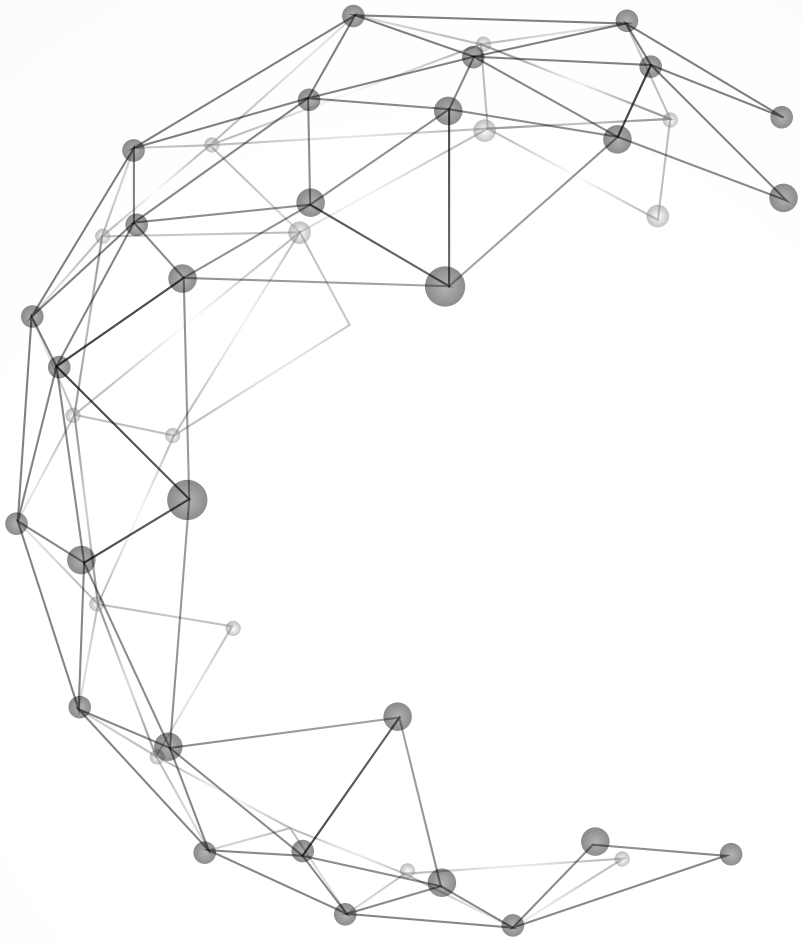
Informe
WannaCry



CERT DE SEGURIDAD E INDUSTRIA

INSTITUTO NACIONAL DE CIBERSEGURIDAD

CENTRO NACIONAL PARA LA PROTECIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

certsi_

www.certsi.es
www.incibe.es
www.cnpic.es

Mayo 2017

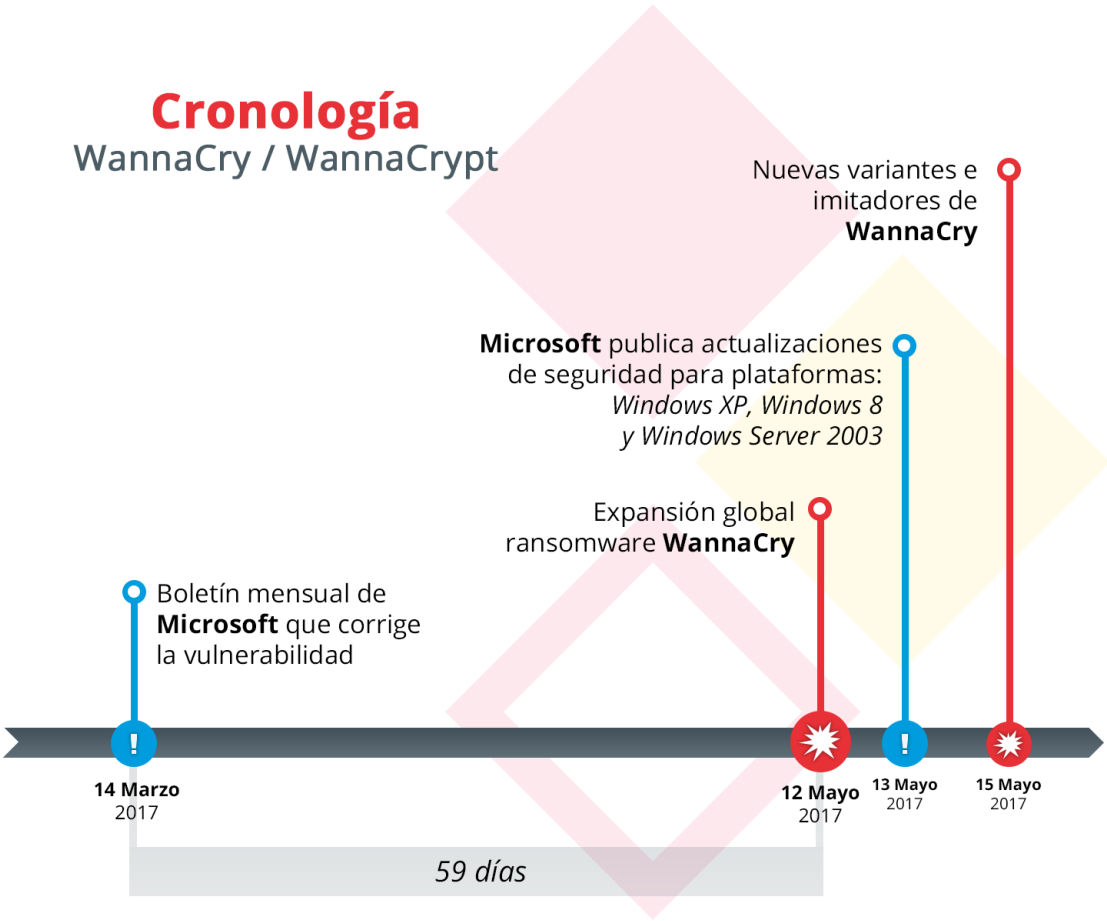
ÍNDICE

Contenido

1. RESUMEN EJECUTIVO

El día 12 de mayo se produjo una campaña de ransomware a nivel mundial. El aspecto novedoso de la campaña es que aprovecha una vulnerabilidad en el protocolo SMB v1, corregida por Microsoft en el boletín mensual que se publicó el 14 de marzo, para propagarse, utilizando para ello los puertos 445 (SMB). El 13 de mayo Microsoft desarrollo actualizaciones de seguridad para esta vulnerabilidad para las plataformas Windows XP, Windows 8 y Windows Server 2003 que están fuera de soporte y cuyo uso significa una alto riesgo.

El ransomware solicita el pago de 300$ para recuperar la información cifrada.



2. 2. INFORME TÉCNICO

- **Alias**: WannaCry, WannaCrypt, WanaCrypt0r, WCrypt, WCRY.
- **Tipo:** Ransomware.
- **Sistemas Operativos afectados:** Toda versión de Windows no parcheada para MS-17-010. Según informa Microsoft, Windows 10 no ha sido foco del ataque. Sin embargo, atendiendo al boletín de Microsoft todas las versiones de Windows 10 son vulnerables, excepto aquellas que hayan instalado el parche que corrige el fallo.
- **Fecha de aparición:** 12/05/2017
- **Vector de ataque:** Mediante el exploit conocido como DOUBLEPULSAR utilizando para ello la vulnerabilidad ETERNALBLUE.
- **Vector de propagación**: Microsoft Server Message Block 1.0 (SMBv1), como se recoge en el boletín MS-17-010 (ETERNALBLUE, publicado 14/03/2017). Dicho boletín recoge las siguientes vulnerabilidades:
  - Windows SMB Remote Code Execution Vulnerability – CVE-2017-0143
  - Windows SMB Remote Code Execution Vulnerability – CVE-2017-0144
  - Windows SMB Remote Code Execution Vulnerability – CVE-2017-0145
  - Windows SMB Remote Code Execution Vulnerability – CVE-2017-0146
  - Windows SMB Information Disclosure Vulnerability – CVE-2017-0147
  - Windows SMB Remote Code Execution Vulnerability – CVE-2017-0148
- **Idiomas**: Según diferentes análisis el mensaje de solicitud de pago que muestra el ransomware está disponible en 28 idiomas:
  - m_bulgarian
  - m_chinese (simplified)
  - m_chinese (traditional)
  - m_croatian
  - m_czech
  - m_danish
  - m_dutch
  - m_english
  - m_filipino
  - m_finnish
  - m_french
  - m_german
  - m_greek
  - m_indonesian
  - m_italian
  - m_japanese
  - m_korean
  - m_latvian
  - m_norwegian
  - m_polish
  - m_portuguese
  - m_romanian
  - m_russian
  - m_slovak
  - m_spanish
  - m_swedish
  - m_turkish
  - m_vietnamese

- **Listado de ficheros utilizados por el ransomware (los nombres varían ligeramente según la muestra analizada):**
  - b.wnry – Fondo de escritorio del ransomware.
  - c.wnry – Fichero de configuración que contiene las direcciones de los servidores C2, carteras bitcoin, etc.
  - r.wnry – Nota de rescate con las instrucciones de pago que muestra el ransomware.
  - s.wnry – Fichero comprimido que contiene el cliente de Tor.
  - t.wnry – El ransomware cifrado, el cual, puede ser descifrado con la contraseña privada que viene embebida en el código "WNcry@2ol7".
  - u.wnry – El fichero que descifra el ransomware.
  - Taskdl.exe – Elimina todos los ficheros temporables que se crean durante el proceso de cifrado (.WNCRYT).
  - Taskse.exe – Ejecuta cualquier programa en todas las sesiones de la máquina.
  - msg* – 28 ficheros de idioma

  Así mismo, durante la ejecución se crean los ficheros que se indican en el apartado «cifrado».
- **Listado de hashes descubiertos**: Existen más de 500 hashes relacionados con la campaña.

2.1. Funcionamiento

- El fichero instalador del malware dropea en un directorio con nombre aleatorio todos los ficheros listados en «Listado de ficheros utilizados por el ransomware», utilizando para ello la contraseña "WNcry@2ol7". Posteriormente, tras establecer permisos de ejecución totales sobre dicha carpeta, ejecuta varios ficheros y comprueba si un dominio en concreto está registrado o no. Dicho dominio funciona a modo de kill switch, por lo que en el caso de que no esté registrado continúa con el proceso de infección. Por el momento, se han identificado 6 dominios diferentes que han sido utilizados con este objetivo:
  - ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf[.]com
  - ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
  - iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
  - iuqerfsodp9ifjaposdfjhgosurijfaewrwergweb[.]com
  - iuqerssodp9ifjaposdfjhgosurijfaewrwergwea[.]com
  - iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

  Cabe destacar que también ha sido identificada una muestra del malware sin kill switch.
- A continuación se crea el servicio mssecsvc2 con el fin de establecer persistencia en el sistema comprometido. Así mismo, se crea una entrada en HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run con el mismo objetivo.
- Una vez establecida la persistencia se inician 2 tareas:
  - Se intenta establecer conexión con todos los equipos de la misma red local a través del puerto TCP 445 (SMB).
  - Se generan direcciones IP públicas aleatorias con el mismo objetivo.

En el caso de que se establezca conexión, se explota la vulnerabilidad SMB mediante el exploit conocido como DOUBLEPULSAR, el cual ejecuta el ransomware WANNACRY en el sistema afectado.

- A continuación se comprueban las unidades del sistema, removibles y mapeadas incluidas.
- Detiene varios procesos relacionados con bases de datos:
  - taskkill.exe /f /im mysqld.exe
  - taskkill.exe /f /im sqlwriter.exe
  - taskkill.exe /f /im sqlserver.exe
  - taskkill.exe /f /im MSExchange*
  - taskkill.exe /f /im Microsoft.Exchange.*
- Posteriormente, lista los ficheros de cada una de las unidades y cifra con una clave asimétrica RSA de 2048 bits todos aquellos que tengan alguna de las extensiones que se indican a continuación: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pst, .ost, .msg, .eml, .vsd, .vsdx, .txt, .csv, .rtf, .123, .wks, .wk1, .pdf, .dwg, .onetoc2, .snt, .jpeg, .jpg, .docb, .docm, .dot, .dotm, .dotx, .xlsm, .xlsb, .xlw, .xlt, .xlm, .xlc, .xltx, .xltm, .pptm, .pot, .pps, .ppsm, .ppsx, .ppam, .potx, .potm, .edb, .hwp, .602, .sxi, .sti, .sldx, .sldm, .sldm, .vdi, .vmdk, .vmx, .gpg, .aes, .ARC, .PAQ, .bz2, .tbk, .bak, .tar, .tgz, .gz, .7z, .rar, .zip, .backup, .iso, .vcd, .bmp, .png, .gif, .raw, .cgm, .tif, .tiff, .nef, .psd, .ai, .svg, .djvu, .m4u, .m3u, .mid, .wma, .flv, .3g2, .mkv, .3gp, .mp4, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .mp3, .sh, .class, .jar, .java, .rb, .asp, .php, .jsp, .brd, .sch, .dch, .dip, .pl, .vb, .vbs, .ps1, .bat, .cmd, .js, .asm, .h, .pas, .cpp, .c, .cs, .suo, .sln, .ldf, .mdf, .ibd, .myi, .myd, .frm, .odb, .dbf, .db, .mdb, .accdb, .sql, .sqlitedb, .sqlite3, .asc, .lay6, .lay, .mml, .sxm, .otg, .odg, .uop, .std, .sxd, .otp, .odp, .wb2, .slk, .dif, .stc, .sxc, .ots, .ods, .3dm, .max, .3ds, .uot, .stw, .sxw, .ott, .odt, .pem, .p12, .csr, .crt, .key, .pfx, .der
- Durante el proceso de cifrado, el malware crea un directorio “Tor” y dropea dentro el fichero tor.exe y 9 librerías que necesita para su funcionamiento. Las direcciones a las que se conecta se indican a continuación:
  - gx7ekbenv2riucmf.onion
  - 57g7spgrzlojinas.onion
  - xxlvbrloxvriy2c5.onion
  - 76jdd2ir2embyv47.onion
  - cwwnhwhlz52maqm7.onion
- Posteriormente, una vez que ha finalizado el proceso de cifrado, se ejecuta el fichero @wanadecryptor@.exe, el cual muestra la pantalla de secuestro:

- El fichero tor.exe se ejecuta con fin de establecer conexión a través de la red Tor para mantener el anonimato y permite establecer una pasarela de pago.
- Así mismo, el ransomware elimina las copias de seguridad (Shadow Copies) del sistema operativo e impide la ejecución del sistema en modo recuperación, utilizando para ello las herramientas del sistema: WMIC.exe, vssadmin.exe y cmd.exe.

2.1.1. Cifrado

- Cada infección genera un nuevo par de llaves RSA-2048.
- La clave pública se exporta como blob y se guarda en 00000000.pky
- La clave privada se cifra con la clave pública ransomware y se guarda como 00000000.eky
- Cada archivo se cifra usando AES-128-CBC, con una clave AES única por archivo.
- Cada clave AES se genera CryptGenRandom.
- La clave AES se cifra utilizando el par de claves RSA específico de la infección.

2.1.2. Bitcoin Wallets

A continuación se indican las carteras de bitcoin identificadas:

https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

2.1.3. Imitadores

En este tipo de casos es normal que surjan imitadores. En relación al WannaCry han surgido clones con un look&feel muy similar, si bien utilizan una funcionalidad parcial, diferentes paneles de control, diferentes carteras de bitcoin, etc.

A continuación se muestran algunos ejemplos:

SHA256

2ffd9ba7b5dbccf734da02498fa2a6af8caaf8b9f98d4b32bc226516eee5c832

b46c6addef8894d5079f592152481d259338175806eb9a983ddb8edb9ec5aa44

925b3acaa3252bf4d660eab22856fff155f3106c2fee7567711cb34374b499f3

cd7542f2d7f2285ab524a57bc04ae1ad9306a15b9efbf56ea7b002d99d4b974f

2.2. Prevención y mitigación

2.2.1. Prevención

Con el fin de prevenir que un equipo se vea afectado por el malware se deben realizar los siguientes pasos:

- Parchear la máquina si fuera vulnerable con el parche de Microsoft MS17-010 (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx)
- En el caso de que no sea posible actualizar el equipo, se recomienda deshabilitar SMBv.1.
- Realizar copias de seguridad.

2.2.2. Mitigación

En el caso de ya haberse visto comprometido al malware se deben realizar los siguientes pasos:

- Aislar todos los equipos de la red.
- Aislar la comunicación a los puertos 137 y 138 UDP y puertos 139 y 445 TCP.
- Parchear la máquina si fuera vulnerable con el parche de Microsoft MS17-010 (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx)
- En el caso de que no sea posible actualizar el equipo, se recomienda deshabilitar SMBv1 desde las «Características de Windows» en el «Panel de Control».
- Bloquear las conexiones salientes a través de los puertos 137,139, 445 y para evitar que se propague.
- Actualizar el fichero de firmas del antivirus instalado y pasarlo para eliminar el malware.
- En el caso de que se tengan copias de seguridad, se deben restaurar. En el caso de que no existan se recomienda contactar con el servicio antiransomware de INCIBE.


certsi_
CERT DE SEGURIDAD E INDUSTRIA