El *carding* y el robo de datos

PID_00269716

Thomas Holt

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Thomas Holt

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Marc Balcells Magrans (2019)

Primera edición: septiembre 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

Las amenazas técnicas planteadas por los *hackers* y los creadores de software malicioso son claras y presentan grandes riesgos para la seguridad de los datos personales y las redes informáticas. Aunque algunos *hackers* están interesados simplemente en obtener acceso a los sistemas para ver si un método de ataque novedoso funcionará, muchos otros también buscan acceder a los datos como ataque informático en sí. De hecho, la cantidad de datos personales financieros y de identidad que ahora se aloja en servidores, ordenadores portátiles y dispositivos móviles conectados a internet convierte estos datos en objetivos directos de ataques informáticos. El desarrollo de sitios de comercio electrónico y banca en línea también simplificó el proceso de uso de información personal para obtener ganancias financieras.

Como consecuencia, la amenaza de fraude cibernético en función de la ciberintrusión ahora es constante. Los ataques que conducen a la pérdida de información personal confidencial han aumentado en la última década, siendo las principales empresas, gobiernos y organizaciones las afectadas, especialmente en Estados Unidos y la Unión Europea (Ponemon Institute, 2019). El desarrollo de *malware* y de herramientas de registro de teclas diseñadas para adquirir subrepticiamente nombres de usuario y contraseñas confidenciales también ha facilitado que los piratas informáticos recopilen más información que puede ser utilizada por una persona o incluso un pequeño grupo de personas (Holt, 2013). En lugar de permitir que una buena información permanezca inactiva, los *hackers* más emprendedores han monetizado los datos personales que pueden usarse para fraude y robo. En algunos aspectos, esta dinámica es similar a lo que se observa en los mercados de *malware* (véase módulo 2): la gente ha encontrado formas de percibir pagos por sus habilidades y experiencia en el hackeo con respecto a aquellos que pueden no tener el mismo conocimiento, pero entienden lo que puede hacerse con tal información personal.

Este módulo proporcionará una descripción general de varias formas de robo que se derivan de actos de ciberintrusión. Se centrará sobre todo en el *phishing* y en la filtración de datos, así como en su vínculo con el cada vez más frecuente mercado negro de compra y venta de información pirateada. El módulo concluye con una discusión sobre las características de la suplantación y robo de identidad en línea para comprender las dimensiones inherentemente humanas de los ciberdelitos.

1. Métodos de obtención ilegal de datos

Existen varias maneras en las que los ciberdelincuentes pueden obtener información confidencial para cometer robos de identidad.

> Por ejemplo, los delincuentes que están dispuestos a correr el riesgo de ser identificados en el espacio físico pueden utilizar un dispositivo llamado *skimmer*, que está diseñado para capturar datos de tarjetas de crédito y débito en cajeros automáticos, terminales de puntos de venta y otros lugares.

Los *skimmers* pueden adquirir diversas formas, aunque todas incluyen un pequeño lector electrónico que puede tener forma de ranura y que permite que una tarjeta pase a través del dispositivo (Holt y Lampke, 2010; Krebs, 2019). El lector registra la información almacenada en la banda magnética que se encuentra en la parte posterior de la tarjeta de crédito o débito conforme se mueve a través de la ranura. Esta información se retiene en la memoria interna del dispositivo para ser posteriormente recuperada por parte del delincuente, ya sea accediendo físicamente al dispositivo o capturándolo de manera inalámbrica (Krebs, 2019).

En cualquier caso, los *skimmers* ofrecen a los delincuentes información valiosa sobre el consumidor y que puede ser utilizada por los propios delincuentes o vendida a cualquier persona interesada con el fin de obtener ganancias.

> Cada año se realizan varios arrestos relacionados con el uso de *skimmers* en el robo de identidad (véase, por ejemplo, Burgos, 2018). En algunos casos, se observó a los delincuentes utilizar los detalles financieros que obtuvieron (Krebs, 2019; Rogoway 2019), aunque muchos otros escapan con éxito de la policía y solo se logra identificar y destruir sus dispositivos (Wilson, 2018).

El uso de dispositivos físicos como los *skimmers* demuestra que los cibercriminales encuentran estrategias ingeniosas para obtener información de valor. Sin embargo, hay formas mucho más comunes y menos arriesgadas en las que los delincuentes pueden intentar obtener información financiera de los consumidores. De hecho, uno de los métodos más comunes se dirige específicamente a individuos, mientras que el otro afecta tanto a las grandes organizaciones como a los consumidores individuales. Ambos métodos pueden generar enormes cantidades de información personal que pueden usarse o venderse a partes interesadas, y generalmente desempeñan un papel importante en el cibercrimen.

2. Correos de *phishing*

Una de las técnicas más exitosas para obtener información personal y detalles financieros en la historia de los *hackers* consiste en la manipulación basada en el correo electrónico.

En concreto, los piratas informáticos desarrollaron una técnica llamada *phishing*, un neologismo derivado en parte de la noción de *phreaking* (véase módulo 2) y del término *pesca* (*fishing* en inglés) de información (James, 2005; Lastdrager, 2014). El *phishing* supone un intento de engañar a los usuarios para que proporcionen al atacante, o *phisher*, información valiosa sobre la base de alguna falsa amenaza (Myers, 2006).

Si bien el *phishing* constituye una amenaza moderna, en realidad es una metodología bastante antigua, nacida en los años noventa, cuando la mayoría de los proveedores de servicios de internet (ISP) cobraban a sus usuarios por hora. Uno de los proveedores más grandes en Estados Unidos en ese momento era America Online (AOL), y sus clientes podían pagar por adelantado cada mes. Aquellos *hackers* emprendedores que no querían usar sus propias conexiones a internet para buscar y piratear sistemas comenzaron a atacar a los clientes de AOL para obtener acceso a sus cuentas y poder usar internet de manera gratuita (Wang, 2003). Los atacantes rastreaban los sitios web y perfiles de AOL para obtener direcciones de correo electrónico y enviaban después correos en los que se alegaba que la información de la cuenta era incorrecta o necesitaba ser validada. Los remitentes solicitaban que el destinatario les proporcionase tanto su nombre de usuario como su contraseña. A su vez, los estafadores retenían la información de la cuenta y la usaban para su propio beneficio o intercambiaban los detalles del usuario con otros como moneda de cambio (Wang, 2003). De hecho, este concepto se hizo tan popular que los *hackers* comenzaron a crear herramientas para obtener nombres de usuario y contraseñas de manera fraudulenta. Una de las más antiguas y populares se llamaba AOHell, que se mofaba del uso de servicios AOL y que presentaba herramientas para enviar *spam* a los usuarios y administrar sus contraseñas y otros tipos de información confidencial (Wang, 2003).

Tal y como internet y las herramientas de comercio electrónico iban aumentado a finales de los años noventa y principios del siglo XXI, los piratas informáticos comenzaron a atacar estos sistemas utilizando técnicas similares. Los mercados clandestinos empezaron a vender listas de *spam* con direcciones de correo electrónico extraídas de internet para así crear una población de posi-

bles víctimas de estafas (Holt, 2013). Estas listas de correo electrónico podrían usarse junto a *malware* de *botnet* para difundir rápidamente mensajes de *phishing* (Holt, 2013).

El correo electrónico es la plataforma preferida para la suplantación de identidad (*phishing*), ya que el remitente puede usar varias herramientas para engañar al destinatario y hacerle creer que la solicitud proviene de un proveedor legítimo, sobre todo si se trata de servicios financieros.

El lenguaje utilizado en los correos electrónicos de *phishing* frecuentemente sugiere a la víctima que la cuenta del destinatario ha sido atacada o que existe un problema que puede hacer que la cuenta quede inactiva (James, 2005). Por lo general, estos mensajes usan un lenguaje especial para sugerir que el problema es urgente y que requiere una respuesta rápida por parte del destinatario si quiere garantizar que no haya interrupciones en sus servicios (Myers, 2006).

La mayoría de los mensajes utilizan múltiples herramientas y técnicas engañosas para aumentar la probabilidad de respuestas. Los mejores *phishers* combinan estos correos electrónicos, que parecen originarse de un proveedor de servicios legítimo, con logotipos y marcas que corresponden al servicio que están imitando. Los *phishers* también proporcionan al destinatario enlaces web aparentemente legítimos para que este haga clic y el atacante pueda administrar de esta manera su cuenta. La URL real y el alojamiento web del sitio redirigen a una página controlada por el estafador, que puede encontrarse en un servicio ilícito que no revelará las intenciones del *hacker*. La página web y el contenido pueden crearse mediante el uso de *kits* de *phishing*, que presentan diferentes logotipos, imágenes, marcas e idioma web para reflejar lo más fielmente posible el sitio original (James, 2005). Se le solicitará al encuestado que ingrese su nombre de usuario, contraseña y otra información confidencial, como el número de cuenta bancaria y el de identificación personal o PIN de la cuenta. Una vez que se ingresan estos datos, se guardan en el servidor para que el *phisher* acceda más tarde, y la víctima es redirigida al sitio web original del proveedor del servicio, o agradece al destinatario haber proporcionado su información (James, 2005).

Las estafas de *phishing* siguen siendo bastante comunes, la mayoría de las cuales están dirigidas a sistemas de servicios financieros y de pago (APWG, 2018). Las estimaciones sugieren que hay cientos de miles de estafas de *phishing* cada año (APWG, 2017; ENISA, 2017). Los sitios que albergan esquemas de *phishing* también pueden encontrarse en todo el mundo, muchos de los cuales actúan en Estados Unidos, Canadá, Alemania, Francia y el Reino Unido (APWG, 2018). Como consecuencia, se estima que las empresas gastan millones cada

año en un intento de minimizar el impacto de los ataques de *phishing*, independientemente de que estos acaben siendo exitosos o no (Ponemon Institute, 2019).

3. Filtración de datos

Conforme los sitios de comercio electrónico y el uso de redes sociales presentan más y más información sobre el consumidor, que se almacena en bases de datos a gran escala conectadas a internet, los *hackers* redirigen sus esfuerzos a estos recursos, especialmente a registros bancarios, a la información personal disponible y a otro tipo de información confidencial (véase Allison y otros, 2005; Furnell, 2002; Newman y Clarke, 2003; Wall, 2001, 2007). Esto incluye sistemas de procesamiento de pagos que pueden estar alojados en instituciones financieras más grandes, o incluso en terminales de punto de venta de tiendas físicas. El *hacker* solo necesita encontrar una manera de acceder a las partes internas y vulnerables de una empresa o institución financiera para obtener acceso a uno de estos repositorios de datos. Si tienen éxito, tendrán acceso a cientos de miles, si no a millones, de datos con información confidencial que pueden monetizarse. El éxito de tales compromisos se evidencia en el hecho de que los delincuentes se dirigen regularmente a estas instituciones para explotar sus recursos al máximo (Ponemon Institute, 2019).

Por lo general, estos incidentes se reconocen como filtraciones de datos, dado que una gran cantidad de datos provenientes de una organización se identifica primero y es filtrada después por parte de los *hackers* de manera ilegal. Una violación o filtración de datos puede darse como resultado de varios errores o ataques deliberados de personas dentro y fuera de dicha organización.

> Por ejemplo, si un empleado de una institución deja un ordenador portátil o un disco duro con información confidencial en un taxi o en un restaurante, otros pueden obtener esta información. Del mismo modo, si la información confidencial se envía inadvertidamente por correo electrónico a otras personas ajenas a la organización, entonces los datos podrían considerarse perdidos. Tales incidentes a menudo se denominan errores de «factor humano» en los informes del Instituto Ponemon, ya que la información se pierde debido a un error o descuido humano.

No obstante, los hackeos son en mayor medida la causa de las filtraciones de datos, independientemente de que provengan de atacantes internos o externos. Como se señaló en el módulo 2, los *hackers* infiltrados difieren de los externos en su fiabilidad dentro de una organización. Los infiltrados pueden participar en diferentes métodos de ataque, como el uso de *malware* para eliminar información confidencial o liberarla a través de medios públicos. Al mismo tiempo, los atacantes externos podrían hacerse pasar por agentes internos de confianza mediante el uso de credenciales obtenidas de manera fraudulenta.

Target

Por ejemplo, en 2013 se produjo una filtración importante en Target, la cadena de tiendas estadounidense, lo que provocó la pérdida de cuarenta millones de registros de tarjetas de crédito y débito de clientes en menos de treinta días (Krebs, 2014). La filtración se llevó a cabo por parte de *hackers* externos que primero identificaron y robaron a un proveedor de servicios externo llamado Fazio Mechanical. La compañía proporcionó mantenimiento de calefacción y refrigeración a las tiendas Target y recibió pagos por sus servicios. Por lo

tanto, los atacantes utilizaron las credenciales de usuario de Fazio para acceder e interactuar con el portal en línea del pago de proveedores de Target.

Una vez que los atacantes tuvieron acceso a la red interna de Target, obtuvieron información confidencial proveniente de varias partes de los sistemas del minorista. Por ejemplo, los clientes que hicieron compras a través del sitio web de la compañía perdieron sus nombres, números de teléfono, correos electrónicos y direcciones postales durante el ataque. Además, los atacantes colocaron software malicioso en los terminales de puntos de venta de ciertas tiendas, lo que les permitió adquirir millones de números de tarjetas de crédito y débito mientras la información se enviaba del registro al procesador de pagos (Krebs, 2014). Se cree que los atacantes pudieron haber vendido entre uno y tres millones de las cuentas que robaron, lo que pudo generar más de cincuenta millones de dólares en ganancias (Krebs, 2014). Sin embargo, las instituciones financieras que tuvieron que emitir de nuevo y administrar las cuentas de las tarjetas atacadas gastaron aproximadamente doscientos millones de dólares para evitar daños mayores a sus clientes (Krebs, 2014). Por lo tanto, el daño económico causado por las filtraciones de datos no puede subestimarse.

4. Robo de datos y mercados de *carding*

Los diversos métodos que utilizan los piratas informáticos y los ciberdelincuentes para obtener enormes cantidades de información confidencial plantean un desafío: cómo explotar toda esta información valiosa al máximo. Si un atacante puede reunir millones de tarjetas de crédito y débito, no hay manera de que pueda usarlas con efectividad, no importa cuántas transacciones intente. Incluso si participaran varios atacantes e intentaran analizar los datos por igual, aún dispondrían de demasiada información. Además, los datos tienen una vida útil limitada porque las instituciones financieras pueden intentar cerrar cuentas afectadas por *phishing* o filtraciones de datos para minimizar el potencial de estas transacciones fraudulentas (Holt y Bossler, 2016).

Para obtener el mayor rendimiento económico posible de los datos adquiridos, los ciberdelincuentes han comenzado a monetizar la información pirateada vendiéndola a otros, tanto en mercados abiertos como cerrados, que se encuentran en internet. Estos mercados permiten a los compradores comprar tarjetas de crédito, información de servicios financieros y herramientas de fraude cibernético a cambio de una tarifa, independientemente de su nivel de habilidad informática o de su conocimiento sobre piratería y fraude (Franklin y otros, 2007; Holt y Lampke, 2010; Motoyama y otros, 2011). Sin embargo, la expansión de estos mercados puede suponer un aumento en la demanda de información robada y en herramientas de cibercrimen. Esto puede incrementar el número de hackeos y las filtraciones de datos, así como el de ataques, para proporcionar a estos mercados un suministro adecuado de datos y bienes (Hutchings y Holt, 2017).

Algunos de estos mercados de datos robados se observaron por primera vez en los canales de Internet Relay Chat, o IRC, donde los *hackers* vendían los datos obtenidos por *phishing* y piratería (Benjamin, Li, Holt y Chen, 2015; Franklin y otros, 2007; Honeynet Project, 2003). Estas comunidades estaban altamente controladas, disponían de muy poca información acerca de las identidades de los atacantes involucrados. Aunque esto parecería beneficioso, redujo el tamaño general del mercado y limitó las oportunidades económicas para los vendedores. Como resultado, los *hackers* comenzaron a migrar a foros con un público potencial mayor (Benjamin y otros, 2015; Holt y Lampke, 2010). Con esta migración, llegó un mayor control por parte de las fuerzas del orden, que intentaron infiltrarse y detener a estos grupos.

ShadowCrew

Por ejemplo, un foro dirigido por un grupo de *hackers* que se hacían llamar ShadowCrew fue eliminado por la policía en 2004 (Lemos, 2004). La investigación condujo al arresto de 28 personas en todo el mundo por su participación en el robo y venta de más de 1,7 millones de tarjetas de crédito y débito, así como datos y servicios relacionados (Lemos, 2004). El arresto de ShadowCrew no eliminó el mercado de datos robados, sino que lo

volvió difuso y más complejo en términos de sofisticación operativa, para así reducir la probabilidad de ser investigados (Hutchings y Holt, 2017).

En la actualidad, existen múltiples entornos que facilitan la mercantilización de información robada y el robo de identidad. Los principales mercados parecen existir en la llamada Open Web, aquella parte de la World Wide Web a la que se puede acceder a través de navegadores web tradicionales y cuyo contenido puede ser capturado por motores de búsqueda como Google (Dupont y otros, 2017; Holt y otros, 2016; Leukfeldt y otros, 2017; Smirnova y Holt, 2017; Yip y otros, 2013). Estos sitios funcionan y se alojan en todo el mundo, aunque muchos de ellos parecen crearse en Rusia, en Estados Unidos y en varias partes de Europa (Dunn, 2012; Holt y otros, 2016; Hutchings y Holt, 2015). Muchos de estos sitios funcionan como foros web, una forma de comunicación mediada por ordenador que permite a sus usuarios conectarse y discutir sus recursos y necesidades (Holt, 2013). Los foros están compuestos de hilos, que comienzan cuando un individuo crea una publicación donde describe un producto o servicio, hace una pregunta, da una opinión o simplemente comparte experiencias pasadas. Otros responden a la publicación inicial con sus propias publicaciones para crear un hilo y mantener así una conversación o diálogo (Holt y otros, 2016).

Los foros que operan como mercados de datos tienen una estructura específica, ya que los participantes tienen la posibilidad de crear hilos únicamente para vender sus productos o solicitar un tipo de datos no tan común. Los vendedores que crean hilos explican lo que tienen a la venta, el precio de sus datos, las reglas de ventas, cómo deben pagarse y las formas en que los compradores pueden comunicarse con compradores potenciales (Hutchings y Holt, 2015; Smirnova y Holt, 2017). Sus posibles clientes pueden crear publicaciones dentro del hilo para hacer preguntas sobre los productos de los vendedores o describir su experiencia con el vendedor en caso de que hayan completado una transacción (Holt y Lampke, 2010; Holt y otros, 2016). En realidad, las ventas se llevan a cabo fuera del foro para ocultar el encuentro y reducir la cantidad de información sobre el intercambio que pueda hacerse pública (véase, por ejemplo, Holt y Lampke, 2010).

Algunos foros también presentan cierto grado de gestión para regular las transacciones y parar los pies a aquellos vendedores sin escrúpulos que busquen engañar a los compradores (Dupont y otros, 2017; Holt y Lampke, 2010). Estos gerentes desempeñan roles específicos, como moderadores o administradores, y pueden tomar medidas para influir en el comportamiento de los usuarios al prohibir o bloquear a aquellos participantes fuera de control (Holt, 2013). Además, aquellos foros bien administrados también pueden tomar muestras de los productos y revisarlos para que los posibles compradores puedan evaluar su calidad (Holt, 2013; Hutchings y Holt, 2015).

En los últimos años, los proveedores han pasado de foros a tiendas de un solo operador, sitios web administrados por un proveedor individual para anunciar directamente sus productos y servicios a los clientes (Martin, 2014; Smirnova

y Holt, 2017). Las tiendas ofrecen un espacio publicitario alternativo sin la supervisión de los moderadores del foro, aunque los proveedores deben encontrar soluciones creativas para atraer a clientes potenciales sin recurrir a la promoción en los hilos del foro. En cualquier caso, las tiendas son similares a los foros, ya que el vendedor publica sus productos, precios y métodos de entrega y pago (Smirnova y Holt, 2017). Los posibles clientes también pueden encontrar difícil determinar la legitimidad de los proveedores, ya que estos pueden no proporcionar comentarios sobre productos o *feedback* que se haya publicado en foros. Por lo tanto, los compradores aceptarían un mayor grado de riesgo al tratar con vendedores en tienda en comparación con aquellos que se anuncian en foros (Smirnova y Holt, 2017).

Además de la Open Web, también existen tiendas y foros de datos en la denominada Dark Web, aquella parte de internet que utiliza cifrado para ocultar información (Barratt, 2012; Office of Public Affairs, 2017; Smirnova y Holt, 2017). La Dark Web depende de un servicio llamado The Onion Router, o TOR, un programa gratuito consistente en un conjunto único de protocolos de cifrado que pone en marcha el tráfico web de un individuo a través de los ordenadores de otros usuarios de TOR en la red (Barratt, 2012; Martin, 2014). Como consecuencia, es difícil identificar la ubicación e identidad de cualquiera que use el servicio, así como la localización física de cualquier sitio web o servicio alojado en TOR, por lo que es complicado desconectarlos (Barratt, 2012; Smirnova & Holt, 2017).

La Dark Web no solo oculta información sobre el usuario, sino que también es útil para ocultar el contenido de los mercados y productos ilícitos. Concretamente, el contenido de los sitios de la Dark Web no puede ser indexado por los motores de búsqueda tradicionales como Google (Barratt, 2012). Además, las personas solo pueden acceder a sitios web basados en TOR mediante el uso del navegador web integrado de TOR. Cualquier otro navegador de la Open Web, como Chrome o Internet Explorer, no podrá acceder al contenido. Por lo tanto, TOR se está convirtiendo rápidamente en una poderosa herramienta para que los ciberdelincuentes reduzcan su riesgo de detección.

5. Productos y servicios en los mercados de datos

Examinar el contenido de los mercados de datos robados demuestra que los ciberdelincuentes obtienen diversos materiales a través de diferentes formas de piratería y robo digital.

Los productos más comúnmente vendidos incluyen cuentas de tarjetas de crédito y débito, que los vendedores y compradores denominan *dumps* (literalmente, 'vertederos') (Franklin y otros, 2007; Holt y Lampke, 2010; Hutchings y Holt, 2015; Motoyama y otros, 2011).Independientemente de si los productos se venden en foros o tiendas, los vendedores anuncian constantemente el país de origen de sus *dumps* y los precios de cada tipo de tarjeta según su localización. Esto era evidente en el lenguaje empleado por una tienda de datos en la Open Web, que enumeró sus precios para varios productos:

LISTA DE PRECIOS DE *DUMPS*

DUMPS 101 DE ESTADOS UNIDOS

- Visa Clásica/MC Standard = 25 $
- Visa Oro, Platinum/MC Oro, Platinum = 35 $
- Visa Negocios, Corporativa/MC Negocios, Corporativa = 40 $
- Visa Compras, Signature/MC Compras, World = 45 $
- Amex Platinum = 35 $
- Discover = 25 $

DUMPS DE EUROPA (REINO UNIDO – ALEMANIA - FRANCIA – ESPAÑA - ITALIA - PAÍSES BAJOS - SUIZA)

101

- Visa Clásica/MC Standard = 35 $
- Visa Oro, Platinum/MC Oro, Platinum = 45 $
- Visa Negocios, Corporativa/MC Negocios, Corporativa = 50 $
- Visa Compras, Signature/MC Compras, World = 55 $
- Amex Platinum = 45 $

201

- Visa Clásica/MC Standard = 30 $
- Visa Oro, Platinum/MC Oro, Platinum = 40 $
- Visa Negocios, Corporativa/MC Negocios, Corporativa = 45 $
- Visa Compras, Signature/MC Compras, World = 50 $

CONTÁCTANOS: hacktransfers@gmail.com - ICQ: 712705321

DUMPS INTERNACIONALES (AUSTRALIA - DUBÁI - CHINA - RUSIA - JAPÓN)

101

- Visa Clásica/MC Standard = 45 $
- Visa Oro, Platinum/MC Oro, Platinum = 55 $
- Visa Negocios, Corporativa/MC Negocios, Corporativa = 60 $
- Visa Compras, Signature/MC Compras, World = 65 $
- Amex Platinum = 55 $

201

- Visa Clásica/MC Standard = 40 $
- Visa Oro, Platinum/MC Oro, Platinum = 50 $
- Visa Negocios, Corporativa/MC Negocios, Corporativa = 55 $
- Visa Compras, Signature/MC Compras, World = 60 $

DUMPS DE SALDOS ELEVADOS

101

- Visa Infinite = 120 $
- Visa Black Card = 120 $
- Amex Centurion = 110 $

NOTA: Nuestros *dumps* NO TIENEN CONTROL REGIONAL, lo que significa que funcionan en cualquier punto de venta a NIVEL MUNDIAL - SIN BLOQUEO REGIONAL. O, de lo contrario, se hará una restitución instantánea.

NOTA: Los *dumps* de SALDOS ELEVADOS tienen una garantía de cambio de 2k-3k $ cada vez. Cualquier *dump* de saldo elevado que falle en este intervalo será remplazado.

Algunos proveedores también ofrecen nombres de usuario y contraseñas que pueden usarse para acceder a cuentas de PayPal y eBay, cuentas bancarias y otros servicios financieros (Holt y otros, 2016; Leukfeldt y otros, 2017). Estos inicios de sesión son claves para realizar transferencias de dinero desde la cuenta de la víctima a una controlada por el comprador, y estafar así a los titulares de la cuenta (Holt y Lampke, 2010; Holt y otros, 2016; Motoyama y otros, 2010). Una parte de los vendedores también ofrece herramientas para ayudar a obtener fondos de cuentas adquiridas ilícitamente, lo que incluye transferencias de dinero y el cobro a cuentas a través de sitios de comercio electrónico controlados por un proveedor de servicios ilegal (Holt y otros, 2016). Algunos *hackers* también utilizan los llamados círculos de mulas de dinero (o *money mule rings*), donde contratarán a terceros desprevenidos para cobrar cheques o aceptar transferencias electrónicas. Luego se les puede pedir que compren productos y los envíen a otra parte o simplemente que envíen los fondos a través de otra transferencia bancaria (Holt y Lampke, 2010; Leukfeldt y otros, 2017).

Una vez que un posible cliente accede a un anuncio, se pondrá en contacto con el vendedor a través de varias plataformas, desde el correo electrónico hasta sistemas de mensajería instantánea (Franklin y otros, 2007; Holt y Lampke, 2010; Holt y otros, 2016; Motoyama y otros, 2011). Luego negociará la cantidad de producto que desea comprar, o aceptará los términos del servicio, y determinará el precio final de dicho producto. Se espera entonces que el comprador ejecute el pago de inmediato, generalmente a través de medios electrónicos como WebMoney, aunque las criptomonedas como BitCoin se están volviendo cada vez más comunes (Smirnova y Holt, 2017).

El aumento de las criptomonedas, que hace referencia al hecho de que los pagos y la información de transferencia están encriptados, lo que dificulta la identificación de las partes en cualquier lado de la transacción, está relacionado con un mayor uso de herramientas TOR y Dark Web (Barratt, 2012; Smirnova y Holt, 2017). Un pequeño número de proveedores también asegura acep-

tar pagos a través de Western Union y MoneyGram, aunque estos servicios de transferencia bancaria aumentan el riesgo de detección porque los fondos a menudo tienen que recaudarse en persona (Holt y Lampke, 2010; Motoyama y otros, 2011). Como resultado, los participantes suelen utilizar pagos electrónicos para reducir su exposición general a los espacios físicos y a los agentes de la policía.

Una vez que se realiza el pago, se espera que el vendedor cumpla con el final de la transacción. No hay garantía de que el vendedor se presente, lo que supone un gran riesgo para los posibles compradores (Holt, Smirnova, Chua y Copes, 2016). Un vendedor podría renegar fácilmente de la transacción y no proporcionar ningún producto, o podría entregar datos o servicios de baja calidad que no son efectivos (Franklin y otros, 2007; Holt y Lampke, 2010). Para reducir el potencial de pérdida, los compradores en los mercados de datos utilizan estrategias que ayudan a determinar la legitimidad de un vendedor antes de realizar cualquier compra. Pueden leer los comentarios de otros en el foro o en la tienda, de manera similar a los comentarios proporcionados en sitios de comercio electrónico legales como Amazon (Holt y otros, 2016; Smirnova y Holt, 2017). Aquellos vendedores con comentarios o reseñas más positivas parecen más propensos a proporcionar productos de calidad, lo que aumentaría su número total de ventas en el mercado (Holt y otros, 2016).

Los compradores también pueden prestar atención al lenguaje utilizado en los anuncios de proveedores para poder determinar si proporcionarían un buen producto. Los proveedores que ofrecen múltiples puntos de contacto y señalan que están disponibles las 24 horas del día, o que tienen cuentas de correo electrónico o de mensajería instantánea dedicadas al servicio al cliente tienen más probabilidades de responder, incluso si hay problemas con la calidad de los datos o servicios (Holt y otros, 2016; Hutchings y Holt, 2017). Los vendedores que además detallan cómo cambian aquellos productos no funcionales o servicios deficientes también tienen más probabilidades de parecer fiables. Cuando se compran grandes cantidades de tarjetas de crédito o débito, es muy posible que algunas de las cuentas queden inactivas o cerradas por la institución financiera. Los vendedores que reconocen este riesgo y ofrecen a sus clientes formas de obtener reemplazos gratuitos tienen más probabilidades de recibir comentarios positivos y absorber una mayor parte del mercado (Holt y Lampke, 2010; Holt y otros, 2017).

No está claro cuántas personas participarían activamente en los mercados de datos robados como compradores o vendedores cada año (Holt y otros, 2016; Yip y otros, 2013). Unos pocos estudios estimaron las ganancias para los vendedores de *dumps* y números de tarjetas de crédito en una muestra de trece foros y descubrieron que pueden haber ganado cientos de miles de dólares o posiblemente millones, dependiendo de la cantidad de tarjetas vendidas (Holt y otros, 2016). La tasa de rentabilidad para los compradores de datos resultó ser similar, aunque hubo una mayor variabilidad debido a cuestiones sobre

funcionamiento real de los datos que compraron (Holt y otros, 2016). Como resultado, no se puede subestimar el mercado de datos robados, pues genera actividades de *phishing* y robo de datos que pueden venderse a otros en línea.

6. Victimización del *phishing* y del robo de identidad

Las razones por las que las personas pueden participar en el *phishing*, filtraciones de datos y mercados de datos robados son relativamente claras: ganancia monetaria y notoriedad entre *hackers* y ladrones de datos (Hutchings y Holt, 2015). Sin embargo, hay un número menor de estudios que tengan en cuenta los factores conductuales y actitudinales asociados a la pérdida de información a través del *phishing* o del fraude electrónico en general. El *phishing* y las filtraciones de datos parecen apuntar indiscriminadamente a las posibles víctimas potenciales, pues tratan de atacar al mayor número posible de personas al mismo tiempo. No obstante, existen algunos factores que están intrínsecamente asociados a la victimización. Aquellos que pasan más tiempo en línea participando en ciertas actividades, como consultar el correo electrónico, comprar y realizar operaciones bancarias, corren un mayor riesgo de victimización (Leukfeldt y Yar, 2016; Pratt y otros, 2010; Reyns, 2013; Reyns y Henson, 2016; van Wilsem, 2013). Las personas que participan en ciertas conductas en línea, como ver pornografía y descargar materiales pirateados, también tienen más probabilidades de denunciar casos de *phishing* (Ngo y Paternoster, 2011) y de robo de identidad (Bossler y Holt, 2009; Holt y Turner, 2012; Paek y Nalla, 2015).

Algunos estudios también han identificado una conexión entre algunas formas de victimización y el robo de identidad posterior. Reyns y Henson (2016) descubrieron que las personas que respondieron a un correo electrónico de *phishing* o que sufrieron un ataque pirata en su ordenador tenían más probabilidades de denunciar robos de identidad. Se observó una relación similar en un estudio de Holt y Turner (2012), lo que sugiere la necesidad de considerar hasta qué punto las herramientas de protección minimizan las infecciones de *malware* y piratería y pueden influir en el riesgo de sufrir un robo de identidad.

El uso de herramientas de software de protección y las habilidades técnicas también se confunden con el riesgo de robo de identidad.

> Por ejemplo, Holt y Turner (2012) encontraron que la presencia de software de protección disminuía la probabilidad de que una persona fuera víctima de robo de identidad. Sin embargo, la mayor parte de la literatura sobre infecciones de *malware* y software de protección no ha encontrado una relación consistente entre su uso y un menor riesgo de sufrir ataques por parte de *hackers* (Bossler y Holt, 2009; Holt y Bossler, 2013; Ngo y Paternoster, 2011). Estudios recientes también han encontrado que la alfabetización digital y la competencia informática pueden reducir el riesgo de responder a correos electrónicos de *phishing* (Arachchilage y Love, 2014; Graham y Triplett, 2017; Luga, Nurse y Erola, 2016).

También hoy existen muy pocas pruebas que demuestren que las personas con poco autocontrol tienen más probabilidades de ser víctimas de robo de identidad. Las personas que son impulsivas, cortas de mira y asumen riesgos no tienden a reconocer los daños potenciales a los que se exponen mientras

están en línea. Son más proclives a participar en malas conductas en línea y a responder correos electrónicos fraudulentos y otras solicitudes que aumentan su riesgo de victimización. Por ello, el bajo autocontrol se correlaciona con la victimización por piratería (Bossler y Holt, 2010; van Wilsem, 2013), con los comportamientos arriesgados de compra en línea (Holtfreter y otros, 2015) y con el fraude en subastas y la victimización por robo de identidad (Kerstens y Janse, 2016; van Wilsem, 2013). También hay pruebas contradictorias de que el bajo autocontrol está asociado con los ataques de *phishing* (De Kimpe y otros, 2018; Ngo y Paternoster, 2011). Por lo tanto, existen varios factores que pueden explicar el riesgo de sufrir robo de identidad a través de diversos medios electrónicos. Un análisis más detallado del asunto es fundamental para mejorar nuestra comprensión de estos factores de riesgo y aumentar el acceso a herramientas y a campañas de concienciación que puedan ayudar a reducir la probabilidad de victimización.

Resumen

En conjunto, el crecimiento de la tecnología no solo ha creado oportunidades únicas para cometer delitos, sino que también ha establecido una economía completamente nueva asociada al uso indebido de información personal. La creatividad que los *hackers* maliciosos demuestran cuando intentan atacar el hardware y el software de un ordenador resulta también evidente en su capacidad para obtener ganancias de sus actividades. El crecimiento de los mercados de datos robados demuestra la profesionalidad de la comunidad de *hackers* y sugiere que sus acciones evolucionarán sin duda con nuestro uso y dependencia de diversas tecnologías. Además, el alcance de este mercado ilegal puede ser la razón por la que las filtraciones e intrusiones de datos continúan aumentando año tras año. Por lo tanto, la policía y los fiscales deben encontrar formas de desmantelar de manera más agresiva estos mercados y detener el flujo de información robada en línea.

Bibliografía

Allison, S. F. H.; Schuck, A. M.; Learsch, K. M. (2005). «Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics». *Journal of Criminal Justice* (núm. 33, págs. 19-29).

APWG (2018). *Phishing Activity Trends Report* (primer trimestre) [en línea]. <http://docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf>

Arachchilage, N. A. G.; Love, S. (2014). «Security awareness of computer users: A phishing threat avoidance perspective». *Computers in Human Behavior* (núm. 38, págs. 304-312).

Barratt, M. J. (2012). «SILK ROAD: EBAY FOR DRUGS: The journal publishes both invited *Addiction* (vol. 107, núm. 3, pág. 683).

Benjamin, V., Li, W., Holt, T.; Chen, H. (mayo de 2015). «Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops». En: *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)* (págs. 85-90). IEEE.

Bossler, A. M.; Holt, T. J. (2009). «On-line activities, guardianship, and malware infection: An examination of routine activities theory». *International Journal of Cyber Criminology* (núm. 3, págs. 400-420).

Bossler, A. M.; Holt, T. J. (2010). «The effect of self-control on victimization in the cyberworld». *Journal of Criminal Justice* (vol. 38, núm. 3, págs. 227-236).

Burgos, M. (22 de noviembre de 2018). «Authorities discover high amount of skimmers across state of Florida in 2018» [en línea]. *ABC News*. <https://www.abcactionnews.com/news/authorities-discover-high-amount-of-skimmers-across-state-of-florida-in-2018>

De Kimpe, L.; Walrave, M.; Wim, H.; Pauwels, L.; Ponnet, K. (2018). «You've got Mail! Explaining individual differences in becoming a phishing target». *Telematics and Informatics*. 10.1016/j.tele.2018.02.009.

Dunn, J. E. (2012). «Russia cybercrime market doubles in 2011, says report» [en línea]. *IT World Today*. <www.itworld.com/security/272448/russia-cybercrime-market-doubles-2011-says-report>

Dupont, B.; Côté, A. M.; Boutin, J. I.; Fernandez, J. (2017). «Darkode: Recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world"». *American Behavioral Scientist* (vol. 61, núm. 11, págs. 1219-1243).

ENISA (2017). *Threat Landscape Report 2016 - 15 Top Cyber-Threats and Trends* [en línea]. European Union Agency for Network and Information Security. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016>

Franklin, J.; Paxson, V.; Perrig, A.; Savage, S. (2007). «An inquiry into the nature and cause of the wealth of internet miscreants». *CCS07* (29 de octubre-2 de noviembre, Alexandria, VA).

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. Boston: Addison-Wesley.

Graham, R.; Triplett, R. (2017). «Capable guardians in the digital environment: the role of digital literacy in reducing phishing victimization». *Deviant Behavior* (vol. 38, núm. 12, págs. 1371-1382).

Holt, T. J. (2013). «Exploring the social organisation and structure of stolen data markets». *Global Crime* (vol. 14, núms. 2-3, págs. 155-174).

Holt, T. J.; Bossler, A. M. (2013). «Examining the relationship between routine activities and malware infection indicators». *Journal of Contemporary Criminal Justice* (vol. 29, núm. 4, págs. 420-436).

Holt, T. J.; Lampke, E. (2010). «Exploring stolen data markets on-line: Products and market forces». *Criminal Justice Studies* (núm. 23, págs. 33-50).

Holt, T. J.; Smirnova, O.; Chua, Y. T. (2016). *Data thieves in action: Examining the international market for stolen personal information*. Nueva York: Springer.

Holt, T. J.; Smirnova, O.; Chua, Y. T.; Copes, H. (2015). «Examining the risk reduction strategies of actors in online criminal markets». *Global Crime* (vol. 16, núm. 2, págs. 81-103).

Holt, T. J.; Turner, M. G. (2012). «Examining risks and protective factors of on-line identity theft». *Deviant Behavior* (vol. 33, núm. 4, págs. 308-323).

Holtfreter, K.; Reisig, M. D.; Pratt, T. C.; Holtfreter, R. E. (2015). «Risky remote purchasing and identity theft victimization among older Internet users». *Psychology, Crime & Law* (vol. 21, núm. 7, págs. 681-698).

Honeynet Research Alliance (2003). «Profile: Automated Credit Card Fraud» [en línea]. *Know Your Enemy paper series*. <http://old.honeynet.org/papers/profiles/cc-fraud.pdf>

Hutchings, A.; Holt, T. J. (2015). «A crime script analysis of the online stolen data market. *British Journal of Criminology* (vol. 55, núm. 3, págs. 596-614).

Hutchings, A.; Holt, T. J. (2017). «The online stolen data market: disruption and intervention approaches». *Global Crime* (vol. 18, núm. 1, págs. 11-30).

Iuga, C.; Nurse, J. R.; Erola, A. (2016). «Baiting the hook: factors impacting susceptibility to phishing attacks». *Human-centric Computing and Information Sciences* (vol. 6, núm. 1, pág. 8).

James, L. (2005). *Phishing Exposed*. Rockland: Syngress.

Kerstens, J.; Janse, J. (2016). «The victim-perpetrator overlap in financial cybercrime: Evidence and reflection on the overlap of youth's online victimization and perpetration». *Deviant Behavior* (núm. 37, págs. 585-600).

Krebs, B. (14 de mayo de 2014). «The Target Breach, By the Numbers. Krebs on Security» [en línea]. <https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/>

Krebs, B. (19 de marzo de 2019). «Insert Skimmer and Camera Cover PIN Stealer» [en línea]. *Krebs on Security* <https://krebsonsecurity.com/2019/03/insert-skimmer-camera-cover-pin-stealer/>

Lastdrager, E. E. H. (2014). «Achieving a consensual definition of phishing based on a systematic review of the literature». *Crime Science* (vol. 3, núm. 9, págs. 1-6).

Lemos, R. (29 de octubre de 2004). «Secret Service busts suspected ID fraud ring» [en línea]. <https://www.cnet.com/news/secret-service-busts-suspected-id-fraud-ring/>

Leukfeldt, E. R.; Kleemans, E. R.; Stol, W. P. (2017). «Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis». *Crime, Law and Social Change* (vol. 67, núm. 1, págs. 39-53).

Leukfeldt, E. R.; Yar, M. (2016). «Applying routine activity theory to cybercrime: A theoretical and empirical analysis». *Deviant Behavior* (vol. 37, núm. 3, págs. 263-280).

Martin, J. (2014). «Lost on the Silk Road: Online drug distribution and the "cryptomarket"». *Criminology & Criminal Justice* (vol. 14, núm. 3, págs. 351-367).

Motoyama, M.; McCoy, D.; Levchenko, K.; Savage, S.; Voelker, G. M. (2011). «An analysis of underground forums». En: *Proceedings of the 2011 ACM SIGCOMM Internet Measurement Conference* (págs. 71-79).

Myers, S. (2006). «Introduction to Phishing». En: M. Jakobsson; S. Myers (eds.). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. John Wiley & Sons.

Newman, G.; Clarke, R. (2003). *Superhighway robbery: Preventing e-commerce crime*. Portland, Oregon: Willan Publishing.

Ngo, F. T.; Paternoster, R. (2011). «Cybercrime Victimization: An examination of Individual and Situational level factors». *International Journal of Cyber Criminology* (vol. 5, núm. 1, págs. 773-793).

Paek, S. Y.; Nalla, M. K. (2015). «The relationship between receiving phishing attempt and identity theft victimization in South Korea». *International Journal of Law, Crime and Justice* (vol. 43, núm. 4, págs. 626-642).

Ponemon Institute (2018). *2018 Cost of Data Breach Study: Impact of Business Continuity Management* [en línea]. Traverse City, MI: IBM. <https://www.ibm.com/downloads/cas/AEJYBPWA>

Pratt, T. C.; Holtfreter, K.; Reisig, M. D. (2010). «Routine online activity and internet fraud targeting: Extending the generality of routine activity theory». *Journal of Research in Crime and Delinquency* (vol. 47, núm. 3, págs. 267-296).

Reyns, B. W. (2013). «Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses». *Journal of Research in Crime and Delinquency* (vol. 50, núm. 2, págs. 216-238).

Reyns, B. W.; Henson, B. (2016). «The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory». *International Journal of Offender Therapy and Comparative Criminology* (vol. 60, núm. 10, págs. 1119-1139).

Smirnova, O.; Holt, T. J. (2017). «Examining the Geographic Distribution of Victim Nations in Stolen Data Markets». *American Behavioral Scientist* (vol. 61, núm. 11, págs. 1403-1426).

Wilsem, J. V. (2013). «Hacking and harassment – Do they have something in common? Comparing risk factors for online victimization». *Journal of Contemporary Criminal Justice* (vol. 29, núm. 4, págs. 437-453).

Wall, D. S. (2001). «Cybercrimes and the Internet». En: D. S. Wall (ed.). *Crime and the Internet* (págs. 1-17). Nueva York: Routledge.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Wang, W. (2003). *Steal This Computer Book 3: What They Don't Tell You About the Internet*. No Starch Press.

Wilson, M. D. (18 de noviembre de 2018). «Flood of credit card skimmers results in few arrests, police say» [en línea]. *Statesman*. <https://www.statesman.com/news/20181118/flood-of-credit-card-skimmers-results-in-few-arrests-police-say>

Yip, M.; Webber, C.; Shadbolt, N. (2013). «Trust among cybercriminals? Carding forums, uncertainty and implications for policing». *Journal of Policing and Society* (núm. 23, págs. 516-525).