VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Agosto 2016

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

- ¿Qué es el ransomware?
- ¿Deberías pagar el rescate?
- Respalda tus archivos
- Otras medias de protección

Ransomware

¿Qué es el ransomware?

El ransomware es un tipo especial de malware que amenaza con destruir los documentos y otros archivos de las víctimas; hoy en día se está propagando activamente a través de Internet. El malware es un software, un programa de computadora, utilizado para realizar acciones maliciosas. Si bien el ransomware es sólo uno de los diferentes tipos de malware, se ha vuelto muy común ya que es rentable para los criminales. Una vez que el ransomware infecta tu equipo, cifra ciertos archivos o incluso todo el disco duro. A continuación, bloquea todo el sistema o no te deja acceder a tus archivos importantes como documentos o fotografías. El malware te informa que la única forma en que puedes descifrar tus archivos y recuperar el sistema es pagar al cibercriminal un rescate (ransom en inglés, de ahí que se llame ransomware), el cual se debe pagar a través de alguna moneda digital como Bitcoin. El ransomware se propaga como otros tipos de malware; el método más común involucra el envío de correos electrónicos maliciosos a las víctimas, los cibercriminales te engañan para que abras un archivo adjunto infectado o hagas clic en un vínculo que te lleva al sitio web del atacante.

Editor Invitado

Lenny Zeltser se encarga de salvaguardar las operaciones de los clientes de TI en NCR Corp y enseña a combatir el malware en el Instituto SANS. Puedes encontrar a Lenny en Twitter como **@lennyzeltser** y en su blog de seguridad **zeltser.com**.

¿Deberías pagar el rescate?

Es una pregunta difícil de contestar. El problema es que cada vez más gente paga cuando son infectados, esto motiva a los criminales para que infecten a otros; sin embargo, es posible que no exista otra opción para recuperar tus archivos. No obstante, advertimos que incluso si pagas el rescate no hay garantía que obtengas los archivos de nuevo. Estás tratando con delincuentes que pueden no descifrar los archivos o inclusive si te proporcionan un método para descifrarlos a cambio de un pago, algo puede ir mal durante el proceso o tu computadora puede ser infectada con malware adicional.

Respalda tus archivos

Tal vez la mejor forma de recuperarte de una infección de ransomware y no pagar por un rescate es recuperar tus archivos a través de copias de seguridad. De esta forma, aunque te infectes con ransomware, tendrás una manera de recuperar los

Ransomware

archivos antes de reconstruir o limpiar tu computadora. Ten en cuenta que si accedes a tu copia de seguridad desde el sistema infectado, el ransomware podría borrar o cifrar tus archivos de respaldo. Por lo tanto, es importante que respaldes los archivos en servicios en la nube de buena reputación o los almacenes en discos duros externos que no siempre estén conectados a tu sistema. Un error común es que la gente asume que las copias de seguridad funcionan sin probar si efectivamente se pueden recuperar los archivos; asegúrate de realizar pruebas regulares para verificar que las copias de seguridad funcionen y puedas recuperar los archivos que necesites en caso de que el sistema sea infectado con ransomware. Las copias de respaldo son importantes ya que te pueden ayudar a recuperar tus archivos si accidentalmente los borras o en el caso que tu disco duro falle.

El ransomware es un malware que, una vez que infecta tu computadora, cifra todos los archivos y te niega el acceso a ellos.

Otras medidas de protección

Puedes protegerte del ransomware de la misma forma que lo haces contra otro tipo de malware: no infectarte. Asegúrate de tener un software antivirus actualizado de un proveedor de confianza. Dichas herramientas, algunas veces llamadas software antimalware, están diseñadas para detectar y detener el malware. Sin embargo, un antivirus no puede bloquear o eliminar todos los programas maliciosos. Los cibercriminales están constantemente innovando, desarrollando nuevo y más sofisticado malware que evada la detección. A su vez, los proveedores de antivirus están actualizando sus productos con nuevas capacidades para detectar malware. En muchos sentidos se ha convertido en una carrera armamentista pues ambas partes tratan de burlar al otro. Desafortunadamente los criminales están un paso adelante, por lo que debes asegurar las copias de respaldo de tus archivos e implementar estas medidas:

- Los delincuentes a menudo infectan computadoras o dispositivos explotando las vulnerabilidades en el software. Entre más actual sea tu software, menos vulnerabilidades tendrá el sistema y será más difícil infectarlo. Por lo tanto, asegúrate que los sistemas operativos, aplicaciones y dispositivos tengan habilitados la instalación de actualizaciones de forma automática.
- En las computadoras utiliza una cuenta estándar que tenga privilegios limitados, en lugar de las cuentas con privilegios de “administrador” o “raíz”. Esto proporciona una protección adicional al prevenir que se instalen distintos tipos de malware.

Ransomware

- Los cibercriminales suelen engañar a la gente para que instalen malware. Por ejemplo, te pueden enviar un correo que parezca ser legítimo (de un banco o un amigo). Al abrir los archivos adjuntos o hacer clic en el enlace contenidos en este correo, podrías activar un código malicioso que instale malware en el sistema. Si el mensaje crea un fuerte sentido de urgencia, es confuso, parece demasiado bueno para ser verdad o está mal redactado podría ser un ataque. Sospecha, el sentido común es tu mejor defensa.

Protégete del ransomware poniendo atención a los archivos adjuntos de un correo electrónico o cuando haces clic en los enlaces, asegúrate que esté actualizado el software antivirus y confirma que tus archivos sean respaldados regularmente y puedan restaurarse.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: securingthehuman.sans.org/ouch/archives

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.

Sitio web: http://www.seguridad.unam.mx

Síguelo en Twitter @unamcert

Recursos

¿Qué es el malware?:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_sp.pdf
Respaldos y recuperación:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_sp.pdf
FBI advierte sobre estafa del CEO:	http://www.seguridad.unam.mx/noticia/?noti=2915
Crypto Ransomware:	https://www.seguridad.unam.mx/vulnerabilidadesDB/?vulne=6521
Protegerse en contra del ransomware:	http://www.seguridad.unam.mx/noticia/?noti=2377
Ciberatacantes presentan rescate por ransomware como servicio público:	http://www.seguridad.unam.mx/noticia/?noti=2891

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traducción: Katia Rodríguez, Célica Martínez

