BOLETÍN DE ALERTA

Boletín Nro.: 2016-10
Fecha de publicación: 12/08/2016
Tema: Campaña de distribución del ransomware Zepto en el país

Descripción:

En los últimos días se ha observado una campaña de distribución de una variante de ransomware llamada Zepto, a través de correos electrónicos maliciosos, que está afectando mayormente a nuestro país. Se trata de una variante del ransomware Locky, cuya proliferación se observó en el país en el mes de marzo. El correo electrónico es entregado a la víctima, aprovechándose de servidores de correo con una configuración poco segura, simulando un remitente de confianza.

¿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?
Si bien, el Ransomware se puede transmitir de diversas formas, en este caso hemos observado una campaña de distribución específica a través de correo electrónico, utilizando servidores de correo con una configuración poco segura, los cuales permiten enviar correos falsos a los usuarios locales, de forma no autenticada.
En la mayoría de los software de correo, por defecto, cuando se establece una conexión SMTP con el servidor de correo y se declara un remitente local, aunque fuera falsificado, el correo podrá ser enviado a los usuarios locales, sin requerir autenticación. Esto permite a un atacante enviar correos maliciosos, simulando un remitente de confianza del propio dominio. Por ejemplo, un usuario victima@dominio.com recibe un correo falsificado desde confiable@dominio.com. Tratándose de un supuesto usuario del propio dominio, la víctima tendrá una mayor confianza. Además, en algunas configuraciones, el filtro antispam no analiza estos correos, por ser entregados de forma local.
En esta campaña de distribución de ransomware, se observó que los delincuentes utilizaron esta configuración para enviar correo maliciosos que contienen un archivo adjunto en formato **.docm** (documento de Microsoft Word con Macros). Al ser abierto, se ejecuta el macro y se descarga 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

ejecuta automáticamente el ransomware Zepto. La máquina queda infectada y los archivos que se encuentran en dicha máquina, así como los recursos compartidos, quedan automáticamente encriptados.
Se ha observado que esta campaña de correo está siendo enviada a principalmente a funcionarios de instituciones gubernamentales.

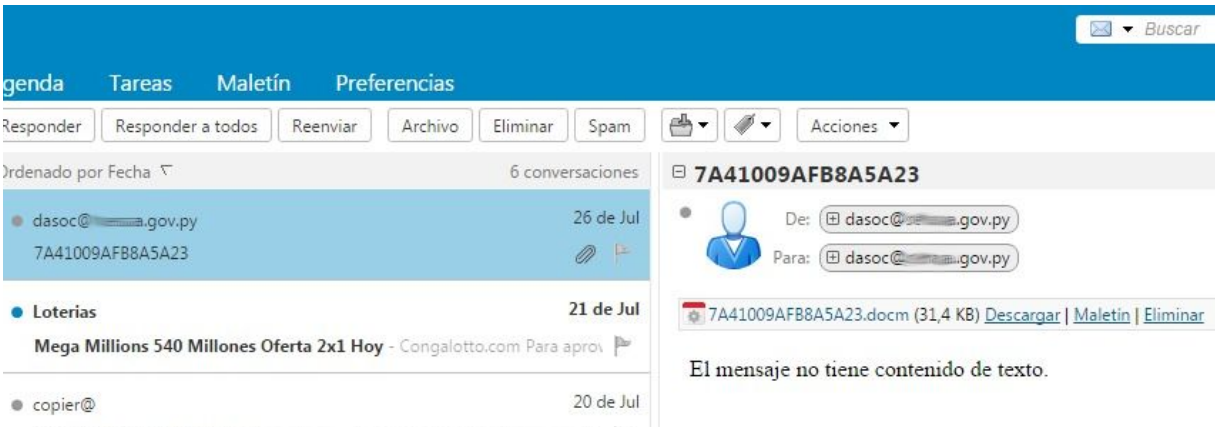

Figura 1: Correo de distribución del downloader de Locky/Zepto

¿Cómo funciona Locky/Zepto?

Cuando se instala el ransomware Zepto, éste crea un ejecutable de nombre aleatorio en el directorio %AppData% o %LocalAppData% , el cual se ejecuta y escanea todas las unidades del equipo, para encriptar los archivos, incluido las unidades compartidas en la red.
El ransomware inmediatamente encripta y renombra todos los archivos y le agrega la extensión .zepto. Al igual que su primera variante Locky, Zepto encripta casi cualquier tipo de archivo: imágenes .JPG, .PNG o .GIF, bases de datos como .DB, .ODB, .MDB, .SQLITEDB o .DBF , videos como .MP4, .MOV o .FLV, proyectos de programación como .JS, .VBS o .JAVA, comprimidos como .ZIP y muchos más. Además, puede cifrar los archivos de aquellos directorios compartidos en red a los que el equipo tiene acceso, afectando así a un amplio número de usuarios.
Luego de encriptar todos los archivos, el ransomware se elimina a sí mismo del equipo infectado y despliega una alerta en pantalla (ver Figura 2), alertando que los todos sus archivos se han cifrado y mostrando en pantalla las instrucciones para pagar el rescate y recuperar los archivos. Esta nota de rescate, en formato .txt y .html (_HELP_instructions.html and _HELP_instructions.txt) son copiadas en cada directorio de la máquina infectada.

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 Zepto

Para proceder al pago, se indican unas URLs de la red TOR en pantalla, con instrucciones específicas para la víctima infectada. El rescate exigido es 0.5 Bitcoins, aproximadamente 300 US$ (ver Figura 3). Zepto también intenta borrar todas las instantáneas de recuperación (*Shadow Volume Copies*) en la máquina infectada, de manera que no se pueden utilizar para restaurar los archivos de la víctima.

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

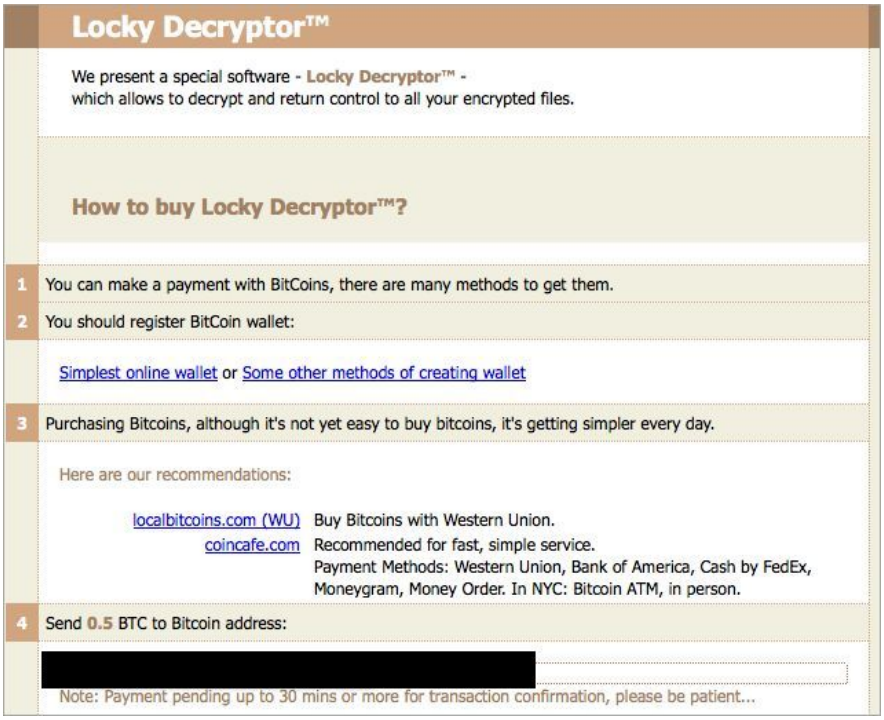

Figura 3: Instrucciones específicas para el pago

¿Qué sistemas operativos afecta?

Zepto afecta a equipos que cuentan con sistema operativo MS Windows ®.

Impacto:

El ransomware Zepto encripta los archivos usando estándares de encriptación aún más robusta que Locky, RSA-2048 + AES-256 en modo ECB, la cual 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.

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

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.
- 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.

Además, habiéndose identificado que estos correos maliciosos son enviados explotando una configuración débil de muchos servidores de correo, se recomienda corregir esta configuración, de modo a evitar que correos falsificados del propio dominio puedan ser enviados a los usuarios locales.

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

En Zimbra, se puede seguir las siguientes guías:

- https://www.jorgedelacruz.es/2014/04/03/zimbra-seguridad-i-parte/
- https://www.jorgedelacruz.es/2014/09/08/zimbra-seguridad-ii-parte-enforcing-a-match-between-from-address-and-sasl-username-en-zimbra-8-5/
- https://www.jorgedelacruz.es/2015/07/21/zimbra-seguridad-iii-parte/

En Exchange:

- http://markgossa.blogspot.com/2016/01/block-spoofed-email-exchange-2010-2013-2016-part1.html
- https://technet.microsoft.com/en-us/library/bb397214(v=exchg.160).aspx

Las instrucciones específicas podrán variar dependiendo de la configuración de su servidor, así como de la versión. Además, es importante contar con software antivirus y antispam en su servidor de correo, y asegurarse de que los mismos tengan activados SPF (*Sender Policy Framework*).

En caso de recibir un correo electrónico con las características mencionadas en este boletín, recomendamos no abrirlo y dar aviso a un responsable de su organización.
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:
http://www.malwarerid.com/malwares/zepto-ransomware
https://nakedsecurity.sophos.com/es/2016/07/05/is-zepto-ransomware-the-new-locky/
http://soft2secure.com/knowledgebase/docm-file-virus

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