Dirigido a:
Clientes y Asesores
Asunto:
Recomendaciones para evitar virus Ransonware

Medellín,
Octubre 24 de 2016

Comunicado Externo CE-1111

Cordial saludo,

En razón que algunas empresas nos han reportado la presencia de un virus que impide el acceso a su información o sistema operativo enviamos el siguiente comunicado de las posibles razones técnicas de porque sucede y como evitarlo

1. Que es Ransomware?

El ransomware es un software malicioso empleado por los cibercriminales para secuestrar tu equipo o ciertos archivos que almacena, y luego pedirte el pago de un rescate a cambio de su recuperación. Lamentablemente, el ransomware es un medio cada vez más popular mediante el cual los creadores de malware extorsionan a empresas y consumidores por igual para quitarles dinero.

Ranson= Secuestro

Ware= Terminación de Software

2. Como se propaga?

* Un método típico es a través de archivos adjuntos de correo electrónico

* Vinculo por correo electrónico de un banco o empresa de mensajería

* Uso de programas para compartir archivos. Algunos P2P como Ares / Torrent haciéndose pasar como claves de activación

* Una vez infectado el equipo se puede propagar a discos duros externos, memorias usb, unidades de red, conexión a servidores por RDP

3. Que tipos hay?

* Codificador de Archivos: Cifra los archivos del usuario o del sistema operativo

* Pantalla de Bloqueo: Impide que uses el equipo hasta haber pagado el rescate

4. Como se pueden recuperar los archivos / hay que pagar?

* Se recomienda no pagar porque no es garantía de la devolución del acceso a la información, al igual que el atacante sigue pidiendo mas dinero por el rescate. Se patrocina al atacante y animándolo a cometer mas ataques

5. Como evitarlo?

* Asegúrate de respaldar diariamente la información critica de tu empresa: Aplicativos, documentos, bases de datos, configuraciones. Backups en discos duros externos que salgan de la empresa o backups en plataforma en la nube

* Utiliza antivirus actualizados

* Desconfía de archivos adjuntos de dudosa procedencia. Consulta con el remitente si envió dicho adjunto

* Muestra las extensiones ocultas de los archivos: "Con frecuencia, una de las maneras en que se presenta Cryptolocker es en un archivo con extensión ".PDF.EXE", aprovechando la configuración predeterminada de Windows de ocultar las extensiones para tipos de archivos conocidos. Si desactivas la casilla correspondiente, podrás ver la extensión completa de cada uno y será más fácil detectar los sospechosos."

* Actualizaciones periódicas de los sistemas operativos

* Evitar descargas de archivos o programas de sitios sospechosos. Prefiera descargas software desde la pagina web del fabricante

* Evitar utilizar activadores de software ilegalmente como crack, keygen, etc

* Consultar con especialistas técnicos en seguridad informática como fortalecer la seguridad de sistemas operativos, red de datos y dispositivos de red: Técnica Hardening

Más opciones:

http://www.welivesecurity.com/la-es/2016/04/12/evitar-ransomware-cifre-servidor-de-ficheros-w2012/

https://mx.norton.com/clubnorton-ransomware-tips

http://computerhoy.com/noticias/software/que-es-ransomware-como-evitarlo-6642

http://blog.elhacker.net/2016/04/como-evitar-prevenir-que-un-ransomware-cifre-secuestre-los-ficheros-archivos-en-servidor-windows.html

http://www.welivesecurity.com/la-es/2015/07/08/11-formas-protegerte-del-ransomware-cryptolocker/

6. Como recuperar el equipo o archivos una vez infectados?

* Utilice herramientas desarrolladas por fabricantes reconocidos para este fin

https://support.kaspersky.com/sp/viruses/disinfection/8005#block7

https://support.kaspersky.com/sp/viruses/disinfection

https://support.kaspersky.com/sp/viruses/solutions

https://noransom.kaspersky.com/

https://blog.kaspersky.com/fantom-ransomware/12891/

https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

7. Que debo tener en cuenta a la hora de hacer backups

* Periodicidad

* Información critica: Aplicativos, bases de datos, documentos

* Información centralizada

* Auditar backups periódicamente

Más opciones

http://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_de_backup_baja.pdf

Otras Referencias:

http://www.welivesecurity.com/la-es/2015/07/08/11-formas-protegerte-del-ransomware-cryptolocker/

https://es.wikipedia.org/wiki/Ransomware

Cordialmente,

_____

Luis Arias López
Jefe de Infraestructura Tecnológica
Ofima S.A.S