GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA

centro nacional de inteligencia
centro criptológico nacional

CCN-CERT
centro criptológico nacional

Balance del CCN-CERT del ataque de la familia Petya

El Sector Público y las empresas estratégicas españolas no se han visto afectadas por la última campaña masiva de ransomware

- **El código dañino utilizado, una variante de la familia Petya, es más sofisticado que en el caso de WannaCry y, en esta ocasión, podría tratarse de un ataque más dirigido.**

- **El correo electrónico y una actualización dañina de un programa comercial de ámbito financiero podrían ser los vectores de infección de este malware.**

Madrid, 28 de junio de 2017.- El CCN-CERT desea realizar un balance de la campaña de **ransomware** detectada ayer día 27 de junio de 2017. La campaña utiliza un posible variante englobada en la **familia Petya** (también llamado Petya, Petna, PetrWrap, Nyetya y NotPetya). Sus primeros casos se detectaron en empresas ubicadas en Ucrania y afectó posteriormente a algunas multinacionales con sede en España (el CERT Gubernamental Nacional no ha detectado ningún organismo del Sector Público o empresa estratégica española afectada).

El código dañino utilizado es **más sofisticado que en el caso de WannaCry** y, en esta ocasión, podría tratarse de un ataque más dirigido ya que la detección inicial del mismo fue localizada con una rápida expansión posterior. Además, da la sensación de que el agresor no parece pretender obtener un beneficio económico, sino perjudicar a las víctimas, ya que no ha adoptado las medidas habituales para conseguir el anonimato y la disponibilidad del servicio de cobro propia de otras campañas de cibercrimen.

En este sentido, el proveedor de servicio de Internet ha bloqueado la dirección de correo utilizada para el pago del rescate, por lo que las víctimas no pueden obtener las claves de recuperación al inhabilitar la vía de comunicación con el atacante.

Software objetivo y métodos de infección

Los sistemas operativos objetivo son los sistemas Windows y como hipótesis de vectores de infección se han planteado dos posibilidades (por confirmar):

•La primera consistiría en un correo electrónico de spear phishing con un fichero adjunto que explotaría la vulnerabilidad de Microsoft (**CVE-2017-0199**)

•La segunda opción podría ser a través una actualización dañina de un programa comercial destinada al ámbito financiero.

COMUNICADO CCN-CERT

28 de junio de 2017

Tras la infección inicial en un equipo, el código dañino intenta obtener privilegios y continúa con un reconocimiento de la red local en busca de otras máquinas para propagarse usando diferentes vías como:

•La ejecución remota con "psexec" a través de carpetas compartidas.

•La ejecución remota con "wmic", con extracción de credenciales mediante el uso de parte del código de "mimikatz" en el equipo inicialmente comprometido.

•La explotación de las vulnerabilidades asociadas a ETERNALBLUE (Microsoft MS 17-010), también usado por WannaCry para ejecutar código.

En las pruebas realizadas en sistemas Windows 10 con privilegios de administrador, el código dañino es detectado y bloqueado por Windows Defender.

Prevención (Vacuna)

Tal y como ha informado el investigador Amit Serper (0xAmint), para evitar la infección por una de las variantes conocidas existe la opción de crear en el equipo varios ficheros (con los nombres perfc.dat, perfc.dll y perfc) en la carpeta c:\Windows. De esta manera el binario interpreta que ya tiene la librería infectada y detiene el procedimiento de infección.

El investigador lo lanzó ayer en un Tweet: https://twitter.com/0xAmit/status/879764284020064256

Recomendaciones

- Aplicar los parches de seguridad existentes para MS Office y sistemas Windows.
- Mantener actualizados las aplicaciones Antivirus.
- Extremar las precauciones para evitar acceder a correos o enlaces no legítimos.
- Por otra parte, para evitar una de las vías de propagación, se puede inhabilitar el acceso a las carpetas compartidas con nombre Admin y Admin$ en la red local.
- Igualmente, se puede activar AppLocker para bloquear la ejecución de la herramienta PsExec de la suite de Microsoft Sysinternals.
- Además, se recomienda inhabilitar la ejecución remota de WMI.
- En el caso de la detección temprana de una infección, se recomienda apagar el ordenador lo más rápido posible y, si ya se hubiera iniciado la propagación a otros equipos, aislarlos en redes VLAN sin conectividad con otras redes.
- Realizar copias de seguridad.
- Aplicar las medidas de seguridad dispuestas en el informe del CCN-CERT contra el ransomware, en el que se incluyen pautas y recomendaciones generales y en el que se detallan los pasos del proceso de desinfección y las principales herramientas de recuperación de los archivos, en este tipo de ataques:

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2091-ccn-cert-bp-04-16-ransomware-1/file.html

En general, el CCN-CERT recuerda que efectuar el pago por el rescate del equipo no garantiza que los atacantes envíen la utilidad y/o contraseña de descifrado, sólo premia su campaña y les motiva a seguir distribuyendo masivamente este tipo de código dañino. En cualquier caso, en esta campaña se ha inhabilitado el medio de pago proporcionado por el atacante.

En el caso de que se hayan visto afectados por esta campaña y no dispongan de copias de seguridad, se recomienda conservar los ficheros que hubieran sido cifrados por la muestra de ransomware antes de desinfectar la máquina, ya que no es descartable que en un futuro apareciera una herramienta que permitiera descifrar los documentos que se hubieran visto afectados.

Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas del sector público**, a **empresas y organizaciones de interés estratégico** para el país y a cualquier sistema clasificado. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

MÁS INFORMACIÓN

CCN-CERT
eventos@ccn-cert.cni.es
+34 670 29 20 05
Síguenos en
www.ccn-cert.cni.es/