Pirateria informàtica i ciberintrusió

PID_00269960

Thomas Holt

Temps mínim de dedicació recomanat: 4 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..... 5

1. Definició de *hacking*..... 7

2. Motivacions del *hacker*..... 11

3. Les correlacions demogràfiques, conductuals i actitudinals dels *hackers*..... 15

4. La subcultura *hacker*..... 20

5. La diferència entre *hackers* basada en el seu prestigi en línia i fora de línia..... 22

6. Les correlacions de la pirateria i de la victimització per *malware*..... 24

7. Història de la pirateria i el *malware*..... 27
7.1. Els començaments 27
7.2. Els anys setanta 28
7.3. Els anys vuitanta 30
7.4. Els anys noranta 32
7.5. Dels 2000 fins avui 35

Resum..... 38

Bibliografia..... 39

Introducció

Quan es pregunta al públic en general sobre els delictes cibernètics, se sol assenyalar els pirates informàtics com els causants d'aquestes infraccions (Furnell, 2002). Això es pot deure a les moltes dècades de cobertura mediàtica que vinculen els *hackers* amb tot un seguit d'atacs altament tècnics contra governs, corporacions i institucions financeres. Els *hackers*, a més, ocupen un lloc destacat en els mitjans de comunicació populars com a experts en tota mena de tecnologia, una figura que va des de Neo a la trilogia de *Matrix* fins al personatge de Nine-ball a *Ocean's 8*. Aquestes representacions contradiuen la realitat del *hacking*, una habilitat que no solament es relaciona amb els atacs a xarxes informàtiques, sinó també amb la protecció d'aquests mateixos atacs. Així mateix, no tots els *hackers* són tècnicament competents, però sí que poden trobar formes més fàcils d'obtenir accés a un sistema informàtic (Ponemon Institute, 2018).

Hi ha una cobertura similar en els mitjans sobre les amenaces que representa el *malware* o el programari maliciós, que també s'atribueix a pirates informàtics (Brenner, 2011; Schell i Dodge, 2002; Wall, 2007). L'ús de *malware* està associat a atacs de sistemes informàtics, al robatori d'informació confidencial, al correu no desitjat i a diverses formes de cibercrim (Holt, 2013; Symantec, 2018; Szor, 2005). No està clar fins a quin punt el públic general comprèn l'abast del *malware* que flueix per internet en qualsevol moment o com funcionen aquestes eines d'atac.

Aquest mòdul proporcionarà una descripció general de les característiques del *hacking* i de la relació entre *hackers*, programari maliciós i tecnologia en general. S'exploraran les característiques dels pirates informàtics i els seus objectius, igual que el vincle entre pirateria i *malware* que permet els delictes informàtics econòmics. Així mateix, es tractarà l'evolució històrica de la tecnologia juntament amb les pràctiques dels pirates informàtics i el *malware* per comprendre el panorama actual dels ciberdelictes econòmics associats amb els actes de ciberintrusió.

1. Definició de *hacking*

Un dels més grans desafiaments per als investigadors radica a definir què constitueix pirateria, ja que aquesta definició no és necessàriament coherent entre diferents poblacions. La definició més àmplia de pirateria hi reconeix la manipulació o modificació de tecnologia de qualsevol tipus, ja afecti el maquinari o el programari, perquè pugui utilitzar-se d'una manera diferent de la del seu propòsit inicial (Holt, 2007; Levy, 2001; Schell i Dodge, 2002; Steinmetz, 2015; Turkle, 1984). Un acte de pirateria es pot dur a terme amb finalitats legítimes o il·legítimes, encara que s'utilitzin les mateixes tècniques, independentment de la motivació de l'atacant.

> Per exemple, alterar el maquinari d'una computadora perquè funcioni a més velocitat de processament seria un exemple de *hacking* legal. No obstant això, aquest acte pot infringir l'acord d'usuari o la garantia proporcionada pel fabricant (Kravets, 2010).

Els actes de pirateria que modifiquen una aplicació per aconseguir subreptíciament les dades de l'usuari i reexpedir-les a una adreça de correu electrònic o servidor web, o per subvertir els protocols de seguretat, són il·legals, en gran manera perquè no fan sinó aconseguir informació sense el consentiment de l'usuari (Brenner, 2008; Holt, 2007; Schell i Dodge, 2002).

Els *hackers*, no obstant això, no solament se centren en la tecnologia, sinó que també tramen formes d'obtenir la informació de diferents grups d'usuaris amb èxit. Els empleats de les principals empreses i organitzacions tenen accés d'arrel a sistemes i informació confidencials que solen estar protegits solament mitjançant un nom d'usuari i una contrasenya. Sovint, aquestes dades es poden adquirir per mitjà dels usuaris sense la necessitat de mètodes de pirateria tècnicament sofisticats. En canvi, els pirates informàtics poden utilitzar diverses formes de frau i tergiversació per obtenir informació sobre la seva víctima. Els *hackers* generalment es refereixen a aquests mètodes com d'enginyeria social, ja que intenten manipular un individu mitjançant l'ús de la comunicació social i de la manipulació psicològica per enganyar-lo i obtenir sense coacció dades que es poden utilitzar per accedir a diferents recursos (Furnell, 2002; Huang i Brockman, 2010; Mitnick i Simon, 2002).

Vegeu també

Per a més exemples, consulteu els mòduls 3 i 4.

Un *hacker* pot utilitzar trucades telefòniques, correus electrònics o llocs web per falsificar la seva identitat i sol·licitar informació d'objectius vulnerables dins d'aquestes organitzacions. Aquests mètodes són amb freqüència efectius, ja que els humans solen ser incapaços de reconèixer totes les formes en què poden ser manipulats, i són més difícils de protegir del risc en comparació amb els sistemes informàtics o els edificis (Huang i Brockman, 2010; Mitnick i Simon, 2002).

Independentment de si un *hacker* desitja atacar una persona, un programa informàtic o un dispositiu, utilitzarà un conjunt únic de termes per descriure el procés. En concret, els pirates informàtics intenten identificar defectes o errors en un dispositiu o en una psique humana fàcilment manipulable, al que es refereixen com a *vulnerabilitats* (Furnell, 2002; Taylor, 1999). Hi ha vulnerabilitats en pràcticament totes les peces de maquinari i programari que existeixen, amb independència del fabricant (Wang, 2006). Això també serveix respecte a la manera en què les persones pensen i actuen en resposta a certs senyals visuals i auditius, la qual cosa pot augmentar la probabilitat que complim una sol·licitud d'informació (Huang i Brockman, 2010; Mitnick i Simon, 2002). Per tant, els *hackers* en general intenten identificar el major nombre de vulnerabilitats possible a l'inici d'un *hacking* per augmentar la seva probabilitat d'èxit.

Després d'identificar les vulnerabilitats que estan presents en el seu objectiu, els pirates informàtics han de seleccionar una vulnerabilitat específica i trobar la manera d'atacar-la. En el context de la tecnologia informàtica, això implica en general l'ús d'un programa informàtic anomenat *exploit*, que pot afectar aquesta vulnerabilitat (Furnell, 2002; Taylor, 1999; Wang, 2006).

Un *exploit* és un mer *script* de codi informàtic que aprofita les limitacions o errors al programari o maquinari per obtenir un major accés al sistema (Furnell, 2002).

Donada la gran varietat de vulnerabilitats que existeixen, hi ha innombrables *exploits* que han estat prèviament escrits i que es poden descarregar de fòrums de *hackers*, llocs de seguretat o fins i tot comprar a proveïdors en mercats negres virtuals (Chu, Holt i Ahn, 2010). Si un pirata informàtic és capaç d'identificar una vulnerabilitat prèviament desconeguda o de dia zero, ha de crear el seu propi codi d'explotació, la qual cosa requereix una gran competència tècnica. Així, aquest tipus de pirateria és vista com una greu amenaça per part dels professionals de seguretat.

L'ús de vulnerabilitats i *exploits* pot ser complicat, per la qual cosa els pirates informàtics sovint troben formes de simplificar i automatitzar el seu ús en atacs. Un dels mètodes clau per aconseguir-ho és amb l'ús de programes que automatitzen l'execució de codi d'explotació i comandos posteriors al sistema (Nazario, 2003; Szor, 2005).

La terminologia comuna utilitzada per descriure aquestes eines és *programari maliciós* o *malware*, ja que combinen múltiples *exploits*, *scripts* i rutines en un sol paquet, que automatitza els atacs.

El *malware* generalment funciona llançant un *exploit* contra una vulnerabilitat per influir en l'objectiu informàtic per mitjà de l'execució d'una càrrega útil o un conjunt de codis que afecten els processos del sistema informàtic (Symantec, 2018; Szor, 2005). La víctima ha d'interactuar amb el programa d'alguna manera per activar la càrrega útil, ja sigui executant un programa o fent clic en un enllaç o aplicació (Dunham, 2008). Una vegada activat, el *malware* pot eliminar o canviar els arxius del sistema, copiar documents i arxius i enviar-los a una ubicació fora del sistema informàtic, recopilar pulsacions de tecles i informació introduïda per l'usuari, així com canviar els processos del sistema per alterar les operacions generals de l'ordinador (Dunham, 2008; Szor, 2005).

La naturalesa interconnectada de les xarxes informàtiques modernes i els dispositius amb accés a internet també permeten que les infeccions de *malware* es propaguin per tot el món conforme es mouen d'un dispositiu a un altre (Brenner, 2008; Leyden, 2012).

Hi ha diverses formes comunes de *malware* utilitzades pels pirates informàtics i els atacants per afectar les víctimes:

1) Una de les formes més freqüents són els virus, que poden ocultar la seva presència en els sistemes i les xarxes d'ordinadors, però no són autònoms, la qual cosa significa que requereixen algun tipus d'interacció amb l'usuari per activar la seva càrrega útil. Per això, els virus generalment es propaguen per mitjà d'arxius adjunts de correu electrònic i missatgeria instantània, així com mitjançant arxius descarregables que la víctima intenta obrir (Kapersky 2003; Symantec, 2018).

2) Una altra forma de *malware* no autònom són els programes de troians, que també arriben per correu electrònic com un arxiu descarregable o adjunt que la gent està disposada a obrir: fotos, vídeos o documents amb títols enganyosos com «XXX Porno» o «Rebut de compra». Quan s'obre l'arxiu, s'executa algun tipus de codi maliciós (Furnell 2002; Szor, 2005). En alguns casos, els virus i els troians poden activar-se visitant llocs web, sobretot pàgines pornogràfiques, que aprofiten defectes en els navegadors web (Symantec, 2018; Szor, 2005).

3) Un altre tipus de *malware* utilitzat per *hackers* són els cucs, que no impliquen tanta interacció de l'usuari, atès que són autònoms o capaços d'autogenerar-se (Nazario, 2003). Els cucs no necessàriament posseeixen una càrrega útil en el mateix sentit que un virus o un troià, i generalment funcionen inserint el seu codi en la memòria de l'ordinador per després usar qualsevol mitjà disponible i propagar-se a altres sistemes informàtics a la mateixa xarxa (Nazario, 2003). Com a resultat, els cucs poden fer que els ordinadors s'alenteixin considera-

blement a causa de la falta de memòria disponible i que redueixin la velocitat d'internet disponible, ja que els cucs ocupen amplada de banda en intentar propagar-se (Nazario, 2003).

4) Una quarta forma de *malware* es denomina *amenaça combinada*, ja que combina les funcionalitats dels virus, els cucs i els troians en un sol paquet de codi maliciós, que es pot executar contra un objectiu (Symantec, 2018).

> Un dels millors exemples d'amenaça de *malware* combinat recent és el *ransomware*, que actua com un troià en el sentit que es propaga per mitjà d'arxius infectats adjunts a correus electrònics o arxius descarregables. Si un usuari obre l'arxiu, el codi maliciós s'executa i la seva càrrega útil s'activa com un virus, inserint un programari de xifrat en el sistema per protegir tots els arxius amb una contrasenya i una clau de desxifrat. En alguns casos, el *malware* també pot modificar arxius clau del sistema perquè els usuaris no puguin accedir a arxius crítics independentment del xifrat (Russinovich, 2013). No obstant això, aquesta informació està oculta per a l'usuari, per la qual cosa no pot accedir a cap dels continguts. Després, s'alerta l'usuari sobre la infecció i se li diu que no podrà accedir als seus arxius fins que pagui a l'atacant una tarifa, o rescat, per desxifrar aquests arxius (Russinovich, 2013). Les dades suggereixen que moltes víctimes paguen el rescat per minimitzar l'impacte de la infecció a les seves xarxes i funcionalitat (IBM, 2016). El cost d'aquests rescats és variable, encara que les grans organitzacions han pagat milers de dòlars per poder recuperar l'accés als seus arxius (IBM, 2016). Per tant, el *ransomware* suposa un gran impacte econòmic per a les víctimes.

En conjunt, la pirateria i el *malware* estan intrínsecament vinculats, perquè els *hackers* poden crear i usar aquestes eines per a altres atacs. No obstant això, el grau de coneixement requerit per crear *malware* significa que no tots ells poden crear o utilitzar *malware* (Holt, Burruss i Bossler, 2018; Leukfeldt i altres, 2017). A més, no tots els *hackers* faran servir *malware*, ja que poden creure innecessària la culminació d'un *hacking*. Els professionals de seguretat també poden escriure o usar *malware* en el curs del seu treball per veure si l'eina pot posar en risc la seguretat dels seus sistemes amb efectivitat (Schell i Dodge, 2002). En qualsevol cas, el *malware* i els *hackers* constitueixen una gran amenaça per als sistemes informàtics i la informació privada en general.

2. Motivacions del *hacker*

Un dels factors més importants que cal tenir en compte en qualsevol discussió sobre ciberdelinqüents, especialment sobre pirates informàtics, és la seva motivació per atacar. Una de les discussions més citades suggereix que hi ha sis motivacions clau en la comunitat de *hackers* (Holt i Kilger, 2012; Kilger, 2010):

- diners
- entreteniment
- ego
- causes ideològiques
- pertinença a un grup social i estatus

Les motivacions poden variar segons el temps i el lloc, de manera que el que és una força impulsora en un país pot estar absent en un altre. A més, els canvis radicals en la tecnologia en les últimes tres dècades han canviat també la rellevància de certs motius al llarg del temps (Kilger, 2010). Finalment, ha de tenir-se en compte que un individu pot estar motivat per múltiples factors en qualsevol moment donat, per la qual cosa és difícil identificar un únic motiu subjacent en la participació en un ciberatac (Kilger, 2010).

Els **diners** són una motivació important en la comunitat moderna de *hackers* i atacants. En la dècada dels vuitanta, els diners tenien inicialment poc valor entre els pirates informàtics, ja que el volum d'informació digital i materials disponibles era limitat (Kilger, 2010; Levy, 2001). La nostra major dependència pel que fa als recursos tecnològics des del desenvolupament de la World Wide Web ha fet augmentar considerablement la quantitat d'informació financera i confidencial que ara està disponible en línia (Franklin, Paxson, Perrig i Savage, 2007; Holt, 2013; Holt i Lampke, 2010; Newman i Clarke, 2003). Com a conseqüència, els *hackers* es dirigeixen amb freqüència a clients i institucions financeres mitjançant atacs de *phishing* (Huang i Brockman, 2010; James, 2005), *malware* de *keylogging* (Chu i altres, 2010; Heron, 2007) i correus electrònics no desitjats (Holt i Graves, 2007; King i Thomas 2009; Wall, 2004). Al seu torn, les dades adquirides mitjançant diferents formes d'atac poden ser venudes per *hackers* en mercats oberts i així generar guanys (Chu i altres, 2010; Franklin i altres, 2007; Holt i Lampke, 2010). A més, un nombre cada vegada major de creadors de *malware* i *hackers* venen accés a eines i serveis de cibercrim com la distribució d'*spam* i atacs de denegació de servei que van més enllà de les habilitats dels *hackers* en potència (Chu i altres, 2010; Holt, 2011; Holt, 2013). Això permet que aquells agents qualificats es beneficiïn de les seves habilitats alhora que augmenta l'eficàcia general de tota la comunitat de *hackers*.

L'entreteniment és una motivació que ha continuat sent important entre els *hackers* des de l'aparició de la tecnologia informàtica (Holt, 2007; Kilger, 2010; Steinmetz, 2016). En els anys setanta i vuitanta, els *hackers* usaven freqüentment tècniques de pirateria per explorar sistemes telefònics, la qual cosa va conduir a la creació de certs recursos d'interès, com les tecnologies *blue box*, que podien manipular els sistemes telefònics en produir els tons d'alta freqüència que controlen els sistemes de commutació telefònica (Furnell, 2002). Els *hackers* moderns encara desitgen manipular la tecnologia amb finalitats lúdiques, tal com es va assenyalar en conferències de *hackers* com la Defcon, on diferents persones participen en concursos de creació tecnològica per refredar ràpidament la cervesa o piratejar automòbils amb la finalitat d'optimitzar el sistema d'ajust i funcionament del vehicle (Holt, 2007).

L'entreteniment també està estretament relacionat amb la motivació de l'**ego**, basat en l'augment de l'autoestima i en el valor intern generat després de finalitzar amb èxit un atac informàtic (Holt i Kilger, 2012; Kilger, 2010; Steinmetz, 2016). De fet, l'ego i la identitat dels *hackers* deriven en gran manera de la manipulació reeixida de la tecnologia, ja sigui per a finalitats legítimes o malicioses (Holt, 2007; Jordan i Taylor, 1998; Taylor, 1999). Els pirates informàtics solen experimentar satisfacció psicològica després d'un pirateig i poden fins i tot obtenir recompenses socials dels seus col·legues i del públic en general, depenent de l'objectiu i el resultat (Holt, 2007; Jordan i Taylor, 1998; Kilger, 2010). De fet, la comunitat de *hackers* posa un gran èmfasi en el domini de la tecnologia, que es demostra mitjançant atacs reeixits (Holt, 2007; Jordan i Taylor, 1998; Steinmetz, 2016; Taylor, 1999). Al seu torn, la satisfacció personal generada per piratejos reeixits constitueix un motiu important al llarg del temps.

La importància de l'**estatus** obtingut per mitjà de la pirateria també està intrínsecament relacionada amb l'ego i amb **l'acceptació en determinats grups socials** (Dupont i altres, 2017; Kilger, 2010). Els *hackers* poden guanyar-se el respecte i el reconeixement dels altres en funció de la seva capacitat per piratejar maquinari i programari de formes noves (Holt, 2007; Jordan i Taylor, 1998; Steinmetz, 2016). A la llum de la creixent globalització en la comunitat de *hackers*, hi ha proves que els *hackers* poden obtenir reconeixement arreu del món en funció de la creació o llançament de *malware* i eines de *hacking* que no existien anteriorment (Chu i altres, 2010). Alternativament, els pirates informàtics poden aconseguir cert estatus pel robatori o l'adquisició d'informació confidencial.

> Per exemple, atacar servidors del govern o sistemes protegits pot demostrar la capacitat general d'un individu i fer-li guanyar prestigi entre la comunitat de *hackers* (vegeu Jordan i Taylor, 2004; i Kilger, 2010, per a una discussió sobre aquest tema).

No obstant això, de vegades el *hacker* ha de revelar com es va completar aquest atac o proporcionar aquesta informació a la resta per fer constar les seves conquestes (Dupont i altres, 2017). Com a conseqüència, en divulgar la informació, el mètode d'atac utilitzat deixa de ser secret i pot cridar l'atenció de les

forces de l'ordre involuntàriament, la qual cosa augmenta la probabilitat que aquests *hackers* puguin ser detectats i identificats (Holt, 2007; Taylor, 1999). Per tant, el prestigi basat en activitats malicioses pot ser difícil de mantenir amb el temps sense que s'augmenti posteriorment el risc d'arrest o sanció (Holt, 2007; Taylor, 1999).

Amb l'expansió d'internet i el seu ús per expressar idees polítiques, nacionalistes i religioses, el nombre d'atacs impulsats per **causes ideològiques** ha augmentat considerablement en l'última dècada (Denning, 2010; Holt, 2012; Kilger, 2010; Jordan i Taylor, 2004). De fet, aquestes causes varien segons la ubicació d'un determinat grup social al món i les seves orientacions culturals, ideològiques, polítiques i religioses. Els *hackers* maliciosos poden emprar els seus coneixements i habilitats per participar en atacs en nom d'un sistema de creences particular i exercir així influencia sobre les polítiques o accions d'un altre grup (Denning, 2010; Kilger, 2010).

> Per exemple, els *hackers* turcs van participar en una campanya de desfiguració web contra diaris i mitjans de comunicació en línia després de la publicació d'una imatge del profeta Mahoma amb una bomba al seu turbant (Holt, Freilich i Chermak, 2017). Aquesta imatge va ofendre molt la comunitat musulmana internacionalment, i els *hackers* turcs van actuar en defensa de la seva religió. Les seves degradacions van fer notar el seu rebuig a la caricatura i van expressar la seva opinió sobre la percepció que altres persones tenen de la seva religió (Holt i altres, 2017). De la mateixa manera, hi ha proves que grups afiliats a al-Qaeda (Denning, 2010) i col·lectius extremistes d'extrema esquerra (Holt, Stonhouse, Freilich i Chermak, 2019) han participat en atacs a una sèrie de llocs web corporatius i governamentals en suport a les seves creences.

Aquells *hackers* motivats per una causa ideològica també poden utilitzar les seves habilitats per robar informació confidencial i així avergonyir un altre grup social o influir-lo (Andress i Winterfeld, 2014; Jordan i Taylor, 2004).

> Per exemple, alguns investigadors van desmantellar una xarxa internacional de sistemes infectats pertanyents a governs, ambaixades i entorns corporatius en 103 països (Information Warfare Monitor, 2009; Markoff, 2009). Aquesta xarxa d'ordinadors afectats, coneguda com a GhostNet, sembla estar controlada per determinats servidors a la Xina amb la finalitat de robar informació confidencial i recopilar subreptíciament dades sobre diversos objectius (Information Warfare Monitor, 2009; Markoff, 2009). Encara que no està clar si aquests atacs van tenir el suport del Govern xinès, o si més aviat es va tractar de *hackers* independents, el que queda clar és que aquests pirates informàtics intentaven obtenir informació per beneficiar el seu país.

De la mateixa manera, els grups Anonymous i LulzSec van perpetuar diversos atacs contra agents polítics, financers i governamentals per expressar la seva insatisfacció amb les polítiques sobre pirateria i llibertat d'informació en línia (Correll, 2010; Holt i altres, 2019). Aquests atacs van implicar persones que no necessàriament tenen habilitats de pirateig, però que són capaces d'atacar un sistema emprant eines de pirateria senzilles i que realitzen la major part del treball elles soles. Per tant, els atacs motivats per causes ideològiques estan canviant després de l'aparició d'eines simples i de poblacions interessades a expressar la seva opinió en espais virtuals (Denning, 2010; Holt i altres, 2019; Kilger, 2010).

Algunes persones també participen en atacs informàtics per obtenir accés a diversos grups, ja sigui per activitats malicioses o no malicioses (Kilger, 2010; Meyer, 1989). Aquest problema és antic i està estretament relacionat amb les creences generals de la comunitat *hacker*, una meritocràcia en la qual els individus són jutjats en funció de les seves habilitats i capacitats generals (Holt, 2007; Jordan i Taylor, 1998; Taylor, 1999). Les persones que desenvolupen i utilitzen les seves habilitats de maneres úniques poden cridar l'atenció d'agents altament qualificats en la comunitat de *hackers* (Dupont i altres, 2017; Holt, 2007; Meyer, 1989). Aquest reconeixement pot comportar la unió a grups que valoren les habilitats de pirateria d'aquesta persona (Kilger, 2010). Això és particularment rellevant tenint en compte la cada vegada major especialització en dispositius de programari i maquinari. Els individus poden presentar una sèrie d'habilitats que uns altres no posseeixen, com la capacitat de codificar en un cert llenguatge de programació o la destresa en una determinada forma d'atac o en un protocol de seguretat (Dupont i altres, 2017; Leukfeldt i altres, 2017; Meyer, 1989). Així doncs, poden integrar-se en un grup que no posseeix aquesta habilitat, però que reconeix el valor intrínsec d'aquest individu.

3. Les correlacions demogràfiques, conductuals i actitudinals dels *hackers*

Encara que és important comprendre les motivacions que hi ha darrere dels atacs informàtics, també ho és identificar la composició demogràfica general de la comunitat *hacker*. La diversitat evident en les destreses i habilitats de la comunitat de *hackers* fa que molts es preguntin com són els pirates informàtics. Hi ha la creença generalitzada que els *hackers* són en la seva majoria homes joves blancs, estudiosos, antisocials que solament són capaços de relacionar-se amb els altres en línia. Aquesta idea persisteix donada la representació de *hackers* en pel·lícules i programes de televisió populars (Thomas, 2002). La recerca empírica centrada en la composició demogràfica de la comunitat *hacker* suggereix que aquesta imatge és fins a cert punt vàlida (Bachmann, 2010; Schell i Dodge, 2002). No obstant això, és difícil documentar amb veracitat les característiques físiques dels *hackers*, ja que es tracta d'una comunitat extremament hermètica (Holt, 2007; Steinmetz, 2016). Molts pirates informàtics pensen que tant els investigadors com els mitjans de comunicació no comprendran el significat de la pirateria, i no volen discutir aquestes qüestions amb ells per temor al fet que siguin mal citats o difamats. A més, els *hackers* que participen en activitats il·legals eviten qualsevol divulgació d'informació personal per temor a ser detectats o arrestats per la policia (Holt, 2007; Leukfeldt i altres, 2017). Per tant, qualsevol discussió sobre la comunitat *hacker* ha de tractar-se acuradament, donada la dificultat inherent d'accedir a aquest sector de la població.

Una de les primeres preguntes que sovint es plantegen els sociòlegs està relacionada amb la mida total de la població de *hackers* en un moment donat. Això és molt difícil de determinar, ja que els pirates informàtics romanen en la clandestinitat i poden utilitzar múltiples identitats en línia per ocultar les seves activitats i minimitzar la probabilitat de detecció.

Per exemple, Jordan i Taylor (1998) van estimar que hi ha almenys 100.000 *hackers*, encara que aquesta xifra pot haver augmentat considerablement en l'última dècada.

Una dada que els pirates informàtics i la recerca científica confirmen constantment sobre la pirateria és que hi ha una proporció molt petita de *hackers* altament qualificats dins de la comunitat de pirates informàtics. En general, aquestes persones són extremament difícils d'identificar perquè oculten les seves veritables identitats als estranys.

Per exemple, Holt, Strumsky, Smirnova i Kilger (2012) van trobar menys de 10 *hackers* altament qualificats dins d'una mostra de gairebé 400 *hackers* russos.

Una raó per a aquesta variació en les habilitats tècniques dels *hackers* pot ser l'edat a la qual un individu està exposat a la tecnologia. Els pirates informàtics més grans solen mostrar una exposició primerenca a la tecnologia, ja si-

gui jugant a videojocs o emprant processos de comunicació simples (Bachman, 2010; Holt, 2007; Holt, 2010; Holt i altres, 2017; Schell i Dodge, 2002; Taylor, 1999). Els pirates informàtics assenyalen freqüentment que disposen d'ordinador propi o que poden accedir a la tecnologia abans dels deu anys o més tard, a l'inici de l'adolescència, la qual cosa sembla que és un element indispensable per despertar l'interès d'algú jove. De la mateixa manera, molts pirates informàtics es consideren curiosos o inquisitius, i volen entendre com funcionen les tecnologies a nivells fonamentals (Holt, 2007; Jordan i Taylor, 1998; Taylor, 1999). La curiositat va ser particularment valuosa per als *hackers* dels anys vuitanta i principis dels noranta, quan la tecnologia era menys accessible a l'usuari general, en tractar-se d'una habilitat indefectible per desenvolupar qualsevol comprensió del maquinari i el programari informàtics (Meyer, 1989; Kilger, 2010; Taylor, 1999). La curiositat segueix sent un factor fonamental entre els pirates informàtics, malgrat que la interfície d'usuari i el programari de la informàtica moderna són cada vegada més simples (Holt, 2007; Steinmetz, 2016).

El desig d'aprendre com es comuniquen els dispositius i el funcionament de les aplicacions pot despertar el desig d'aquestes persones de comprendre millor la funcionalitat de la tecnologia informàtica en general.

La majoria dels pirates informàtics experts sol trobar-se en l'adolescència o rondar els vint anys, encara que els pirates informàtics més veterans suposen un sector cada vegada més gran en la comunitat *hacker* (vegeu, per exemple, Bachmann, 2010; Steinmetz, 2016). Els pirates informàtics de més edat també semblen tenir una ocupació remunerada, i molts treballen en l'àmbit de la seguretat informàtica, mentre que els *hackers* més joves poden no tenir feina (Schell i Dodge, 2002). Els membres de la comunitat *hacker* solen presentar una combinació d'educació formal i informal, ja que els *hackers* fomenten la cerca del coneixement mitjançant la lectura i l'aprenentatge experimental (Bachmann, 2010; Holt, 2007; Steinmetz, 2016). La limitació de les dades disponibles suggereix que una part dels *hackers* qualificats tindria almenys un grau de formació professional, mentre que un nombre menor disposaria de títols universitaris de quatre anys (Bachmann 2010; Holt i altres, 2010; Schell i Dodge, 2002).

Així mateix, la majoria dels estudis assenyalen que els pirates informàtics són predominantment homes, independentment de la seva participació en el *hacking* maliciós o en el *cracking* (Gilboa, 1996; Grabosky, Russell, Smith i Urbas, 2004; Jordan i Taylor, 1998; Schell i Dodge, 2002). Es considera que menys del 20% dels *hackers* són dones, encara que és difícil identificar el seu veritable nombre, ja que tendeixen a protegir el seu gènere dels altres mentre estan en

línia per reduir el risc de sofrir assetjament (Gilboa, 1996; Hutchings & Chua, 2017; Schell & Dodge, 2002; Taylor 1999). Per tant, es desconeix quantes dones participarien en realitat en la pirateria informàtica.

Els *hackers* també informen constantment de com estableixen relacions amb altres persones que comparteixen els seus interessos, malgrat el mite generalitzat que els pirates informàtics són solitaris i passen molt temps socialitzant únicament amb altres usuaris en línia (Holt, 2009; Holt i Kilger, 2008; Leukfeldt i altres, 2017; Meyer, 1989; Schell i Dodge, 2002). Nombrosos estudis suggereixen que els *hackers* mantenen relacions amb persones tant al món real com en entorns en línia, encara que els seus companys virtuals poden tenir més importància, ja que solen ser incapaços d'identificar altres persones al món real que comparteixin els seus mateixos interessos en la informàtica (Holt, 2009; Holt i Kilger, 2008; Meyer, 1989; Schell i Dodge, 2002; Steinmetz, 2016). Aquells les amistats dels quals estan interessades en la informàtica són en realitat un predictor molt important de participació en el *hacking* (Bossler i Burruss, 2010; Holt, 2009; Holt, Bossler, i Burrus, 2010; Marcum i altres, 2014; Skinner i Fream, 1997). Establir amistats amb altres persones que puguin augmentar el teu coneixement i proporcionar-te informació que no tens i, en general, donar suport als teus interessos, pot garantir un interès a llarg termini en la tecnologia (Bossler i Burruss, 2010; Holt, 2009; Holt i altres, 2010; Skinner i Fream, 1997).

Al mateix temps, les relacions entre companys són fonamentals per a la participació en delictes i infraccions cibernètiques, ja que proporcionen informació sobre els mètodes i justificacions per a aquestes conductes a la xarxa (Bossler i Burruss, 2010; Higgins i Makin, 2004; Higgins i Wilson, 2006; Holt i altres, 2010; Ingram i Hinduja, 2008; Skinner i Fream, 1997). De fet, les relacions d'amistat entre *hackers* maliciosos poden servir com a fonts d'inspiració per als més joves, que poden imitar les accions dels seus companys. Skinner i Fream (1997) van descriure succintament aquesta qüestió i van afirmar que els companys que participen en ciberdelictes ajuden els seus amics a «aprendre no solament com operar un equip altament tècnic, sinó també procediments específics, programació i tècniques per fer servir un ordinador de manera il·legal» (Skinner i Fream, 1997, 498).

A més, les amistats entre *hackers* maliciosos suposen una important font de validació per a la creença que no hi ha lleis reals sobre el comportament en línia i que tant el bon ús com l'ús indegut d'un ordinador pot ser acceptable depenent de certes circumstàncies (vegeu, per exemple, Holt i altres, 2010; Ingram i Hinduja, 2008; Skinner i Fream, 1997).

Per exemple, Gordon (2000) va descobrir que, amb freqüència, els creadors de virus no estaven preocupats pels efectes dels seus productes, fins i tot si sabien que eren il·legals i nocius. A més, els *hackers* argumenten que les seves accions generalment no causen dany (Gordon i Dt., 2003; Turgeman-Goldschmidt, 2005), i culparien les víctimes de tenir poca habilitat o seguretat per evitar aquest atac (Chua i Holt, 2017; Jordan i Taylor, 1998).

Mantenir relacions amb els altres companys dins de la comunitat *hacker* també és fonamental, ja que es reforça la participació en males conductes cibernètiques al llarg del temps per mitjà de l'acceptació social i l'aprovació per participar en atacs reeixits i en la recopilació de materials piratejats.

Per exemple, aquells que fan comentaris positius sobre la participació en un delicte cibernètic augmenten la probabilitat que es cometin futurs delictes (Bossler i Burruss, 2010; Holt i altres, 2010; Ingram i Hinduja, 2008; Skinner i Fream, 1997).

El reforç social per cometre delictes és un factor indispensable en el crim tant en línia com en entorns reals, raó per la qual les relacions socials entre els pirates informàtics són un aspecte important en la seva participació a llarg termini en atacs informàtics.

A més de les relacions entre *hackers* maliciosos, la recerca recent també ha començat a considerar el paper de l'autocontrol sobre la probabilitat de participar en un ciberdelicte (Bossler i Burruss, 2010; Gordon i Dt., 2003; Holt, Bossler i May, 2012; Holt i Kilger, 2008). En els estudis criminològics, l'autocontrol es tracta com un tret individual que es desenvolupa durant la primera infància amb el control i la correcció dels pares en resposta a males conductes (Gottfredson i Hirschi, 1990). Els pares que controlen, reconeixen i castiguen els mals comportaments quan aquests es donen tenen més probabilitats de vincular-se emocionalment amb els seus fills. Al seu torn, els nens desenvolupen alts nivells d'autocontrol o la capacitat de regular i controlar el seu comportament davant l'oportunitat de cometre delictes (Gottfredson i Hirschi, 1990). Els fills els pares dels quals no aconsegueixen controlar el seu comportament tenen més probabilitats de desenvolupar un baix autocontrol i, per tant, són més proclius a participar en activitats de risc o fins i tot delictives. Les persones amb poc autocontrol són impulsives, insensibles, no verbals, assumeixen riscos i prefereixen les tasques simples (Gottfredson i Hirschi, 1990). D'aquesta manera, no són capaces de valorar completament les conseqüències i els beneficis de les seves accions, per la qual cosa són propenses a cometre delictes i a mostrar comportaments arriscats.

Les persones amb baix autocontrol mostren més tendència a participar en actes de delinqüència de carrer (Pratt i Cullen, 2000) i en ciberdelictes, com la descàrrega il·legal de música i de programari (vegeu Higgins i Makin, 2004; Higgins i Wilson, 2006). No està clar quin paper pot exercir l'autocontrol en el *hacking*, donada la diversitat d'atacs que poden qualificar-se com a pirateig (Bossler i Holt, 2010; Holt i Kilger, 2008).

Per exemple, la pirateria pot abastar des de pràctiques simplistes, com deduir contrasenyes, fins a delictes més greus i tecnològicament sofisticats, com la producció de *malware*.

Com a resultat, l'autocontrol pot variar segons les habilitats i l'actitud general del *hacker*. Per exemple, Holt i Kilger (2008) van trobar que els pirates informàtics, tant en entorns universitaris com en la població en general, tenien nivells relativament alts d'autocontrol. A més, un estudi de Bossler i Burruss (2010) va trobar una relació interessant entre l'autocontrol, els companys de la co-

munitat *hacker* i la pirateria. Més concretament, aquelles persones que estableixen relacions amb altres *hackers* presentaven nivells més alts d'autocontrol. Les persones amb companys *hackers* tenien nivells més baixos d'autocontrol i es beneficiaven d'aquestes relacions socials amb altres pirates per reforçar les seves activitats i aprendre mètodes de pirateria (Bossler i Burruss, 2010). Bossler, Holt i May (2011) van assenyalar resultats similars en una mostra d'estudiants de secundària i batxillerat que participen en delictes informàtics.

Aquestes troballes proporcionen informació inicial sobre la influència que teòricament exerceix un baix nivell d'autocontrol en el desenvolupament general de les habilitats i capacitats de tota la comunitat *hacker*. Aquells pirates informàtics amb poc autocontrol poden començar a participar en ciberdelictes perquè veuen l'oportunitat de col·laborar en activitats perilloses o de risc, inclosos els actes de *hacking* més simples, com desxifrar contrasenyes i agregar o eliminar informació dels sistemes. No obstant això, amb el temps, els pirates informàtics amb poc autocontrol també poden ser capaços de no anar més enllà d'aquests atacs bàsics perquè, en general, tindran poc interès a dedicar el seu temps al pirateig. La seva incapacitat per concentrar-se i comprendre millor la complexitat de certs actes de pirateria pot limitar la seva capacitat general. Les persones amb nivells més alts d'autocontrol no necessàriament s'enfronten a aquests problemes, i els resulta més fàcil perfeccionar els seus coneixements i habilitats amb el pas del temps. Al seu torn, poden perpetrar atacs més sofisticats i sobrepassar els seus col·legues *hackers* amb un baix nivell d'autocontrol. Hauria d'estudiar-se més a fons aquesta qüestió per aclarir la relació entre baixos nivells d'autocontrol i la pirateria, encara que s'entén que aquesta pot ser una correlació clau per comprendre les característiques generals de la comunitat de *hackers*.

4. La subcultura *hacker*

Tal com es va assenyalar, els *hackers* estableixen vincles socials amb altres pirates tant en línia com al món real. Es creu que les relacions entre ells són l'origen d'una subcultura corrupta i, en alguns casos, criminal basada en valors i interessos compartits que guien l'acció individual d'aquests *hackers* (vegeu Miller, 1959; Short, 1958). Els estudis sobre la subcultura *hacker* són extremament valuosos, ja que mostren les normes i creences dels pirates informàtics i identifiquen variacions en la seva estructura al llarg del temps. No obstant això, hi ha tres qüestions clau que semblen influir en els comportaments dels *hackers*, la primera de les quals és la importància de la tecnologia (Holt, 2007; Jordan i Taylor, 1998; Meyer, 1989; Steinmetz, 2016; Taylor, 1999; Thomas, 2002). Els interessos i les activitats dels *hackers* se centren en el programari i el maquinari informàtics, així com en altres formes tecnològiques associades a la informàtica. Així mateix, la connexió d'un individu amb la tecnologia ajuda a desenvolupar la seva capacitat de pirateig (Holt i altres, 2017; Jordan i Taylor, 1998; Steinmetz, 2016; Taylor, 1999). Per establir aquesta connexió, els pirates informàtics han de desenvolupar «una relació fàcil, si no voraç», amb la tecnologia informàtica i de comunicacions, així com la voluntat d'explorar-la i utilitzar-la de maneres noves (Jordan i Taylor, 1998, pàg. 764).

Per tant, el coneixement i el domini de la tecnologia exerceixen un paper important en la subcultura *hacker* (Holt, 2007; Meyer, 1989, Thomas, 2002).

Els *hackers* passen una quantitat significativa de temps aprenent sobre tecnologia per conèixer amb detall com funcionen els dispositius informàtics. Això augmenta la importància de la destresa tecnològica en la subcultura *hacker*, demostrada en actes de pirateria al món real (Furnell, 2002; Holt, 2007; Steinmetz, 2016). Els *hackers*, a més, demostren els seus coneixements sobre la cultura *hacker* fent referències a la història de la pirateria o emprant l'argot *hacker* quan es comuniquen amb els seus companys (Loper, 2000, pàg. 66). Aquestes demostracions destaquen la connexió dels *hackers* amb la tecnologia i els permeten guanyar prestigi entre els membres de la comunitat (Holt, 2007; Loper, 2000).

Amb tot, la naturalesa il·legal d'algunes formes de pirateria pot explicar la importància de l'anonimat en la cultura *hacker* (Holt, 2007; Jordan i Taylor, 1998; Taylor, 1999; Thomas, 2002). En concret, els pirates informàtics intenten protegir les seves activitats pel que fa a les forces policials i els agents del Govern (Taylor, 1999, pàg. 29). L'ús d'identificadors o sobrenoms en entorns en línia i al món real fa més difícil conèixer la veritable identitat d'un *hacker* (Dupont

i altres, 2017 Furnell, 2002; Jordan i Taylor, 1998). Els *hackings* i atacs que s'efectuen amb èxit s'atribueixen a la seva identitat i habilitat en línia, la qual cosa suscita un desig de presumir i compartir amb els altres aquestes destreses (Dupont i altres, 2017; Holt, 2007; Jordan i Taylor, 1998). Això pot ajudar un individu a guanyar prestigi dins de la comunitat *hacker*, encara que posa el *hacker* en risc de ser detectat per la policia (Furnell, 2002; Leukfeldt i altres, 2017). Per tant, els pirates informàtics han de mantenir-se en una línia molt fina entre compartir informació i mantenir la privadesa de certs coneixements (Holt, 2007; Jordan i Taylor, 1998). Al seu torn, l'anonimat reforça i manté la barrera entre els pirates informàtics i la policia (Dupont i altres, 2017; Taylor, 1999).

5. La diferència entre *hackers* basada en el seu prestigi en línia i fora de línia

Els motius per piratejar poden variar segons l'individu i els seus interessos i habilitats. Les tècniques que empren els pirates informàtics poden diferir en part en funció de la seva capacitat per accedir a sistemes informàtics i informació clau.

Amb aquesta finalitat, els *hackers* poden classificar-se depenent de si ja exerceixen un paper important dins d'una organització o empresa, o si actuen de manera independent.

Aquelles persones que ja estan treballant dins d'una institució corporativa o governamental i que decideixen participar en atacs informàtics poden ser vistes com a «persones amb informació privilegiada», en el sentit que tenen accés exclusiu a certs recursos i la capacitat de moure's en un entorn fiable com a administradors de sistemes o professionals de seguretat (Cappelli, Moore, Shimeall i Trzeciak, 2006; Dhillon i Moores, 2001; Shaw, Post i Ruby, 1998). Els seus esforços i activitats queden fàcilment en secret quan ostenten aquest control administratiu, encara que els seus atacs també passarien desapercebuts perquè tendeixen a robar subreptíciament informació o a instal·lar *malware* inactiu en cas que els acomiadin (Cappelli i altres, 2006; Dhillon i Moores, 2001).

Donada la naturalesa general de les amenaces internes, és possible que tinguin motivacions diferents de les dels *hackers* externs.

Per exemple, una recerca de Shaw, Ruby i Post (1999) va trobar diversos comportaments típics que definirien el *hacker* infiltrat. En concret, són introvertits i no tenen bones habilitats socials, la qual cosa els dificulta interactuar amb altres persones dins i fora de les estructures corporatives tradicionals. A més, els *hackers* infiltrats mostren una actitud negativa cap a l'autoritat a conseqüència de problemes familiars a llarg termini (Shaw i altres, 1999).

Aquests problemes s'uneixen a la forta necessitat de socialitzar amb altres en entorns virtuals, on poden interactuar més còmodament. També mostren una ètica canviant i una falta d'empatia pels altres, per la qual cosa neguen la seva participació en comportaments il·legals (Shaw i altres, 1999). També es perceben a si mateixos amb dret a piratejar, la qual cosa els porta a buscar formes de rebre el reconeixement i el privilegi que senten que unes altres persones els deuen. Les seves diferències psicològiques i actitudinals solen dificultar-los respondre en situacions estressants de manera constructiva. En el seu lloc, solen respondre en aquests moments de tensió amb comportaments irracionals

o perillosos. Finalment, els *hackers* infiltrats tendeixen a utilitzar atacs simples depenent de l'objectiu i el servei que aprofiten, encara que de vegades s'han emprat mètodes més complexos (Cappelli i altres, 2006).

Les amenaces internes van ser la preocupació més comuna entre els professionals de la seguretat cibernètica durant els anys vuitanta i noranta a causa de la petita població d'usuaris qualificats i les limitacions en la connectivitat a internet en general (Andress i Winterfeld, 2014). L'amenaça externa va augmentar a la fi de la dècada de 1990, a mesura que la tecnologia informàtica es va tornar cada vegada més accessible, la qual cosa va suposar un augment significatiu en el nombre d'atacs contra corporacions i governs (Taylor, 1999). Fins avui, la majoria dels atacs cibernètics procedirien de persones externes, encara que aquelles amb informació interna encara poden representar una amenaça per als sistemes i la informació confidencials.

6. Les correlacions de la pirateria i de la victimització per *malware*

Encara que cada vegada hi ha més recerca sobre els predictors conductuals i actitudinals per a la participació en ciberdelictes, els estudis sobre la victimització són escassos. Això es deu en part a les dificultats per identificar víctimes de pirateria informàtica i certes formes de cibercrim (Bossler i Holt, 2009, 2010; Holt, 2003; Yar, 2005). És possible que les víctimes no sàpiguen que han estat atacades, ja que les infeccions de programari maliciós poden emular fallades de sistemes informàtics i maquinari (Bossler i Holt, 2009, 2010; Holt i Bossler, 2013; Holt, van Wilsem, van de Weine i Leukfeldt, 2019). A més, els usuaris solament poden adonar-se que algun tipus de pirateig els ha afectat després que la seva informació s'hagi eliminat o corromput d'alguna manera (Holt, 2003; Ngo i Patternoster, 2011). De la mateixa manera, alguns casos de victimització estan completament fora del control d'un individu, com el filtratge de dades a gran escala en una empresa on es roben les dades del client (Bossler i Holt, 2009; Holt i Lampke, 2010). La institució que administra les dades és responsable d'aquesta desprotecció, per la qual cosa les víctimes queden exemptes de qualsevol responsabilitat pel que fa a l'atac. Finalment, quan un atac es duu a terme, aquest pot no ser reportat a la policia donada la preocupació sobre si aquest atac es prendrà seriosament o si algú podrà investigar el delicte (Holt, 2003; Newman i Clarke, 2003; Wall, 2001).

Per tant, suposa tot un desafiament comprendre completament el nombre de *malwares* i víctimes de ciberdelictes que es produeixen cada any. Diverses estadístiques suggereixen que aquestes formes de cibercrim són extremament costoses, ja que van des de milions fins a milers de milions, depenent de l'objectiu.

> Per exemple, l'Oficina d'Estadístiques Judicials dels Estats Units (o BJS, Bureau of Justice Statistics) va assenyalar que 2/3 de les empreses van sofrir algun tipus de delicte cibernètic, la qual cosa suposava un total en pèrdues de 867 milions de dòlars el 2007, la majoria d'ells relacionats amb *malware* (Rantala, 2008).

Les enquestes corporatives més recents suggereixen que un sol atac de *malware* pot costar una mitjana de cinc milions de dòlars a les grans organitzacions, que majorment resulta de la pèrdua de productivitat dels empleats (Fruhlinger, 2018). Aquestes són, no obstant això, estimacions limitades, posades en qüestió per part d'alguns estudiosos a causa de les seves mides de mostra i les fonts de finançament d'aquests estudis (vegeu, per exemple, Levi i altres, 2018).

Donada la limitació de dades disponibles sobre les víctimes de ciberdelictes, els investigadors han intentat explorar la seva correlació utilitzant dades «autoreportades», o proporcionades per les mateixes víctimes (Bossler i Holt, 2009; 2010; Choi, 2008; Holt i altres, 2019; Ngo i Patternoster, 2011). Les anàlisis d'aquestes dades suggereixen que hi ha poques correlacions per a la infecció de programari maliciós, el frau i les víctimes de pirateria. L'edat, la raça i el gènere

no suposen una relació real amb el risc d'infecció o dany, la qual cosa reflectiria els desitjos dels creadors de *malware* i *hackers* d'afectar punts objectius com sigui possible (Bossler i Holt, 2009, 2010; Holt i altres, 2019). Amb la finalitat de tenir èxit, els pirates informàtics llancen xarxes àmplies per atacar milers, si no milions d'usuaris, ja que és probable que solament quedés infectada una petita part de tots els ordinadors (Chu i altres, 2010; Furnell, 2002; Gordon i Dt., 2003). Per tant, pot ser difícil destriar tendències demogràfiques úniques en el risc de victimització.

A més, el temps que s'està en línia i l'ús de programari de protecció, com ara antivirus i altres eines, semblen tenir un impacte mínim en el risc de victimització (Bossler i Holt, 2009; Choi, 2008; Holt i Bossler, 2013; Holt i altres, 2019). La relativa escassa importància del temps que es passa connectat és lògica, ja que les infeccions i els atacs poden perpetuar-se independentment de si un individu està interactuant amb altra gent en línia o no (Yar, 2005). En canvi, els *hackers* només necessiten un sistema que estigui connectat a internet per poder infectar-lo. L'ordinador en tant que objectiu disponible és tot el que el *hacker* requereix per intentar accedir a informació confidencial (Yar, 2005). A més, la naturalesa asincrònica d'algunes formes de comunicació en línia, com el correu electrònic, dificulta la identificació de correlats de risc basats en l'ús de la tecnologia (Bossler i Holt, 2009). Un *malware* pot enviar-se a una adreça de correu electrònic i romandre inactiu fins que l'usuari obre el correu electrònic i executa l'arxiu (Szor, 2005). Això pot trigar deu segons o deu hores, depenent de la freqüència amb la qual l'individu comprova els seus missatges. Per tant, l'exposició a delinqüents en entorns en línia mitjançant l'ús de la tecnologia en general pot constituir un factor més pertinent en el risc de victimització que el temps que es passa en fòrums o a Facebook.

L'ús de programari de protecció, com antivirus i altres eines, també sembla exercir un paper mínim en la reducció del risc de victimització (Bossler i Holt, 2009; Holt i altres, 2019). Encara que els programes de seguretat poden defensar els usuaris d'atacs aleatoris, l'eficàcia d'aquests programes està limitada en funció de l'administració d'aquestes eines per part dels mateixos usuaris (Brenner, 2008).

> El programari antivirus, per exemple, ha d'actualitzar-se i executar-se regularment per garantir que l'usuari està protegit en tot moment per versions més actualitzades del programa (Bossler i Holt, 2009). Amb tot, molts usuaris no dediquen temps a aquestes pràctiques de seguretat, la qual cosa dificulta predir amb quina freqüència aquestes eines protegeixen els usuaris. De fet, un estudi va revelar que gairebé el 25% dels ordinadors personals amb programes de seguretat arreu del món tenen programari maliciós, com un virus, emmagatzemat en la seva memòria (PandaLabs, 2007). Per tant, moltes persones resulten ser víctimes d'atacs informàtics malgrat la presència i l'ús de programari antivirus i altres programes de protecció per defensar el seu equip contra piratejos maliciosos comesos aleatòriament.

Un dels pocs predictors fiables de victimització per pirateria i *malware* és la participació de l'individu en certes formes de cibercrim (Bossler i Holt, 2009, 2010; Holt i Bossler, 2013). Això reflectiria el risc general d'exposició a ciberdelinqüents que resultaria d'activitats com la pirateria digital o la descàrrega il·legal de pel·lícules o música. Els creadors de *malware* reconeixen que, atès

que les persones freqüentment descarreguen materials piratejats o veuen pornografia en línia, insereixen codi maliciós en el que sembla un arxiu de música o multimèdia amb l'esperança que algú descarregui l'element i executi el codi (Chu i altres, 2010). De fet, un dels pocs correlats d'infecció de *malware* en un estudi de Bossler i Holt (2009) va assenyalar que aquells que es dediquen a la pirateria presenten un major risc d'infecció.

Un altre correlat de victimització són les activitats d'amics i companys en línia. En entorns virtuals, les activitats d'una persona exposen els altres a danys, sigui directament o indirectament.

> Per exemple, si l'ordinador d'un individu està infectat amb *malware*, alguns programes intentaran replicar-se i propagar-se enviant arxius infectats a altres persones per mitjà de l'*spam*. En aquest sentit, Bossler i Holt (2009) van descobrir que les persones els amics de les quals veien pornografia en línia tenien més risc d'infeccions de *malware*. Bossler i Holt (2010) van obtenir resultats similars pel que fa a la victimització per *malware*, el frau i la pirateria. Les persones amb companys que participaven en diverses formes de cibercrim tenien més probabilitats de perdre informació i dades de targetes de crèdit o de ser atacades com a conseqüència que els seus amics els ataquessin voluntàriament o que augmentessin indirectament el seu risc de ser atacats a causa d'un comportament negligent.

Donada la falta de dades sobre predictores i correlats coneguts de victimització per cibercrim, cal considerar per què hi ha tan pocs predictors d'atacs informàtics. Una de les explicacions més significativa radica en el fet que els sistemes informàtics individuals poden ser atacats d'innombrables maneres en línia. Els missatges d'*spam* enviats a un individu poden contenir programari maliciós, igual que els llocs web que utilitzen eines com el *malware* iFrame, que infecta el navegador amb la simple connexió al lloc web (Chu i altres, 2010; Holt i Graves, 2007; Wall, 2004). Encara que aquest tipus d'atacs són ben coneguts, els usuaris majorment ingenus se'n veuen afectats (Wall, 2007). Tots els dies es llancen a la xarxa atacs més peculiars que utilitzen *exploits* i *malware* nous i desconeguts, per la qual cosa és difícil protegir-se per complet de l'atac (Chu i altres, 2010; Gordon i Dt., 2003). A més, les filtracions de dades a gran escala en empreses afecten l'usuari individual, la qual cosa dificulta que les víctimes puguin controlar alguns riscos. Per tant, sabem molt més sobre els delinqüents que de les víctimes, malgrat el significatiu dany potencial que el públic en general pot experimentar a les mans de pirates informàtics i creadors de *malware*.

7. Història de la pirateria i el *malware*

7.1. Els començaments

Encara que la comunitat moderna de *hackers* està composta per individus amb diversos nivells d'habilitat i diversos principis ètics, aquesta comunitat ha canviat significativament des dels seus humils orígens. Per observar com ha evolucionat la pirateria, és important situar la seva aparició en el context de la innovació social i tecnològica. Els *hackers* han existit des dels principis de la informàtica, a la fi de la dècada de 1950, encara que la tecnologia era molt diferent de la disponible actualment. De fet, alguns investigadors sostenen que el terme *pirateria* o *hacking* va sorgir entre els estudiants d'enginyeria de l'Institut de Tecnologia de Massachusetts (MIT) a la dècada de 1950 (Levy, 2001). Els estudiants van emprar aquest terme per referir-se a manipulacions lúdiques, encara que hàbils, de l'electrònica, i va ser en gran part sinònim de «divertir-se» o «fer el ximple».

Amb el temps, els estudiants van començar a utilitzar aquest terme per descriure una patenta universitària, única en l'entorn altament tècnic del MIT. No obstant això, aquests atacs mai van ser obertament maliciosos, i sovint requerien una demostració de destresa tècnica per ser considerats i vists com un acte de *hacking*. Aviat, els estudiants del MIT van usar el terme *hacking* per descriure més activitats inquisitives al campus, incloses les incursions en els túnels de vapor del campus, com el «hacking de túnels», i la manipulació del sistema telefònic, anomenada «hacking de telèfons». A més, el Tech Model Railroad Club (TMRC) del MIT va prendre el terme com a part d'un llenguatge cada vegada més especialitzat per descriure el seu treball en els sistemes ferroviaris del club. Per a aquest grup, la pirateria va ser un procés desordenat i lúdic de resolució de problemes que contrastava amb les tècniques convencionals (Levy, 2001). De fet, l'edició de 1958 del diccionari del TMRC proporciona la següent entrada per al terme *piratejar*: «1) una cosa fet sense una finalitat constructiva; 2) un projecte dut a terme amb un mal assessorament; 3) un generador d'entropia; 4) cometre, o intentar cometre, un acte de hacking».

Encara que el MIT va exercir un paper fonamental en la creació del terme *pirateig* i el seu significat, també es va relacionar amb l'aparició de la informàtica a la dècada de 1950 en entorns universitaris. En aquest moment, les unitats centrals (o *mainframes*) informàtiques eren sistemes enormes que ocupaven per complet sales climatitzades i que presentaven una memòria i potència de processament general relativament limitades (Levy, 2001). Els ordinadors eren, a més, extremament cars i es trobaven solament a les universitats, com ara MIT, Cornell i Harvard. Aquests dispositius tampoc estaven vinculats entre si de cap manera, i qualsevol utilització innovadora dels recursos solia ser

de collita pròpia. De fet, els programadors informàtics responsables d'aquestes infraestructures tecnològiques van intentar identificar tècniques per accelerar i avançar en aquests sistemes lents. La creació de solucions sofisticades i innovadores per a aquests problemes es va denominar *hacks*, i els programadors responsables van ser identificats com a *hackers* d'acord amb el concepte original generat entre l'alumnat del MIT (Levy, 2001).

La percepció del pirata informàtic com un programador i manipulador expert va continuar durant la dècada de 1960, encara que l'agitació social i els disturbis civils alterarien la forma en què els pirates informàtics veien la seva relació amb la tecnologia i el món en general. A mesura que la tecnologia informàtica va passar de les universitats a les aplicacions militars, els anomenats pirates informàtics van mostrar insatisfacció pel que van veure com un ús inadequat d'un recurs meravellós (Thomas, 2002). Per tant, els programadors van començar a desenvolupar una sèrie d'ideals, coneguts com a ètica *hacker* (Levy, 2001; Thomas, 2002). Aquesta sèrie de sis principis pot resumir-se de la següent manera (Furnell, 2002, pàg. 64; Levy, 2001):

- L'accés a ordinadors, i qualsevol cosa que pugui ensenyar-te quelcom sobre com funciona el món, ha de ser il·limitat i total.
- Tota la informació ha de ser lliure.
- Desconfia de l'autoritat: promou la descentralització.
- Els pirates informàtics han de ser jutjats per les seves habilitats de pirateria, no per falsos criteris com la titulació, l'edat, la raça o la posició social.
- Pots crear art i bellesa amb un ordinador.
- Els ordinadors poden canviar la teva vida per a millor.

La creença bàsica que la informació hauria de ser de lliure accés i gratuïta per a tots era fonamental perquè tothom pogués entendre com funcionen les coses i identificar les maneres en què podrien millorar-se (Thomas, 2002, pàg. 15). De fet, la tecnologia hauria de ser un mitjà d'informació per als altres. Aquesta ètica va guiar les activitats dels *hackers* en aquell moment i va assentar les bases de la cultura *hacker* contemporània (Levy, 2001).

7.2. Els anys setanta

A la dècada de 1970, la percepció de la pirateria com una finalitat ètica va començar a canviar amb el sorgiment de dues activitats: el *phreaking* i el *homebrew computing*. L'aparició del «*phreaking* telefònic», o la manipulació de la tecnologia telefònica per comprendre i controlar els sistemes telefònics, va ser promoguda per sectors contraculturals dels anys seixanta (Landreth, 1984). El *phreaking* va permetre que les persones fessin trucades gratuïtes a qualsevol

persona arreu del món controlant els interruptors del sistema telefònic. Per tant, el *phreaking* és vist com una de les primeres formes principals de frau electrònic, ja que implica l'ús il·legal i el robatori de serveis de telefonia (Grabosky, 2001). Aquesta activitat té el seu origen en les protestes d'Abbie Hoffman, el Technology Assistance Party (TAP) i el Youth International Party Line (YIPL) contra el monopoli de la telefonia per part de les empreses (Landreth, 1984). El *phreaking* també va arribar al públic en general de la mà d'un home anomenat Cap'n Crunch (John Draper), que va bufar un xiulet d'una caixa de cereals al receptor del seu telèfon (Landreth, 1984). El xiulet va crear el to perfecte de 2.600 megahertzs, el qual, en aquest moment, s'usava per connectar un individu a línies de llarga distància. Aquesta simple joguina va obrir una nova àrea tecnològica perquè les persones exploressin, utilitzessin i defraudessin les companyies telefòniques d'acord amb els orígens de la pirateria.

La pràctica del *phreaking* es va tornar maliciosa arran de la publicació d'un article a la revista *Esquire* sobre Draper i altres *phreaks* el 1971. L'atenció que va cridar aquest article sobre l'activitat va conduir a una sèrie de mesures enèrgiques contra els *phreaks* conjuminant els esforços de la policia i dels funcionaris de seguretat telefònica. En aquest moment no hi havia lleis reals contra l'exploració i la manipulació d'ordinadors i telèfons, encara que el robatori de serveis podia ser processat. No obstant això, la publicació d'aquest article i la seva posterior recerca per part dels principals mitjans de comunicació van cridar cada vegada més l'atenció del poder legislatiu i de la policia a la fi de la dècada de 1970 (Parker 1980). De fet, una de les primeres lleis de delictes informàtics als Estats Units es va aprovar a Florida el 1978, la qual cosa convertia l'accés no autoritzat als sistemes informàtics en un delicte greu de tercer grau. Amb tot, la implantació d'aquestes lleis no es va fer amb serietat fins a mitjan anys vuitanta.

La dècada de 1970 també va veure el sorgiment de grups d'afeccionats centrats en el desenvolupament de maquinari i la programació informàtica, especialment el Homebrew Computer Club el 1975. Aquestes reunions informals es van centrar en la construcció i discussió d'ordinadors personals, bé mitjançant dissenys personalitzats i innovadors, bé per mitjà del cada vegada major nombre de *kits* comercials disponibles en anuncis de revistes fins a principis dels anys setanta. La majoria dels membres eren, efectivament, *hackers*, ja que usaven mètodes i principis de pirateria per avançar encara més en l'estat de la informàtica personal. No obstant això, aquests grups rares vegades van emprar el terme *hacker* per referir-se a si mateixos o a les seves activitats en els seus butlletins informatius.

Gràcies en gran part als esforços dels *hackers* a la llar i a la indústria privada, l'ordinador personal va aconseguir llançar-se el 1977 (Ceruzzi, 1998). L'adopció d'aquesta tecnologia va ser inicialment lenta i no es va establir fins a principis de la dècada de 1980, quan les famílies de classe alta i mitjana van començar a comprar cada vegada més ordinadors per a les seves llars. La creació i venda de tecnologia de mòdem, que connecta uns ordinadors amb uns altres i

diferents xarxes mitjançant línies telefòniques, també va millorar i es va tornar més accessible immediatament per a l'usuari comú. Com a resultat, aquelles persones que mai abans havien tingut accés a la tecnologia informàtica ara podien detectar i explorar xarxes informàtiques (Furnell, 2002). Així mateix, l'explosió simultània de videojocs i altres sistemes d'entreteniment electrònic a la llar va posar en contacte els joves amb la tecnologia com mai abans.

7.3. Els anys vuitanta

L'auge dels ordinadors personals a principis dels anys vuitanta va despertar l'interès dels joves, especialment dels homes, que van començar a explorar-los i usar-los de maneres que excedien el seu propòsit com a eines d'aprenentatge o ajudes educatives. Això va marcar el començament de la unió de la cobertura mediàtica, centrada en el ràpid avanç i adopció de tecnologies informàtiques, i de l'ús d'aquestes tecnologies amb finalitats malicioses i delictives. El principal catalitzador d'aquesta cobertura va ser l'estrena de la pel·lícula *WarGames* (*Jocs de guerra*), que presentava Matthew Broderick com un *hacker* adolescent que, sense sospitar-ho, obté accés a sistemes informàtics militars i gairebé produeix un holocaust nuclear (Schneider, 2008).

Un mes després de l'estrena de la pel·lícula, l'FBI va començar a registrar i a presentar demandes contra els membres d'un grup local de pirates informàtics coneguts com els «414», el codi d'àrea de Milwaukee (Krance, Murphy i Elmer-Dewitt, 1983). Encara que aquests nois van participar en intrusions relativament innòcues de xarxes protegides i no van causar danys físics als sistemes o les dades, la policia va intentar publicitar les batudes (Hollinger i Lanza-Kaduce, 1988). Els mitjans de comunicació van publicar ràpidament històries sobre aquestes recerques per treure profit de l'interès públic per l'ús indegut d'ordinadors, derivat de la pel·lícula *WarGames* (Marbach, 1983). A més, els mitjans es referien als membres del grup com a *hackers*, ja que era aquest el terme que usaven per caracteritzar les seves accions. Això va marcar, doncs, un abans i un després en l'ús del terme *hacker*, que va canviar pel que fa a la seva connotació original als anys cinquanta i seixanta, relacionada amb ajustos informàtics ètics. El vincle entre pirateria i delinqüència proporcionat pels mitjans de comunicació va ajudar a persuadir tant el públic com els legisladors que era necessari aplicar sancions legals per fer front a les activitats dels *hackers*.

A mesura que la gent va començar a adoptar les tecnologies de PC i a explorar altres sistemes connectats amb mòdems, les comunitats en línia van començar a sorgir per mitjà dels sistemes de butlletins electrònics o BBS (*Bulletin Board Systems*). En concret, els BBS es van convertir en un recurs important per als nous *hackers*, impulsats en part per les gestes observades en els mitjans i en relats de ficció com *WarGames*. Tant els usuaris tecnològics experimentats com els *hackers* van compartir informació detallada sobre els sistemes que van explorar i es van jactar de les seves proeses (Landreth, 1984). Aquests sistemes també van permetre que els pirates informàtics formessin grups amb xarxes

privades i creessin panells protegits amb contrasenya per mantenir a ratlla els iniciats i salvaguardar la seva privadesa (Landreth, 1984; Meyer, 1989). Els grups de *hackers* locals també es van fer prominents en funció de les seves gestes i intrusions en sistemes informàtics sensibles, com els *Masters of Disaster* i la *Legion of Doom* ('mestres del desastre' i 'legió de la perdició', respectivament).

Segons anava creixent la població de *hackers*, una nova escissió va sorgir amb la publicació d'un breu text anomenat «La consciència d'un hacker» o «El manifest del hacker». El document va ser publicat pel Mentor (The Mentor) el 1986, com a diatriba contra els adults, la policia i les escoles (Furnell, 2002, pàg. 59). El Mentor assenyalava que els *hackers* busquen el coneixement, fins i tot si això significa irrompre o obtenir accés il·legal en sistemes informàtics per protegir-los. Aquestes activitats, no obstant això, no converteixen els *hackers* en delinqüents. Aquests, en canvi, solen rebre la incomprensió i el rebuig de la població adulta desconeixedora del valor de la tecnologia. El Mentor, a més, va instigar els pirates informàtics a participar en actes de *phreaking*, ja que les companyies telefòniques estan «dirigides per avariciosos i aprofitats» (Furnell, 2002, pàg. 59; The Mentor, 1986). Aquest document va donar suport en certa manera a la concepció cada vegada més delictiva de la pirateria, en contrast, doncs, amb la noció del *hacking* dels anys seixanta i l'«ètica *hacker*». Com a conseqüència, una bretxa va començar a obrir-se entre els *hackers* que donaven suport al citat manifest i aquells altres més alineats amb l'ètica *hacker*, així com va canviar la percepció que es tenia de la pirateria maliciosa i exploratòria.

L'èmfasi cada vegada major en la faceta delictiva de la pirateria va començar a canviar la percepció dels *hackers*, que van passar d'agents ètics qualificats a entitats criminals malicioses. Aquesta concepció es va emparar, al seu torn, en la Llei d'Abús i Frau Informàtic en Dispositius d'Accés Fraudulent de 1984, així com en la seva posterior revisió el 1986. La llei de 1984 es va centrar inicialment en l'ús i ús indegut de la informació continguda en targetes de crèdit, i va establir que qualsevol delicte de 5.000 $ de pèrdua o més es consideraria un delicte federal que passaria a controlar el Servei Secret. La revisió de 1986 d'aquesta llei, no obstant això, va ampliar la protecció legal a tota aquella informació computaritzada en bancs i institucions financeres. Així mateix, la llei va afegir tres noves infraccions, inclòs l'accés no autoritzat a sistemes informàtics amb vista a estafar i causar perjudicis, així com el tràfic de contrasenyes informàtiques amb intenció de frau. En incloure aquestes activitats, els legisladors van criminalitzar moltes de les accions efectuades per *hackers* joves i que no necessàriament tenien mala fe.

La proclamació d'aquestes noves lleis va proporcionar a les forces de seguretat millors eines per investigar i enjudiciar eficaçment els atacs de *hackers* a tot el país (Sterling, 1992). De fet, nombroses recerques d'alts càrrecs policials es van dur a terme a la fi dels anys vuitanta i principis dels noranta, com la

batalla entre els grups *hackers* Legion of Doom i Masters of Deception (Slatalla i Quittner, 1995), així com els actes ciberdelictius de Kevin Mitnick (Shimomura i Markoff, 1996) i Kevin Poulson (Littman, 1997).

La dècada de 1980 també va veure l'aparició de les primeres formes de programari maliciós, o *malware*, dissenyat per infectar els sistemes de PC i els usuaris domèstics. Les primeres formes de *malware* solien reproduir melodies simples o eliminaven lletres de documents, i es propagaven d'un ordinador a un altre amb disquets. No obstant això, la creació i distribució del primer cuc conegut d'internet va demostrar el dany que podia causar un programari maliciós.

El 1988, Robert Morris va voler comprendre i documentar la mida d'internet i el nombre d'ordinadors connectats al mateix temps (Holt, Bossler i Seigfried-Spellar, 2017). Va escriure un fragment de codi dissenyat per recopilar aquesta informació de manera remota movent-se lentament d'un ordinador a un altre, encara que a causa d'una fallada en la seva programació va aprofitar sense adonar-se'n les vulnerabilitats de desbordament de búfer en el programari. Com a conseqüència, el cuc es va propagar més de pressa del previst i l'*exploit* va causar un atac de denegació de servei, o DoS (*denial of service attack*), que va deixar, en aquest moment, tota internet inactiva (Holt, 2003). Morris va rebre una multa de 10.050 $, va obtenir una sentència de llibertat condicional de tres anys i va ser obligat a 400 hores de servei comunitari per les seves accions, una sentència significativa en aquell moment (Holt i altres, 2017). Aquest incident va tenir un major impacte en la creació de comunitats de seguretat informàtica, en donar lloc a la formació del primer Computer Emergency Response Team ('equip de resposta a emergències informàtiques', CERT) a la Carnegie Mellon per respondre davant de noves amenaces en línia (Holt, 2003).

7.4. Els anys noranta

El dany significatiu que el cuc de Morris va produir en el processament del sistema va assentar les bases per a un nou tipus de *malware* a finals dels anys vuitanta i principis dels noranta. A mesura que la tecnologia es va fer cada vegada més accessible i assequible a principis de la dècada de 1990, la població de *hackers* va continuar expandint-se i el terme *hacking* es va relacionar cada vegada més amb activitats malicioses. A principis de la dècada de 1990, els funcionaris de les forces de l'ordre públic estatals i federals van tractar d'eliminar sistemàticament les xarxes informàtiques del que es percebia com un nombre cada vegada major de *hackers*. Aquest procés, denominat per Sterling (1992) «la repressió dels *hackers*» (o «The Hacker Crackdown»), va consistir en gran manera en operacions encobertes per part d'investigadors que actuaven com a *hackers* en taulers d'anuncis i sales de xat falses per guanyar-se la confiança dels pirates informàtics.

Malgrat la creixent bretxa cultural i generacional entre els *hackers* originals del MIT i la nova generació de pirates informàtics a la internet dels noranta, tots ells van compartir elements comuns amb la cultura *hacker* original. Per exemple, els pirates informàtics moderns generalment intenten reunir documents interns després d'accedir a un sistema, tant per fanfarronejar com per permetre el lliure intercanvi d'informació per la xarxa de *hackers* (Holt i Kilger, 2012). Aquest desig de difondre informació i debatre mètodes d'atac va permetre a la policia reunir proves d'activitats il·legals. Com a conseqüència, el lliure intercanvi d'informació dins de la comunitat *hacker* va començar a evolucionar

per disminuir la probabilitat de ser detinguts o rebre condemnes. Els grups de *hackers* locals van començar a donar suport a conferències sobre pirateria, incloses Defcon, Hackers On Planet Earth i PhreakNIC (Holt i altres, 2017).

Aquestes reunions van oferir als *hackers* l'oportunitat de relacionar-se en el món real i va atorgar-los cert aire de respectabilitat davant les cada vegada més freqüents condemnes a grups de *hackers*. Al mateix temps, els pirates informàtics van establir vincles directes amb la comunitat *underground* a causa de les presentacions sobre activitats de pirateria que infringirien la llei (Holt, 2007).

Per exemple, el grup de *hackers* anomenat Cult of the Dead Cow (cDc) va llançar un programa de *malware* troià creat durant un panell en el Defcon de 1999 (Messmer, 1999). Van llançar CD amb el *malware* al públic i van encoratjar la gent a utilitzar l'eina perquè podia aplicar-se a la seguretat informàtica. En concret, el programa va permetre als usuaris controlar de manera remota els ordinadors que tenien el programari instal·lat en el seu sistema. Podien ajudar l'usuari controlant el seu ratolí o els seus arxius sense la necessitat d'estar presents a la mateixa habitació. Així mateix, el programa instal·lava portes posteriors en el sistema que no podien eliminar-se, i permetia eliminar o alterar els arxius del sistema i capturar totes les pulsacions de teclat i contrasenyes (Sourceforge, 1999). Com a resultat, aquesta eina es va utilitzar més com un recurs d'atac de *malware* que com una eina legítima de seguretat (Messmer, 1999).

El llançament del BO2K és un bon exemple de la relació dinàmica entre seguretat i pirateria maliciosa que va començar a la fi dels anys noranta. Aquesta relació es va veure agreujada en part quan els professionals de la seguretat informàtica van incorporar un ús ètic de les tècniques de pirateria per defensar-se dels atacants. A mesura que les empreses i les agències governamentals utilitzaven amb cada vegada més freqüència ordinadors connectats a xarxes internes i a la resta de sistemes arreu del món, la necessitat de protegir els actius sensibles de l'amenaça dels pirates informàtics i de l'ús indegut de la informàtica va augmentar considerablement (Taylor, 1999). La comercialització massiva d'ordinadors personals també va augmentar la necessitat de mesures de seguretat personal i aïllament pel que fa a atacants de tot el món.

Per exemple, el virus Melissa va infectar ordinadors a tot el món en enviar correus electrònics infectats dissenyats per propagar el virus, la qual cosa va suposar almenys 80.000.000 $ en danys (Furnell 2002). De la mateixa manera, els cucs ILOVEYOU i Code Red van suposar pèrdues de milers de milions de dòlars en els primers anys del nou mil·lenni (Holt i altres, 2017).

L'evolució de la comunitat de seguretat informàtica en la dècada de 1990 es va produir arran de la incorporació de *hackers* qualificats que entenien el procés d'identificació i protecció de programari i maquinari vulnerables en càrrecs de la indústria privada i del govern. Això va generar una nova tensió dins de la comunitat de *hackers* entre els pirates informàtics suposadament ètics que treballaven per a la indústria privada i en empreses de seguretat de nova creació i aquells altres *hackers* poc ètics que utilitzaven les mateixes tècniques per explorar i atacar sistemes (Taylor, 1999). Mentre que alguns van percebre aquest fet com una tornada a la idea original de l'ètica *hacker*, altres van considerar que la transició del *hacker* al professional de seguretat era vendre l'ànima al diable i trair la naturalesa de l'obertura d'informació en la comunitat *hacker*.

La condemna i detenció de Kevin Mitnick va avivar aquesta tensió a mitjan anys noranta. Mitnick va ser considerat un heroi a la comunitat *hacker* per la seva gran habilitat per a

la pirateria i pel tracte excessivament sever que va rebre a les mans de la policia i els fiscals. De fet, els fiscals federals van prohibir que Mitnick utilitzés ordinadors o dispositius connectats a internet durant diversos anys després d'haver sortit d'una presó federal pel temor al fet que pogués causar un gran dany a la telefonia o la indústria privada (Loper, 2000). Molts *hackers* van donar diners al fons de defensa legal de Mitnick, i van sentir que era un simple boc expiatori de la por dels legisladors i les forces de l'ordre a la comunitat *hacker*. Poc després de la seva sortida de presó, Mitnick va fundar una consultoria de seguretat informàtica, que alguns van veure com una traïció als principis bàsics de la comunitat *hacker* (Loper, 2000). Com a resultat, va perdre respecte entre els membres de la comunitat *hacker*, encara que va servir de model perquè uns altres passessin de ser delinqüents coneguts a experts de seguretat informàtica en una societat cada vegada més depenent de la tecnologia.

A finals dels noranta, la World Wide Web i els PC havien canviat radicalment la naturalesa dels negocis i les comunicacions. L'expansió global i la connectivitat que ofereix internet van conduir a la digitalització d'informació confidencial financera i governamental, i a la creació d'enormes bases de dades accessibles en línia. Els proveïdors de serveis financers, les xarxes socials i les plataformes comercials es van traslladar a entorns en línia per oferir directament serveis als usuaris de PC, oferint-los comoditat per a la comunicació i les compres. Com a conseqüència, el panorama i la dinàmica del *hacking*, així com la indústria de seguretat informàtica, van canviar.

La gent va començar a aplicar tècniques i habilitats de pirateria en atacs motivats políticament i socialment contra objectius governamentals i de la indústria privada.

Per exemple, els membres del col·lectiu de *hackers* Electronic Disturbance Theatre van crear i van llançar una eina d'atac anomenada FloodNet (Jordan i Taylor, 2004; Schell i Dodge, 2002). Aquest programa va ser dissenyat com una eina independent per permetre a pirates no qualificats participar en atacs de denegació de servei en diversos serveis governamentals com una forma de «desobediència civil» (Schell i Dodge, 2002). Un atac així impedeix que la gent pugui usar els serveis de comunicacions, la qual cosa els torna inútils. Així mateix, nombrosos *hackers* dels Estats Units i de la Xina van participar en una sèrie de desfiguracions de xarxa atacant-se els uns als altres com a forma d'expressió política quan un avió espia nord-americà es va estavellar a la Xina (Denning, 2003). Les desfiguracions web permeten a l'atacant reemplaçar la pàgina web original amb contingut propi, incloent-hi text i imatges.

Un atac així és ideal perquè els *hackers* amb motivació política mostrin les seves actituds i creences a tothom (Andress i Winterfeld, 2014). Per tant, el nombre de desfiguracions va augmentar dramàticament durant aquest període a mesura que més països es van connectar a internet i van veure-hi un mitjà per expressar les seves idees polítiques i religioses.

Durant aquest període, es va llançar un notable programa de *malware* troià anomenat Sub7, famós per la seva capacitat per infectar totes les variants dels sistemes operatius Windows (Crapanzano, 2003). El *malware* podia enviar-se com a arxiu adjunt de correu electrònic i emular diferents tipus d'arxius populars, com .doc o .ppt, així com arxius d'imatge. Una vegada s'executava el programa, la seva càrrega útil permetia a un atacant administrar l'ordinador infectat a distància, la qual cosa incloïa la capacitat d'afegir o eliminar arxius, capturar pulsacions de tecles i contrasenyes emmagatzemades a la memòria cau, i controlar la càmera del sistema, el micròfon, les unitats de disc i les pantalles de l'escriptori (Crapanzano, 2003). A més, el *malware* proporcionaria

actualitzacions a l'atacant en temps real, la qual cosa els permetia saber quan s'estava utilitzant el sistema i la víctima es trobava en línia. Així, aquesta eina es va fer molt popular entre els *hackers* per la seva facilitat d'ús i el seu poder sobre sistemes específics.

7.5. Dels 2000 fins avui

La dècada dels 2000 va suposar encara més canvis en la pirateria, més concretament la transició cap a la professionalització dels *hackers*. Les motivacions de la pirateria van passar de l'adquisició de prestigi i acceptació social en la comunitat *hacker*, que van predominar en els anys vuitanta i noranta, a la cerca del benefici econòmic (Holt i Lampke 2010; Chu i altres, 2010). La complexitat de les eines utilitzades per *hackers* va augmentar, i el seu propòsit va passar d'infecció i degradació de xarxes globals a l'atac i el robatori subrepticis d'informació confidencial. Per exemple, la creació i adopció de *malware* de *botnet* va tenir un gran impacte en les pràctiques de pirateria i de *malware* (Bacher i altres, 2005). El codi de *botnet* constitueix una amenaça combinada, ja que conjumina *malware* de troians i virus, propagant-se de la mateixa manera que els programes de troians o altres mètodes d'infecció (Chu i altres, 2010). En executar la càrrega útil del *malware*, el codi instal·la un programa *bot*, que converteix el dispositiu en un *zombi* que pot controlar-se a distància per mitjà d'un protocol de missatgeria instantània anomenat Internet Relay Chat (IRC) (Bacher i altres, 2005; Chu i altres, 2010). El canal IRC per controlar el sistema infectat està preprogramat en el codi, la qual cosa permet a l'operador de *botnet* enviar comandos al sistema. A més, es poden infectar diversos dispositius amb aquest *malware* i contactar simultàniament amb el canal, creant una xarxa *bot* o una xarxa de dispositius zombis. Al seu torn, el controlador del *bot* pot emprar la seva xarxa de dispositius infectats per enviar *spam* o participar en atacs DDoS contra diversos objectius (Chu i altres, 2010).

El sorgiment de *botnets* va ser de gran ajuda a la comunitat *hacker*, ja que proporcionava una plataforma d'atac estable fàcil d'administrar i mantenir.

Per exemple, els sistemes infectats controlats per l'operador de *botnet* poden usar-se per enviar correu no desitjat, verificar targetes de crèdit obtingudes de manera fraudulenta o arrendar els sistemes infectats com a serveis *proxy* per ocultar un tràfic web maliciós (Holt, 2013).

Vegeu també

Per a més informació sobre el robatori de dades, vegeu el mòdul 3.

A més, els *botnets* poden emprar-se per participar en atacs de denegació de servei, on cada ordinador a la xarxa intenta contactar el mateix ordinador o servidor de contingut en línia. Les sol·licituds es poden ajustar perquè ocorrin en un període de temps determinat, per exemple, cada 0,5 mil·lisegons, per així saturar l'ordinador amb aquestes sol·licituds. Per tant, el sistema en qüestió no pot resoldre les sol·licituds que arriben i no quedarà disponible fins que les sol·licituds s'aturin (Holt, 2013). Aquests atacs poden ser extremament costosos per a les empreses si els clients no poden fer servir els seus recursos durant llargs períodes de temps (Bacher i altres, 2005; CSI, 2010).

Així mateix, els *hackers* van començar a llogar els seus *botnets* a altres per obtenir beneficis de la seva infraestructura (Chu i altres, 2010; Franklin i altres, 2007). Els operadors de *botnets* podrien guanyar amb això milers de dòlars cada setmana o més, depenent del seu abast a sistemes infectats i recursos operatius (Holt, 2013). L'aparició d'aquest mercat ha perjudicat greument la comunitat *hacker*, ja que es requereix una habilitat menor per piratejar (Holt, 2013). Per contra, els usuaris poden pagar altres *hackers* perquè ataquin en el seu nom sense la necessitat de crear les seves pròpies eines o infeccions. Com a resultat, alguns membres de la comunitat de ciberseguretat es van referir al *malware* de *botnet* com a *crimeware*, ja que aquests permeten a les parts interessades una via directa per participar en ciberdelictes a baix cost (Bacher i altres, 2005).

El model proporcionat pel *malware* de *botnet* també va suposar que una sèrie de *malwares* i serveis de pirateria estiguessin disponibles a baix cost en diferents mercats clandestins (Holt, 2013). Els atacants venien l'accés a codis exclusius de programari maliciós, troians i altres eines, com a paquets d'*exploits*, que infecten sistemes informàtics per mitjà d'*exploits* en navegadors web. De la mateixa manera, la gent ven bases de dades de correu electrònic que podrien utilitzar-se per enviar correu no desitjat, dades confidencials obtingudes a partir de troians espia i altres serveis que podrien usar-se per participar en atacs informàtics i ciberdelictes econòmics (Holt, 2013).

L'evolució dels *smartphones* i altres dispositius connectats a la xarxa wifi a mitjan 2000 també va portar els *hackers* a atacar aquests sistemes, atrets per la informació confidencial que contenen. Per exemple, la capacitat d'accedir a comptes bancaris i llocs de comerç electrònic per mitjà d'aplicacions mòbils ofereix l'oportunitat als atacants que adquireixin aquesta informació. Els *hackers* i els escriptors de *malware* van començar a interessar-se a piratejar aquests dispositius i van adaptar el *malware* a aquestes plataformes (BitDefender, 2009). Una de les eines de *malware* més notables utilitzades per atacar telèfons mòbils era coneguda pels proveïdors de ciberseguretat com Zeus (Panda Security, 2015). Aquest troià es va adaptar als dispositius mòbils utilitzant sistemes operatius Android, i es va dissenyar i va publicar com una aplicació bancària (Leyden, 2012). El programa capturava els missatges SMS per autenticar transaccions entre la institució financera i el client (FBI, 2010; Leyden, 2012). Una vegada adquirit, el *malware* podia usar aquests detalls financers per realitzar transferències bancàries fraudulentes sense que els clients ho sabessin. Com a resultat, aquests ciberdelinqüents han pogut guanyar amb èxit desenes de milions de dòlars fent transaccions bancàries fraudulentes a Europa i els Estats Units (FBI, 2010; Leyden, 2012).

Els Estats nació també van començar a participar en operacions sofisticades de pirateria per adquirir informació confidencial i propietat intel·lectual d'empreses, universitats i agències governamentals.

Vegeu també

Per a més informació sobre aquest tema, vegeu el mòdul 5.

Per exemple, un grup que es fa dir Guardians of Peace ('Guardians de la pau') va atacar la seu de Sony Pictures el 2014 utilitzant una sofisticada quantitat d'eines de *malware* i tècniques de pirateria (Robb, 2014). Els atacants van obtenir *terabytes* de dades,

des d'informació sobre els empleats fins a correus electrònics confidencials, guions i pel·lícules sense estrenar (Robb, 2014). Tota aquesta informació es va publicar en línia en un intent d'avergonyir la companyia i avergonyir-los perquè no estrenessin la pel·lícula anomenada *The Interview*, que parlava d'un complot per assassinar el líder nord-coreà Kim Jong-un (Robb, 2014). Les anàlisis posteriors a l'atac realitzades per les forces de l'ordre i les agències d'intel·ligència van vincular l'atac al Govern de Corea del Nord, o almenys a *hackers* que treballen en el seu nom (Zetter, 2016).

Per tant, la pirateria ha canviat dràsticament des del seu ús inicial en universitats i organitzacions.

Resum

En general, els actes de ciberintrusió relacionats amb la pirateria informàtica i el programari maliciós són el resultat directe de la nostra cada vegada major dependència social pel que fa a la tecnologia. No tots els *hackers* són delinqüents, encara que les tècniques que fan servir poden utilitzar-se per participar en activitats il·legals. El *hacking* en general suposa utilitzar coneixements sobre els sistemes i programes informàtics, encara que el seu resultat pot anar des de la modificació dels processos del sistema fins a la interrupció de la xarxa i el dany econòmic greu. L'evolució de la pirateria en els últims cinquanta anys demostra com les motivacions dels *hackers* maliciosos han canviat per centrar-se més en el guany econòmic, ja sigui amb la venda d'eines i serveis de pirateria, o per l'ús indegut d'informació confidencial. És probable que aquesta tendència continuï, sempre que els pirates informàtics puguin beneficiar-se de les seves accions, encara que han de seguir elaborant-se estudis per avaluar aquestes qüestions (vegeu el mòdul 6).

Bibliografia

Andress, J.; Winterfeld, S. (2013). *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier.

Bacher, P.; Holz, T.; Kotter, M.; Wicherski, G. (2005). *Tracking botnets: Using honeynets to learn more about bots* [en línia]. The Honeynet Project and Research Alliance. <www.honeynet.org/papers/bots/>

Bachmann, M. (2010). «The risk propensity and rationality of computer hackers». *The International Journal of Cyber Criminology* (núm. 4, pàg. 643-656).

BitDefender (2009). «Trojans continue to dominate BitDefender's top ten e-threats». *BitDefender*. [en línia]. <www.bitdefender.com/news/trojans-continue-to-dominate-bitdefender%E2%96%93s-top-ten-e-threats-for-october-1208.html>

Bossler, A. M.; Burruss, G. W. (2011). «The General Theory of Crime and Computer Hacking: Low Self-Control Hackers?». A: T. J. Holt i B. H. Schell (eds.). *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pàg. 38-67). Hershey, PA: ISI Global.

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).

Bossler, A. M.; Holt, T. J.; May, D. C. (2012). «Predicting online harassment among a juvenile population». *Youth and Society* (núm. 44, pàg. 500-523).

Brenner, S. W. (2008). *Cyberthreats: The Emerging Fault Lines of the Nation State*. Nova York: Oxford University Press.

Brenner, S. W. (2011). «Defining Cybercrime: A Review of Federal and State Law». A: R. D. Clifford (ed.). *Cybercrime: The Investigation, Prosecution, and Defense of a Computer Related Crime* (3a. ed., pàg. 15-104). Raleigh, NC: Carolina Academic Press.

Cappelli, D. M.; Moore, A. P.; Trzeciak, R. F.; Shimeall, T. J. (2008). «Common Sense Guide to Prevention and Detection of Insider Threats». *CERT Insider Threat Study Team*. Carnegie Mellon University.

Ceruzzi, P. (1998). *A History of Modern Computing*. Cambridge, MA: MIT Press.

Choi, K. S. (2008). «Computer crime victimization and integrated theory: An empirical Assessment». *International Journal of Cyber Criminology* (vol. 2, núm. 1).

Chu, B.; Holt, T. J.; Ahn, G. J. (2010). *Examining the Creation, Distribution, and Function of Malware On-Line* [en línia]. Washington, DC: National Institute of Justice. <www.ncjrs.gov/pdffiles1/nij/grants/230112.pdf>

Chua, Y. T.; Holt, T. J. (2016). «A cross-national examination for the techniques of neutralization to account for hacking behaviors». *Victims & Offenders* (vol. 11, núm. 4, pàg. 534-555).

Correll, S. P. (2010). «An interview with Anonymous». *PandaLabs Blog* (núm. 29).

Crapanzano, J. (2003). «Deconstructing SubSeven, the Trojan Horse of Choice» [en línia]. *SANS Reading Room*. <https://www.sans.org/reading-room/whitepapers/malicious/deconstructing-subseven-the-trojan-horse-of-choice-953>

Denning, D. E. (gener de 2003). «Cyber Security as an Emergent Infrastructure». A: *World Conference on Information Security Education* (pàg. 1-2).

Denning, D. E. (2010). «Cyber-Conflict as an Emergent Social Problem». A: T. J. Holt i B. Schell (eds.). *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pàg. 170-186). Hershey, PA: IGI-Global.

Dhillon & Dhillon, G.; Moores, S. (2001). «Computer crimes: theorizing about the enemy within». *Computers & Security* (vol. 20, núm. 8, pàg. 715-723).

Dunham, K. (2008). *Mobile Malware Attacks and Defense*. Burlington, MA: Syngress.

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, pàg. 1219-1243).

Federal Bureau of Investigation (2010). «Cyber banking fraud: Global partnerships lead to major arrests» [en línia]. <www.fbi.gov/news/stories/2010/october/cyber-banking-fraud>

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).

Fruhlinger, J. (2018). «What Is WannaCry Ransomware, How Does It Infect, and Who Was Responsible?». *CSO* [en línia]. <https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html>

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

Gilboa, N. (1996). «Elites, Lamers, Narcs, and Whores: Exploring the Computer Underground». A: L. Cherny; E. R. Weise (eds.). *Wired_Women* (pàg. 98-113). Seattle: Seal Press.

Gordon, S. (2000). *Virus Writers: The End of the Innocence?* [en línia]. <http://vxheaven.org/lib/asg12.html>

Gordon, S.; Ma, Q. (2003). *Convergence of virus writers and hackers: Factor or fantasy*. Cupertino, CA: Symantec Security White Paper.

Gottfredson, M. R.; Hirschi, T. (1990). *A General Theory of Crime*. Stanford, CA: Stanford University Press.

Grabosky, P. N. (2001). «Virtual criminality: Old wine in new bottles?». *Social & Legal Studies* (vol. 10, núm. 2, pàg. 243-249).

Grabosky, P.; G. Smith, Russell; Urbas, G. (2004). *Cyber Criminals on Trial*. Cambridge University Press.

Higgins, G. E.; Makin, D. A. (2004). «Does social learning theory condition the effects of low self-control on college students' software piracy». *Journal of Economic Crime Management* (vol. 2, núm. 2, pàg. 1-22).

Higgins, G. E.; Wilson, A. L. (2006). «Low self-control, moral beliefs, and social learning theory in university students' intentions to pirate software». *Security Journal* (vol. 19, núm. 2, pàg. 75-92).

Hollinger, R.; Lanza-Kaduce, L. (1988). «The process of criminalization: The case of computer crime laws». *Criminology* (núm. 26, pàg. 101-126).

Holt, T. J. (2003). «Examining a transnational problem: An analysis of computer crime victimization in eight countries from 1999 to 2001». *International Journal of Comparative and Applied Criminal Justice* (vol. 27, núm. 2, pàg. 199-220).

Holt, T. J. (2007). «Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures». *Deviant Behavior* (núm. 28, pàg. 171-198).

Holt, T. J. (2009). «Lone Hacks or Group Cracks: Examining the Social Organization of Computer Hackers». A: F. Schmalleger; M. Pittaro (eds.). *Crimes of the Internet* (pàg. 336-355). Upper Saddle River, NJ: Pearson Prentice Hall.

Holt, T. J. (2012). «Exploring the intersections of technology, crime, and terror». *Terrorism and Political Violence* (vol. 24, núm. 2, pàg. 337-354).

Holt, T. J. (2013). «Examining the forces shaping cybercrime markets online». *Social Science Computer Review* (núm. 31, pàg. 165-177).

Holt, T. J.; Bossler, A.; Seigfried-Spellar, K. C. (2017). *Cybercrime and Digital Forensics: An Introduction* (2a. ed). Londres: Routledge.

Holt, T. J.; Burruss, G. W.; Bossler, A. M. (2010). «Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world». *Journal of Crime and Justice* (núm. 33, pàg. 15-30).

Holt, T. J.; Burruss, G. W.; Bossler, A. M. (2018). «Assessing the macro-level correlates of malware infections using a routine activities framework». *International journal of offender therapy and comparative criminology* (vol. 62, núm. 6, pàg. 1720-1741).

Holt, T. J.; Freilich, J. D.; Chermak, S. M. (2017). «Exploring the subculture of ideologically motivated cyber-attackers». *Journal of contemporary criminal justice* (vol. 33, núm. 3, pàg. 212-233).

Holt, T. J.; Graves, D. C. (2007). «A qualitative analysis of advance fee fraud e-mail schemes». *International Journal of Cyber Criminology* (vol. 1, núm. 1, pàg. 137-154).

Holt, T. J.; Kilger, M. (2008). «Techcrafters and makecrafters: A comparison of two populations of hackers». *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing* (pàg. 67-78).

Holt, T. J.; Kilger, M. (2012). «Know your enemy: The social dynamics of hacking». *The Honeynet Project* [en línia]. <https://honeynet.org/files/Holt%20and%20Kilger%20-%20KYE%20-%20The%20Social%20Dynamics%20of%20Hacking.pdf>

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.; Stonhouse, M.; Freilich, J.; Chermak, S. M. (2019). «Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups». *Terrorism and Political Violence* (pàg. 1-22).

Holt, T. J.; Strumsky, D.; Smirnova, O.; Kilger, M. (2012). «Examining the Social Networks of Malware Writers and Hackers». *International Journal of Cyber Criminology* (vol. 6, núm. 1).

Holt, T. J.; van Wilsem, J.; van de Weijer, S.; Leukfeldt, R. (2018). «Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization». *Social Science Computer Review* (0894439318805067).

Huang, W.; Brockman, A. (2010). «Social Engineering Exploitations in Online Communications: Examining Persuasions used in Fraudulent E-mails». A: Holt, T. J. (ed.). *Crime Online: Causes, Correlates, and Context* (pàg. 87-112). Raleigh, NC: Carolina Academic Press.

Hutchings, A.; Chua, Y. T. (2016). «Gendering cybercrime». A: *Cybercrime Through an Interdisciplinary Lens* (pàg. 181-202). Londres: Routledge.

IBM (2016). *IBM study: Businesses more likely to pay ransomware than consumers* [en línia]. <http://www-03.ibm.com/press/us/en/pressrelease/51230.wss>

Information Warfare Monitor (2009). «Tracking ghostnet: Investigating a cyber espionage network» [en línia]. <https://ora.ox.ac.uk/objects/uuid:6d1260fd-b8ee-4a11-8a5f-e7708d543651>

Ingram, J. R.; Hinduja, S. (2008). «Neutralizing music piracy: An empirical examination». *Deviant Behavior* (vol. 29, núm. 4, pàg. 334-365).

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

Jordan, T.; Taylor, P. (1998). «A sociology of hackers». *The Sociological Review* (núm. 46, pàg. 757-780).

Jordan, T.; Taylor, P. (2004). *Hacktivism and Cyber Wars*. Londres: Routledge.

Kaspersky, E. V. (2003). «The classification of computer viruses» [en línia]. Berna: Metropolitan Network BBS Inc. <www.avp.ch/avpve/classes/classes.stm>

Kilger, M. (2010). «Social Dynamics and the Future of Technology-Driven Crime». A: T. J. Holt i B. Schell (eds.). *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pàg. 205-227). Hershey, PA: IGI-Global.

King, A.; Thomas, J. (2009). «You can't cheat an honest man: Making $$$ and sense of the Nigerian Email Scams». A: F. Schmalleger i M. Pittaro (eds.). *Crimes of the Internet* (pàg. 206-224). Upper Saddle River, NJ: Pearson Prentice Hall.

Krance, M.; Murphy, J.; Elmer-Dewitt, P. (1983). «The 414 Gang Strikes Again» [en línia]. *Time*. <www.time.com/time/magazine/article/0,9171,949797,00.html>

Kravets, D. (2010). «U. S. declares iPhone jailbreaking legal, over Apple's objections» [en línia]. *Wired Threat Level* <www.wired.com/threatlevel/2010/07/feds-ok-iphone-jailbreaking/>

Landreth, B. (1985). *Out of the Inner Circle*. Seattle, WA: Microsoft Press.

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

Levi, M.; Reuter, P.; Halliday, T. (2018). «Can the AML system be evaluated without better data?». *Crime, Law and Social Change* (pàg. 1-22).

Levy, S. (2001). *Hackers: Heroes of the Computer Revolution*. Nova York: Penquin.

Leyden, J. (2012). «Major £30m cyberheist pulled off using MOBILE malware» [en línia]. *The Register* (7 de desembre). <www.theregister.co.uk/2012/12/07/eurograbber_mobile_malware_scam/>

Littman, J. (1997). *The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen*. Nova York: Little Brown.

Loper, K. (novembre de 2000). «Profiling hackers: beyond psychology». A: *Annual meeting of the American Academy of Sociology*.

Marbach, W. (1983b). «Cracking Down on Hackers». *Newsweek* (núm. 34).

Marcum, C. D.; Higgins, G. E.; Ricketts, M. L.; Wolfe, S. E. (2014). «Hacking in high school: Cybercrime perpetration by juveniles». *Deviant Behavior* (vol. 35, núm. 7, pàg. 581-591).

Markoff, J. (2009). «Vast spy system loots computers in 103 countries». *The New York Times* (núm. 29).

Kaspersky, E. V. (2003). «The classification of computer viruses» [en línia]. Berna: Metropolitan Network BBS Inc., Bern, Switzerland. <www.avp.ch/avpve/classes/classes.stm>

Meyer, G. R. (1989). *The Social Organization of the Computer Underground* (tesis de máster). Northern Illinois University.

Miller, W. B. (1958). «Lower class culture as a generating milieu of gang delinquency». *Journal of Social Issues* (vol. 14, núm. 3, pàg. 5-19).

Mitnick, K. D.; Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Nova York: Wiley Publishing.

Nazario, J. (2003). *Defense and Detection Strategies against Internet Worms*. Artech House.

Newman, G.; Clarke, R. (2003). *Superhighway Robbery: Preventing E-commerce Crime*. Cullompton, NJ: Willan Press.

Ngo, F. T.; Paternoster, R. (2011). «Cybercrime victimization: An examination of individual and situational level factors». *International Journal of Cyber Criminology* (núm. 5, pàg. 773-793).

PandaLabs (2013). «Malware infections in protected systems» [en línia]. <http://research.panadasecurity.com/blogs/images/wp_pb_malware_infections_in_protected_Systems.pdf>

Panda Security (2015). *Annual Report PandaLabs 2015 Summary* [en línia]. <http://www.pandasecurity.com/mediacenter/src/uploads/2014/07/Pandalabs-2015-anual-EN.pdf>

Parker, D. B. (1980). «Computer abuse research update». *Computer/LJ* (núm. 2, pàg. 329).

Ponemon Institute (2018). *2018 Cost of Data Breach Study: Impact of Business Contiunity Management* [en línia]. <https://ibm.co/2L7Th4P>

Pratt, T. C.; Cullen, F. T. (2000). «The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis». *Criminology* (núm. 38, pàg. 931-964).

Rantala, R. R. (2008). *Cybercrime against businesses, 2005* (NCJ 221943) [en línia]. Bureau of Justice Statistics <www.bjs.gov/content/pub/pdf/cb05.pdf>

Robb, D. (2015). «The Sony Hack one year later: Just who are the Guardians of Peace?» [en línia]. *Deadline* (24 de novembre). <https://deadline.com/2015/11/sony-hack-guardians-of-peace-one-year-anniversary-1201636491/>

Russinovich, M. (2013). «Hunting down and killing ransomware (scareware)» [en línia]. *Microsoft TechNet Blog*. <http://blogs.technet.com/b/markrussinovich/archive/2013/01/07/3543763.aspx>

Schell, B. H.; Dodge, J. L. (2002). *The Hacking of America: Who's Doing it, Why, and How*. Westport, CT: Quorum Books.

Schneider, H. (2008). *Wargames*. United Artists.

Shaw, E. D.; Ruby, K. G.; Post, J. M. (1998). «The insider threat to information systems». *Security Awareness Bulletin* (vol. 2, núm. 98, pàg. 1-10).

Shimomura, T.; Markoff, J. (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw –by the Man Who Did It*. Nova York: Hyperion.

Short, J. F. (1968). *Gang Delinquency and Delinquent Subcultures*. Oxford: Harper & Row.

Skinner, W. F.; Fream, A. M. (1997). «A social learning theory analysis of computer crime among college students». *Journal of Research in Crime and Delinquency* (núm. 34, pàg. 495-518).

Slatalla, M.; Quittner, J. (1995). *Masters of Deception: The Gang that Ruled Cyberspace*. Nova York: Harper Collins Publishers.

Sourceforge (1999). *Basic BO2K setup tutorial* [en línia]. <http://bo2k. sourceforge.net/docs/bo2k_1_1_5/BasicTutorial.html>

Steinmetz, K. F. (2015). «Craft(y)ness: An ethnographic study of hacking». *British Journal of Criminology* (55, pàg.125-145).

Steinmetz, K. F. (2016). *Hacked: A radical approach to hacker culture and crime*. NYU Press.

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Nova York: Bantam Books.

Symantec (2018). *Internet Security Threat Report 2018* [en línia] (vol. 23). <https://resource.elq.symantec.com/LP=6819?inid=symc_threat-report_istr_to_leadgen_form_LP-6819_ISTR-2019-report-main&cid=70138000001Qv0PAAS>

Szor, P. (2005). *The Art of Computer Virus Research and Defense*. Nova York: Addison-Wesley.

Taylor, P. (1999). *Hackers: Crime in the Digital Sublime*. Londres: Routledge.

Thomas, D. (2002). *Hacker Culture*. Mineàpolis, MN: University of Minnesota Press.

Turgeman-Goldschmidt, O. (2005). «Hacker's accounts: Hacking as a social entertainment». *Social Science Computer Review* (núm. 23, pàg. 8-23).

Turkle, S. (1984). *The Second Self: Computers and the Human Spirit*. Nova York: Simon and Schuster.

Wall, D. S. (2004). «Digital realism and the governance of spam as cybercrime». *European Journal on Criminal Policy and Research* (núm. 10, pàg. 309-335).

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

Wang, W. (2006). *Steal This Computer Book 4.0: What They Won't Tell You About the Internet*. Boston, MA: No Starch Press.

Yar, M. (2005). «The novelty of "cybercrime": An assessment in light of routine activity theory». *European Journal of Criminology* (vol. 2, núm. 4, pàg. 407-427).

Zetter, K. (2016). «The Sony Hackers were causing mayhem for years before they hit the company» [en línia]. *Wired* (24 de febrer) <https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company/>