Publicado en Ciudad de México el 16/08/2017

# [Así hay que protegerse del Ransomware y sus variantes](http://www.notasdeprensa.es)

## Ransomware, una amenaza que se debe tomar en serio

 Por Ramón Castillo, Ingeniero de Preventa Senior en Forcepoint para México y Centroamérica El ransomware es un tipo de software malicioso que amenaza con publicar los datos de la víctima o bloquear permanentemente su acceso a menos que se pague un rescate. A través de una notificación se nos informa que el acceso a nuestros datos o dispositivo está restringido y que debemos realizar el pago para recuperar dicho acceso. Una vez efectuado el pago, el ransomware nos garantiza el acceso a nuestra información o a nuestros sistemas. Algunos ejemplos de ransomware son: SCAREWARE: Exige un pago utilizando amenazas de acción futura con tácticas de intimidación. Los archivos o sistemas del usuario no han sido afectados. LOCKERS: Hace la promesa de volver a conceder acceso a la pantalla o al sistema del usuario al mismo tiempo que pide el pago. CRIPTO-RANSOMWARE: Habiendo cifrado los archivos del usuario, el Cripto-ransomware ofrece la clave de descifrado a la víctima a cambio de una retribución. El Cripto-ransomware puede afectar archivos locales y archivos hospedados en redes compartidas. Los archivos cifrados que no pueden recuperarse se convierten en un incidente de “destrucción de datos”. El ejemplo más claro y reciente es WannaCry. ¿Cómo funciona el Ransomware? El ransomware se disemina, principalmente, a través de archivos adjuntos en el correo electrónico (los documentos de Microsoft Office son particularmente populares). También se distribuye con programas infectados o al descargar archivos ocultos de malware (drive-by) desde sitios web comprometidos. Los autores del ransomware utilizan técnicas de ingeniería social para alentar a los usuarios finales a descargar, ejecutar o hacer clic en el contenido malicioso. Finalmente y después de ejecutarse, el ransomware comienza a hacer el cifrado de los datos una vez que ha enumerado todos los controladores y buscado los tipos de archivo objetivo. Muchos de los ataques que involucran ransomware también son Ataques Persistentes Avanzados (APTs). Estos ataques se realizan en siete fases: 1.- Reconocimiento 2.- Señuelo En estas dos primeras fases el atacante se enfoca en obtener información de inteligencia de su objetivo (compañía o empleados específicos). Con esa información el atacante puede desarrollar un señuelo destinado a conseguir el acceso confiable hacia la red. El objetivo aquí es hacer que el usuario haga clic en la URL de un mensaje de correo electrónico, de un mensaje personal o de alguna otra forma de enlace web. 3.- Redireccionamiento El atacante puede enviar una URL como parte de un mensaje. Esto puede ser completamente inofensivo y hasta parecer benigno para la mayoría de las soluciones de seguridad instaladas. Sin embargo, el malware contenido en el mensaje puede estar a muchos clics de distancia, o puede tener un código oculto que automáticamente redirecciona al usuario al sitio que si contiene el malware. 4.- Explotación de Vulnerabilidad El kit de explotación es una pieza de software lo suficientemente inteligente para detectar brechas en las defensas de seguridad. Si existen brechas, se desplegará y se instalará. Durante esta etapa, la seguridad en tiempo real es esencial. Es necesario tener la capacidad para inspeccionar el tráfico en el momento en que se hace clic. 5.- Archivo detonante 6.- Alerta al cibercriminal Estas dos fases, son pasos adicionales que puede realizar un atacante. El kit de explotación puede traer consigo un archivo cuentagotas que se descarga en el equipo de cómputo una vez que tiene acceso a información confidencial. También puede generar una llamada a casa al atacante para seguir recibiendo instrucciones. 7.- Robo de datos En esta etapa final el atacante ha logrado atravesar las defensas. Puede tratarse también de un empleado que ha sido vulnerado o que tiene malas intenciones y que intentará enviar información confidencial a través de diversos canales web, email o endpoints. En ese momento, la organización necesita una solución que pueda detectar cualquier intento de robo de datos. ¿Cómo me protejo? Es importante contar con tecnologías de seguridad para defenderse en vectores de ataque relevantes, en este caso la web y el correo electrónico. Asimismo, se requieren herramientas de monitoreo y elaboración de informes para detectar y derrotar a las amenazas entrantes. Se debe implementar un programa continuo de educación para el usuario y capacitación para alertar al personal sobre los peligros de visitar páginas web inseguras así como de la apertura de correos sospechosos o de phising. También se necesita establecer un proceso de copia de seguridad de datos confiable y evaluado (preferentemente fuera de línea) en toda la empresa. Esto puede ayudar a recuperar los archivos sin pagar por un rescate. Al notificar a los usuarios finales sobre los incidentes de Ransomware y determinar si hay puntos débiles en la infraestructura o procesos que puedan ser aprovechados por tácticas de Ransomware se pueden eliminar las brechas de seguridad. Es indispensable diseñar e implementar un plan de respuesta a incidentes para que pueda reaccionar ante el Ransomware. El pago de un rescate para recuperar datos sería mejor aprovechado si se invierte en medidas de seguridad más efectivas para evitar incidentes similares en el futuro (como la educación para los usuarios y un entorno seguro de URL y archivos). Debemos implementar controles en los puntos de salida de la red, tales como: · Reglas de firewall para bloquear el tráfico de comando y control, así como neutralizar las técnicas de evasión que se pueden utilizar para entregar cargas maliciosas. · Controles avanzados de protección contra amenazas, que incluyen entorno seguro, para proporcionar una defensa contra ataques de día cero y otras técnicas de malware altamente evasivas. · Soluciones de seguridad web para bloquear destinos desconocidos (no categorizados) y realizar un análisis en tiempo real del contenido en la web. · Soluciones de seguridad de correo electrónico para bloquear las amenazas que ingresan por esa vía. Las siguientes medidas de control en dispositivos finales deben ser tomadas en cuenta, en especial para usuarios remotos e itinerantes. · Mantener el antivirus actualizado. · Usar una herramienta para dispositivos finales para bloquear aplicaciones maliciosas y prevenir la fuga de datos. · Aplicar seguridad web para dispositivos finales que están fuera de la red. · Hacer un análisis del comportamiento de los usuarios para identificar y bloquear la actividad sospechosa en dispositivos finales clave, incluso cuando operan fuera de la red.

**Datos de contacto:**

ARTURO MARTINEZ

5527680410

Nota de prensa publicada en: [https://www.mexicopress.com.mx/asi-hay-que-protegerse-del-ransomware-y-sus](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: E-Commerce Software Ciberseguridad



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)