BOLETÍN DE ALERTA

Boletín Nro.: 2017-10
Fecha de publicación: 27/06/2017
Tema: Ransomware Petya y variantes
Fecha de actualización: 28/06/2017

Descripción:

Recientemente se ha observado un aumento significativo de los casos de infección de una variante de ransomware llamada Petya, que ha afectado a personas y empresas de varios países. Se trata de una nueva variante de una familia de ransomware conocida que, al igual que WannaCry, explota una vulnerabilidad de SMBv1.0 para propagarse por computadoras vulnerables de la red, infectando a una gran cantidad de víctimas en poco tiempo. De forma adicional, utiliza técnicas de robo de credenciales y/o reutilización de sesiones para propagarse, pudiendo afectar incluso a máquinas totalmente actualizadas, lo que lo hace más peligroso. Se ha reportado casos de Petya/PetrWrap que han afectado a numerosas personas, empresas y organizaciones de diversos sectores en varios países: bancos, industrias, instituciones gubernamentales, telecomunicaciones, entre otros.

¿Qué es el Ransomware?
Ransomware es un tipo de software malicioso (malware) que infecta un dispositivo y restringe el acceso al mismo, en la mayoría de los casos, encriptando documentos personales hasta que la víctima pague un "rescate" exigido por el malware para desencriptarlos.

¿Cómo se transmite?
El Ransomware se puede transmitir de diversas formas, siendo los vectores iniciales más frecuentes:

- Correos electrónicos con archivos adjuntos (.zip, .pdf, .docx, etc.) o con enlaces que redirigen a sitios de descarga del malware
- Sitios web o servicios de actualización legítimos que han sido infectados previamente
- Ataques de fuerza bruta a RDP
- Explotación de otros servicios expuestos a Internet.

En el caso particular de la campaña de distribución de Petya/PetrWrap se han reportado múltiples vectores iniciales, entre ellos, correos electrónicos con un enlace, sitios web comprometidos y un servicio de actualización de un software específico (M.E.Doc) comprometido, previamente.
Además, es posible que el ransomware se propage de forma lateral a otras máquinas de una misma red. En el caso de Petya, esta propagación se realiza a través de la explotación de vulnerabilidades y

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

otras técnicas como el robo de credenciales o reutilización de sesiones activas, pudiendo infectar tanto a máquinas vulnerables como actualizadas, de una misma red.

¿Cómo funciona Petya?

A diferencia de la mayoría de las familias de ransomware recientes, Petya cifra el MFT (Master File Table) del disco duro, dejando el MBR (Master Boot Record) inoperable, con lo cual impide el acceso al sistema y deja el disco duro inutilizable, ya que cifra la información sobre los nombres de archivos, tamaños y localización de los mismos en el disco duro. Además, Petya reemplaza el MBR con su propio código malicioso con la nota del rescate.

Cuando el ransomware infecta inicialmente el equipo, realiza varias acciones a modo de preparar el cifrado de los archivos, entre ellas el movimiento lateral a otras máquinas y la modificación del MBR, previo al reinicio. Recién luego de completar estas acciones, el ransomware fuerza el reinicio del ordenador, al menos 10 minutos después de su ejecución inicial (el tiempo es aleatorio). En este momento, nos mostrará un mensaje falso de CHKDSK. Durante esta fase, los archivos todavía no están cifrados, por lo que si la víctima reacciona a tiempo y apaga el equipo antes de que el ransomware finalice esta etapa, podrá recuperar los archivos, por ejemplo, arrancando el equipo con un LiveCD.

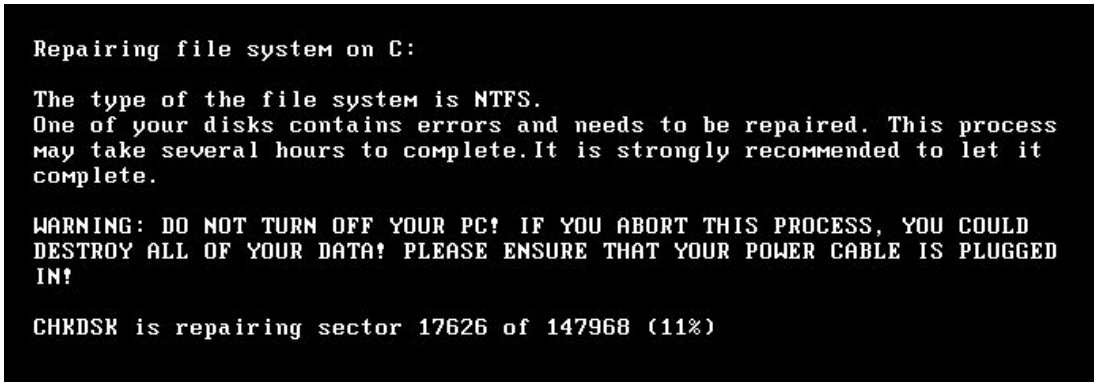

Figura 1: Falso mensaje de CHKDSK, previo al reinicio y cifrado de archivos

Luego de completar esta fase, sin embargo, los archivos y la MFT se encuentran cifrados, y se despliega la nota, en la que se exige un rescate de 300USD en Bitcoins y se indican las instrucciones específicas para el pago.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Figura 2: Nota de rescate de Petya/PetrWrap

El ransomware Petya, además, previo al reinicio, intenta propagarse de múltiples formas a otras máquinas de la red.

Otro detalle interesante es que Petya no necesita contactar con ningún servidor para el intercambio de claves. En cambio, Petya genera un ID de usuario único, el cual el usuario debe enviar manualmente por correo electrónico, luego del pago, de modo a que los cibercriminales, luego de verificar el pago, puedan realizar el proceso de desencripción.

¿Cómo ocurre la propagación?

En algunas ocasiones, el ransomware se mueve lateralmente a través de la red, afectando a otros equipos de la misma, ya sea aprovechándose de males configuraciones y/o controles débiles, o explotando vulnerabilidades de los sistemas.

El ransomware Petya, previo al reinicio, intenta propagarse de múltiples formas: explotando vulnerabilidades de SMBv1.0, a través del robo de credenciales y/o reutilización de sesiones activas, y mediante la trasferencia de archivos maliciosos a través de recursos compartidos de red. La infección de un solo equipo podría llegar a comprometer a toda la red corporativa, aun las máquinas actualizadas.

En el caso de esta variante de Petya, explota una vulnerabilidad de ejecución remota de código de SMBv1.0 (MS17-010), la misma que fue explotada por WannaCry y otros malwares recientes. De esta manera, puede propagarse rápidamente, afectando al resto de sistemas Windows conectados en esa misma red que no estén debidamente actualizados.

Además, utiliza técnicas de robo las credenciales de acceso de administrador, reutilización de credenciales cacheadas, reutilización de sesiones, entre otras, y con la ayuda de herramientas de

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

manejo del sistema como Windows PsExec y WMI (Windows Management Instrumentation), logra propagarse a otras máquinas de la red, incluso aquellas que se encuentran actualizadas.

¿Qué sistemas operativos afecta?

Petya y sus variantes afectan a equipos que cuentan con sistema operativo Windows, tanto aquellos actualizados, como no actualizados.

Sin embargo, es importante notar que las vulnerabilidades de SMB mencionadas se explotan con fines de propagación únicamente: una máquina no vulnerable igualmente podría ser afectada por el ransomware mediante los otros mecanismo.

Impacto:

El ransomware Petya utiliza estándares de encriptación robusta, la cual por el momento no es reversible, por lo tanto lleva a una pérdida total de toda la información del disco duro, entre ellos los archivos.

Esto genera enormes daños, entre ellos:

- Pérdida temporal o permanente de información confidencial o de propiedad;
- La interrupción de las operaciones regulares, principalmente en los negocios o empresas;
- Las pérdidas financieras contraídas para restaurar los sistemas y archivos; y
- Daño potencial a la reputación de una organización.

En el caso que se cuente con copias de seguridad actualizadas de los archivos y/o del sistema, el impacto puede ser significativamente menor. Se debe tener en cuenta que, como esta variante deja inutilizado todo el disco, en el caso de equipos que ejecutan sistemas críticos, la restauración del mismo puede demorar un tiempo significativo si es que no se cuenta con una copia de seguridad del disco completo.

Mitigación y Prevención:

Si se interrumpe la ejecución del ransomware en el momento en que se visualiza el falso mensaje de CHKDSK, los archivos no se cifrarán. Al ver la pantalla de la Figura 1, se debe apagar el equipo. Luego, se puede arrancarlo con un LiveCD o similar y de esta manera recuperar los archivos, copiandolos a otro dispositivo. Sin embargo, como en esta fase el MBR estará corrupto, se deberá reinstalar el sistema operativo para luego restaurar el sistema con los archivos que fueron copiados

Además, al detectar que una máquina ha sido afectada por el ransomware, se recomienda aislar la máquina de la red, para evitar la propagación. Sin embargo, como la propagación ocurre antes de la aparición de la nota de la Figura 1, el tiempo de reacción para ello es limitado. En caso de observar los primeros indicios, es fundamental estar atento a signos en las demás máquinas de la red, de modo a interrumpir la ejecución antes de que los archivos se cifren.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Hasta el momento no existen mecanismos para desencriptar los archivos sin la clave que está en poder de los atacantes, por lo que, en caso de haberse completado la fase de cifrado de archivos, éstos no podrán recuperarse. Sin embargo, en ocasiones, es posible que después de un tiempo se descubra una solución. Esto normalmente se puede dar de dos formas:

1. Se descubre una falla de seguridad en el propio ransomware, que puede ser explotada y permite recuperar los archivos
2. Una investigación del grupo criminal lleva a la recuperación de las claves de las víctimas.

Es posible que en un futuro se diera una de estas situaciones, encontrándose así una solución. Es por eso que se recomienda realizar una copia completa del disco encriptado, no formatearlo.
Por lo general, las herramientas que se ofrecen en Internet para desencriptar archivos encriptados por ransomware son en su mayoría software malicioso, por lo que al tratar de desencriptar los archivos, se corre un alto riesgo de quedar infectado con otro malware.

Es por esto que las acciones preventivas son fundamentales:

- No abrir nunca correos sospechosos, tanto si vienen de usuarios conocidos como desconocidos. Asegurarse siempre de que la persona que le ha enviado el correo realmente le quería remitir ese adjunto.
- Evitar abrir los archivos adjuntos sospechosos. Incluso los archivos aparentemente inofensivos, como los documentos de Microsoft Word o Excel, pueden contener un virus, por lo que es mejor ser precavido.
- No ingresar a enlaces dudosos que le son enviados a través de correo electrónico, servicios de mensajería, redes sociales, etc.
- Realizar copias de seguridad (backup) de toda la información crítica para limitar el impacto de la pérdida de datos o del sistema y para facilitar el proceso de recuperación. Idealmente, estos datos se debe mantener en un dispositivo independiente, y las copias de seguridad se deben almacenar offline.
- Contar con soluciones de antivirus/firewall y mantenerlo actualizado, de modo a prevenir la infección.
- Mantener su sistema operativo y el software siempre actualizado, con los últimos parches.
- No acceder nunca a ningún pago u acción exigida por el atacante.

Adicionalmente, se recomienda tomar medidas preventivas de modo a evitar la propagación del ransomware, las cuales incluyen:

- Actualizar los sistemas vulnerables o aplicar el parche publicado. Para los sistemas sin soporte o parche se recomienda aislar de la red y/o apagar y en lo posible, deshabilitar SMBv1.0.
- Controlar granularmente los recursos compartidos
- Evitar la compartición de credenciales entre equipos y aislar los equipos entre sí, en la medida de las posibilidades
- No iniciar sesión con usuarios administradores de equipos críticos en equipos menos protegidos.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Para variantes más antiguas de Petya existen herramientas para recuperar los archivos, las cuales se aprovechan de vulnerabilidades en el ransomware. Sin embargo, éstas no están presentes en las nuevas variantes. En caso de haber sido afectado por alguna de las variantes previas, puede seguir la siguiente guía: http://blog.segu-info.com.ar/2017/06/recuperar-los-archivos-de-petya.html

En caso de víctima de ransomware se recomienda realizar la denuncia a los organismos correspondientes; puede reportarlo al Centro de respuestas ante Incidentes Cibernéticos (CERT-PY).

Información adicional:

https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/
https://securelist.com/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/77762/
http://blog.segu-info.com.ar/2017/06/recuperar-los-archivos-de-petya.html
https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak/
https://www.adslzone.net/2017/06/27/wannacry-2-0-el-ransomware-petya-ataca-nuevas-empresas-de-espana-y-europa/
http://thehackernews.com/2017/06/petya-ransomware-attack.html

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py