Boletín Informativo / Mayo 2017
UPCLC/CFT

Tema: AMERICAN BANKER (Política y Regulación, Tecnología)

Publicado
May 11 2017, 4:05pm EDT

El ataque de ransomware WannaCry que azotó el mundo el viernes, afectando a varios hospitales en el Reino Unido y causando estragos en decenas de miles de computadoras, sigue activo, dejando en riesgo a los escritorios y servidores.

Los efectos del ransomware son claramente devastadores. Los archivos están bloqueados e inaccesibles hasta que se pague un rescate, normalmente alrededor de $ 300 de bitcoin.

Ningún banco ha confirmado que ha sido afectado por WannaCry. Los sitios de noticias informaron el viernes que BBVA y Santander se habían visto afectados en España, pero portavoces de ambos bancos afirmaron firmemente que los bancos no habían sido afectados en España o Estados Unidos.

Sin embargo, los bancos siguen siendo un objetivo principal para el ransomware y sería un riesgo sustancial para el negocio si un banco se convirtiera en una víctima. Imagine las consecuencias si los bancos se bloquearon de los registros de clientes o transacciones durante un largo período de tiempo.

La buena noticia es que cualquier computadora cargada con software actualizado y bien remendado, herramientas anti-phishing y anti-malware eficaces y respaldo en caliente y frío debería estar en teoría a salvo del ransomware.

Pero incluso en las empresas más conscientes de la seguridad, hay grietas en esa suposición de seguridad.

Los ordenadores de sobremesa y las computadoras portátiles de los empleados que trabajan fuera de casa que no utilizan la VPN de la empresa o cuyos equipos no se mantienen tan seguros como el equipo local, por ejemplo, están en peligro. (Era un ordenador personal cuyo acceso a la red no se había actualizado a la autenticación de dos factores que permitió a los piratas informáticos romper 83 millones de registros en JPMorgan Chase en 2014, por ejemplo).

Los sistemas a los que acceden terceros, como proveedores de servicios de marketing o de infraestructura, también son vulnerables; existe la posibilidad de que no mantengan protocolos de seguridad sólidos. La brecha de Target fue un ejemplo destacado de esto.

En algunos casos, el ransomware de WannaCry irrumpió en la red de una empresa a través de un exitoso ataque de phishing. Hay ataques de phishing que pueden derrotar a los mejores filtros de phishing, por ejemplo, donde los hackers toman el control de un servidor de correo electrónico legítimo y envían mensajes maliciosos desde el mismo. Ningún filtro que mira a los nombres de dominio podría cuestionarlos. Sin embargo, el software que abre todos los vínculos y archivos adjuntos en una bóveda segura puede ayudar en este escenario.

Los peligros de no parchear

El ataque de ransomware de WannaCry subraya la importancia de mantener actualizados los programas informáticos, tales como los sistemas operativos Windows, y el hecho de que muchas empresas no lo hacen.

WannaCry utiliza un exploit llamado EternalBlue que generalmente se cree que ha sido desarrollado por la Agencia de Seguridad Nacional de EE.UU. para romper en las computadoras a través de una debilidad en el código del sistema operativo Windows. Fue filtrada por el grupo de hackers Shadow Brokers en abril. El mes anterior, Microsoft lanzó parches para él y otras vulnerabilidades de Windows. En otras palabras, las personas que instalaron esa actualización están en gran medida protegidas de la vulnerabilidad.

El viernes, Microsoft tomó el inusual paso de proporcionar también una actualización de seguridad para Windows XP, Windows 8 y Windows Server 2003, aunque estas versiones han superado sus ciclos de soporte.

"Incluso si usted tiene un gran filtrado de spam y buena formación de empleados, sin embargo, tiene un entorno grande y no está en un buen ciclo de parche, potencialmente hay la posibilidad de ser comprometido a través de una vulnerabilidad de Microsoft Windows", dijo Austin Berglas, jefe De cyberdefense para K2 Intelligence, un proveedor de consultoría y servicios de cumplimiento y ciberseguridad. "Este caso ha demostrado que las organizaciones están lamentablemente detrás de los tiempos en sus ciclos de parcheo. Se puso a disposición un parche y las organizaciones no lo desplegaron ".

Mantener el software actualizado parece una tarea sencilla y un hecho para cualquier empresa consciente de la seguridad, como un banco. Pero los expertos dicen que no es tan fácil como suena.

Una encuesta realizada en marzo por 1E de más de 1.000 profesionales de TI estadounidenses encontró que sólo el 9% de las empresas habían completado sus migraciones de Windows 10, mientras que otro 38% dijo que sus migraciones estaban en marcha. En el 64%, la mayoría de los encuestados predijo que sus migraciones tardarían más de un año en completarse.

Puerta abierta

"Este caso ha demostrado que las organizaciones están lamentablemente detrás de los tiempos en sus ciclos de parche", dice Austin Berglas, jefe de cyberdefense en K2 Intelligence. "Se puso a disposición un parche y las organizaciones no lo desplegaron". Las actualizaciones de software en una organización grande son difíciles y hay a menudo poca recompensa visible por el esfuerzo.

"Las compañías han visto generalmente las migraciones como un gran proyecto enorme y un proyecto que puede aplazar ad infinitum", dijo Sumir Karayi, fundador y CEO de 1E, una empresa que ofrece servicios de parches de software. "Si usted tiene otro proyecto que viene que se trata de crear más valor de negocio o ventaja competitiva, entonces por supuesto que va a elegir que en lugar de la migración de Windows, que no le da ventaja competitiva. Es sólo otra versión de Windows ".

Las actualizaciones de Windows tienden a tomar varios años en las grandes empresas, dijo.

"Si piensas en un proyecto que dura de un año a dos años, si no tengo que hacerlo, probablemente no quiero hacerlo, o quiero aplazarlo hasta el último momento", dijo Karayi. "Esto es lo que ocurrió con las migraciones de Windows XP a Windows 7 la última vez".

Algunos hospitales de U.K. que fueron víctimas de WannaCry no habían hecho la migración a Windows 7, que salió en 2009.

"A menos que esta mentalidad cambie, la gente no se mantendrá actualizada", dijo Karayi.

Los usuarios finales se han acostumbrado a la idea de parches porque sus aplicaciones móviles se actualizan todo el tiempo, señaló.

"Pero TI tiene que aceptar el cambio", dijo. Karayi recomienda que cada empresa ejecute un informe regular que muestra si se está ejecutando el software actual o no. "Ciertamente el CIO debe saber", dijo.

Los expertos recomiendan automatizar el proceso de parches de software.

"No deje la gestión de parches a los empleados", aconsejó Al Pascual, director de investigación de Javelin Strategy & Research. "Las compañías intentan evitar la creación de interrupciones de negocio permitiendo a los empleados dictar cuando se aplican las actualizaciones. Con las vulnerabilidades más rápidamente armadas que nunca, las empresas que opten por instituir un parche deben hacerlo de manera uniforme e inmediata, al menos durante la noche y fuera de las horas de oficina.

Más allá de las actualizaciones de software y parches

Buenas prácticas de parcheo no son suficientes para evitar el ransomware - el siguiente ataque, después de todo, podría implicar un exploit de día cero para el que no se ha emitido ningún parche. La defensa de una empresa contra ransomware, como casi cualquier cyberthreat, requiere una defensa en capas.

Una práctica de seguridad que podría ayudar es la segmentación - asegurándose de que una vez que el adversario ha entrado, sólo pueden ir tan lejos y no puede llegar a los activos críticos.

"La práctica del privilegio mínimo es asegurarse de que sus usuarios sólo tengan acceso a las áreas de información en su red que necesitan para hacer su trabajo", dijo Berglas. "Sobreprivileges puede permitir la propagación de este tipo de infección rápidamente."

La sensibilización de los empleados y la formación siempre es importante.

"Las compañías deben proveer entrenamiento y auditorías regulares en el conocimiento de phishing", dijo Pascual. "La única constante en todos los dispositivos es el usuario, y es la debilidad de la que más dependen los criminales".

Otro esfuerzo consiste en detectar la actividad de malware, en este caso, las exploraciones internas y externas maliciosas para vulnerabilidades de software.

Y no es el mantenimiento y el uso de todos los indicadores de compromiso que se pueden encontrar en los digeridos profesionales y blogs, por lo que puede bloquear los correos electrónicos, dominios, direcciones IP que están asociados con una campaña de ransomware, dijo Berglas.

Respaldo en caliente y en frío

Si todo lo demás falla, y el ransomware rompe todas las defensas de una compañía, una medida de seguridad permanece: buena copia de seguridad. Si se realiza una copia de seguridad efectiva de una computadora y la copia de seguridad no se ve afectada por ransomware, se puede cerrar la computadora infectada y reiniciarse una nueva instancia en una nueva pieza de hardware.

Pero la copia de seguridad eficaz no es universal.

"Hemos encontrado muchas compañías que no respaldan adecuadamente", dijo Berglas.

Y los sistemas utilizados para la copia de seguridad en tiempo real también pueden ser infectados por ransomware.

"Cuando usted tiene una fila agresiva de ransomware que se mueve rápidamente a través del ambiente y va a buscar cualquier tipo de infraestructura conectada, si su copia de seguridad es siempre caliente, lo que significa que siempre está conectado, hay un potencial que podría convertir sus sistemas el lunes Mañana y encontrar que su copia de seguridad está cifrada también ", dijo Berglas. "Las organizaciones que practican la copia de seguridad en frío y desconectan la copia de seguridad en determinados momentos de la red corporativa serán más seguras en situaciones como esta".

Información extraída de la fuente:

https://www.americanbanker.com/articles/cybercrime-outbreak-targets-french-banking-customers

https://hipertextual.com/2017/05/el-ataque-de-ransomware-wannacry-ya-es-un-problema-global

http://www.elladodelmal.com/2017/05/el-ataque-del-ransomware-wannacry.html

http://www.elladodelmal.com/2015/04/un-phishing-bancario-un-spam-en-unicode.html

https://blog.malwarebytes.com/cybercrime/2017/05/wanna-cry-some-more-ransomware-roundup-special-edition/

http://www.nebtechit.com/?q=what-we-do

https://es.dreamstime.com/imagenes-de-archivo-computadora-port%C3%A1til-3d-con-el-bloqueo-y-el-clave-seguridad-de-ordenador-image20925294

http://www.informatica-hoy.com.ar/seguridad-informatica/Copias-de-seguridad-Herramientas-y-consejos.php