Fuerza Aérea de Chile
Centro de Estudios Estratégicos y Aeroespaciales
Estrategia, Aeronáutica, Espacio, Tecnología & Innovación

BOLETÍN INFORMATIVO Y DE ANÁLISIS N° 28-2017 Santiago, 18 de mayo de 2017

"IMPACTO DE LOS CIBERATAQUES A LA SEGURIDAD INTERNACIONAL"

El pasado viernes 12 de mayo, las redes de alerta mundiales anunciaban que decenas de miles de computadores alrededor del mundo, incluido Chile, habían sido blanco de un ataque informático, en forma de programa de rescate ("***ransomware***", de *'ransom'*, rescate en inglés, y *'ware'* por *'software'*), denominado ***WannaCry***, aprovechando una debilidad en el sistema operativo *Windows* XP de *Microsoft*, una versión que ya no tenía soporte técnico del gigante estadounidense.

Cuadro: Mapa mundial que muestra la extensión hasta el momento del ataque del ransomware 'WannaCry'. Fuente: Agencia France Presse.

El ataque del WannaCry.

El *ransomware WannaCry* bloquea el acceso a los archivos del usuario y solicita dinero en forma de *bitcoin* - moneda virtual - para desencriptar esos archivos. Hasta el momento, a las víctimas del *hackeo* se les ha pedido un rescate de 300 USD en *bitcoins*. Se exige que el pago se haga efectivo en tres días. De lo contrario la tarifa se duplica y, si no se paga esa suma incrementada en el plazo de siete días, amenazan con borrar definitivamente los archivos, de acuerdo con el mensaje que aparece en las pantallas afectadas.

Las víctimas más notorias del ataque a escala mundial son hospitales en Gran Bretaña, la empresa española de telecomunicaciones *Telefónica*, el fabricante francés de automóviles *Renault*, la empresa de correos estadounidense *FedEx*, el Ministerio del Interior ruso y el operador de ferrocarriles alemán *Deutsche Bahn*. La compañía de ciberseguridad *F-Secure*, con sede en Finlandia, sostiene que fueron 130.000 sistemas en más de 100 países. De acuerdo a esa fuente, se confirma que Rusia e India fueron los países más intensamente golpeados, porque muchos seguían usando allí *Windows XP*.

Foto: Pantalla que aparece en los computadores atacados por el ransomware WannaCry, indicando la captura de archivos y la petición de pago en bitcoins. Fuente: Informe Código Dañino CCN-CERT ID-17/17, del Centro Criptográfico Nacional de España.

El uso de Bitcoins es clave.

La moneda digital *bitcoin* no trabaja con entidades financieras ni está regulado por ninguna entidad estatal, sino por la oferta y demanda de sus mismos usuarios. Tampoco hay una cuenta asociada a un nombre y un apellido. Más bien se trata de un sistema descentralizado, en donde los valores están esparcidos en miles de servidores en todo el mundo, asociados a un código para reunirlos cuando se requiera emplear, lo que permite realizar transferencias desde y hacia cualquier parte del mundo y en forma anónima.

Foto: Representación de la moneda bitcoin. Fuente: http://tn.com.ar/tecno.

Se reconoce que más de 6 millones de personas usan *bitcoins* para realizar transacciones diarias (enviar, recibir y pagar) y alrededor de 100 mil comercios y sitios *web* que las aceptan como forma de pago. Argentina y Brasil son los países de mayor adopción de *bitcoins* en América Latina y el mundo. Hoy, la cotización de esta moneda ronda los 1.700 USD, mientras que a mediados de 2013 no superaba los 100 USD.

Todas y cada una de las transacciones en *bitcoins* quedan registradas en una cadena de bloques (*blockchain*), que funciona como un libro contable público. La cadena revela la dirección de origen y destino de cada transacción más el monto enviado, pero no la identidad de las partes. Esto hace que, por un lado, *Bitcoin* sea la red más segura y privada para enviar dinero y, por otro, un método atractivo para los rescates de delitos informáticos. Por eso también lo utilizan los delincuentes para tráfico de armas o de drogas. "Desde que apareció *bitcoin*, este tipo de ataques se ha disparado", señala la experta en criptografía de la Universidad *Pompeu Fabra*, Vanesa Daza. También añade: "El *ransomware* existe desde los 80, pero estaba en desuso porque no habían monedas que permitieran no ser rastreados".

¿Quién está detrás de estos ciberdelitos?

Las primeras informaciones sobre los posibles autores vincularon a la NSA (*National Security Agency*) de los EE.UU. de Norteamérica, ya que se estima que las deficiencias del sistema *Windows XP* empleadas para infiltrar los archivos, era un defecto descubierto por la NSA (en forma de *exploits* o fragmentos de *software*) y que mantenía en su poder para aprovechar vulnerabilidades de diferentes sistemas, en sus funciones de inteligencia. Uno de ellos, denominado *Eternal Blue*, habría sido filtrado por el grupo de hackers *Shadow Brokers*, grupo que se adjudicó el *hackeo* a la NSA en 2016, consiguiendo varios archivos de armas cibernéticas. Estos archivos también estaban en poder del sitio *WikiLeaks*, que liberó algunos datos que afectaban a los programas de vigilancia electrónica de la CIA (Central de Inteligencia Americana) y la NSA.

El fin de semana, en el sitio *blog* de la compañía, el Presidente de *Microsoft*, *Brad Smith*, señaló que los ataques recientes destacan los peligros de que la NSA o que la CIA almacenen o desarrollen códigos secretos que después son usados en contra de sus sistemas operativos. "Hemos visto que las vulnerabilidades guardadas por la

CIA aparecen en *WikiLeaks*," señalando además que, "y ahora esta vulnerabilidad robada desde la NSA ha afectado a nuestros clientes alrededor del mundo." Dada las repercusiones políticas, *Tom Bossert,* el principal asesor del Presidente *Donald Trump* en materias de Ciberseguridad y *Homeland Security,* ha desmentido rápidamente las versiones que vinculaban a parte de su administración con los ataques.


Foto izq.: Brad Smith, Presidente de Microsoft, quien culpa en parte a la NSA por la responsabilidad de los ciberataques; Foto der.: el Almirante Michael S. Rogers, Director de la NSA, en pugna por la responsabilidad. Fuente: The New York Times.

El Presidente ruso *Vladimir Putin* también se hizo eco de estas versiones que apuntaban el dedo a los EE.UU. "[Si se deja suelto un genio de la lámpara] de este tipo, creado especialmente por los servicios secretos, puede luego dañar a sus autores y creadores", señaló el líder ruso durante una cumbre en Pekín. Por su parte, dado que Rusia ha sido acusada anteriormente de espionajes y acciones cibernéticas en contra de varios países, también fue cuestionada por el origen de los ataques, pero *Putin* aseguró que su país no tenía nada que ver con ellos. Cabe recordar que en el pasado autoridades de distintos países han conseguido identificar y arrestar a algunos ciudadanos rusos "ciberdelincuentes" que habían llevado a cabo ataques parecidos, en parte porque en los países de Europa de Este, este tipo de delitos no es penalizado con la misma fuerza que en occidente.

Las dudas sobre Corea del Norte.

En un artículo del periódico electrónico *Hindustan Times*, de la India, uno de los países severamente afectados por el ataque cibernético, se dio a entender que existen signos de un potencial involucramiento de Corea del Norte. En las primeras pistas acerca del origen del *ransomware*, el investigador de *Google, Neel Mehta,* mostró códigos de computación que muestran similitudes entre el *WannaCry* y un esfuerzo anterior de *hackeo* atribuido ampliamente a Pionyang.

Otros expertos rápidamente coincidieron con esa comparación como una señal, aunque no concluyente, de que Corea del Norte podría haber estado detrás de los últimos ataques. "Creemos que esto puede ser la clave para resolver alguno de los misterios acerca de este ataque", dijeron investigadores de la firma rusa de seguridad *Kaspersky Lab*, basada en Moscú. También estuvo de acuerdo con la atribución del ataque a los norcoreanos, la firma basada en Israel *Intezer Labs*.

Otras voces acusatorias han surgido desde la misma península coreana. *Choi Sang-myung*, un asesor de la Comando Surcoreano de Ciberguerra e investigador de seguridad de la firma *Hauri Inc.,* dijo que la lógica del algoritmo del ataque de *ransomware* del viernes 12 es similar al utilizado en ataques anteriores en contra de la compañía *Sony Pictures* y la empresa de sistemas de mensajería internacional de bancos *Swift*, ambos rastreados hasta Corea del Norte. Lo anterior, dado que la técnica empleada por el *ransomware* para borrar los archivos de computación se asemejan a los usados por el Grupo *Lazarus*, el nombre que utilizan los expertos para identificar al grupo norcoreano acusado del ataque a *Sony*.

Foto: Empleados de Agencia Coreana de Seguridad de Internet, KISA, en Seúl, monitoreando el alcance del ciberataque con ransomware, el pasado lunes 15 de mayo. Fuente: Agencia France-Presse.

También se cree que el Partido de los Trabajadores y el Ejército Popular de Corea (del norte), llevan a cabos sus propias operaciones de *hackeo*, en una suerte de competencia entre ellos. Esto ha llevado a especular que a veces los *hackers* norcoreanos pueden dejar algunas pistas de sus trabajos, para ganar el crédito y reconocimiento en sus respectivas organizaciones. Estas afirmaciones van a la par con otras acusaciones, que hablan de ciberataques deliberadamente programados por parte de Corea del Norte, para coincidir con las pruebas de misiles balísticos lanzados el domingo 14 de mayo. Lo anterior, como una forma de hacer alarde de los avances tecnológicos del país, a pesar de su aislamiento global.

Por otra parte, también se reconoce que puede que Corea del Norte no tenga nada que ver con los ataques, sino que, dada las características técnicas de *WannaCry*, el creador podría haber sido una banda organizada o incluso, una sola persona. Con ello, se comprueba que la detección de este tipo de delitos es bastante difícil, aunque no imposible. Una de las dificultades proviene de la falta de cooperación internacional a nivel global. El único acuerdo en esta materia es la *Convención de Budapest*, que países como Rusia y China se han negado a firmar, porque permitiría a agentes de otros Estados investigar libremente en su territorio, quedando en la práctica este pacto limitado a las democracias occidentales. Posterior a los últimos ataques, que afectó significativamente a ambas potencias, se piensa que puede existir un mejor ánimo para acuerdos globales en materia de defensa contra ciberataques.

Cómo estamos en Chile.

En nuestro país, algunas informaciones cifran hoy en al menos 270 los afectados por el ataque del *WannaCry,* sin mayor conocimiento de sus efectos finales. Por otra parte, Chile ha dado los primeros pasos "para alcanzar el objetivo de contar con un ciberespacio libre, abierto, seguro y resilente", mediante la publicación de la "Política Nacional de Ciberseguridad", en un esfuerzo para coordinar las medidas de prevención y mitigación de riesgos informáticos tanto al sector civil, en donde radica el control de la mayoría de los servicios básicos del país, la banca y el sector estatal, incluyendo al sector de Defensa. Los resultados de esta política y de las primeras acciones que considera, debieran concretarse de aquí al 2022, las que necesariamente debieran ir acompañadas de inversiones en capacitación e infraestructura acorde a las vulnerabilidades enfrentadas.

Adaptaciones de los artículos: "Lo que se sabe del ataque cibernético mundial", www.eluniverso.com; ¿Por qué es tan difícil rastrear quién está detrás del virus WannaCry que afectó a computadoras en 150 países?", BBC Mundo; "Global ransomware attacks show signs of North Korea link: Security researchers", HindustanTimes; "Focus Turns to North Korea Sleeper Cells as Possible Culprits in Cyberattack", New York Times; y, "Qué son los bitcoins y por qué es la moneda que eligen los hackers", en http://tn.com.ar/tecno; más otros antecedentes del autor. MQS.