El *carding* i el robatori de dades

PID_00269715

Thomas Holt

Temps mínim de dedicació recomanat: 2 hores

Universitat Oberta de Catalunya

Thomas Holt

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats pel professor: Marc Balcells Magrans (2019)

Primera edició: setembre 2019

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

Índex

Introducció

Les amenaces tècniques plantejades pels *hackers* i els creadors de programari maliciós són clares i presenten grans riscos per a la seguretat de les dades personals i les xarxes informàtiques. Mentre que alguns *hackers* tan sols volen tenir accés als sistemes per provar un nou mètode d'atac, d'altres busquen accedir-hi per dur a terme un atac informàtic. De fet, la quantitat de dades personals financeres i d'identitat allotjada en servidors, ordinadors portàtils i dispositius mòbils connectats a internet converteix aquestes dades en objectius d'atacs informàtics. El desenvolupament de llocs web de comerç electrònic i banca en línia també va simplificar el procés d'ús d'informació personal per obtenir guanys financers.

Com a conseqüència, l'amenaça de frau cibernètic en funció de la ciberintrusió ara és constant. Els atacs que condueixen a la pèrdua d'informació personal confidencial han augmentat l'última dècada, i les principals empreses, governs i organitzacions són les afectades, especialment als Estats Units i la Unió Europea (Ponemon Institute, 2019). El desenvolupament de programari maliciós (*malware*) i d'eines de registre de tecles dissenyades per adquirir subreptíciament noms d'usuari i contrasenyes confidencials també ha facilitat que els pirates informàtics recopilin més informació que pot ser utilitzada per una persona o, fins i tot, un petit grup de persones (Holt, 2013). En lloc de permetre que una bona informació romangui inactiva, els *hackers* més emprenedors han monetitzat les dades personals que es poden fer servir per frau i robatori. En alguns aspectes, aquesta dinàmica és similar a la que s'observa en els mercats de *malware* (vegeu el mòdul 2): la gent ha trobat formes de rebre pagaments per les seves habilitats i experiència en el *hacking* pel que fa a aquells que poden no tenir el mateix coneixement, però entenen el que es pot fer amb tal informació personal.

Aquest mòdul proporciona una descripció general de diverses formes de robatori derivades dels actes de ciberintrusió. A més, se centrarà en el *phishing* i en la filtració de dades, així com en el seu vincle amb el mercat negre de compra i venda d'informació piratejada més freqüent. Finalment, hi ha un comentari sobre les característiques de la suplantació i del robatori d'identitat en línia per entendre les dimensions inherentment humanes dels ciberdelictes.

1. Mètodes d'obtenció il·legal de dades

Els ciberdelinqüents poden obtenir informació confidencial per cometre robatoris d'identitat de diverses maneres.

> Per exemple, els delinqüents que estan disposats a córrer el risc de ser identificats en l'espai físic poden utilitzar un dispositiu anomenat *skimmer*, dissenyat per capturar dades de targetes de crèdit i dèbit en caixers automàtics, terminals de punts de venda i altres llocs.

Malgrat que els *skimmers* poden presentar diverses formes, totes inclouen un petit lector electrònic que pot tenir forma de ranura i que permet que una targeta passi pel dispositiu (Holt i Lampke, 2010; Krebs, 2019). El lector enregistra la informació emmagatzemada a la banda magnètica que hi ha a la part posterior de la targeta de crèdit o dèbit a mesura que es mou per mitjà de la ranura. Aquesta informació queda retinguda a la memòria interna del dispositiu i posteriorment és recuperada pel delinqüent, accedint físicament al dispositiu o capturant-lo sense fil (Krebs, 2019).

En qualsevol cas, els *skimmers* ofereixen als delinqüents informació valuosa sobre el consumidor que pot ser utilitzada pels delinqüents o venuda a qualsevol persona interessada amb la finalitat d'obtenir guanys.

> Cada any es fan diversos arrestos relacionats amb l'ús de *skimmers* en el robatori d'identitat (vegeu Burgos, 2018). En alguns casos es va observar que alguns delinqüents utilitzaven els detalls financers obtinguts (Krebs, 2019; Rogoway, 2019), mentre que d'altres aconsegueixen escapar-se de la policia i només es poden identificar i destruir els seus dispositius (Wilson, 2018).

L'ús de dispositius físics com els *skimmers* demostra que els cibercriminals troben estratègies enginyoses per obtenir informació de valor. No obstant això, els delinqüents poden intentar obtenir informació financera dels consumidors amb formes molt més comunes i menys arriscades. De fet, un dels mètodes més habituals s'adreça específicament a individus, mentre que l'altre afecta grans organitzacions i els consumidors individuals. Tots dos mètodes poden generar quantitats d'informació personal enormes, que poden utilitzar-se o vendre a parts interessades i que generalment tenen un paper important en el cibercrim.

2. Correus *phishing*

Una de les tècniques més reeixides per obtenir informació personal i detalls financers en la història dels *hackers* consisteix en la manipulació basada en el correu electrònic.

En concret, els pirates informàtics van desenvolupar una tècnica anomenada *phishing*, un neologisme derivat en part de la noció de *phreaking* (vegeu el mòdul 2) i del terme *pesca* (en anglès, *fishing,*) d'informació (James, 2005; Lastdrager, 2014). El *phishing* suposa un intent d'enganyar els usuaris perquè proporcionin a l'atacant, o *phisher*, informació valuosa a partir d'alguna falsa amenaça (Myers, 2006).

Encara que el *phishing* sigui una amenaça moderna, en realitat és una metodologia força antiga, nascuda als anys noranta, quan la majoria dels proveïdors de serveis d'internet (ISP) cobraven als seus usuaris per hora. Un dels proveïdors més grans dels Estats Units aleshores era America Online (AOL), i els seus clients podien pagar per avançat cada mes. Aquells *hackers* emprenedors que no volien emprar les seves connexions a internet per buscar i piratejar sistemes van començar a atacar els clients d'AOL per accedir als seus comptes i poder utilitzar internet de manera gratuïta (Wang, 2003). Els atacants rastrejaven els llocs web i perfils d'AOL per obtenir adreces de correu electrònic i després enviaven correus en què s'al·legava que la informació del compte era incorrecta o que calia que fos validada. Els remitents sol·licitaven que el destinatari els proporcionés tant el nom d'usuari com la contrasenya. Al seu torn, els estafadors retenien la informació del compte i la feien servir en benefici propi o intercanviaven els detalls de l'usuari amb d'altres com a moneda de canvi (Wang, 2003). De fet, aquest concepte esdevingué tan popular que els *hackers* van començar a crear eines per obtenir noms d'usuari i contrasenyes de manera fraudulenta. Una de les més antigues i populars es deia AOHell, que feia mofa de l'ús de serveis AOL i que presentava eines per enviar *spam* als usuaris i administrar les seves contrasenyes i altres tipus d'informacions confidencials (Wang, 2003).

A mesura que internet i les eines de comerç electrònic anaven creixent a finals dels anys noranta i principis del segle XXI, els pirates informàtics van començar a atacar aquests sistemes amb tècniques similars. Els mercats clandestins van començar a vendre llistes de *spam* amb adreces de correu electrònic extretes d'internet per crear una població de possibles víctimes d'estafes (Holt, 2013). Aquestes llistes de correu electrònic podrien emprar-se al costat de *malware* de *botnet* per difondre ràpidament missatges de *phishing* (Holt, 2013).

El correu electrònic és la plataforma preferida per a la suplantació d'identitat (*phishing*), ja que el remitent pot fer servir diverses eines per enganyar el destinatari i fer-li creure que la sol·licitud ve d'un proveïdor legítim, sobretot en el cas dels serveis financers.

El llenguatge utilitzat en els correus electrònics de *phishing* sovint suggereix a la víctima que el compte del destinatari ha estat atacat o que hi ha un problema que pot fer que el compte quedi inactiu (James, 2005). En general, aquests missatges empren un llenguatge especial per suggerir que el problema és urgent i que requereix una resposta ràpida del destinatari si vol garantir que no hi hagi interrupcions de serveis (Myers, 2006).

La majoria dels missatges utilitzen nombroses eines i tècniques enganyoses per augmentar la probabilitat de respostes. Els millors *phishers* combinen aquests correus electrònics, que sembla que s'originin d'un proveïdor de serveis legítim, amb logotips i marques que corresponen al servei que estan imitant. Els *phishers* també proporcionen al destinatari enllaços web aparentment legítims perquè aquest faci clic i l'atacant pugui administrar d'aquesta manera el seu compte. La URL real i l'allotjament web de la pàgina redirigeixen a una pàgina web controlada per l'estafador, que pot trobar-se en un servei il·lícit que no revelarà les intencions del *hacker*. La pàgina web i el contingut poden crear-se mitjançant l'ús de *kits* de *phishing*, que presenten diferents logotips, imatges, marques i idioma web per reflectir de la manera més fidel possible el lloc original (James, 2005). Se sol demanar a l'usuari que introdueixi el nom, la contrasenya i més informació confidencial, com ara el número de compte i el d'identificació personal o PIN del compte. Un cop introduïdes les dades, es desen al servidor perquè el *phisher* hi accedeixi més tard, i la víctima és redirigida al lloc web original del proveïdor del servei, o agraeix al destinatari que li hagi proporcionat la informació (James, 2005).

Les estafes de *phishing* continuen essent força comunes, i la majoria estan dirigides a sistemes de serveis financers i de pagament (APWG, 2018). Les estimacions suggereixen que hi ha centenars de milers d'estafes de *phishing* cada any (APWG, 2017; ENISA, 2017). Els webs que allotgen esquemes de *phishing* també poden trobar-se a tot el món, molts dels quals actuen als Estats Units, al Canadà, a Alemanya, a França i al Regne Unit (APWG, 2018). Com a conseqüència, s'estima que les empreses es gasten milions cada any en un intent de minimitzar l'impacte dels atacs de *phishing*, independentment que aquests acabin amb èxit o sense (Ponemon Institute, 2019).

3. Filtració de dades

A mesura que els llocs web de comerç electrònic i l'ús de xarxes socials presenten cada cop més informació sobre el consumidor, que s'emmagatzema en bases de dades a gran escala connectades a internet, els *hackers* redirigeixen els esforços a aquests recursos, especialment a registres bancaris, a la informació personal disponible i a un altre tipus d'informació confidencial (vegeu Allison i altres, 2005; Furnell, 2002; Newman i Clarke, 2003; Wall, 2001, 2007). Això inclou sistemes de processament de pagaments que poden estar allotjats en institucions financeres més grans, o fins i tot en terminals de punt de venda de botigues físiques. El *hacker* només cal que trobi una manera d'accedir a les parts internes i vulnerables d'una empresa o institució financera per accedir a un d'aquests repositoris de dades. Si tenen èxit, accediran a centenars de milers, sinó a milions, de dades amb informació confidencial que es poden monetitzar. L'èxit d'aquests compromisos s'evidencia en el fet que els delinqüents es dirigeixen regularment a aquestes institucions per explotar els seus recursos al màxim (Ponemon Institute, 2019).

En general, aquests incidents es reconeixen com a filtracions de dades, atès que una gran quantitat de dades provinents d'una organització s'identifica primer i és filtrada després pels *hackers* de manera il·legal. Una violació o pèrdua de dades pot produir-se com a resultat de diversos errors o atacs deliberats de persones dins i fora d'aquesta organització.

> Per exemple, si un treballador d'una institució deixa un ordinador portàtil o un disc dur amb informació confidencial en un taxi o en un restaurant, d'altres poden obtenir aquesta informació. De la mateixa manera, si la informació confidencial s'envia inadvertidament per correu electrònic a altres persones alienes a l'organització, llavors les dades es podrien considerar perdudes. Aquests incidents sovint s'anomenen errors de «factor humà» en els informes de l'Institut Ponemon, ja que la informació es perd per un error o un descuit humà.

No obstant això, els *hackings* són principalment la causa de les filtracions de dades, independentment que provinguin d'atacants interns o externs. Com es va assenyalar en el mòdul 2, els *hackers* infiltrats difereixen dels externs en la seva fiabilitat dins d'una organització. Els infiltrats poden participar en diferents mètodes d'atac, com ara l'ús de programari maliciós per suprimir les dades confidencials o alliberar-les a través de mitjans públics. Al mateix temps, els atacants externs podrien fer-se passar per agents interns de confiança mitjançant l'ús de credencials obtingudes de manera fraudulenta.

Target

El 2013 una filtració important a la cadena de botigues nord-americana Target va provocar la pèrdua de quaranta milions de registres de targetes de crèdit i dèbit de clients en menys de trenta dies (Krebs, 2014). Diversos *hackers* externs van identificar i robar a un proveïdor de serveis extern, Fazio Mechanical. La companyia va proporcionar manteniment de calefacció i refrigeració a les botigues Target i va rebre pagaments pels seus

serveis. Per tant, els atacants van utilitzar les credencials d'usuari de Fazio per accedir i interaccionar amb el portal en línia del pagament de proveïdors de Target.

Quan els atacants van accedir a la xarxa interna de Target, van obtenir informació confidencial provinent de diverses parts dels sistemes del minorista. Per exemple, els clients que van comprar pel lloc web de la companyia van perdre els noms, els números de telèfon, els correus electrònics i les adreces postals durant l'atac. A més, els atacants van col·locar programari maliciós en els terminals de punts de venda de certes botigues, la qual cosa els va permetre adquirir milions de números de targetes de crèdit i dèbit mentre la informació s'enviava del registre al processador de pagaments (Krebs, 2014). Es creu que els atacants podrien haver venut entre un i tres milions dels comptes que van robar, cosa que va poder generar més de cinquanta milions de dòlars en guanys (Krebs, 2014). No obstant això, les institucions financeres que van haver d'emetre i administrar de nou els comptes de les targetes atacades es van gastar, aproximadament, dos-cents milions de dòlars per evitar danys majors als seus clients (Krebs, 2014). Per tant, el dany econòmic causat per les filtracions de dades no es pot subestimar.

4. Robatori de dades i mercats de *carding*

Els mètodes que utilitzen els pirates informàtics i els ciberdelinqüents per obtenir enormes quantitats d'informació confidencial plantegen un desafiament: com explotar al màxim aquesta informació valuosa. Encara que un atacant pugui reunir milions de targetes de crèdit i dèbit i que intenti fer nombroses transaccions, no podrà utilitzar-ho amb efectivitat. Fins i tot si hi participessin diversos atacants i provessin d'analitzar les dades de la mateixa manera, continuarien tenint massa informació. A més, les dades tenen una vida útil limitada perquè les institucions financeres poden intentar tancar comptes afectats per *phishing* o filtracions de dades per minimitzar el potencial d'aquestes transaccions fraudulentes (Holt i Bossler, 2016).

Per obtenir el màxim rendiment econòmic de les dades adquirides, els ciberdelinqüents han començat a monetitzar la informació piratejada venent-la a d'altres, tant en mercats oberts com tancats, que es troben a internet. Aquests mercats permeten als compradors adquirir targetes de crèdit, informació de serveis financers i eines de frau cibernètic a canvi d'una tarifa, independentment del nivell d'habilitat informàtica o del seu coneixement sobre pirateria i frau (Franklin i altres, 2007; Holt i Lampke, 2010; Motoyama i altres, 2011). Amb tot, l'expansió d'aquests mercats pot suposar un augment de la demanda d'informació robada i de les eines de cibercrim. Això pot incrementar el *hacking* i les filtracions de dades, així com el nombre d'atacs, per proporcionar a aquests mercats un subministrament adequat de dades i béns (Hutchings i Holt, 2017).

Alguns d'aquests mercats de dades robades es van observar per primera vegada als canals d'internet Relay Chat, o IRC, on els *hackers* venien les dades obtingudes per *phishing* i pirateria (Benjamin, Li, Holt i Chen, 2015; Franklin i altres, 2007; Honeynet Project, 2003). Aquestes comunitats estaven altament controlades, disposaven de molt poca informació sobre les identitats dels atacants involucrats. Encara que això pugui semblar beneficiós, va reduir la mida general del mercat i va limitar les oportunitats econòmiques per als venedors. Com a resultat, els *hackers* van començar a migrar cap a fòrums amb un públic potencial més gran (Benjamin i altres, 2015; Holt i Lampke, 2010). Amb aquesta migració va arribar un control superior per part de les forces de l'ordre, que van intentar infiltrar-s'hi per aturar aquests grups.

ShadowCrew

Un fòrum dirigit per un grup de *hackers* que es feien dir ShadowCrew fou eliminat per la policia el 2004 (Lemos, 2004). Arran de la investigació van arrestar 28 persones a tot el món per haver participat en el robatori i la venda de més d'1,7 milions de targetes de crèdit i dèbit, així com de dades i serveis relacionats (Lemos, 2004). L'arrest de ShadowCrew no va eliminar el mercat de dades robades, sinó que el va tornar difús i més com-

plex en termes de sofisticació operativa, per reduir així la probabilitat de ser investigades (Hutchings i Holt, 2017).

Actualment hi ha múltiples entorns que faciliten la mercantilització d'informació robada i el robatori d'identitat. Els mercats principals semblen existir en l'anomenada Open Web, aquella part de la World Wide Web a la qual es pot accedir per navegadors web tradicionals amb contingut que pot ser capturat per motors de cerca com Google (Dupont i altres, 2017; Holt i altres, 2016; Leukfeldt i altres, 2017; Smirnova i Holt, 2017; Yip i altres, 2013). Aquests llocs web funcionen i s'allotgen a tot el món, encara que molts sembla que es creïn a Rússia, als Estats Units i en diverses parts d'Europa (Dunn, 2012; Holt i altres, 2016; Hutchings i Holt, 2015). Molts d'aquests webs funcionen com a fòrums, una forma de comunicació intervinguda per ordinador que permet que els usuaris es connectin i discuteixin els seus recursos i necessitats (Holt, 2013). Els fòrums estan compostos de fils, que s'inicien quan un individu crea una publicació en què descriu un producte o servei, fa una pregunta, dona una opinió o simplement comparteix experiències passades. D'altres responen a la publicació inicial amb les seves publicacions per crear un fil i mantenir així una conversa o diàleg (Holt i altres, 2016).

Els fòrums que operen com a mercats de dades tenen una estructura específica, ja que els participants poden crear fils únicament per vendre els seus productes o sol·licitar un tipus de dades no tan comú. Els venedors que creen fils expliquen el que tenen en venda, el preu de les dades, les regles de les vendes, com cal pagar i les formes en què els compradors poden comunicar-se amb compradors potencials (Hutchings i Holt, 2015; Smirnova i Holt, 2017). Els possibles clients poden crear publicacions dins el fil per fer preguntes sobre els productes dels venedors o descriure la seva experiència amb el venedor en cas que hagin completat una transacció (Holt i Lampke, 2010; Holt i altres, 2016). En realitat, les vendes es duen a terme fora del fòrum per ocultar la trobada i reduir la quantitat d'informació sobre l'intercanvi que pugui fer-se pública (vegeu, per exemple, Holt i Lampke, 2010).

Alguns fòrums també presenten un cert grau de gestió per regular les transaccions i parar els peus a aquells venedors sense escrúpols que busquin enganyar els compradors (Dupont i altres, 2017; Holt i Lampke, 2010). Aquests gerents exerceixen rols específics, com ara moderadors o administradors, i poden prendre mesures per influir en el comportament dels usuaris en prohibir o bloquejar aquells participants fora de control (Holt, 2013). A més, aquells fòrums ben administrats també poden prendre mostres dels productes i revisar-los perquè els possibles compradors puguin avaluar-ne la qualitat (Holt, 2013; Hutchings i Holt, 2015).

Els últims anys, els proveïdors han passat de fòrums a botigues d'un sol operador, llocs web administrats per un proveïdor individual per anunciar directament els seus productes i serveis als clients (Martin, 2014; Smirnova i Holt, 2017). Les botigues ofereixen un espai publicitari alternatiu sense la supervisió dels moderadors del fòrum, tot i que els proveïdors han de trobar solucions

creatives per atraure clients potencials sense recórrer a la promoció en els fils del fòrum. En qualsevol cas, les botigues són similars als fòrums, ja que el venedor publica els productes, els preus i els mètodes de lliurament i pagament (Smirnova i Holt, 2017). Els possibles clients també poden trobar difícil determinar la legitimitat dels proveïdors, ja que aquests poden no proporcionar comentaris sobre productes o *feedback* que s'hagi publicat en fòrums. Per tant, els compradors acceptarien un grau de risc més gran en tractar amb venedors en botiga en comparació amb aquells que s'anuncien en fòrums (Smirnova i Holt, 2017).

A més de l'Open Web també hi ha botigues i fòrums de dades en l'anomenada Dark Web, aquella part d'internet que utilitza l'encriptació per ocultar informació (Barratt, 2012; Office of Public Affairs, 2017; Smirnova i Holt, 2017). La Dark Web depèn d'un servei anomenat The Onion Router (TOR), un programa gratuït que consisteix en un conjunt únic de protocols d'encriptació que posa en funcionament el trànsit web d'un individu a través dels ordinadors d'altres usuaris de TOR a la xarxa (Barratt, 2012; Martin, 2014). Com a conseqüència, és difícil identificar la ubicació i la identitat de qualsevol que faci servir el servei, així com la localització física de qualsevol lloc web o servei allotjat en TOR, per la qual cosa és complicat desconnectar-los (Barratt, 2012; Smirnova & Holt, 2017).

La Dark Web no només oculta informació sobre l'usuari, sinó que també és útil per ocultar el contingut dels mercats i productes il·lícits. Concretament, el contingut dels llocs de la Dark Web no pot ser indexat pels motors de cerca tradicionals com Google (Barratt, 2012). A més, les persones només poden accedir a llocs web basats en TOR mitjançant l'ús del navegador web integrat de TOR. Qualsevol altre navegador de l'Open Web, com ara Chrome o Internet Explorer, no podrà accedir al contingut. Per tant, TOR s'està convertint ràpidament en una poderosa eina perquè els ciberdelinqüents redueixin el risc de detecció.

5. Productes i serveis en els mercats de dades

Examinar el contingut dels mercats de dades robades demostra que els ciberdelinqüents obtenen diversos materials mitjançant formes diferents de pirateria i robatori digital.

Els productes més venuts inclouen comptes de targetes de crèdit i dèbit, que els venedors i compradors anomenen *dumps* (literalment, 'abocadors') (Franklin i altres, 2007; Holt i Lampke, 2010; Hutchings i Holt, 2015; Motoyama i altres, 2011). Independentment de si els productes es venen en fòrums o botigues, els venedors anuncien constantment el país d'origen dels *dumps* i els preus de cada tipus de targeta segons la localització. Això era evident en el llenguatge emprat per una botiga de dades en l'Open Web, que va indicar els preus per a diversos productes:

Llista de preus de *dumps*

DUMPS 101 DELS ESTATS UNITS

- Visa Clàssica / MC Standard = 25 $
- Visa Or, Platinum / MC Or, Platinum = 35 $
- Visa Negocis, Corporativa / MC Negocis, Corporativa = 40 $
- Visa Compres, Signature / MC Compres, World = 45 $
- Amex Platinum = 35 $
- Discover = 25 $

DUMPS D'EUROPA (REGNE UNIT - ALEMANYA - FRANÇA - ESPANYA - ITÀLIA - PAÏSOS BAIXOS - SUÏSSA)

101

- Visa Clàssica / MC Standard = 35 $
- Visa Or, Platinum / MC Or, Platinum = 45 $
- Visa Negocis, Corporativa / MC Negocis, Corporativa = 50 $
- Visa Compres, Signature / MC Compres, World = 55 $
- Amex Platinum = 45 $

201

- Visa Clàssica / MC Standard = 30 $
- Visa Or, Platinum / MC Or, Platinum = 40 $
- Visa Negocis, Corporativa / MC Negocis, Corporativa = 45 $
- Visa Compres, Signature / MC Compres, World = 50 $

CONTACTE: hacktransfers@gmail.com - ICQ: 712705321

DUMPS INTERNACIONALS (AUSTRÀLIA - DUBAI - XINA - RÚSSIA - JAPÓ)

101

- Visa Clàssica / MC Standard = 45 $
- Visa Or, Platinum / MC Or, Platinum = 55 $
- Visa Negocis, Corporativa / MC Negocis, Corporativa = 60 $
- Visa Compres, Signature / MC Compres, World = 65 $
- Amex Platinum = 55 $

201

- Visa Clàssica / MC Standard = 40 $
- Visa Or, Platinum / MC Or, Platinum = 50 $
- Visa Negocis, Corporativa / MC Negocis, Corporativa = 55 $
- Visa Compres, Signature / MC Compres, World = 60 $

DUMPS DE SALDOS ELEVATS

101

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

NOTA: Els nostres *dumps* NO TENEN CONTROL REGIONAL, la qual cosa significa que funcionen en qualsevol punt de venda a ESCALA MUNDIAL - SENSE BLOQUEIG REGIONAL. En cas contrari, es farà una restitució instantània.

NOTA: Els *dumps* de SALDOS ELEVATS tenen una garantia de canvi de 2k-3k $ cada vegada. Qualsevol *dump* de saldo elevat que falli en aquest interval serà substituït.

Alguns proveïdors també ofereixen noms d'usuari i contrasenyes que poden emprar-se per accedir a comptes de PayPal i eBay, comptes bancaris i altres serveis financers (Holt i altres, 2016; Leukfeldt i altres, 2017). Aquests inicis de sessió són la clau per fer transferències de diners des del compte de la víctima a un de controlat pel comprador, i estafar així els titulars del compte (Holt i Lampke, 2010; Holt i altres, 2016; Motoyama i altres, 2010). Una part dels venedors també ofereix eines per ajudar a obtenir fons de comptes adquirits il·lícitament, la qual cosa inclou transferències de diners i el cobrament a comptes per mitjà de llocs web de comerç electrònic controlats per un proveïdor de serveis il·legal (Holt i altres, 2016). Alguns *hackers* també utilitzen els coneguts com a cercles de mules de diners (*money mule rings*), en què contracten tercers desprevinguts per cobrar xecs o acceptar transferències electròniques. Després se'ls pot demanar que comprin productes i que els enviïn a un altre lloc o, simplement, que enviïn els fons a través d'una altra transferència bancària (Holt i Lampke, 2010; Leukfeldt i altres, 2017).

Quan un possible client accedeix a un anunci, es posarà en contacte amb el venedor a través de diverses plataformes, des del correu electrònic fins a sistemes de missatgeria instantània (Franklin i altres, 2007; Holt i Lampke, 2010; Holt i altres, 2016; Motoyama i altres, 2011). Després negociarà la quantitat de producte que vol comprar, o acceptarà els termes del servei, i ha de determinar el preu final del producte. Aleshores s'espera que el comprador executi el pagament de manera immediata, generalment per mitjans electrònics com WebMoney, encara que les criptomonedes com bitcoin són cada vegada més comunes (Smirnova i Holt, 2017).

L'augment de les criptomonedes, que fa al·lusió al fet que els pagaments i la informació de transferència estan encriptats, de manera que dificulta la identificació de les parts en qualsevol banda de la transacció, està relacionat amb un ús més gran d'eines TOR i Dark Web (Barratt, 2012; Smirnova i Holt, 2017). Un petit nombre de proveïdors també accepta pagaments a través de Wes-

tern Union i MoneyGram, encara que aquests serveis de transferència bancària augmenten el risc de detecció perquè els fons sovint han de recaptar-se en persona (Holt i Lampke, 2010; Motoyama i altres, 2011). Com a resultat, els participants solen utilitzar pagaments electrònics per reduir la seva exposició general als espais físics i als agents de la policia.

Un cop fet el pagament, s'espera que el venedor compleixi el final de la transacció. No hi ha cap garantia que el venedor es presenti, la qual cosa suposa un gran risc per als possibles compradors (Holt, Smirnova, Chua i Copes, 2016). Un venedor podria renegar fàcilment de la transacció i no proporcionar cap producte, o podria lliurar dades o serveis de baixa qualitat que no són efectius (Franklin i altres, 2007; Holt i Lampke, 2010). Per reduir el potencial de pèrdua, els compradors en els mercats de dades utilitzen estratègies que ajuden a determinar la legitimitat d'un venedor abans de fer qualsevol compra. Poden llegir els comentaris d'altres al fòrum o a la botiga, de manera similar als comentaris proporcionats en pàgines web de comerç electrònic legals com Amazon (Holt i altres, 2016; Smirnova i Holt, 2017). Aquells venedors amb comentaris o ressenyes més positives semblen més propensos a fabricar productes de qualitat, la qual cosa en faria augmentar el nombre total de vendes en el mercat (Holt i altres, 2016).

Els compradors també poden prestar atenció al llenguatge utilitzat en els anuncis de proveïdors per poder determinar si proporcionarien un bon producte. Els proveïdors que ofereixen múltiples punts de contacte i assenyalen que estan disponibles les vint-i-quatre hores del dia, o que tenen comptes de correu electrònic o de missatgeria instantània dedicats al servei al client, tenen més probabilitats de respondre, fins i tot si hi ha problemes amb la qualitat de les dades o serveis (Holt i altres, 2016; Hutchings i Holt, 2017). Els venedors que, a més, detallen com canvien aquells productes no funcionals o serveis deficients també tenen més probabilitats de semblar fiables. Quan es compren grans quantitats de targetes de crèdit o de dèbit, és molt possible que alguns comptes quedin inactius o tancats per la institució financera. Els venedors que reconeixen aquest risc i ofereixen als clients formes d'obtenir reemplaçaments gratuïts tenen més probabilitats de rebre comentaris positius i d'absorbir una major part del mercat (Holt i Lampke, 2010; Holt i altres, 2017).

No queda clar quantes persones participaren activament en els mercats de dades robades com a compradores o venedores cada any (Holt i altres, 2016; Yip i altres, 2013). Tan sols alguns estudis van estimar els guanys per als venedors de *dumps* i números de targetes de crèdit en una mostra de tretze fòrums i van descobrir que podrien haver guanyat centenars de milers de dòlars o, probablement, milions, en funció de la quantitat de targetes venudes (Holt i altres, 2016). La taxa de rendibilitat per als compradors de dades va ser similar, tot i que hi hagué una variabilitat més gran a causa de qüestions sobre funciona-

ment real de les dades que van comprar (Holt i altres, 2016). Com a resultat, no es pot subestimar el mercat de dades robades, ja que genera activitats de *phishing* i robatori de dades que es poden vendre a altres en línia.

6. Victimització del *phishing* i del robatori d'identitat

Les raons per les quals les persones participen en el *phishing*, en filtracions de dades i en mercats de dades robades són relativament clares: guany monetari i notorietat entre *hackers* i lladres de dades (Hutchings i Holt, 2015). Amb tot, hi ha menys estudis que tinguin en compte els factors de conducta i actitud associats a la pèrdua d'informació a través del *phishing* o del frau electrònic en general. El *phishing* i les filtracions de dades sembla que apunten indiscriminadament les possibles víctimes potencials, ja que tracten d'atacar el màxim nombre de persones alhora. No obstant això, hi ha alguns factors que estan intrínsecament associats a la victimització. Aquells que passen més temps en línia participant en certes activitats, com ara consultant el correu electrònic, comprant i fent operacions bancàries, tenen un risc més elevat de victimització (Leukfeldt i Yar, 2016; Pratt i altres, 2010; Reyns, 2013; Reyns i Henson, 2016; Van Wilsem, 2013). Les persones que participen en determinades conductes en línia, com ara el consum de pornografia i la descàrrega de material piratejat, també tenen més probabilitats de denunciar casos de *phishing* (Ngo i Paternoster, 2011) i de robatori d'identitat (Bossler i Holt, 2009; Holt i Turner, 2012; Paek i Nalla, 2015).

Alguns estudis també han identificat que hi ha una relació entre algunes formes de victimització i el robatori d'identitat posterior. Reyns i Henson (2016) van descobrir que les persones que van respondre un correu electrònic de *phishing* o que van patir un atac de pirateria a l'ordinador tenien més probabilitats de denunciar robatoris d'identitat. Es va observar una relació semblant en un estudi de Holt i Turner (2012), la qual cosa suggereix la necessitat de considerar fins a quin punt les eines de protecció minimitzen les infeccions de programari maliciós i pirateria i poden influir en el risc de patir un robatori d'identitat.

L'ús d'eines de programari de protecció i les habilitats tècniques també es confonen amb el risc de robatori d'identitat.

> Per exemple, Holt i Turner (2012) van adonar-se que la presència de programari de protecció disminuïa la probabilitat que una persona fos víctima d'un robatori d'identitat. Amb tot, la majoria de la literatura sobre infeccions de programari maliciós i programari de protecció no ha trobat una relació consistent entre el seu ús i un risc inferior de patir atacs per part de *hackers* (Bossler i Holt, 2009; Holt i Bossler, 2013; Ngo i Paternoster, 2011). Alguns estudis recents també han destacat que l'alfabetització digital i la competència informàtica poden reduir el risc de respondre a correus electrònics de *phishing* (Arachchilage i Love, 2014; Graham i Triplett, 2017; Luga, Nurse i Erola, 2016).

Actualment, també hi ha molt poques proves que demostrin que les persones amb poc autocontrol tenen més probabilitats de ser víctimes d'un robatori d'identitat. Les persones que són impulsives, amb poques mires i que assumeixen riscos no tendeixen a reconèixer els danys potencials als quals s'exposen mentre estan en línia. Són més proclius a participar en males conductes en línia i a respondre correus electrònics fraudulents i altres sol·licituds que aug-

menten el risc de victimització. Per això, el baix autocontrol es correlaciona amb la victimització per pirateria (Bossler i Holt, 2010; Van Wilsem, 2013), amb els comportaments arriscats de compra en línia (Holtfreter i altres, 2015) i amb el frau en subhastes i la victimització per robatori d'identitat (Kerstens i Janse, 2016; Van Wilsem, 2013). També hi ha proves contradictòries del fet que el baix autocontrol està associat amb els atacs de *phishing* (De Kimpe i altres, 2018; Ngo i Paternoster, 2011). Per tant, hi ha diversos factors que poden explicar el risc de patir robatoris d'identitat per diversos mitjans electrònics. Una anàlisi més detallada del tema és fonamental per entendre millor aquests factors de risc i augmentar l'accés a eines i a campanyes de conscienciació que puguin ajudar a reduir la probabilitat de victimització.

Resum

En general, el creixement de la tecnologia no tan sols ha creat oportunitats úniques per cometre delictes, sinó que també ha establert una nova economia associada a l'ús indegut d'informació personal. La creativitat dels *hackers* maliciosos en intentar atacar el maquinari i el programari d'un ordinador també és evident en la seva capacitat per obtenir guanys de les activitats que duen a terme. El creixement dels mercats de dades robades demostra la professionalitat de la comunitat de *hackers* i posa de manifest que les seves accions anirant evolucionant, sens dubte, amb el nostre ús i la nostra dependència vers les diverses tecnologies. A més, l'abast d'aquest mercat il·legal pot ser la raó per la qual les filtracions i les intrusions de dades continuen augmentant cada any. Per tant, la policia i els fiscals han de trobar maneres de desmantellar més agressivament aquests mercats i aturar el flux d'informació robada en línia.

Bibliografia

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, pàg. 19-29).

APWG (2018). *Phishing Activity Trends Report* (primer trimestre) [en línia]. <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, pàg. 304-312).

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

Benjamin, V., Li, W., Holt, T.; Chen, H. (maig de 2015). «Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops». A: *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pàg. 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, pàg. 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, pàg. 227-236).

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

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

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

ENISA (2017). *Threat Landscape Report 2016 - 15 Top Cyber-Threats and Trends* [en línia]. 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 d'octubre-2 de novembre, 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, pàg. 1371-1382).

Holt, T. J. (2013). «Exploring the social organisation and structure of stolen data markets». *Global Crime* (vol. 14, núm. 2-3, pàg. 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, pàg. 420-436).

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

Holt, T. J.; Smirnova, O.; Chua, Y. T. (2016). *Data thieves in action: Examining the international market for stolen personal information*. Nova 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, pàg. 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, pàg. 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, pàg. 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, pàg. 596-614).

Hutchings, A.; Holt, T. J. (2017). «The online stolen data market: disruption and intervention approaches». *Global Crime* (vol. 18, núm. 1, pàg. 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, pàg. 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, pàg. 585-600).

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

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

Krebs, B. (19 de març de 2019). «Insert Skimmer and Camera Cover PIN Stealer» [en línia]. *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, pàg. 1-6).

Lemos, R. (29 d'octubre de 2004). «Secret Service busts suspected ID fraud ring» [en línia]. <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, pàg. 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, pàg. 263-280).

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

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

Myers, S. (2006). «Introduction to Phishing». A: M. Jakobsson; S. Myers (ed.). *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, pàg. 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, pàg. 626-642).

Ponemon Institute (2018). *2018 Cost of Data Breach Study: Impact of Business Continuity Management* [en línia]. 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, pàg. 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, pàg. 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, pàg. 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, pàg. 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, pàg. 437-453).

Wall, D. S. (2001). «Cybercrimes and the Internet». A: D. S. Wall (ed.). *Crime and the Internet* (pàg. 1-17). Nova 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 novembre de 2018). «Flood of credit card skimmers results in few arrests, police say» [en línia]. *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, pàg. 516-525).