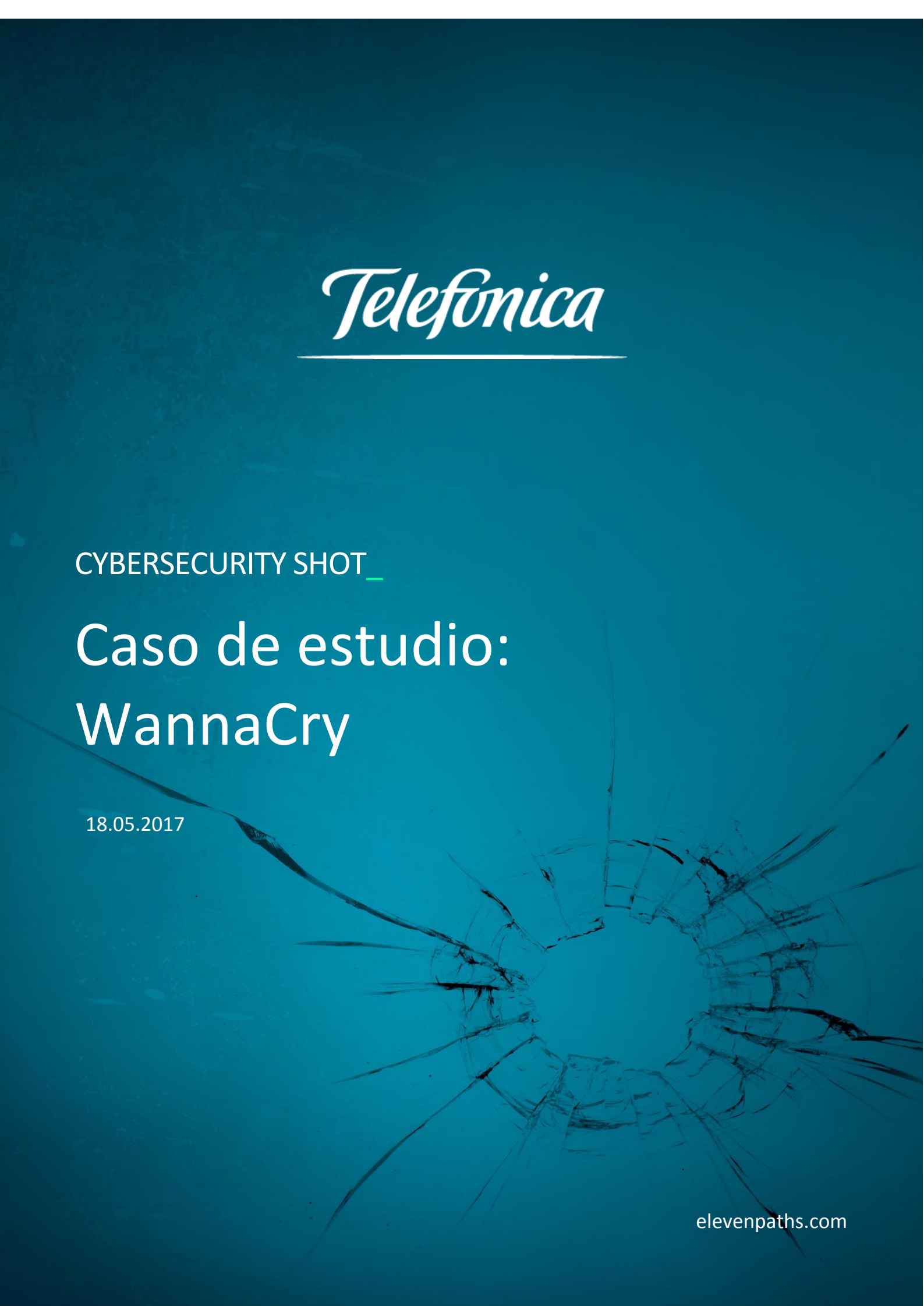
Telefónica

CYBERSECURITY SHOT_

Caso de estudio: WannaCry

18.05.2017



elevenpaths.com

Caso de estudio: WannaCry

El malware WannaCry inició una infección masiva el pasado 12 de mayo, habiendo llegado a más de 150 países. WannaCry es un malware de tipo ransomware que afecta a diferentes versiones de equipos Windows, en los cuales cifra la información de los equipos infectados y solicita un pago en Bitcoins por su "rescate".

El día 12 de mayo se desencadenó una infección a nivel global del malware WannaCry, de tipo Ransomware. Esta infección afectó a empresas y particulares de más de 150 países, incluyendo Estados Unidos, Reino Unido, Rusia, Taiwán, Francia, Japón o España, siendo dicho malware capaz de ejecutarse en 27 idiomas distintos. Solamente en la primera hora de propagación, infectó a más de 7000 PCs.

La última versión de esta variante de Ransomware, conocida como WannaCry, Wcry o Wanna Decrytor, pide un rescate de 0,1781 Bitcoins, lo que equivale a unos 300 dólares, a través de tres posibles cadenas de bitcoins. A la fecha de publicación de este informe, apenas ha recaudado más de 80.000 dólares.

Aunque WannaCry ha sido el último caso con repercusión mediática, lo cierto es que hay unos 2.000 casos de ransomware diarios, globalmente. Este malware es también famoso por explotar una vulnerabilidad de Windows que salió a la luz después de que la Agencia de Seguridad Nacional de EEUU (NSA) perdiera el control de su arsenal de ciberarmas.

Qué es el Ransomware

Un Ransomware es un malware, o dicho de otra forma, un software o programa informático malintencionado que restringe el acceso a determinados archivos o carpetas que ha infectado, algunos de ellos cifran los archivos del sistema operativo inutilizando el dispositivo.

El fin de estos programas malintencionados no es otro más que el conseguir dinero a corto plazo. El método de pago generalmente consiste en sistema de pago electrónico o por medio de Bitcoins lo que comúnmente se realiza a través de conexiones a la red de TOR. A pesar de realizar el pago exigido, nada asegura que la información será devuelta.

A fecha de publicación, aún se cuentan casi 520.000 hosts con sistema operativo Windows que son susceptibles de ser infectados por WannaCry, al tener el puerto 445 abierto.

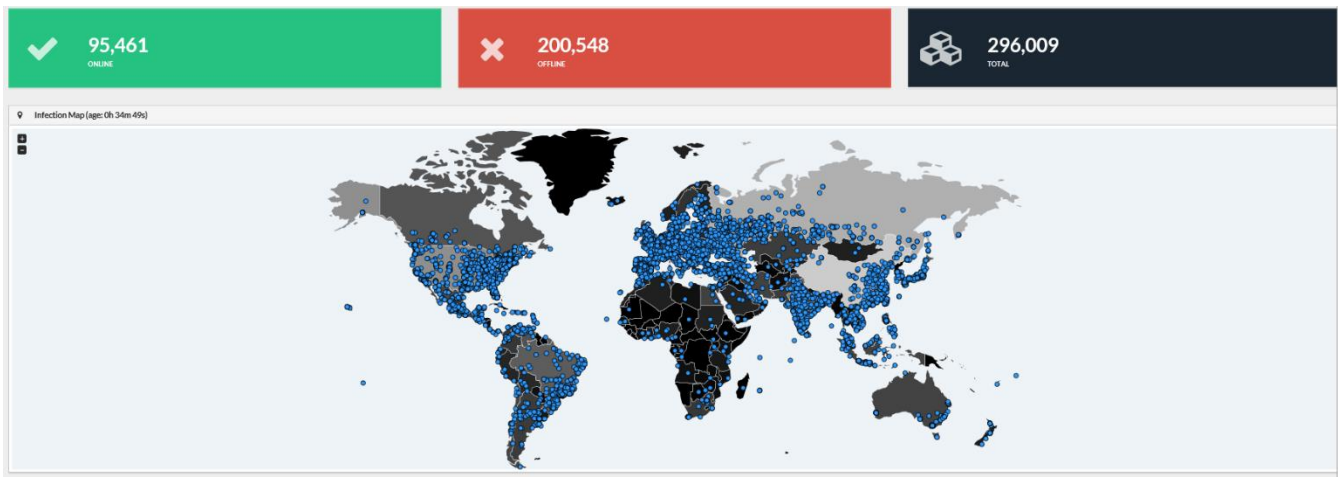


Ilustración 1: geografías afectadas por WannaCry

Acerca del malware WannaCry

El Ransomware WCRY o WannaCry es un malware no dirigido que se aprovecha de una vulnerabilidad de Microsoft Windows (MS17-10), conocida como *EternalBlue*, que afecta a diferentes versiones de Windows y se propaga exclusivamente por medio del puerto 445 (SMB). La diferencia de este Ransomware con otros es que utiliza los vectores de entrada más recientes divulgados por ShadowBrokers, el grupo de hackers que divulgaron exploits descubiertos y utilizados por la NSA y que siguen sacando a la luz más vulnerabilidades.

Aunque habitualmente esta clase de malware se suele distribuir a través correo electrónico o spear phishing, en este caso no se ha hallado ninguna evidencia de que haya sido así. Sólo se ha comprobado con certeza la distribución vía SMB. De manera irrefutable, no hay evidencias de propagación por RDP ni se ha evidenciado en el código del malware.

En el momento que el malware entra en equipo se ejecutan las siguientes acciones:

1. Propagarse por la red buscando otros equipos con aún vulnerables para ser explotados sin la necesidad de ejecutar ningún archivo por parte del usuario final. Para ello se realiza un descubrimiento de la red LAN en busca de equipos que presenten la vulnerabilidad de Windows antes mencionada con el fin de intentar explotar esta y así continuar con la propagación, así como a direcciones IP aleatorias de Internet.
2. El malware incluye dentro de sí mismo el payload del ransomware que se encargará del cifrado de los ficheros, sin necesidad de descargar nada del exterior. El proceso de cifrado comienza justo después de la infección, y en paralelo a la difusión y búsqueda de nuevas víctimas. Posteriormente, muestra una primera pantalla indicando que los ficheros están encriptados, para después mostrar una ventana de información en varios idiomas, donde se solicita pagar la suma de bitcoins para que el usuario pueda recuperar la información cifrada.

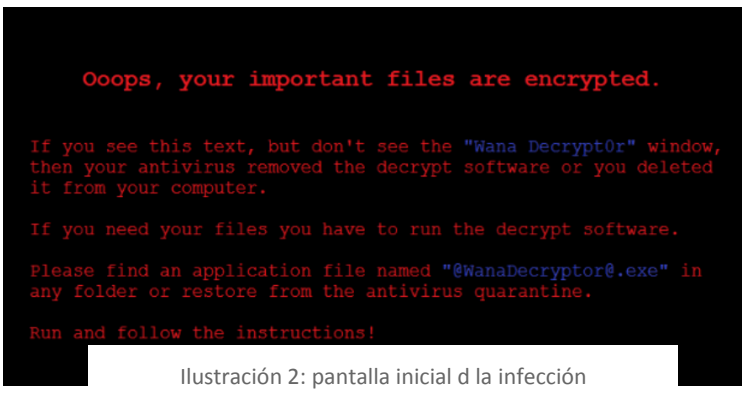


Ilustración 2: pantalla inicial d la infección

Ilustración 3: pantalla final de la infección

En la siguiente imagen se puede ver el ciclo completo de WannaCry:

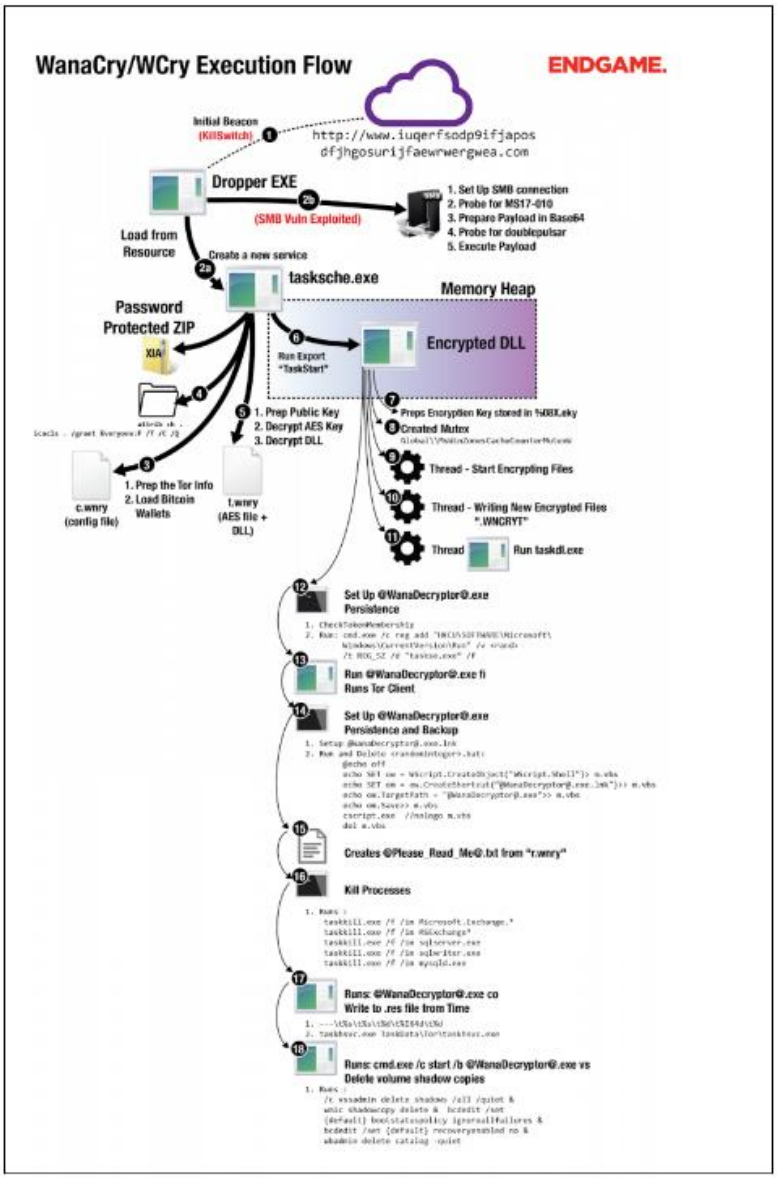


Ilustración 4: ciclo completo de WannaCry. Fuente: Endgame

En el código de WannaCry se identifican tres direcciones Bitcoin a las cuales se deben realizar el pago del rescate:

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

Cabe destacar, en primer lugar, este comportamiento peculiar respecto a otras familias de *ransomware*. Habitualmente cada afectado dispone de una dirección Bitcoin específica a la que realizar el pago, lo que además de facilitar su identificación cuando dicho pago se realiza, hace más complejo el rastreo de las transacciones (al existir cientos o miles de direcciones de entrada). En este caso, con sólo tres direcciones en la que todos los afectados envían pagos, los criminales necesitarán información adicional que les permita determinar qué víctima ha realizado el pago, y por qué importe (las víctimas podrán realizar varias transacciones hasta completar el importe reclamado). Se

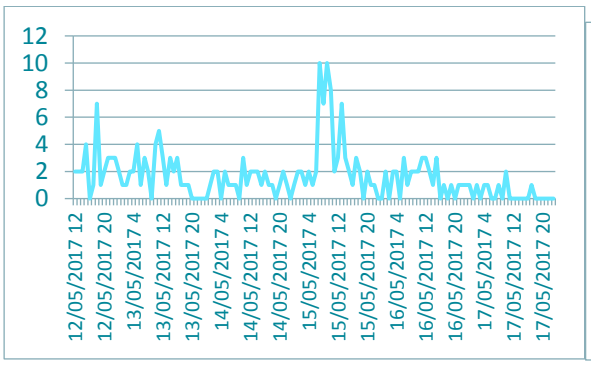
desconoce si, una vez realizado el pago, deben ponerse en contacto con los criminales para identificar las transacciones realizadas o las direcciones desde las que se generan (lo que hace más complejo el proceso para los responsables).

Las transacciones generadas en la red de Bitcoin son públicas, por lo que podemos analizar la distribución de los pagos en el tiempo, y el volumen obtenido por los criminales.

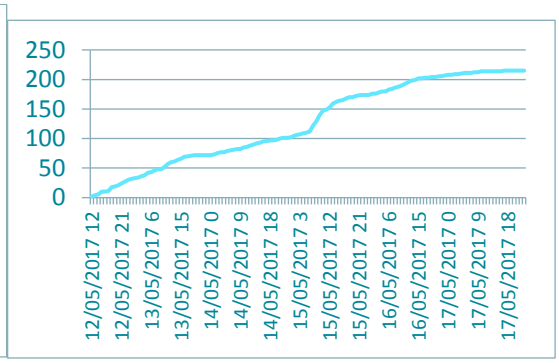
En el momento de redacción de este informe se han registrado un total de 290 transacciones, por un importe total de 44,3318544 bitcoins (al tipo de cambio en este momento, supone unos 80.000$, pues el valor de Bitcoin fluctúa de forma considerable, por lo que todos los importes serán aproximados). El primer pago se realizó el 12/5/2017 a las 12:04:11 (por un importe de 572$). Descartando las transacciones inferiores a 100$ para el análisis, existen 216 pagos con importes comprendidos entre 176$ y 3598$, con la siguiente distribución:

Importe	Num trans	% trans
> 700$	1	0,46%
400 - 700$	32	14,81%
100 - 300$	183	84,72%

Se ha realizado un pago anormalmente alto, 3.548$, el 13/5 a las 7:12:09. A priori no hay más información destacable en la transacción que permita obtener información adicional. Exceptuando este pago, el volumen restante es consistente con las instrucciones indicadas: se reclamaban 300$ con un período de pago de 3 días; una vez rebasado, el rescate se duplica (los pagos en torno a 600$ se registran, salvo algún caso puntual previo, a partir del día 15/5 a las 18h). Hay que recordar que una misma víctima podría fraccionar el pago en varias transacciones, originadas desde direcciones Bitcoin diferentes, con lo que no es posible realizar un análisis concluyente en base a los importes. En la siguiente gráfica se puede observar cómo se han distribuido los pagos en el tiempo:



Pagos registrados por hora



Pagos totales

Cabe destacar el pico producido el 15/5 entre las 7 y las 11 de la mañana (registrándose 35 pagos) y a las 13h del mismo día (10 transacciones). El volumen de transacciones decrece sensiblemente a partir del 16/5 (sólo 8 transacciones el día 17/5, con los datos analizados hasta las 22h).

No existe ninguna transacción de salida por el momento (es decir, los responsables no han tratado de mover el dinero obtenido en bitcoins). En base al comportamiento habitual en otras familias de ransomware (como Cryptolocker o Cryptowall) los criminales tratarán de aplicar estrategias de *mixing*, fraccionando las cantidades obtenidas entre miles de direcciones Bitcoin en sucesivas iteraciones, para acabar en una o varias direcciones que aglutinen los bitcoins obtenidos, desde la que poder hacer efectivo el importe en alguna de las casas de cambio existentes (asumiendo que el proceso de *mixing* hace imposible relacionar estas direcciones con el pago de rescates).

Una vez se inicie este proceso, será posible aplicar técnicas de Data Analytics sobre la información existente en la cadena de bloques de Bitcoin, incorporando información adicional para tratar de identificar las direcciones involucradas en el proceso con individuos o empresas (en el caso de que en el proceso se cometa algún error, utilizando

alguna de estas direcciones en foros, redes sociales, fuentes públicas de información, etc.). Además, en el caso de que del análisis de las transacciones que se generen durante el proceso de *mixing* se obtenga algún patrón, se podrían aplicar técnicas de Machine Learning para identificar todas las transacciones relacionadas con el movimiento de estos bitcoins, y determinar si dichas transacciones terminan en algún momento en direcciones conocidas de casas de cambio (en cuyo caso las autoridades podrían reclamar a dichas casas de cambio la identificación del cliente relacionado con la dirección en cuestión; muchas casas de cambio requieren el cumplimiento de las leyes AML/KYC, aunque otras no). Ninguna de estas estrategias garantiza obtener resultados. **Todas las direcciones IP de pago localizadas están ubicadas en la red TOR**.

Cómo infecta WannaCry

La infección en el equipo se produce mediante otra máquina infectada utilizando el exploit *Eternalblue* que afecta a todos los equipos Windows que no tengan instalado el parche MS17-010. El gusano se propaga **exclusivamente** por protocolo SMB (TCP/445). Los informes iniciales que indicaban que también se propagaba por RDP (escritorio remoto) no están confirmados. La secuencia de infección y propagación que se produce una vez ejecutado el virus inicial en el equipo de la víctima es la siguiente:

Una vez ejecutado el código dañino se realizan algunas acciones en el equipo de la víctima:

- Comprueba la existencia de un dominio en Internet (killswitch), si existe y puede conectar por el puerto 80, finaliza su ejecución.
- Crea un servicio en el sistema para conseguir persistencia del binario principal, que actuará como difusor.
- Crea copias de sí mismo en determinadas carpetas.
- Extrae de un fichero zip incluido dentro del binario original, del que extrae los ficheros correspondientes al ransomware que realizarán el cifrado de los ficheros.
- Crea una entrada en el registro de Windows para asegurar la persistencia del ransomware.
    - reg.exe reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "mzaiifkxcyb819" /t REG_SZ /d "\"C:\WINDOWS\tasksche.exe\"" /f
    - reg.exe add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v “RANDOM_CHARS” /t REG_SZ /d '\%COMMON_APPDATA%\tasksche.exe\" /f
- Crea numerosos hilos para distintas tareas.
- Detiene determinados procesos de programas de bases de datos o máquinas virtuales para poder cifrar sus archivos relacionados.
- Cifra todos los archivos encontrados que cumplan un patrón de extensión en todas las unidades que encuentre en el sistema comprometido.
- Procede a propagarse mediante dos caminos diferenciados:
    - Primero, escanea todas las IP de las redes accesibles desde todos los interfaces del equipo, como la red local, teniendo en cuenta máscara de red y buscando máquinas con puerto 445/TCP abierto. Cuando encuentra una máquina ejecuta exploit de *Eternalblue*, y si funciona instala el backdoor *Doublepulse* a través del cual copiara y ejecutara el virus en la víctima. Solo son vulnerables las máquinas que no tengan instalado el parche MS17-010.
    - Segundo, empieza a escanear direcciones IP públicas de internet, totalmente al azar, en busca de máquinas con puerto 445/TCP abierto. Cuando encuentra alguna, escanea toda la clase c (/24, 255 ip’s) en busca de más víctimas. Para cada una encontrada repite la secuencia de ataque de la red local.

Cómo se propaga WannaCry

A la hora de propagarse, el malware utiliza el exploit *Eternalblue* contra la vulnerabilidad descrita para propagarse hacia todas las máquinas que no tengan parcheada esta vulnerabilidad.

El exploit es utilizado para acceder a máquinas tanto en la red local como en Internet.

Para ello el malware crea dos hilos. La primera acción de esta función consiste en obtener la DLL "stub" que se usará para componer el payload que será enviado a las maquinas víctimas, a este "stub" se le añade el propio código dañino. Esta dll contiene una función llamada "PlayGame", que se encarga de extraer y ejecutar el recurso de la propia dll, que en este caso es el propio código dañino. De este modo cuando se produce la llamada a la función "PlayGame" se desencadena la infección de la máquina. Esta dll no toca el disco de la máquina, ya que se inyecta en el proceso "LSASS" tras la ejecución del exploit, aunque aún no está verificado si instala el backdoor Doublepulse (como el exploit original de la NSA) o no.

Propagación por red local: esta función tiene como objetivo obtener información del adaptador de red local y generar direcciones IP dentro de su rango de red. Posteriormente inicia el hilo encargado de realizar la explotación, enviando el "payload" que contiene el código dañino, que será inyectado en el sistema objetivo dentro del proceso "LSASS" mediante el uso del Exploit Eternalblue (MS17-010). El escaneo de la red local se realiza de forma consecutiva e incremental.

Propagación por Internet: dentro de la función encargada de la propagación hacia internet se encuentra el código empleado para la generación de rangos de IPs aleatorias. Una vez tiene generadas dichas IPs procede a lanzar el exploit.

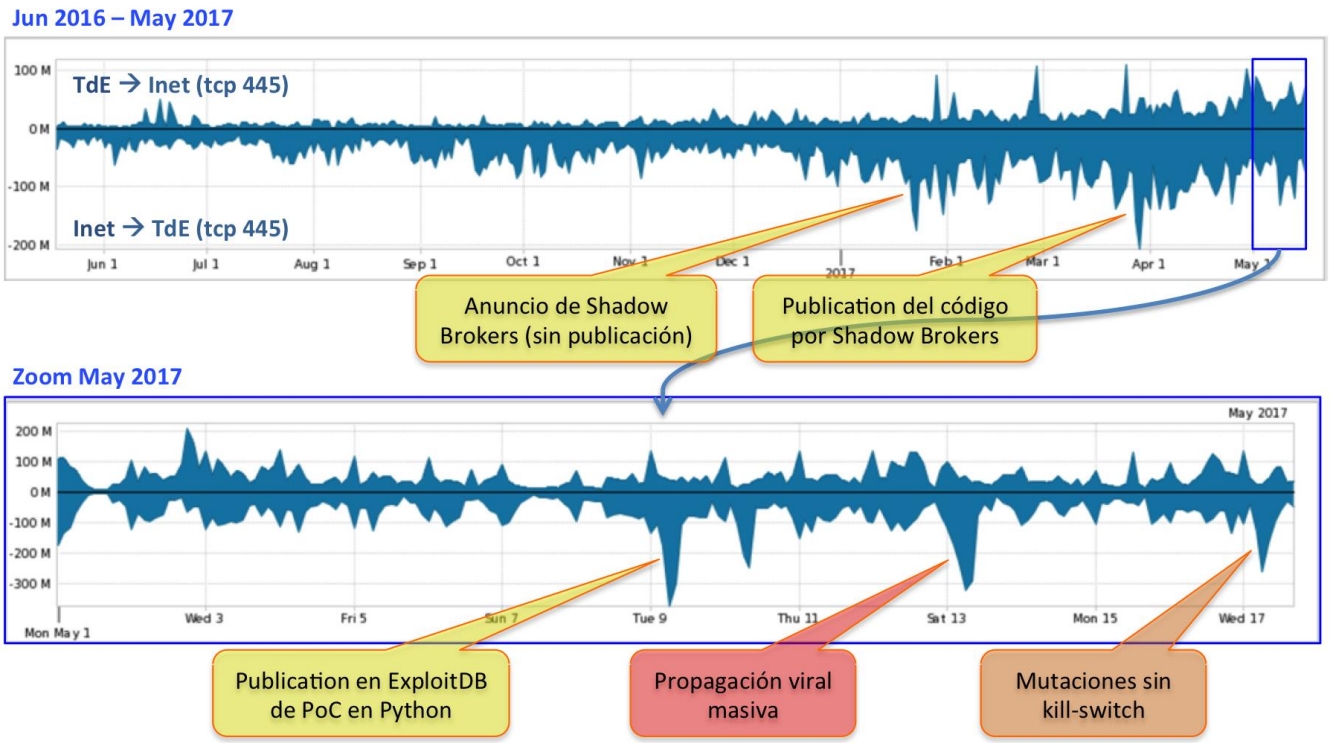
En las direcciones IP que genera para internet, cuando el primer octecto generado al azar es 127 o 224, los excluye y genera uno nuevo, para evitar las direcciones de loopback (localhost) que se vuelvan contra si mismo.

Cuando encuentra un equipo vulnerable en cualquier IP, escanea toda la clase C (/24) correspondiente a ese equipo. Dado que dentro de esos rangos al azar estaría también el rango 10.x.x.x, basta con que encuentre un PC 10.x.x.x.x al azar, para luego escanear todo ese subsegmento, infectando a segmentos de redes internas que no estén aislados a nivel de firewall entre ellas, aunque sean diferentes VLAN.

El método principal de propagación del malware a través de Internet se articula mediante intentos de conexión aleatorios a direcciones IPs públicas al puerto TCP 445.

Este puerto está vinculado al servicio SMB (Server Message Block) profusamente utilizado por los sistemas Microsoft Windows en diferentes usos, ninguno de los cuales aconseja su utilización a través de Internet. Pese a ello, siempre hay un determinado volumen de tráfico viajando por Internet, ya sean intentos de conexión, conexiones maliciosas o simplemente inadecuadamente implementadas.

En los datos estadísticos del tráfico por el puerto TCP 445 manejados por Telefónica en España, se aprecian incrementos significativos, coincidiendo con los diferentes anuncios y publicaciones relacionados con los mecanismos de explotación. En el detalle del mes de Mayo se hacen mucho más patentes.



Gráficas que muestran la actividad del puerto TCP 445 hacia/desde Internet.

Tanto en la propagación por Internet como por la red local acaba llamando a la función RUN_ETERNAL_BLUE, que será la encargada de enviar el exploit.

EternalBlue es el nombre que recibe un exploit supuestamente creado por la Agencia Nacional de Seguridad de EEUU, NSA. El código dañino utilizado en este caso es idéntico al original, pero sin la necesidad de usar otro exploit llamado "DoublePulsar", ya que sólo se inyecta en el proceso "LSASS". Al hacerse uso de un exploit con código de kernel (ring0) todas las operaciones realizadas por el código dañino disponen de los privilegios de SYSTEM. Esta vulnerabilidad, según Microsoft Security Bulletin, afecta a los siguientes sistemas operativos Microsoft:

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

Cómo cifra WannaCry

Antes de comenzar el cifrado del equipo, el código dañino verifica la existencia de dos mutex en el sistema. En caso de existir alguno de ellos no realiza cifrado:

- 'Global\MsWinZonesCacheCounterMutexA'
- 'Global\MsWinZonesCacheCounterMutexW'

El código dañino genera una clave única aleatoria por cada fichero cifrado. Esta clave, de 128bits y empleada con el algoritmo de cifrado AES, se almacena cifrada con una clave RSA pública en una cabecera personalizada que el código dañino añade en todos los ficheros cifrados. El descifrado de los archivos sólo es posible si se dispone de la clave privada RSA correspondiente a la clave pública empleada para cifrar la clave AES, que es la usada para cifrar los ficheros.

La clave aleatoria AES es generada con la función de Windows "CryptGenRandom", que no contiene debilidades conocidas, por lo que actualmente no es posible desarrollar ninguna herramienta para descifrar estos ficheros sin conocer la clave privada RSA utilizada.

El código dañino crea varios hilos y realiza el siguiente proceso para el cifrado de los documentos:

- Lee el fichero original y lo copia añadiéndole la extensión .wnryt
- Crea una clave AES de 128 bits aleatoria
- Cifra el fichero copiado utilizando el algoritmo AES
- Añade una cabecera con la clave AES cifrada con la clave pública RSA que lleva la muestra
- Sobrescribe el fichero original con la copia cifrada
- Finalmente renombra el fichero original con la extensión .wnry

Por cada directorio que el código dañino ha terminado de cifrar, genera los ficheros:

- @Please_Read_Me@.txt
- @WanaDecryptor@.exe

WannaCry cifrará archivos de 176 tipos de archivos diferentes, entre las que se encuentran:

- Extensiones de ofimática: ppt, doc, docx, xlsx, sxi.
- Formatos de oficina menos comunes: SXW, odt, hwp.
- Archivos multimedia: zip, rar, tar, bz2, mp4, mkv.
- Email: eml, msg, ost, pst, edb.
- Bases de datos: sql, accdb, mdb, dbf, odb, myd.
- Código de programación: php, java, cpp, pas, asm.
- Llaves de encriptación y certificados: key, pfx, pem, p12, csr, gpg, aes.
- Diseño gráfico: vsd, odg, raw, nef, svg, psd.
- Máquinas virtuales: vmx, vmdk, vdi.
- El código dañino puede presentar una serie de archivos en el sistema comprometido dependiendo de su estado de ejecución, a continuación, se listan los archivos que pueden existir:

<%COMMON_APPDATA%>

Nombre	Fecha de Creación	Tamaño Bytes	Hash SHA1
tasksche.exe	<varia>	3723264	e889544aff85ffaf8b0d0da705105dee7c97fe26
<varia>			
Nombre	**Fecha de Creación**	**Tamaño Bytes**	**Hash SHA1**
c.wnry	<varia>	780	f6b08523b1a836e2112875398ffefffde98ad3ca
s.wnry	<varia>	3038286	d1af27518d455d432b62d73c6a1497d032f6120e
b.wnry	<varia>	1440054	f19eceda82973239a1fdc5826bce7691e5dcb4fb
r.wnry	<varia>	864	c3a91c22b63f6fe709e7c29cafb29a2ee83e6ade t
t.wnry	<varia>	65816	7b10aaeee05e7a1efb43d9f837e9356ad55c07dd
u.wnry	<varia>	245760	45356a9dd616ed7161a3b9192e2f318d0ab5ad10
taskdl.exe	<varia>	20480	47a9ad4125b6bd7c55e4e7da251e23f089407b8f
taskse.exe	<varia>	20480	be5d6279874da315e3080b06083757aad9b32c23
<varia\msg>			
Nombre	**Fecha de Creación**	**Tamaño Bytes**	**Hash SHA1**
m_<idioma>.wnry	<varia>	<varia>	<varia>
<%WINDOWS%>			
Nombre	**Fecha de Creación**	**Tamaño Bytes**	**Hash SHA1**
tasksche.exe	<varia>	3723264	e889544aff85ffaf8b0d0da705105dee7c97fe26

Seguimiento del ataque

El Consejo Nacional de ciberseguriad da por controlado el virus: Reunido en la tarde de hoy en el Departamento de Seguridad Nacional, el Consejo Nacional de Ciberseguridad, ha dado por controlado la propagación del virus WannaCry.


mercadofinanciero europa press

El Consejo Nacional de Ciberseguridad da por controlado el virus WannaCry, pero no descarta más incidentes

Falsos descrifradores de WannaCry: actualmente no existe ninguna solución real que permita descifrar los archivos encriptados por Wannacrypt, a un ransomware es difícil realizarle ingeniería inversa y obtener el algoritmo utilizado para generar la clave de cifrado, pero como en cualquier caso de ransomware, aparecen actores que intentan sacar beneficios engañando a las víctimas, como los perfiles mencionados en el anterior informe que fueron detectados en Twitter.

Se ha detectado una web que facilita dos noticias en las que dejan disponible la descarga de herramientas de eliminación del Ransomware, una de ellas publicada hace 3 días[1] y [2].


"Oops, Your Files Have Been Encrypted!" – WannaCry Virus Removal Guide

Gergana Ivanova+ 3 hours ago Ransomware 33

Share Tweet Share Share

A pop up that starts with the phrase "**Oops, your files have been encrypted!**" displayed on your PC screen is a sign of **WannaCry ransomware virus** infection that is running on the machine. WannaCry virus targets vulnerable Windows systems all around the world aiming to encrypt sensitive data and extort victims for around $300 ransom payment. You can **remove WannaCry ransomware virus** via:

- **Our manual removal guide at bottom of the article, or**
- **A quality virus removal tool.**

Once WannaCry ransomware virus is removed successfully and the annoying "Oops your files have been encrypted" pop-up window associated with the threat is gone, you can try to **restore** your corrupted files following our instructions below.

DOWNLOAD WannaCry Removal Tool

SpyHunter anti-malware tool will diagnose all current threats on the computer. By purchasing the full version, you will be able to remove all malware threats instantly. Additional information about SpyHunter / Help to uninstall SpyHunter

[1] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-135-01

[2] https://www.us-cert.gov/ncas/alerts/TA17-132A

Microsoft se defiende responsabilizando a los administradores de TI: el presidente de Microsoft, Brad Smith, respondió a las críticas contra su compañía culpando públicamente del problema a las empresas que no mantenían los parches críticos de seguridad.

Los comentarios de Smith surgieron en respuesta a las críticas que habían culpado a Microsoft de dejar los sistemas vulnerables en primer lugar al no hacer lo suficiente antes para ayudar a los clientes y por poner fin a los parches de seguridad en sistemas operativos antiguos como Windows XP y Windows Server 2003. Muchas empresas, y una amplia gama de negocios, todavía se basan en sistemas que ejecutan sistemas operativos antiguos o sistemas operativos incorporados, dejándolos abiertos a los ataques de piratas informáticos y de malware.

Smith dijo que el ataque proporcionó pruebas gráficas sobre "el grado en que la seguridad cibernética se ha convertido en una responsabilidad compartida entre las empresas de tecnología y los clientes". La propagación y la interrupción de WannaCry "es un poderoso recordatorio de que los fundamentos de la tecnología de la información como mantener las computadoras actualizadas y parcheadas son una alta responsabilidad para todos, y es algo que todos los ejecutivos deben apoyar". Pero Smith no se detuvo allí. También criticó la manera en que las agencias gubernamentales han manejado revelaciones confidenciales de seguridad.

As WannaCrypt Recovery Continues, Analysts Back Microsoft's Leader

Todd R. Weiss — May 17, 2017

EMAIL SHARE Tweet G+1 COMMENTS 0

Microsoft president Brad Smith says the attacks were partly the fault of companies that don't patch their systems. Analysts agree.

UIWIX no es WannaCry: contrariamente a las noticias recientes citando a UIWIX como la nueva versión de WannaCry, un análisis en curso de TrendLabs indica que es una nueva familia que usa las mismas vulnerabilidades de SMB (MS17-010, con el nombre de *EternalBlue* tras su divulgación pública por ShadowBrokers) que WannaCry explota para infectar sistemas propagándose dentro de las redes y escaneando Internet para infectar más víctimas.

Según esta investigación Uiwix es diferente porque parece que no tiene archivos, es decir, UIWIX se ejecuta en memoria después de explotar *EternalBlue*. Las infecciones sin archivos no implican la escritura de archivos o componentes reales en los discos de la computadora, lo que reduce enormemente su huella y, a su vez, hace que la detección sea más complicada.

Ademas, UIWIX es también “stealthier”, optando por terminar si detecta la presencia de una máquina virtual (VM) o sandbox. Basado en las cadenas de código de UIWIX, parece tener rutinas capaces de recopilar el inicio de sesión del navegador infectado, el Protocolo de transferencia de archivos (FTP), el correo electrónico y las credenciales de mensajería.

	WannaCry	UIWIX
Attack Vectors	SMB vulnerabilities (MS17-010), TCP port 445	SMB vulnerabilities (MS17-010), TCP port 445
File Type	Executable (EXE)	Dynamic-link Library (DLL)
Appended extension	{original filename}.WNCRY	_{unique id}.UIWIX
Autostart and persistence mechanisms	Registry	None
Anti-VM, VM check, or anti-sandbox routines	None	Checks presence of VM and sandbox-related files or folders
Network activity	On the internet, scans for random IP addresses to check if it has an open port 445; connects to .onion site using Tor browser	Uses *mini-tor.dll* to connect to .onion site
Exceptions (doesn't execute if it detects certain system components)	None	Terminates itself if found running in Russia, Kazakhstan, and Belarus
Exclusions (directories or file types it doesn't encrypt)	Avoids encrypting files in certain directories	Avoids encrypting files in two directories, and files with certain strings in their file name
Network scanning and propagation	Yes (worm-like propagation)	No
Kill switch	Yes	No
Ransom amount	$300 paid in Bitcoins	$200 paid in Bitcoins

Adylkuzz usaba la misma vulnerabilidad SMB de Windows semanas antes que WannaCry: una publicación en Proofpoint informa que cientos de miles de ordenadores en todo el mundo han sido infectadas con un malware de minería de criptomoneda llamado "Adylkuzz".

Explica que también un grupo de ciberdelincuentes llevaba utilizando la misma vulnerabilidad de Windows SMB por al menos dos semanas antes del estallido de los ataques de ransomware de WannaCry. Según Kafeine, un investigador de seguridad de Proofpoint, este malware no instala ransomware ni notifica a las víctimas, por lo que esta campaña ha pasado desapercibida durante semanas. En su lugar, infecta silenciosamente las computadoras sin parchear con el malware "Monero", una criptomoneda parecida al Bitcoin (Un Monero está actualmente valorado en alrededor de US $ 26,77).

Las publicaciones añaden que el malware de Adylkuzz cierra los puertos SMB para evitar que se produzcan nuevas infecciones, y considera que esto puede también haber salvado indirectamente a cientos de miles de computadoras de ser hackeadas por el WannaCry ransomware.

Proofpoint cree que el ataque de Adylkuzz sigue creciendo y amenazando máquinas Windows y se teme que decenas de miles de computadoras en todo el mundo hayan sido infectadas por el malvare Adylkuzz.

Recopilación de los conponentes maliciosos de Wannacry: la firma de seguridad Cylance ha hecho una recopilación de los componentes del Ransomware Wannacry.

- Worm (Tambien conocido como mssecsvc.exe): es el Dropper de la primera etapa y es responsable del comportamiento de este ransomware. Tiene un tamaño de 3,6 MB (3723264 bytes) y contiene la URL "kill-switch" junto con el exploit de SMB para MS17-10. Contiene el Dropper de la segunda etapa con un recurso denominado 'R', Dado que el Dropper está en claro y no comprimido u obcecado, las detecciones basadas en secuencias hechas para el Dropper siempre afectarán al gusano, a menos que se añadan otras condiciones a esas reglas. La propagación trabaja aleatoriamente generando direcciones IP y tratando de conectar y luego explotar el sistema remoto. La carga útil se genera en la memoria y se entrega a través de la red a la memoria del proceso explotado. Una vez que la ejecución del código se pasa a la carga útil, su único propósito es colocar una copia del gusano en el disco y ejecutarla.
- Dropper (También conocido como tasksche.exe): es el Dropper de la segunda etapa. El archivo tiene un tamaño de 3.4MB (3514368 bytes), sin ningún mecanismo de conmutación o de propagación. Está configurado para funcionar como un servicio por el gusano o puede funcionar por sí mismo. Contiene un archivo protegido por contraseña en la sección de recursos del archivo que normalmente se llama XIA.
- Decryptor (También conocido como @WanaDecryptor@): presenta una interfaz gráfica de usuario para el usuario final y exige el pago. Si bien no es malintencionado, puede presentar un cuadro de diálogo de aspecto espeluznante si se hace doble clic. Este archivo es inofensivo sin los otros componentes de WannaCry, es decir, los archivos de idioma y el cliente Tor, y lo más importante, el ransomware.

- Ransomware (También conocido como wnry): este componente se presenta como un Dropper cifrado mientras este en el disco. El ransomware no puede hacer ningún daño mientras este en este estado y debe ser cargado y descifrado por el Dropper.

Cómo desinfectar WannaCry y qué medidas tomar

Para detectar si una máquina ha sido infectada se pueden comprobar los siguientes cambios o modificaciones en ficheros y registros de Windows:

- Verificar el registro de Windows:
  - HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run ;
  - Clave: [a-z]{12,14}[0-9]{3} = c:\windows\tasksche.exe
- Comprobar la existencia de los siguientes archivos en la máquina:
  - @Please_Read_Me@.txt
  - taskdl.exe
  - tasksche.exe
  - taskse.exe
  - @WanaDecryptor@.exe
  - @WanaDecryptor@.bmp
  - @WanaDecryptor@.exe.lnk
  - mssecsvc.exe

Para proteger el sistema del malware se deberán realizar los siguientes pasos:

- Parchear las máquinas para impedir la explotación de la vulnerabilidad de SMB. Para ello se deberá aplicar el parche de este enlace, o bien instalar el último parche acumulativo de Microsoft publicado el 9 de Mayo.
- Para aquellas máquinas que por algún motivo no puedan ser parcheadas, se recomienda la desactivación del protocolo SMB v1 en Windows, al menos en equipos Workstation. El protocolo SMBv1 solo es usado por Windows Xp y Windows 2003. De Windows 7 en adelante no necesitan el SMBv1.
- Se recomienda permitir el tráfico hacia los dominios que actúan como *killswitch*, tanto de la muestra original como de la múltiples variantes que han surgido en las horas y días siguientes:
  - iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
  - ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com
  - iuqerfsodp9ifjaposdfjhgosurijfaewrwergweb.com
  - iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com
  - ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com
- Si un equipo resuelve y puede conectar a estos dominios, el malware no se propaga por la red.
- De forma general también se debe permitir hacia las siguientes direcciones IP, a ser posible con conexión directa por puerto tcp/80 (ya que el malware no sabe usar configuraciones de proxy), a las que hasta ahora han resuelto alguna vez estos dominios.
  - 184.168.221.43
  - 144.217.254.3
  - 144.217.74.156
  - 54.153.0.145
  - 52.57.88.48
  - 52.170.89.193
  - 217.182.141.137
  - 217.182.172.139
  - 79.137.66.14
  - 144.217.74.156
  - 144.217.254.3
- Para que la propagación de WannaCry se mitigue dentro de la red interna y hacia redes externas, en aquellas redes en las que no existe posibilidad de dar salida directa (sin proxy) a las direcciones anteriores, es necesario implementar un servidor sinkhole mediante:
  - Resolver en servidores DNS INTERNOS los dominios anteriores hacia una ip accesible en la red interna.
  - Desplegar un servidor web, que responda en esa IP con una simple página estática de texto (por ejemplo, que indique “sinkhole”). Es necesario que el malware pueda establecer una conexión por puerto 80 y que conteste un servidor web. Si no se establece una conexión http el killswitch no funciona.
- El sinkhole lo que podría garantizar, mientras permanezca activo, es que siempre se resuelva, independientemente de si lo hace o no en internet. El sinkhole también podría proporcionar información sobre

la dimensión de la infección de este malware, almacenando en sus logs las direcciones IP's de los equipos afectados.
- Se deben bloquear las conexiones entrantes a puertos SMB (TCP/445) desde equipos externos a la red, y en la medida de lo posible entre distintos segmentos y redes internas.

Para la limpieza del sistema infectado, la forma más sencilla es mantener actualizado el antivirus, ya que actualmente es detectado por la totalidad de antivirus y antimalware. No obstante, donde no puedan ser usados, para una limpieza manual se pueden seguir los siguientes pasos:

- Eliminar el servicio con las siguientes características:
  - Nombre: mssecsvc2.0
  - Descripción: Microsoft Security Center (2.0) Service
  - Ruta: %WINDIR%\mssecsvc.exe
  - Comando: %s -m security
- Eliminar las entradas de registro:
  - reg.exe reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "mzaiifkxcyb819" /t REG_SZ /d "\"C:\WINDOWS\tasksche.exe\"" /f
  - reg.exe add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "RANDOM_CHARS" /t REG_SZ /d '\%COMMON_APPDATA%\tasksche.exe\'' /f
- Eliminar los siguientes archivos en cualquier carpeta del sistema:
  - @Please_Read_Me@.txt
  - @WanaDecryptor@.exe
- Eliminar todos los archivos existentes indicados en el apartado titulado "Listado de Archivos".

De forma alternativa a las anteriores, existen métodos para impedir la ejecución del malware en sistemas vulnerables no parcheados, que se basan en la desactivación del malware o bien usando sus propios mecanismos de detectar si ya ha infectado un sistema (mutex) o bien creando ficheros vacíos usados por el malware que consiguen que cuando el malware los intenta leer falle y se detenga el proceso por error.

Para la creación del mutex se puede usar la herramienta desarrollada por CCN-CERT llamada NoMoreCry. Para la creación de los ficheros vacios que hacen fallar al malware en su proceso de arranque, se puede usar la herramienta desarrollada por CCN-CERT llamada WannaCry Prevention.

Hemos detectado algunos perfiles en la red social Twitter relativos a la existencia de descrifradores de WannaCry:

- https://twitter.com/x0rz/status/864034802512646144
- https://twitter.com/malwrhunterteam/status/864073497517150209

A un ransomware es difícil realizar ingeniería inversa y obtener el algoritmo utilizado para generar la clave de cifrado. La información necesaria con el fin de descifrar la mayoría de estos ransomware ha sido publicada de forma gratuita por los creadores del propio ransomware. Para detectar que un descrifrador falso, se debe pedir principalmente una prueba de que funciona solicitando el descrifrado de un archivo. Actualmente no existe ninguna solución real que permita descifrar los archivos encriptados por Wannacrypt, que como en cualquier caso de ransomware, aparecen actores que intentan sacar beneficios engañando a las víctimas, como los perfiles mencionados anteriormente detectados en Twitter.

Tras realizar una búsqueda en GitHub se encuentran herramientas que podrían ser funcionales pero que requieren la clave privada de descifrado, que aún no se conoce.

Hemos observado que el ransomware tiene dos formas identificadas de llevar a cabo el proceso de cifrado. En ambas formas Wannacry utiliza una carpeta temporal para mover los archivos elegidos que el malware va a cifrar. Gracias a esto, hemos desarrollado un script para poder recuperar parte de los archivos afectados por el ransomware.

Buenas prácticas como medidas de prevención

Con la finalidad de minimizar la **propagación** de la infección se pueden acometer tanto medidas paliativas como definitivas.

La medida definitiva para evitar la propagación por red es la aplicación de los parches de seguridad recomendados por el fabricante Microsoft.

En aquellos casos en los que la aplicación de este parche no sea posible por razones de negocio o de compatibilidad con otras aplicaciones se pueden llevar a cabo otras medidas paliativas. Parar los servicios de SMB 1.0 evitan que el exploit sea efectivo en la infección por red.

Para evitar que el virus sea ejecutado en la víctima en caso de que se distribuya por otros medios (USB, correo electrónico, etc), son recomendables los controles de ejecución de código del propio sistema operativo, los antimalware y los antivirus actualizados.

Enfocándonos en la prevención y respuesta contra **ransomware** en general, se recomienda seguir las siguientes pautas de seguridad.

Realizar periódicamente copias de seguridad de todos los datos importantes según las estaciones de trabajos y/o servidores que considere en la compañía. Estas copias de seguridad no deben ser accesibles directamente desde el equipo de forma física (como, por ejemplo, discos duros externos USB) o mediante recursos compartidos de los sistemas, lo cual evidentemente ha sido una vía para la propagación de malware. En algunos casos, el ransomware tiene capacidad de navegar por las unidades del sistema, De esta forma si un USB conectado al sistema infectado se emplea para guardar copias de seguridad, corre el riesgo de ser infectado también.

Por otro lado, estas acciones dañinas afectarían también a aplicaciones de almacenamiento virtual, así como las que utilizan unidades de almacenamiento local. Desde Windows es posible programar copias de seguridad de forma sencilla desde la opción “Copias de Seguridad y Restauración” que se encuentran en el Panel de Control.

Algunas de las vulnerabilidades detectadas se producen a través de servicios de escritorio remoto. Servicios como RDP (TCP 3389) han sido constantemente utilizados últimamente para tratar de infectar equipos con ransomware. Los atacantes utilizan diversas herramientas y scripts con diccionarios de palabras para tratar de obtener credenciales válidas de usuarios. En el caso de necesitar exponer este tipo de servicios al exterior, la recomendación es hacerlo siempre desde una VPN cifrada.

Es importante destacar que existen vulnerabilidades que explotan Web Exploit Kits, así como archivos de ofimática dañinos que puedan llegar al equipo por medio de correo electrónico, redes sociales, etc. Se recomienda mantener el software correctamente actualizado.

Descargar Latch ARW, la solución anti Ransomware creada por 11Paths.

El navegador suele ser una vía de infección, donde versiones antiguas de Java, Flash o Adobe Acrobat suelen ser susceptibles de ataques de este tipo, adicionalmente a las de plataforma Windows. Debido a lo anterior se indican los parches de seguridad considerando esta vulnerabilidad:

Nombre	Vulnerabilidad	Parche
EternalBlue EternalSynergy EternalRomance EternalChampion	MS17-010	msft-cve-2017-0143 msft-cve-2017-0144 msft-cve-2017-0145 msft-cve-2017-0146 msft-cve-2017-0147 msft-cve-2017-0148
EmeraldThread	MS10-061	WINDOWS-HOTFIX-MS10-061
EducatedScholar	MS09-050	WINDOWS-HOTFIX-MS09-050
EclipsedWing	MS08-067	WINDOWS-HOTFIX-MS08-067

Detalle de Exploits utilizados por el malware para la explotación de las vulnerabilidades:

Nombre	Vulnerabilidad	Módulo Metasploit
EternalBlue	MS17-010	auxiliary/scanner/smb/smb_ms17_010
EmeraldThread	MS10-061	exploit/windows/smb/psexec
EternalChampion	MS17-010	auxiliary/scanner/smb/smb_ms17_010
EternalRomance	MS17-010	auxiliary/scanner/smb/smb_ms17_010
EducatedScholar	MS09-050	auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh, auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff, exploits/windows/smb/ms09_050_smb2_negotiate_func_index
EternalSynergy	MS17-010	auxiliary/scanner/smb/smb_ms17_010
EclipsedWing	MS08-067	auxiliary/scanner/smb/ms08_067_check exploits/windows/smb/ms08_067_netapi

Análisis de futuros riesgos

Existe una potencial aparición de nuevos malwares basados en los leaks publicados por ShadowBroker. A continuación, se muestran una serie de exploit para windows, linux y otros que se publicaron tras el robo a la NSA:

Operating System	Exploit Name	Description	Systems Affected	Used in Malware?	Patch Available?
Windows	**ETERNALBLUE**	SMBv2 exploit	Windows 7 SP1	Ransomware Wannacry	**MS17-010**
Windows	**CVE-2017-0290**	**The Microsoft Malware Protection Engine does not properly scan a specially crafted file leading to memory corruption**	Windows Defender Windows Intune Endpoint Protection Microsoft Security Essentials Microsoft System Center Endpoint Protection Microsoft Forefront Security for SharePoint Microsoft Endpoint ProtectionMicrosoft Forefront Endpoint Protection	No	**Micro Patch**
Windows	**ETERNALSYNERGY**	SMBv3 remote code execution flaw	Windows 8 Server 2012	No	**MS17-010**
Windows	**ERRATICGOPHER**	SMBv1 exploit targeting	Windows XP Server 2003	No	No
Windows	**EMERALDTHREAD**	Remote SMB exploit	Windows XP Server 2003	No	**MS10-061**
Windows	**EASYFUN**	EasyFun 2.2.0 Exploit	WDaemon IIS MDaemon WorldClient pre 9.5.6	No	**¿?**
Windows	**EXPLODINGCAN**	Exploit Buffer Overflow Vulnerability that creates a remote backdoor	IIS 6.0	No	No
Windows	**ETERNALROMANCE**	SMB1 exploit over TCP port 445 and gives SYSTEM privileges	Windows XP Windows 2003 Windows Vista Windows 7 Windows 8 Server 2008 Server 2008 R2	No	**MS17-010**
Windows	**EDUCATEDSCHOLAR**	SMB exploit	Windows Vista Windows Server 2008	No	**MS09-050**
Windows	**ETERNALCHAMPION**	SMBv1 exploit	Windows Vista SP2 Windows 7 SP1	No	**CVE-2017–0146**

Operating System	Exploit Name	Description	Systems Affected	Used in Malware?	Patch Available?
			Windows 8.1 Server 2008 Server 2008 R2 Server 2012 Server 2016 Windows 10		CVE-2017–0147
Windows	**ESKIMOROLL**	Kerberos exploit targeting domain controllers	Server 2000 Server 2003 Server 2008; Server 2008 R2	No	MS14–068
Windows	**ESTEEMAUDIT**	RDP exploit and backdoor	Windows XP Windows Server 2003	No	No
Windows	**ECLIPSEDWING**	RCE exploit forServer	Windows Server 2008 and later	No	MS08-067
Windows	**EXPIREDPAYCHECK**	IIS6 exploit	IIS6.0	No	¿?
Windows	**EAGERLEVER**	NBT/SMB exploit	Windows NT4.0 Windows 2000 Windows XP SP1 & SP2 Server 2003 SP1 & Base Release	No	¿?
Windows	**EASYFUN**	WordClient / IIS6.0 exploit	IIS6.0	No	¿?
Linux	**EARLYSHOVEL**	Sendmail 8.11.x exploit	RedHat 7.0 - 7.1	No	¿?
Linux	**ECHOWRECKER**	Remote Samba linux exploit	Samba 3.0.x	No	¿?

Otros Exploits también relevantes:

- EBBISLAND (EBBSHAVE) root RCE via RPC XDR overflow in Solaris 6, 7, 8, 9 & 10 (possibly newer) SPARC&x86.
- EASYBEE appears to be an MDaemon email server vulnerability
- EASYPI is an IBM Lotus Notes exploit that gets detected as Stuxnet
- 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
- 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

Acerca de ElevenPaths

En ElevenPaths, la unidad de Ciberseguridad de Telefónica, creemos en la idea de desafiar el estado actual de la seguridad, característica que debe estar siempre presente en la tecnología. Nos replanteamos continuamente la relación entre la seguridad y las personas con el objetivo de crear productos innovadores capaces de transformar el concepto de seguridad y de esta manera, ir un paso por delante de nuestros atacantes, cada vez más presentes en nuestra vida digital.

Más información

www.elevenpaths.com
@ElevenPaths
blog.elevenpaths.com