# BOLETÍN DE ALERTA

**Boletín Nro.**: 2017-04
**Fecha de publicación**: 12/05/2017
**Tema**: Campaña de distribución del ransomware WannaCry

**Descripción**:

El día de hoy se ha observado una campaña de distribución de una variante de ransomware llamada WannaCry, que ha afectado a personas y empresas de varios países. Ha cobrado notoriedad debido a su rápida diseminación, alcanzando una gran cantidad de víctimas en pocas horas.

**¿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 una de las más frecuentes los correos electrónicos con archivos adjuntos (.zip, .pdf, .docx, etc.) o con enlaces que redirigen a sitios de descarga del malware, así como también sitios web legítimos que han sido infectados previamente. En el caso particular de la campaña de distribución de WannaCry todavía no se ha confirmado cual fue el vector utilizado por los cibercriminales, pero se sospecha que ha sido mediante correos electrónicos.
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. En el caso de WannaCry, explota una vulnerabilidad de ejecución remota de código a través de SambaB, pudiendo de esta manera propagarse, afectando al resto de sistemas Windows conectados en esa misma red que no estén debidamente actualizados. De esta manera, la infección de un solo equipo podría llegar a comprometer a toda la red corporativa. El análisis preliminar del código del ransomware indica que para explotar esta vulnerabilidad utiliza un exploit conocido como EternalBlue, publicada en abril por un grupo denominado Shadowbrokers.



**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

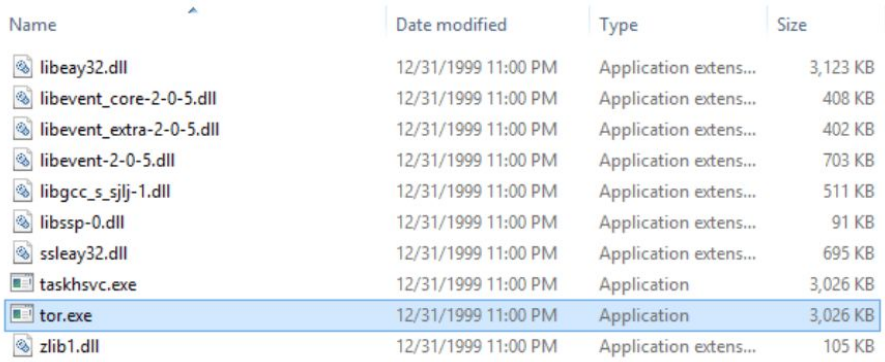
**¿Cómo funciona WannaCry?**

Al quedar infectado por WannaCry, el ransomware inmediatamente encripta y añade la extensión ".WCRY".

El ransomware encripta archivos con una gran cantidad de extensiones:

1. Extensiones de ofimática comunes y no comunes (.ppt, .doc, .docx, .xlsx, .sxi, .sxw, .odt, .hwp).
2. Archivadores y multimedia (.zip, .rar, .tar, .bz2, .mp4, .mkv)
3. Correos y bases de datos de correo (.eml, .msg, .ost, .pst, .edb).
4. Bases de datos (.sql, .accdb, .mdb, .dbf, .odb, .myd).
5. Códigos fuentes, proyectos y archivos relacionados a desarrollo (.php, .java, .cpp, .pas, .asm).
6. Certificados y claves (.key, .pfx, .pem, .p12, .csr, .gpg, .aes).
7. Archivos de diseño gráfico (.vsd, .odg, .raw, .nef, .svg, .psd).
8. Máquinas virtuales (.vmx, .vmdk, .vdi).

Para poder establecer comunicaciones con los servidores de comando y control, el ransomware extrae y utiliza un ejecutable del servicio TOR con las dependencias necesarias:



| Name | Date modified | Type | Size |
|---|---|---|---|
| libeay32.dll | 12/31/1999 11:00 PM | Application extens... | 3,123 KB |
| libevent_core-2-0-5.dll | 12/31/1999 11:00 PM | Application extens... | 408 KB |
| libevent_extra-2-0-5.dll | 12/31/1999 11:00 PM | Application extens... | 402 KB |
| libevent-2-0-5.dll | 12/31/1999 11:00 PM | Application extens... | 703 KB |
| libgcc_s_sjlj-1.dll | 12/31/1999 11:00 PM | Application extens... | 511 KB |
| libssp-0.dll | 12/31/1999 11:00 PM | Application extens... | 91 KB |
| ssleay32.dll | 12/31/1999 11:00 PM | Application extens... | 695 KB |
| taskhsvc.exe | 12/31/1999 11:00 PM | Application | 3,026 KB |
| tor.exe | 12/31/1999 11:00 PM | Application | 3,026 KB |
| zlib1.dll | 12/31/1999 11:00 PM | Application extens... | 105 KB |

Figura 1**:** Archivos adicionales para levantar el servicio TOR

Luego de encriptar todos los archivos, el ransomware se comunica con los servidores para enviar las claves y luego ejecuta un comando para borrar todas las instantáneas de recuperación (*Shadow Volume Copies*), de manera que no se pueden utilizar para restaurar los archivos de la víctima.

Al finalizar esto, el ransomware ejecuta una herramienta que despliega un mensaje de alerta en pantalla (ver Figura 2), indicando que los todos sus archivos se han cifrado y mostrando en pantalla las instrucciones para pagar el rescate y recuperar los archivos. Incluye instrucciones en varios idiomas



**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: Mensaje de alerta desplegado por WannaCry

Además, el ransomware establece un mensaje de alerta como fondo de pantalla.

El pago exigido es en bitcoins, en algunas variantes se exige 0.16 BTC, equivalente a 300 USD aproximadamente, y en otras variantes se exige 0.32 BTC (600 USD). Para proceder al pago, la herramienta tiene un botón “Decrypt” que dirige a la víctima a una página de pagos btcfrog, en la que se observa un código QR que enlace a la dirección de la billetera de bitcoins.



**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 3: Página con la dirección de la billetera Bitcoin

El ransomware, además, intenta explotar una vulnerabilidad crítica de ejecución remota de código que afecta a SMB de modo a propagarse en las máquinas de la misma red que sean vulnerables. Se trata de una vulnerabilidad conocida, para la cual Microsoft ha publicado un parche el 14 de marzo (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx), incluso antes de que sea publicado el exploit EternalBlue.

**¿Qué sistemas operativos afecta?**

WannaCry afecta a equipos que cuentan con sistema operativo Windows. Los sistemas más expuestos son aquellos que están afectados por la vulnerabilidad mencionada:

- 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

Sin embargo, es importante notar que dicha vulnerabilidad se explota con fines de propagación únicamente: una máquina no vulnerable igualmente podría ser afectada por el ransomware mediante otro mecanismo.



**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

**Impacto**:
El ransomware WannaCry encripta los archivos usando estándares de encriptación robusta (probablemente RSA + AES-128), la cual por el momento no es reversible, por lo tanto lleva a una pérdida de 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, el impacto puede ser significativamente menor.

**Mitigación y Prevención:**
Hasta el momento no existen mecanismos para desencriptar los archivos sin la clave que está en poder de los atacantes. 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 guardar los archivos encriptados, no eliminarlos.
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.



**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

- 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 mediante de la vulnerabilidad de SMB, 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.
- Actualizar y/o incluir firmas en su antivirus e IDS.
- Controlar y/o aislar la comunicación a los puertos 137 y 138 UDP y puertos 139 y 445 TCP en las redes de las organizaciones.
- Descubrir qué sistemas, dentro de su red, pueden ser susceptibles de ser atacados a través de la vulnerabilidad mencionada, en cuyo caso, puedan ser aislados, actualizados y/o apagados. Para ello, puede seguir la siguiente guía: https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_ms17_010

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://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/
https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_ms17_010



**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