VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Junio 2017

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

- Descripción general
- Actualizar
- Copias de seguridad
- Phishing

Lecciones que podemos aprender de WannaCry

Descripción general

Recientemente, es probable que hayas visto una tremenda cobertura informativa de un nuevo ataque cibernético llamado “WannaCry”. Este malware infectó más de 200,000 computadoras, bloqueando los datos de varias organizaciones, incluyendo hospitales en el Reino Unido. Hay varias razones por las que este ataque generó tanta atención. En primer lugar, se extendió rápidamente de una computadora a otra atacando una debilidad conocida en computadoras con sistema Windows. En segundo lugar, el ataque fue un tipo de malware llamado “ransomware”, lo que significa que una vez que infectó tu computadora cifró todos tus archivos, bloqueando tus datos. La única manera de recuperar los datos es mediante copias de seguridad o pagando al atacante un rescate de $300 USD para descifrar los archivos. En tercer lugar y el más importante, este ataque nunca debió haber sucedido. La debilidad que WannaCry atacaba en computadoras con sistema Windows era bien conocida por Microsoft, que había lanzado una corrección meses antes. Pero muchas organizaciones no pudieron instalar la corrección, o todavía usaban sistemas operativos como Windows XP que son tan viejos que no hay ningún parche disponible. Aquí hay tres sencillos pasos que puedes tomar para asegurarte de que ataques como WannaCry nunca te infecten.

Editor Invitado

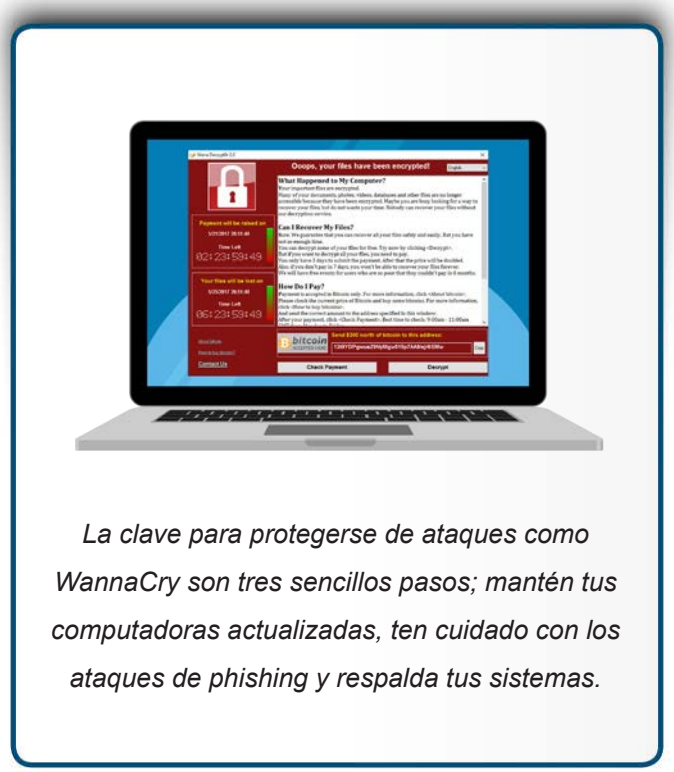
El Dr. Johannes Ullrich es Decano de investigación para el Instituto de Tecnología SANS y fundador de DShield.org. Es responsable del **Centro de Tormentas de Internet SANS** que monitorea las amenazas de seguridad cibernética actuales. Enseña seguridad de aplicaciones web (**DEV522**), detección de intrusiones (**SEC503**) e IPv6 (**SEC546**).

Actualizar

En primer lugar, asegúrate de que tus equipos, dispositivos móviles, aplicaciones y cualquier otra cosa que conectes a Internet estén actualizados. Los ciberdelincuentes constantemente están buscando nuevas vulnerabilidades en el software que usan los dispositivos. Cuando descubren las vulnerabilidades, utilizan programas especiales para atacar los aparatos que se están utilizando. Mientras tanto, las empresas que crearon el software están trabajando duro para corregir estas vulnerabilidades mediante la publicación de actualizaciones. Asegurando que tus computadoras y unidades móviles tengan estas actualizaciones, se hace mucho más difícil que alguien los ataque. Eso es lo que es tan frustrante sobre la propagación de WannaCry. Las actualizaciones para corregir y detener este ataque habían sido lanzadas casi dos meses antes por Microsoft. Si las organizaciones hubieran mantenido sus computadoras actualizadas, este ataque nunca habría funcionado. Para garantizar que tus dispositivos permanezcan actualizados, activa la actualización automática siempre que

Lecciones que podemos aprender de WannaCry

sea posible. Esta regla se aplica a casi cualquier tecnología conectada a una red, no solo a tus computadoras y dispositivos móviles, sino a los televisores conectados a Internet, routers domésticos, consolas de juegos o, algún día, tal vez incluso tu automóvil. Si tus sistemas operativos o dispositivos son tan antiguos que ya no son compatibles con actualizaciones de seguridad, como Windows XP, sustitúyelas por otros compatibles.



La clave para protegerse de ataques como WannaCry son tres sencillos pasos; mantén tus computadoras actualizadas, ten cuidado con los ataques de phishing y respalda tus sistemas.

Copias de seguridad

En algunos casos, ciberataques como el ransomware pueden incluso infectar sistemas actualizados. Una segunda forma de protegerse es hacer copias de seguridad de tu información. Las copias de seguridad son copias de tu información almacenada en algún lugar que no sea en tu computadora o dispositivo móvil. Cuando pierdes datos valiosos, puedes recuperar esos datos de tus copias de seguridad. Desafortunadamente, demasiadas personas no realizan copias de seguridad regulares, aunque son simples y baratas. Existen dos maneras de hacer una copia de seguridad de tus datos: medios físicos o almacenamiento en la nube. Cada enfoque tiene ventajas y desventajas. Puedes utilizar ambas al mismo tiempo si no estás seguro de qué método utilizar.

Los medios físicos son dispositivos que tú controlas, como unidades externas USB o unidades conectadas en red ubicadas en tu hogar u oficina. La ventaja de utilizar tus propios medios físicos es que te permiten hacer copias de seguridad y recuperar grandes cantidades de datos muy rápido. La desventaja de este enfoque es que si se infecta con malware, como ransomware, es posible que la infección se extienda a tus copias de seguridad. Si estás utilizando medios físicos para copias de seguridad, debes almacenar copias de tu copia de seguridad fuera de sitio en una ubicación segura. Asegúrate de que las copias de seguridad que almacenas estén correctamente etiquetadas. Las soluciones basadas en la nube son servicios en línea que respaldan y almacenan tus archivos en Internet. Normalmente, instalas un programa en tu computadora que se encarga de todo. Las ventajas de las soluciones en la nube son su simplicidad. Además, si se infecta con ransomware, la infección normalmente no puede acceder a tus copias de seguridad basadas en la nube. Las desventajas son que puede tomar mucho tiempo para realizar las copias de seguridad o recuperar grandes cantidades de datos. Asegúrate de investigar la privacidad y la seguridad de las copias de seguridad en la nube. ¿Ofrece el servicio de copias de seguridad una seguridad fuerte, como cifrar tus datos y autenticación fuerte?

Lecciones que podemos aprender de WannaCry

Phishing

Finalmente, los ciberdelincuentes siempre están actualizando y cambiando sus métodos de ataque. Usan a menudo otro método de ataque llamado phishing para atacar e infectar a las víctimas. El phishing sucede cuando los ciberdelincuentes envían un correo electrónico intentando engañarte para que abras un archivo adjunto infectado o visites un sitio web malicioso. Si lo haces, tu computadora puede infectarse. Mientras que WannaCry no utilizó este método de ataque, es comúnmente utilizado para muchos otros tipos de ataques, incluyendo la mayoría de los tipos de ransomware. Además, los cibercriminales que desarrollaron WannaCry sin duda actualizarán sus métodos de ataque en los próximos meses y utilizarán nuevas técnicas como el phishing para infectar aún más computadoras. La clave para protegerte contra ataques vía correo electrónico es el sentido común. Si un correo electrónico o mensaje parece extraño, sospechoso o demasiado bueno para ser verdad, lo más probable es que sea un ataque.

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

Consejos para enfrentar WannaCry:	https://www.seguridad.unam.mx/consejos_unam_cert#WannaCry
Tendencias de seguridad 2017. ¿Estás preparado?:	https://revista.seguridad.unam.mx/numero28/tendencias-de-seguridad-2017
Medidas preventivas para resguardar la información:	https://revista.seguridad.unam.mx/node/2235
Tips de seguridad:	https://revista.seguridad.unam.mx/node/2098
Ingeniería social, técnica de ataque eficaz en contra de la seguridad informática:	https://revista.seguridad.unam.mx/node/2090
Phishing:	https://www.seguridad.unam.mx/animaciones?page=4

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traducción: Alicia Manjarrez, Raúl Abraham González, Célica Martínez

