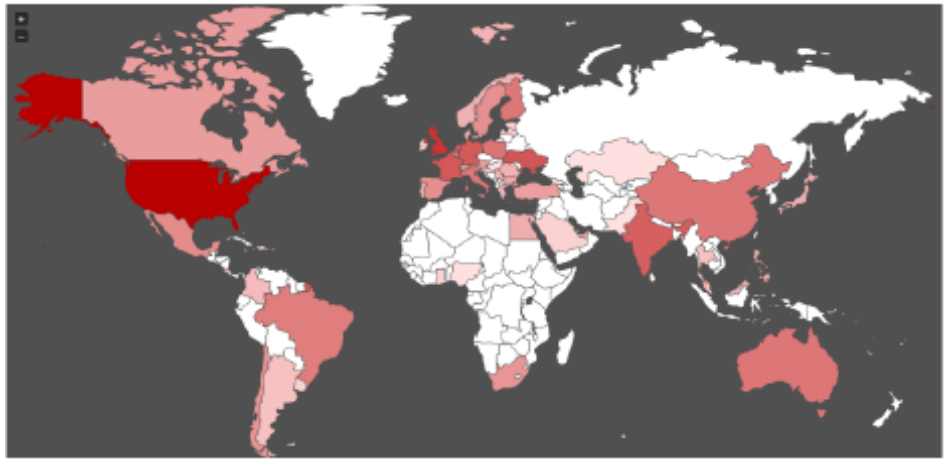
Petya

- Vector de ataque inicial basado en la explotación del **mecanismo de actualización de un software de contabilidad (M.E. Doc).**
- Los movimientos laterales constituyen el verdadero peligro vía "psexec" y "WMIC", de tal manera que máquinas parcheadas podían resultar infectadas.
- Petya no contiene ningún mecanismo de mando y control que se conozca.
- **Capacidades destructivas,** los sectores de arranque cifrados no pueden ser restaurados e incluso pueden ser borrados en su totalidad.
- La configuración de la parte de pago del malware sugiere que el rescate sólo se agregó como cobertura, no para ganar dinero (causar el mayor daño posible).
- La comunicación sobre los pagos mediante una única dirección de correo electrónico, retirada de inmediato por ISP (ningún medio para recuperar archivos).



Petya y su impacto

- No ha tenido impacto en el Sector Público español, a pesar de que se trata de un código dañino más sofisticado que en el caso de WannaCry.
- Se tiene constancia de que algunas filiales de empresas multinacionales radicadas en España han sido afectadas, siendo la más significativa la empresa danesa de transporte marítimo MAERSK.
- No solo cifra archivos del sistema sino que puede cifrar el disco duro completo del equipo afectado.
- Todo indica, que podría tratarse de un ataque de falsa bandera para ocultar las verdaderas pretensiones del agresor.



E-Mails

- ccn-cert@cni.es
- info@ccn-cert.cni.es
- **ccn@cni.es**
- Sat-inet@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- organismo.certificacion@cni.es

Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

Gracias

CCN Centro Criptológico Nacional