La industrialización de la CIBERDELINCUENCIA

La piratería solitaria se convierte en negocio establecido

Tamas Gaidosch

La ciberdelincuencia es actualmente un sector maduro que se atiene a principios muy similares a los de negocios legítimos que persiguen el lucro. La lucha contra la proliferación de la ciberdelincuencia consiste en desmantelar un modelo de negocios que emplea herramientas sencillas para generar altas utilidades en un entorno de bajo riesgo.

Hace mucho, fines de la década de 1980, que se acabó la época de los legendarios hackers solitarios cuyo principal aliciente al irrumpir en las computadoras era poder lucir sus habilidades técnicas. A partir de la década de 1990, el afán de lucro empezó a ser el nuevo objetivo de los hackers y ello engendró la industria actual de la ciberdelincuencia que reúne todas las características de los negocios normales: mercados, bolsas, especialistas, subcontratación de proveedores de servicios, cadenas de suministro integradas, etc. Varios Estados-nación se han valido de esa misma tecnología para crear armas informáticas sumamente eficaces que permiten recabar información, llevar a cabo operaciones de espionaje industrial y desestabilizar las infraestructuras vulnerables de sus adversarios.

Evolución

La ciberdelincuencia ha proliferado a pesar de que la oferta de especialistas se ha mantenido a la zaga de la creciente maestría técnica necesaria para poder llevar a cabo ataques lucrativos con impunidad. Cerraron esa brecha el uso de herramientas muy avanzadas y la automatización. En las dos últimas décadas, las herramientas de los hackers han evolucionado extraordinariamente. En los años noventa, las pruebas de intrusión para detectar vulnerabilidades en los sistemas informáticos eran el último grito de la profesión. La mayor parte de las herramientas disponibles eran sencillas, a menudo hechas a medida, pero exigían conocimientos considerables de programación, protocolos de red, sistemas operativos y otros temas sumamente técnicos. En consecuencia, eran pocos los profesionales capaces de detectar una vulnerabilidad aprovechable.

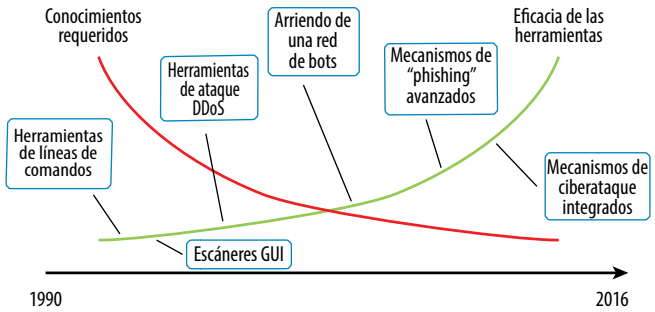
A medida que las herramientas se fueron mejorando y simplificando, gente joven menos adepta pero motivada empezó a emplearlas con relativo éxito. Hoy en día, realizar una operación de "phishing" —la práctica fraudulenta que consiste en enviar un correo electrónico cuyo remitente parece ser alguien respetable a fin de obtener información confidencial de forma capciosa— no exige más que conocimientos básicos, voluntad y un poco de dinero. Ser ciberpirata es ahora fácil (véase el gráfico).

Cuantificar el riesgo cibernético es notoriamente difícil. Los datos sobre pérdidas son escasos y poco fiables, en parte porque los incentivos para declarar una pérdida de este tipo son reducidos, especialmente si el caso no sale a luz o no está cubierto por un seguro. La rapidez con que estos peligros evolucionan reduce la utilidad de los datos históricos para pronosticar la cuantía de pérdidas futuras.

Los modelos basados en escenarios, que calculan el costo de incidentes específicos que afectan a algunas economías, arrojan estimaciones que llegan a los cientos de miles de millones de dólares. Según estimaciones de Lloyd's de Londres, el costo para las economías avanzadas de un corte de los servicios de la nube de dos días y medio a tres es de USD 53.050 millones, y en el escenario base de un modelo del FMI, las pérdidas anuales agregadas alcanzan un promedio de USD 97.000 millones y, en el caso más pesimista, de aproximadamente USD 250.000 millones.

ILUSTRACIÓN: ISTOCK / UGURHAN; YANREEEL

Juego de niños
Con herramientas más avanzadas, la piratería exige menos conocimientos técnicos y se vuelve más fácil.



Fuente: Universidad de Carnegie Mellon.
Nota: DDoS = denegación de servicios distribuidos; GUI = interfaz gráfica de usuario.

Causas y consecuencias

En el mundo físico, la delincuencia —con el propósito de enriquecerse— suele obedecer al simple afán de obtener un lucro muy superior al de un negocio lícito, beneficio que los delincuentes consideran como pago por asumir un alto riesgo. En el mundo de la ciberdelincuencia, las ganancias posibles son similares, o incluso mayores, pero el riesgo es mucho menor: menos probabilidades de ser detectado o procesado y casi ningún riesgo de ser baleado. Se estima que la tasa de rentabilidad del "phishing" podría ascender a más de 1.000 puntos porcentuales, pero solo podemos especular acerca de las ganancias que los ciberpiratas más malévolos logran mediante el robo de la propiedad intelectual. No obstante, las cuestiones básicas son parecidas: herramientas efectivas y una relación riesgo-recompensa muy positiva resultan claramente persuasivas y explican el pronunciado aumento de la industrialización de la ciberdelincuencia.

La ciberdelincuencia crea riesgos sistémicos en varios sectores. Aunque los efectos varían de un sector a otro, el financiero es quizás el más vulnerable. Una amenaza relativamente nueva se presenta en la forma de ataques que solo buscan destruir. Cuando los ciberpiratas desean desestabilizar el sistema financiero, se fijan en los blancos más prometedores. La infraestructura de los mercados financieros es la más vulnerable debido a su función central en los mercados financieros mundiales. Dada la dependencia del sector financiero de un conjunto relativamente pequeño de sistemas técnicos, los efectos en cadena por cesación de pagos o demoras atribuibles a ataques exitosos pueden ser generalizados y sistémicos.

Debido a la inherente interconectividad de los agentes del sector financiero, una alteración de los sistemas de pago, compensación o liquidación —o el robo de información confidencial— tendría efectos de contagio de amplio alcance y comprometería la estabilidad financiera.

Afortunadamente, aún no ha habido un ciberataque con secuelas sistémicas. No obstante, dados los recientes ataques a redes de cajeros automáticos, servicios bancarios en línea, bancos centrales y sistemas de pagos, los encargados de formular políticas y reglamentar el sistema financiero están cada vez más atentos.

El sector financiero depende de la tecnología de la información desde hace décadas, y tiene un historial de someterla al riguroso control que prescribe la reglamentación. Aunque es el sector de mayor riesgo de ciberataque, para los delincuentes es también el que conlleva el mayor riesgo, en parte porque el sistema está vigilado de cerca. Asimismo, el sector financiero presta mayor apoyo a las fuerzas del orden, por ejemplo, manteniendo registros de amplio alcance de gran valor para las investigaciones forenses. En general, con presupuestos más amplios pueden lograrse soluciones de ciberseguridad más efectivas. (Una notable excepción reciente fue el caso de Equifax, cuyo ataque presumiblemente se produjo porque el régimen que regulaba la ciberseguridad no era proporcional al riesgo).

El sector de atención de la salud es diferente. Salvo en los países más ricos, este sector suele carecer de recursos para montar defensas cibernéticas eficaces. Ello resulta evidente, por ejemplo, en los ataques de chantaje (*ransomware*) de este año contra los sistemas informáticos de la empresa de historiales médicos electrónicos Allscripts y dos hospitales regionales en Estados Unidos. Aunque también está muy reglamentado y sujeto a normas estrictas de protección de datos, el sector de atención a la salud no adoptó la TI con el mismo grado que el sector financiero y, por consiguiente, no desarrolló una cultura de control estricto. Por lo tanto, el sector es más proclive a ataques informáticos, y lo más inquietante es que, a diferencia del sector financiero, son personas las que están en juego si se atacan los equipos informatizados que las mantienen con vida.

Los servicios públicos, especialmente las redes eléctricas y de comunicaciones, suelen citarse como el siguiente sector en que un ciberataque a gran escala tendría consecuencias graves. La principal preocupación en ese caso, sin embargo, es que estados rivales interrumpan el servicio o se infiltren en los sistemas, directa o indirectamente a través de terceros. Como dejó patente el ataque de gran alcance a la infraestructura de

La cooperación internacional en la lucha y procesamiento judicial de la ciberdelincuencia está muy a la zaga del alcance mundial de esta amenaza.

Internet de Estonia en 2017 —que interrumpió servicios financieros en línea, medios de comunicación y agencias de gobierno—, cuanto mayor sea el grado de avance de una economía y su uso de Internet, más devastadores serán los ciberataques. Estonia se cuenta entre las sociedades más digitalizadas del mundo (véase "El despegue de e-Estonia" en el número de *F&D* de marzo de 2018).

Contramedidas

Si una red eléctrica, de telecomunicaciones o transporte se ve afectada, o si las autoridades no pueden recaudar impuestos o prestar servicios esenciales tras un ataque, las repercusiones económicas pueden ser sistémicas y comprometer la salud y la seguridad públicas. En esos casos, el riesgo agregado para la economía mundial podría exceder del riesgo total que correrían las personas debido al alcance internacional de las redes y plataformas de TI, el carácter nacional de las estructuras de respuesta, la ineficacia de la cooperación internacional o incluso la participación de Estados-nación en los ataques.

La cooperación internacional en la lucha y procesamiento judicial de la ciberdelincuencia está muy a la zaga del alcance mundial de esta amenaza. La mejor forma de afrontar la ciberdelincuencia es atacando su modelo de negocios, basado en su extraordinaria relación riesgo/beneficio y alto grado de impunidad. Al respecto, debe elevarse significativamente el riesgo comercial que asumen los atacantes, pero ello solo es posible con una mejor cooperación internacional.

Las operaciones de los ciberdelincuentes pueden afectar varias jurisdicciones, lo cual dificulta su neutralización y procesamiento judicial. Algunas jurisdicciones son lentas en hacer frente al problema, responden en forma ineficaz o sencillamente no cooperan. Una cooperación más estrecha permitiría identificar y enjuiciar a los sospechosos más rápida y eficazmente.

En el sector financiero, los reguladores han adoptado normas de evaluación específicas, fijado pautas y expectativas aplicables y fomentado el intercambio de información y la colaboración entre empresas y reguladores. En las pruebas de esfuerzo a que se someten los bancos y en los planes de resolución y supervisión de la seguridad que forman parte de su examen de la TI, los reguladores tienen en cuenta el grado de preparación en ciberseguridad. Algunos exigen simulacros de ciberataques específicos para cada empresa empleando datos y conocimientos especializados de organismos estatales y del sector privado para determinar la capacidad de resistencia a un ataque. ¿Las empresas también han aumentado la inversión en ciberseguridad y han incorporado la preparación ante un ataque como parte de la gestión de riesgo; algunas, a su vez, han procurado transferir parte del riesgo a los seguros cibernéticos.

La situación actual de la ciberseguridad sigue siendo desigual y descentralizada, y los riesgos se gestionan como problemas idiosincráticos locales. Aunque hay algunos mecanismos de cooperación, y los gobiernos y reguladores han intensificado sus esfuerzos, el grado de ciberseguridad depende en gran parte de las necesidades de cada empresa. Si el objetivo es mejorar la resiliencia general a estos riesgos, esto debe cambiar. Todos los sectores requieren sólidas medidas preventivas a nivel reglamentario y tecnológico. Entre las más importantes se cuenta la adopción de normas mínimas de ciberseguridad cuya aplicación coordinarían los reguladores. Una mayor concientización de la ciberseguridad contribuirá a evitar las vulnerabilidades técnicas básicas y los errores de los usuarios que causan la mayor parte de los ataques.

Ya que los ciberataques y la intrusión de los sistemas de ciberseguridad parecen inevitables, también debemos poner más atención en la rapidez con que detectamos los ataques, la eficacia con que respondemos y la velocidad con que restablecemos nuestras operaciones. FD

TAMAS GAIDOSCH, Experto Principal en cuestiones del sector financiero del Departamento de Mercados Monetarios y de Capital del FMI, es un profesional en ciberseguridad con una trayectoria de más de 20 años que incluye la detección de vulnerabilidades en los sistemas bancarios. Anteriormente estuvo a cargo del Departamento de Supervisión de la Tecnología de la Información del Banco Central de Hungría.