El ciberataque para el que nadie está protegido

Por: Nicole Perlroth. The New York Times. 01/07/2017

NEWARK, Nueva Jersey — En los últimos meses, Golan Ben-Oni ha sentido que grita hacia el vacío. El 29 de abril alguien atacó a su empleador, IDT Corporation, con dos ciberarmas que le fueron robadas a la Agencia de Seguridad Nacional (NSA, por su sigla en inglés).

Ben-Oni, el director de información global del IDT, pudo repelerlas pero el ataque lo dejó consternado. En 22 años de lidiar con *hackers* de todo tipo, nunca había visto nada parecido. ¿Quién estaba detrás de eso? ¿Cómo pudieron evadir todas sus defensas? ¿Cuántos más habían sido atacados pero no estaban conscientes de eso?

Desde entonces, Ben-Oni ha expresado su preocupación llamando a cualquiera que lo escuche en la Casa Blanca, el Buró Federal de Investigación (FBI, por su sigla en inglés) y las compañías más importantes de ciberseguridad para advertirles sobre un ataque que aún podría estar dañando invisiblemente a víctimas por todo el mundo.

Dos semanas después de lo sucedido en IDT, el ciberataque conocido como WannaCry causó estragos en hospitales de Inglaterra, universidades de China, sistemas ferroviarios de Alemania e incluso plantas automotrices de Japón. Sin duda fue muy destructivo.

Sin embargo, lo que Ben-Oni atestiguó fue mucho peor y, con todas las miradas puestas en la destrucción causada por WannaCry, pocas personas se han fijado en el ataque contra los sistemas de IDT… y otros similares que seguramente se han producido en otros lugares.

El ataque a IDT, un conglomerado cuyas oficinas centrales tienen una gran vista del horizonte de Manhattan, fue similar a WannaCry en un sentido: los *hackers* encriptaron los datos de IDT y exigieron un rescate para desbloquearlos. No obstante, la exigencia del rescate solo fue una cortina de humo para ocultar un ataque mucho más invasivo que se robó las credenciales de los empleados.

Con esas credenciales, los *hackers* podrían haber circulado libremente por la red informática de la empresa, llevándose información confidencial o destruyendo los equipos.

Lo peor es que el ataque, que nunca antes se había reportado, no fue detectado por algunos de los productos de ciberseguridad líderes en Estados Unidos ni por los principales ingenieros de seguridad de las compañías tecnológicas más grandes ni por los analistas gubernamentales de inteligencia.

Si no hubiera sido por una caja negra digital que grabó todo lo que sucedió en la red de IDT, y por la tenacidad de Ben-Oni, el ataque pudo haber pasado inadvertido. Los escaneos realizados a las dos herramientas usadas en contra de IDT indican que la empresa no está sola. De hecho, las mismas armas de la NSA tuvieron acceso ilegal a decenas de miles de sistemas de cómputo en todo el mundo.

Ben-Obi y otros investigadores de seguridad temen que muchas de esas computadoras infectadas estén conectadas a redes de transporte, hospitales, plantas de tratamiento de agua y otros servicios. Un ataque a esas redes, advierte el experto en informática, podría poner en riesgo muchas vidas.

“El mundo está escandalizado con WannaCry, pero esto es una bomba nuclear en comparación con WannaCry”, dijo Ben-Oni. “Esto es distinto. Es mucho peor. Se roba las credenciales. No puedes atraparlo y está sucediendo frente a nuestros ojos”. Y añadió: “El mundo no está preparado para esto”.

Ataque al centro neural

En IDT, Ben-Oni se ha topado con cientos de miles de *hackers* de todo tipo de causas y niveles de habilidad. Según calcula, los negocios que trabajan con IDT experimentan cientos de ataques al día, pero quizá solo cuatro incidentes le

preocupan cada año.

Sin embargo, ninguno se compara con el ataque sufrido en abril. Al igual que el ataque WannaCry de mayo, el realizado contra IDT fue hecho con ciberarmas desarrolladas por la NSA que fueron filtradas en línea por un misterioso grupo que se hace llamar Shadow Brokers, que se piensa que está integrado por ciberdelincuentes respaldados por Rusia, un infiltrado en la NSA o por ambos.

El ataque con WannaCry —que tanto la NSA como los investigadores de seguridad han vinculado a Corea del Norte— usó una ciberarma de la NSA; el ataque a IDT usó dos.

Las oficinas de la NSA en Fort Meade, Maryland. Decenas de miles de sistemas computaciones han sido “hackeados” con herramientas desarrolladas por esta agencia que fueron robadas en abril.Credit Patrick Semansky/Associated Press

Tanto en WannaCry, como en el incidente de IDT utilizaron una herramienta de

hackeo que la agencia llamó EternalBlue. Esa aplicación se aprovechó de los servidores de Microsoft que no tenían las actualizaciones de seguridad para propagar automáticamente el programa malicioso de un servidor a otro, de tal manera que en 24 horas los hackers ya habían contagiado su *ransomware* a más de 200.000 servidores en todo el planeta.

El ataque a IDT fue un paso más allá: usó otra ciberarma robada a la NSA llamada DoublePulsar. La NSA la desarrolló para infiltrarse en sistemas informáticos sin activar las alarmas de seguridad. Eso permitió que los espías de la NSA pudieran inyectar sus herramientas al centro neural del sistema informático de un objetivo, llamado kernel o núcleo, que gestiona la comunicación entre el hardware y el software de una computadora.

En el orden jerárquico de un sistema de cómputo, el núcleo está en la cima, por lo que permite que cualquiera que tenga acceso secreto a él pueda tomar el control total de un equipo. También es un peligroso punto ciego para la mayor parte del software de seguridad, pues permite a los atacantes hacer lo que quieran sin ser detectados.

Luego los *hackers* activaron el programa de secuestro (*ransomware*) como una pantalla para cubrir su motivo real: un acceso más amplio a los negocios de IDT. Ben-Oni se enteró del ataque cuando una contratista, que trabajaba desde casa, prendió su computadora y se dio cuenta de que todos sus datos estaban encriptados y los atacantes exigían un rescate para desbloquearlos. Ben-Oni pudo haber supuesto que se trataba de un simple caso de programa de secuestro.

Sin embargo, le pareció peculiar. Para empezar, estaba perfectamente sincronizado con el *sabbat*. Los atacantes entraron a la red de IDT a las 18:00 en punto de un sábado, dos horas y media antes de que terminara el *sabbat* y por lo tanto un momento en que la mayoría de los empleados de IDT —el 40 por ciento de los cuales se identifican como judíos ortodoxos— estaban descansando. Además, los atacantes se infiltraron en la computadora de la contratista a través del módem de su casa, lo cual se le hizo muy extraño.

La especie de caja negra, un dispositivo de grabación de la red fabricado por la empresa israelí de seguridad Secdo, muestra que primero los atacantes se robaron las credenciales de la contratista. Se las arreglaron para evitar todos los

mecanismos de detección de seguridad con los que se encontraron. Finalmente, antes de salir, encriptaron su computadora con un programa de secuestro y le exigieron 130 dólares para desbloquearla. Así encubrieron el ataque, mucho más invasivo, que habían realizado en su computadora.

Ben-Oni calcula que ha hablado con 107 expertos e investigadores de seguridad sobre este ataque, incluyendo a los directores de casi todas las principales compañías de ciberseguridad y los jefes de inteligencia contra amenazas de Google, Microsoft y Amazon.

Con excepción de Amazon, que encontró que algunas de las computadoras de sus clientes habían sido escaneadas por la misma computadora que atacó IDT, nadie había visto ningún rastro del ataque antes de que Ben-Oni les avisara. “Comencé a sentir que éramos el conejillo de indias”, dijo. “Pero lo grabamos”.

Desde el ataque a IDT, Ben-Oni se ha puesto en contacto con muchos de sus contactos para advertirles de un ataque que aún podría estar sucediendo, sin ser detectado, a través de los sistemas de las víctimas. “Se está acabando el tiempo”, dijo Ben-Oni. “Hay que entender que esto es, en realidad, una guerra: con la ofensiva de un lado e instituciones, organizaciones y escuelas del otro, defendiéndose de un adversario desconocido”.

‘Nadie se está haciendo cargo’

Desde que los Shadow Brokers filtraron las codiciadas herramientas de ataque en abril, los hospitales, escuelas, ciudades, departamentos de policía y compañías alrededor del mundo han tenido que arreglárselas por sí mismos para defenderse o protegerse ante las armas desarrolladas por el atacante más sofisticado del mundo: la NSA.

En marzo, Microsoft lanzó un parche para software con el fin de que los equipos pudieran defenderse de las herramientas de ataque informático de la NSA, lo que sugiere que la agencia le había avisado a la compañía. No todas las empresas lo instalaron a tiempo y fueron afectadas por WannaCry. Ben-Oni dijo que instaló los parches de Microsoft en cuanto estuvieron disponibles pero los atacantes lograron tener acceso al módem de la casa de la contratista de IDT.

Hace seis años, Ben-Oni se encontró con un empleado de la NSA en una conferencia y le preguntó cómo defenderse ante las amenazas cibernéticas actuales. El hombre le aconsejó “ejecutar tres de todo”: tres cortafuegos, tres antivirus, tres sistemas de detección de intrusión. Y así lo implementó.

Pero en este caso, los sistemas de detección y las actualizaciones no detuvieron el ataque a IDT. Tampoco lo hicieron con ninguno de los 128 proveedores de inteligencia contra amenazas públicamente disponibles a los que IDT está suscrito. Ni siquiera lo notaron los diez proveedores de inteligencia contra amenazas en las que su empresa gasta medio millón de dólares anuales por información urgente. Desde entonces ha dicho que podrían regresarles sus productos.

“A nuestra industria le gusta trabajar con problemas conocidos”, dijo Ben-Oni. “Este es un problema desconocido. No estamos preparados para él”.

No ha hablado con nadie que sepa si ha sufrido un ataque, pero ahora hay videos en YouTube que les enseñan a los criminales cómo atacar sistemas usando las mismas herramientas de la NSA empleadas en contra de IDT, y Metasploit, una herramienta de ataques informáticos automatizada, permite que cualquiera realice estos ataques con solo un clic.

Lo que es peor, dijo Ben-Oni, es que “nadie se está haciendo cargo”.

En mayo, él mismo le presentó un resumen al analista del FBI encargado de investigar el ataque con WannaCry. Le dijo que la agencia se había centrado en WannaCry y que, a pesar de que el ataque a su empresa era más invasivo y sofisticado, técnicamente era algo distinto, y por lo tanto el FBI no podía atender su caso. (El FBI no respondió a nuestras solicitudes de comentarios).

Así que Ben-Oni le ha dado seguimiento, en gran medida, por sus propios medios. Su equipo en IDT pudo rastrear parte del ataque a un teléfono Android personal en Rusia, y ha estado proporcionando sus hallazgos a Europol, la agencia europea con sede en La Haya.

Las probabilidades de que IDT haya sido la única víctima de este ataque son pocas. Sean Dillon, un analista sénior en RiskSense, una compañía de seguridad de Nuevo México, fue de los primeros analistas de seguridad en escanear el internet en busca

de la herramienta DoublePulsar de la NSA. Encontró decenas de miles de computadoras huéspedes infectadas, que los atacantes pueden usar a su antojo.

“Una vez que DoublePulsar está en el equipo, nada puede evitar que otro llegue y entre por la puerta trasera”, dijo Dillon. Es aún más preocupante que Dillon probó los principales productos antivirus contra la infección de DoublePulsar, pero 99 por ciento de ellos no pudieron detectarlo.

“Hemos revisado las mismas computadoras infectadas con DoublePulsar durante dos meses y no sabemos cuántos programas maliciosos hay en esos sistemas”, dijo Dillon. “En este momento no tenemos idea de qué ha sido infiltrado en estas organizaciones”.

En el peor de los casos, dijo Dillon, los atacantes podrían usar esas puertas secretas para desatar el programa maligno destructivo en infraestructura crucial, inmovilizar sistemas ferroviarios, causar apagones en hospitales o incluso paralizar los servicios de electricidad.

¿Podría avecinarse un ataque así? Los Shadow Brokers volvieron a salir a la luz en mayo, cuando prometieron un cargamento fresco de herramientas de ataque de la NSA e incluso se las ofrecieron a los suscriptores que pagaran mensualmente.

Ben-Oni está convencido de que IDT no es la única víctima y de que estas herramientas pueden usarse —y se usarán— para hacer mucho más daño. “Creo que esta situación es de vida o muerte”, dijo. “Hoy somos nosotros, pero mañana puede ser alguien más”.

Fuente: https://www.nytimes.com/es/2017/06/26/idt-ciberataque-fbi-hackers-ransomware-nsa/?mc=adglobal&mcid=facebook&mccr=ES&subid=MC18&subid1=TAFI

Fotografía: flipboard

Fecha de creación
2017/07/01