BOLETÍN DE ALERTA

Boletín Nro.: 2016-06
Fecha de publicación: 17/03/2016
Tema: Campaña de distribución del ransomware Locky en el país

Descripción:

En los últimos días se ha observado una campaña de distribución de una variante de ransomware llamada Locky, a través de correos electrónicos maliciosos, que está afectando mayormente a nuestro país. Se trata de una nueva variante de ransomware, probablemente relacionada a la botnet Dridex.

¿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, hemos observado una campaña de distribución específica a través de correo electrónico. Los correos electrónicos contienen un archivo adjunto comprimido .zip, con diferentes nombres, por ejemplo: Info.zip, Document9.zip, etc. Estos archivos adjuntos contienen un archivo javascript que al ser abiertos se ejecutan de forma automática y descargan, ejecutan e instalan el ransomware Locky.
Una vez que se abrió el archivo adjunto, la máquina queda infectada por Locky y los archivos que se encuentran en dicha máquina quedan automáticamente encriptados.
Se ha observado que esta campaña de correo está siendo enviada a ciudadanos paraguayos de diversas industrias: gobierno, educativo, empresas de tecnología, PYMES, 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

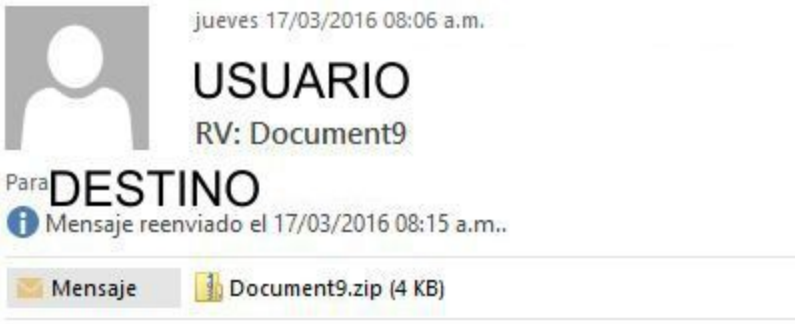

Figura 1: Correo de distribución del downloader de Locky

¿Cómo funciona Locky?

Al quedar infectado por Locky, el ransomware inmediatamente encripta y renombra todos los archivos y le agrega la extensión .locky. El nombre de los archivos tiene el siguiente formato: *{USERID}{random_hash}*, donde USERID es un valor único para cada víctima, y el random_hash es una cadena pseudo-aleatoria que se genera para cada archivos.

A diferencia de otros ransomware que solo encriptan los tipos de archivos más conocidos, Locky se caracteriza por encriptar 164 tipos de archivo, pudiendo afectar a prácticamente cualquier archivo de la computadora: 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. También puede cifrar los archivos de aquellos directorios compartidos en red a los que el equipo tiene acceso.

Luego de encriptar todos los archivos, el ransomware se elimina a sí mismo del equipo infectado.

Al finalizar esto, el ransomware 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. Además, el ransomware establece la nota de rescate como fondo de pantalla.

Esta nota de rescate, en formato .txt y .bmp (_Locky_recover_instructions.txt y _Locky_recover_instructions.bmp) 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

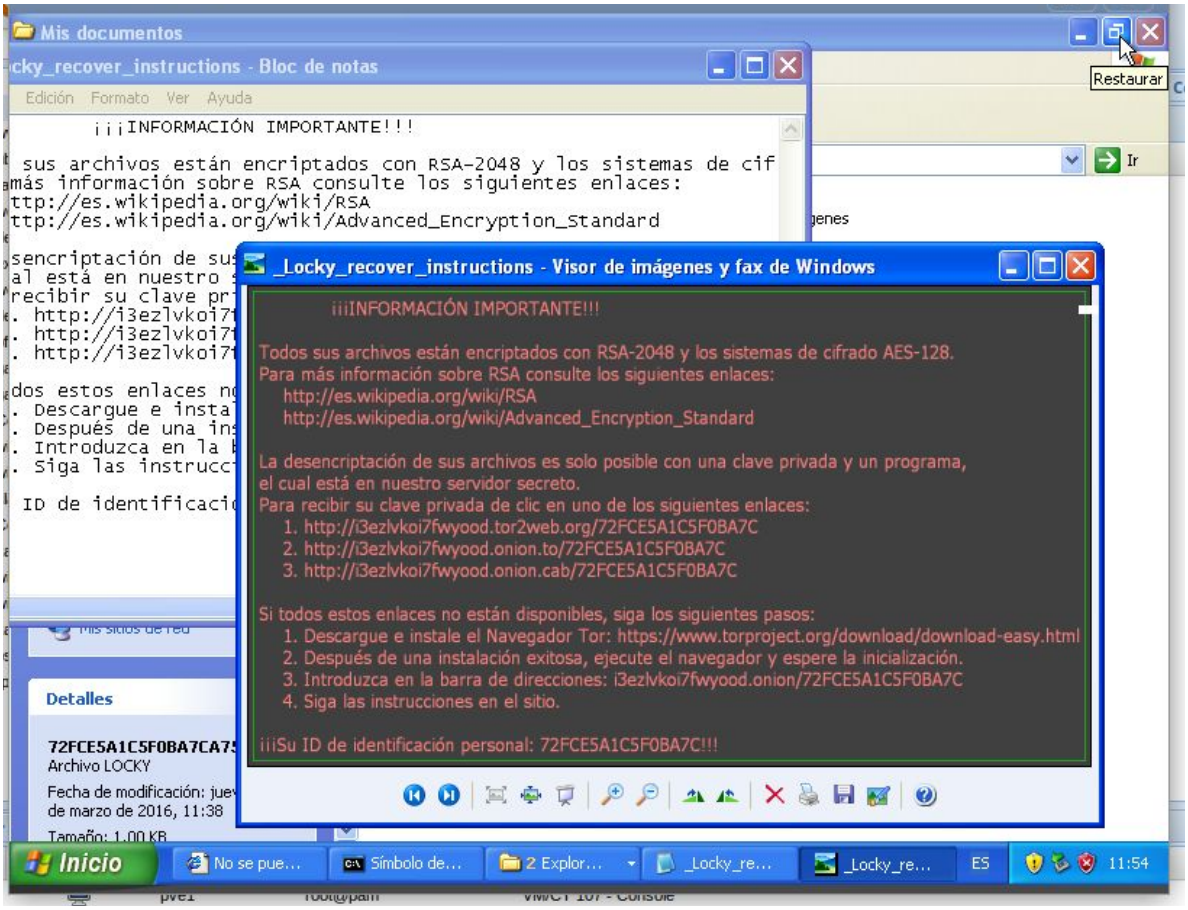

Figura 2: Mensaje de alerta desplegado por Locky

Para proceder al pago, se indican unas URLs en pantalla, con instrucciones específicas para la víctima infectada. Algunas de las URLs pertenecen a la red Tor. El rescate exigido es 3 Bitcoins, aproximadamente 1200 US$ (ver Figura 3).

Locky 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?

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

Impacto:

El ransomware Locky encripta los archivos usando estándares de encriptación robusta (RSA-2048 + AES-128 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.

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 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:
https://nakedsecurity.sophos.com/es/2016/02/17/locky-ransomware-what-you-need-to-know/
http://www.welivesecurity.com/la-es/2016/02/19/locky-nuevo-ransomware-latinoamerica/
https://blog.avast.com/a-closer-look-at-the-locky-ransomware
https://blog.malwarebytes.org/intelligence/2016/03/look-into-locky/
http://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/

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