Programari maliciós

PID_00245418

Erik de Luis Gargallo

Universitat Oberta de Catalunya

Cap part d'aquesta publicació, incloent-hi el disseny general i la coberta, no pot ser copiada, reproduïda, emmagatzemada o transmesa de cap manera ni per cap mitjà, tant si és elèctric com químic, mecànic, òptic, de gravació, de fotocòpia o per altres mètodes, sense l'autorització prèvia per escrit dels titulars del copyright.

Índex

Introducció 5

Objectius 6

1. Classificació del programari maliciós 7
- 1.1. Portes posteriors i troians 7
- 1.2. Virus i cucs 9
- 1.3. Enregistradors de teclat i eines d'intrusió 11
- 1.4. Programari espia i programari de publicitat 13

2. Tipus d'atacs 14
- 2.1. Falsejament d'identitat 15
- 2.2. *Sniffing* 18
- 2.3. Pesca (*phishing*) 19
- 2.4. Injecció SQL 20
- 2.5. *Cross-site scripting* (XSS) 22
- 2.6. DOS i DDOS 22

Resum 25

Activitats 27

Bibliografia 28

Introducció

D'acord amb l'*Informe de tendències en l'activitat d'Anti-Phising Working Group* (APWG), durant el primer semestre del 2016 van ser detectades 873.488 campanyes de correu electrònic relacionades amb accions de pesca. Consisteix en l'enviament massiu de missatges que, aparentant provenir de fonts fiables, intenten aconseguir que l'usuari proporcioni dades confidencials.

APWG

APWG és una coalició internacional que pretén unificar una resposta global als delictes informàtics en tots els sectors de la indústria, el govern, les forces de l'ordre i les ONG.

En els tres primers mesos del 2016 es va registrar el nombre més gran de casos de pesca fins avui, 557.964. Les campanyes de pesca estaven destinades principalment a empreses del sector serveis (43% dels casos) i del sector financer (16% dels casos), amb una mitjana mensual de 418 atacs.

Les xifres parlen per si soles: indubtablement, ens trobem en un moment de creixement del programari maliciós (*malware*), entenent-lo com qualsevol programa l'objectiu del qual és causar danys a les xarxes i els sistemes informàtics. La paraula *malware* prové de la composició de les paraules angleses *malicious* i *software*, és a dir, programa maliciós. Actualment és molt freqüent sentir parlar de les famoses campanyes de programari maliciós de rescat (*ransomware*), l'objectiu del qual és lucrar l'atacant per mitjà de rescats econòmics.

Durant anys molt programari maliciós no ha estat tingut en compte perquè tant els usuaris convencionals com els administradors de sistemes d'informació han cregut que els antivirus estàndard se n'encarregaven.

Avui, res més lluny de la realitat, no només cal disposar d'altres eines per a fer front al potent programari maliciós actual, sinó saber com actuar en cas de resultar infectats. Els objectius del programari maliciós són molt variats, encara que destaquen l'obtenció d'informació, les estafes en línia o directament el dany dels sistemes, per posar tres exemples.

En aquest mòdul farem una classificació bàsica dels diferents tipus de programari maliciós que podem trobar, així com els tipus d'atacs que, en siguin causa o no, podem rebre com a usuaris d'un sistema informàtic.

Objectius

Els materials didàctics d'aquest mòdul proporcionen els continguts i eines imprescindibles per a assolir els objectius següents:

1. Conèixer el diferent programari maliciós existent actualment.

2. Identificar els principals tipus d'atacs presents a internet.

1. Classificació del programari maliciós

Tal com s'ha descrit anteriorment, el codi maliciós o programari maliciós fa referència a programes instal·lats en un ordinador o sistema informàtic (cosa que inclou dispositius electrònics diversos) amb la intenció de comprometre la confidencialitat, integritat o disponibilitat del sistema, les aplicacions i les dades.

El fet que el programari maliciós canviï amb molta freqüència (se sol utilitzar el terme *mutar*), així com el comportament tan variat que té, fa difícil la seva classificació. Cada dia sorgeixen noves mostres de programari maliciós susceptibles de mutar o transformar-se per a adquirir noves funcionalitats.

Les vies d'infecció per programari maliciós són molt variades: baixada de programari no oficial, les xarxes de compartició de fitxers tipus P2P o el simple intercanvi de documents infectats, normalment adjunts a correus electrònics o llapis de memòria tipus USB.

A continuació s'establirà una classificació bàsica sobre els tipus de programari maliciós més comuns que podem trobar.

1.1. Portes posteriors i troians

S'entén per porta posterior (*backdoor*) el programari maliciós capaç de saltar-se els controls d'accés, identificació i autenticació d'usuaris i permetre accessos no controlats a un entorn.

Se l'anomena *porta posterior* per analogia al que seria una suposada entrada posterior o de servei en una empresa. A l'entrada principal hi hauria molta seguretat (guàrdies, arc de control, càmeres, etc.) però no a la porta de servei. Qualsevol atacant que conegués la porta de servei la podria fer servir per a accedir a les instal·lacions saltant-se tots els controls de seguretat. Les portes posteriors aprofiten errors en el sistema per a crear portes que permetin entrar al sistema saltant-se els controls de seguretat.

També rep el mateix nom el conjunt d'instruccions no documentades dins d'un programa o sistema operatiu (recordem que els programes informàtics estan formats per instruccions) que permeten accedir o prendre el control de

l'equip saltant-se els controls de seguretat. Així, per tant, els *backdoor kits* són un programari maliciós l'objectiu del qual és l'explotació d'aquestes portes posteriors.

Mitjançant una porta posterior podem dur a terme una incursió il·legal en servidors o estacions de treball i prendre el control dels sistemes compromesos, amb els danys conseqüents que això implica.

Remote administration tool

En anglès la porta posterior també rep el nom de *remote administration tool* (RAT), encara que en principi els RAT són programes lícits que permeten als administradors de sistemes accedir als ordinadors dels treballadors de l'empresa per a solucionar problemes o instal·lar aplicacions (també es pot fer servir per a reparar ordinadors domèstics a distància). Els RAT no s'haurien d'ocultar mai a l'usuari, però en podem trobar algun que sí que s'oculti, i en aquest cas podria ser usat com a porta posterior.

Aquest tipus de programari maliciós té dos components principals:

- el programa Servidor, que s'instal·la a l'ordinador de la víctima (el servidor serveix les dades), i
- el programa Client, que actua en la computadora de l'atacant (el client rep les dades), el qual disposa d'un programa que li permet executar diferents funcions.

Dins d'aquestes funcions podem trobar l'eliminació de fitxers o la destrucció de la informació del disc dur, la captura i reenviament de dades confidencials a un usuari no autoritzat o l'obertura de ports de comunicacions, cosa que permet que un possible intrús controli el sistema de forma remota.

És important destacar que mitjançant aquest programari maliciós un atacant podrà executar les mateixes accions que l'usuari infectat; és a dir, tindrà els mateixos privilegis en el sistema. Per tant, com més privilegis tingui l'usuari, més accions podrà dur a terme.

Els troians o cavalls de Troia, en record de l'antic cavall de Troia de la mitologia grega, no poden penetrar en els sistemes per si mateixos com fan els virus, sinó que es troben a l'interior d'un altre programari aparentment inofensiu, que sembla que duu a terme una funció útil per a qui l'executa, però que en realitat executa una acció generalment nociva i que l'usuari desconeix.

A diferència dels virus, un troià no es reprodueix i infecta altres fitxers ni es propaga fent còpies de si mateix com fan els cucs. La seva finalitat, com en el cas de les portes posteriors, és obtenir informació de la màquina amfitriona sense que l'usuari se n'adoni i sense que doni el seu consentiment. Causa desperfectes en el sistema, envia correus electrònics il·lícitament i massivament o destrueix dades amb finalitats recaptatòries (troià Cryptolocker).

Cryptolocker

Cryptolocker és un programari maliciós que xifra un equip o certs arxius emmagatzemats i, posteriorment, demana un rescat a canvi del seu alliberament. Les tècniques utilitzades per a instal·lar-se a la màquina de la víctima solen consistir en l'ús d'enginyeria social o l'explotació de vulnerabilitats del programari instal·lat.

Entre les funcions o accions més conegudes podem destacar:

- Prendre el control de l'ordinador atacat.

- Utilitzar el sistema infectat per a atacar altres sistemes.

- Robar la informació continguda. En aquest cas, agafa una importància especial la informació sensible, com per exemple les dades bancàries (troià Zeus).

- Fer canvis en el sistema informàtic.

Zeus

Zeus és un troià que infecta ordinadors amb el sistema operatiu Windows amb l'objectiu de robar les credencials bancàries o obtenir altres tipus d'informació rellevants. També permet a l'atacant executar programes a l'ordinador infectat. Quan un ordinador és infectat amb aquest troià passa a formar part d'una xarxa zombi d'ordinadors, amb la qual cosa pot ser utilitzat per a cometre accions criminals o malicioses.

Com a norma general els antivirus, a mesura que es van descobrint noves versions o tipus de troians, emmagatzemen les seves signatures. Així i tot, és possible que aquest programari maliciós sigui capaç de modificar el comportament de l'antivirus i no ser detectat.

Signatura

Una signatura és una cadena de caràcters (nombres, lletres i símbols) que representa inequívocament un programari maliciós.

1.2. Virus i cucs

Els virus són programes que es reprodueixen i es copien dins d'altres arxius, de manera que quan l'usuari obre l'arxiu infectat executa sense voler el virus, que aprofita per a infectar nous arxius. Per aquesta capacitat de copiar-se a si mateixos es diu que són autoreplicables.

Els virus poden ser des de molestos fins a destructius. Per tant, un virus és considerat programari maliciós primer per la infecció d'arxius que duu a terme, i segon, per l'execució d'accions molestes o nocives. Se sol considerar que els virus tenen dos objectius ben definits: produir danys i reproduir-se. La infecció té lloc quan s'executa el codi que conté el virus.

Una de les vies principals d'infecció per virus ha resultat ser les cadenes de missatges de correu electrònic que reenviaven presentacions en PowerPoint. Dit això, podem avançar que un dels millors mètodes per a mitigar el risc és la conscienciació de l'usuari i la millora del concepte de cultura de la seguretat.

La classificació dels virus no sempre ha estat senzilla, encara que des d'un punt de vista d'afectació els podríem classificar en:

- **nocius**, impedint, per exemple, l'arrencada normal d'un sistema,

- **invisibles**, en el sentit que l'usuari en desconeix l'existència en el sistema encara que funcionin en segon pla, i

- de **script**, capaços d'executar-se utilitzant un altre programari normalment relacionat amb l'ofimàtica.

És cert que fa uns anys els virus representaven l'amenaça principal per als equips informàtics. Alguns han resultat tenir renom internacional, com per exemple Jerusalem o Michelangelo. Avui dia, han quedat enrere pel que fa a nombre d'amenaces en favor d'un altre tipus de programari maliciós, els troians, que han cobrat més importància.

Virus Michelangelo

El dia 6 de març, el virus Michelangelo inutilitza el disc dur dels ordinadors infectats. El virus Michelangelo es transmet per mitjà de disquets infectats i va tenir molta rellevància el 1991, ja que abans del 6 de març molts ordinadors n'havien estat infectats.

En la dècada dels anys noranta, juntament amb els virus, apareixen els cucs. El terme *cuc*, encunyat el 1975 en l'obra de ciència-ficció de John Brunner *The Shockwave Rider*, fa referència a programes capaços de «viatjar» per si mateixos a través de xarxes de computadors per a dur a terme qualsevol activitat una vegada assolida una màquina destinació.

Els cucs són programes que es repliquen a si mateixos, de sistema a sistema, sense utilitzar altres arxius per a fer-ho. En això es diferencien dels virus, que necessiten estendre's mitjançant un arxiu infectat. Els cucs fan servir els recursos de xarxa per a distribuir-se.

Com a programari maliciós que són, es distribueixen per mitjà de correus electrònics, missatgeria instantània, xarxes de compartició d'arxius (P2P), dispositius d'emmagatzematge massiu, etc.

Atès que la finalitat principal del cuc és distribuir-se, la seva funció principal en penetrar en un equip és obtenir les adreces de xarxa que pugui acollir per a començar a enviar còpies de si mateix.

Majoritàriament, els cucs utilitzen els correus electrònics com a mitjà de propagació, en molts casos fent servir les agendes d'adreces del client de correu electrònic, per exemple.

És tal el potencial de propagació dels cucs que els considerats cucs de xarxa de ràpida distribució han estat capaços de distribuir-se per continents en qüestió de minuts. Aquest nivell de propagació ve donat per la seva senzillesa i finalitat: primer, no necessiten infectar altres fitxers per a reproduir-se, ja que es propaguen fent còpies de si mateixos, i segon, tenen com a objectiu col·lapsar les xarxes en les quals s'infiltren.

El 2 de novembre del 1988, Robert T. Morris va saltar a la fama quan un dels seus programes es va convertir en «El Cuc» amb majúscules, en «*The Worm*» d'internet. Aquest programari maliciós aprofitava vulnerabilitats en programes molt utilitzats en l'entorn Unix de l'època i va motivar que en poques hores milers d'equips connectats a internet deixessin de funcionar.

Alguns dels cucs més coneguts són: I Love You, Navidad, Pretty Park, Happy99, ExploreZip, Conficker, Stuxnet, Blaster o Sasser.

Cuc Stuxnet

El gener del 2010, el cuc Stuxnet va prendre el control de mil màquines que participaven en la producció de materials nuclears a l'Iran i els va enviar instruccions perquè s'autodestruïssin.

Es tracta d'un programari maliciós que aprofita una vulnerabilitat de Windows per a instal·lar-se a l'ordinador i, una vegada dins, duu a terme un atac dirigit amb l'objectiu de recopilar informació.

Encara que el 2011 es va dir que el cuc havia estat creat en un laboratori pels Estats Units i Israel per a sabotejar el programa nuclear de l'Iran, aquesta informació mai no va arribar a ser confirmada pels països en qüestió.

1.3. Enregistradors de teclat i eines d'intrusió

La paraula *keylogger* prové dels termes anglesos *key*, que significa 'tecla', i *logger*, que es tradueix per 'enregistrador'. Els enregistradors de teclat són programes espia que prenen el control dels equips per a espiar i robar informació enregistrant les pulsacions del teclat i/o del ratolí i robar informació, com ara les contrasenyes i els noms d'usuari.

Un enregistrador de teclat és un tipus de programari que té la capacitat d'enregistrar en un diari (*log*) cada pulsació de teclat.

Diari

Un diari és un registre d'activitat d'un sistema, que generalment es desa en un fitxer de text, al qual es van afegint línies a mesura que es fan accions sobre el sistema. En el cas dels enregistradors de teclat, la informació que s'afegeix són les diverses tecles premudes en el teclat del sistema infectat.

Un enregistrador de teclat pot enregistrar qualsevol tipus d'informació escrita mitjançant la utilització del teclat, com per exemple els missatges instantanis o els correus electrònics. El diari creat per l'enregistrador de teclat pot ser enviat a un destinatari concret, utilitzant una característica afegida al programari maliciós per a transmetre les dades enregistrades a l'ordinador objectiu i situar les dades disponibles en una ubicació remota.

Els enregistradors de teclat es classifiquen en:

- **Enregistradors de teclat de maquinari**: són els dispositius físics que s'encarreguen de detectar les diferents pulsacions en el teclat.

- **Enregistradors de teclat de programari**: són dispositius tipus programari que, com en el cas anterior, enregistren les pulsacions del teclat i/o del ratolí.

Lògicament, una de les maneres més senzilles i efectives d'evitar la instal·lació de dispositius enregistradors de teclat en la seva versió maquinari és la prohibició de l'accés físic als sistemes. Evidentment, dur a terme inspeccions visuals és el millor mètode per a descobrir-los.

En la seva versió programari, cal dir que les companyies d'antivirus afegeixen a la seva base de signatures les dels enregistradors de teclat, de manera que detecten i adverteixen l'usuari de l'aparició d'algun virus en cas que resultin infectats.

Haxdoor

Alguns dels enregistradors de teclat més coneguts són Revealer Keylogger i Haxdoor. Aquest últim va ser utilitzat per a dur a terme un atac al banc suec Nordea (companyia bancària resultat de múltiples unions i adquisicions de bancs suecs, finlandesos, danesos i noruecs), mitjançant un troià que encapsulava un enregistrador de teclat, que li va fer perdre 1,5 milions de dòlars l'agost del 2006.

Els clients de Nordea van començar a rebre correus electrònics que simulaven ser del banc, amb ofertes per a instal·lar un filtre antiinundació (*anti-spamming*) suposadament adjunt al missatge. En el moment en què l'usuari tractava d'obrir l'arxiu i baixar-lo al seu ordinador, aquest s'infectava amb el conegut troià Haxdoor, que s'activava quan les víctimes es registraven en el servei en línia de Nordea. El troià llançava aleshores una notificació d'error i sol·licitava a l'usuari tornar a introduir la informació proveïda en el moment de registrar-se. Després, un enregistrador de teclat que venia incorporat en el troià gravava totes les dades introduïdes pels clients del banc i, tot seguit, procedia a enviar tota la informació recollida a l'atacant. D'aquesta manera els atacants accedien als comptes dels clients i transferien els fons que hi havia.

Filtre antiinundació

Un filtre antiinundació evita que el correu brossa inundi la safata d'entrada d'un client de correu electrònic amb missatges de correu no sol·licitats, sobretot desplaçant aquest correu no sol·licitat a una carpeta de correu destinada a aquest efecte.

Les eines d'intrusió, més que un programa maliciós, són un conjunt de programes l'objectiu dels quals és permetre a un furoner evitar ser detectat mentre duu a terme la seva comesa, que consisteix principalment a obtenir un accés no autoritzat al sistema ocultant objectes com ara processos, arxius o entrades del registre del sistema operatiu.

Per a aconseguir aquest propòsit, aquest programa maliciós executarà un dels dos mètodes següents: o bé reemplaçarà biblioteques del sistema que s'infecta, o bé instal·larà un mòdul en el *kernel* del sistema.

Kernel

El *kernel* d'un sistema programari constitueix una part fonamental del sistema operatiu. És l'encarregat que el programari i el maquinari d'un ordinador treballin junts.

Posteriorment, s'instal·larà l'eina d'intrusió que li permetrà una elevació de privilegis com a usuari del sistema fins a aconseguir accés com a administrador.

Resumint, una eina d'intrusió és una col·lecció d'eines utilitzades per a ocultar una intrusió i obtenir accés amb privilegis d'administrador en un sistema. Les eines d'intrusió poden incorporar altres funcions ocultes que faciliten, entre altres coses, el control remot de l'equip compromès.

Una de les eines d'intrusió més conegudes, en aquest cas per a la plataforma Linux, és t0rn.

Eina d'intrusió t0rn

L'eina d'intrusió t0rn està composta per un conjunt d'eines dissenyades per a fer més difícil la detecció i extirpació d'un intrús informàtic, i incorpora portes posteriors per a proporcionar un subsegüent accés fàcil al sistema per part de l'atacant.

Aquesta eina d'intrusió afegeix, a més, un sistema estàndard d'esborrament de diaris anomenat t0rnsb, un detector (*sniffer*) anomenat t0rns i un modificador de diaris anomenat t0rnp.

1.4. Programari espia i programari de publicitat

S'entén per *programa espia* el programari maliciós que recol·lecta informació d'un usuari sense que aquest hagi donat el seu consentiment.

En la majoria dels casos, l'obtenció d'informació es duu a terme sense que l'usuari sigui conscient de la recollida. Normalment recol·lecten informació sobre el programari que utilitza l'usuari o les seves accions en el sistema, encara que s'han donat casos en els quals la recol·lecció ha deixat pas a una redirecció del tràfic, bo i mostrant a l'usuari una pàgina web que no es correspon amb la que havia sol·licitat, sinó amb la que el programari maliciós ha volgut mostrar.

Principalment, el programari espia recull dades sobre hàbits d'ús d'internet de l'usuari i els envia a empreses de publicitat, que poden fer servir la informació per a enviar-li anuncis publicitaris o vendre el seu perfil a tercers. El programari espia pot ser instal·lat en el sistema per nombroses vies, en molts casos sense que hi intervingui el consentiment exprés de l'usuari, així com el seu coneixement respecte a la recopilació i/o ús de les dades ja esmentades.

Per a dur a terme la seva comesa poden monitorar l'ús del teclat, analitzar arxius del disc de forma arbitrària, espiar altres aplicacions com processadors de text, llegir i interpretar les galetes o monitorar diversos aspectes del comportament de l'usuari, entre altres.

Galeta

Una galeta és un arxiu de petita grandària que conserva informació sobre l'ús d'un lloc web, bé de forma temporal per a una sessió, bé de forma persistent per a identificar un usuari en visites successives.

Les galetes persistents poden ser utilitzades com a programari espia per a rastrejar la navegació web de l'usuari.

D'altra banda, el programari de publicitat són els programes que mostren publicitat a l'usuari mitjançant múltiples finestres utilitzant qualsevol tipus de mitjà, com per exemple finestres emergents, bàners, canvis en la pàgina d'inici o de cerca del navegador, etc., sense que l'usuari hi tingui cap control.

El programari de publicitat s'instal·la a l'equip en accedir a webs de contingut sexual, programari pirata o publicitat.

També se sol trobar acompanyant un altre programari que acostuma a ser gratuït, i la publicitat apareix a la interfície d'ús. En alguns casos, aquest programari també recol·lecta i envia dades de l'usuari de caràcter personal.

Les recomanacions per a evitar aquest programari maliciós, preventivament, són que mai no s'instal·li ni s'accepti cap tipus de connector o complement quan es navegui per pàgines web de reputació dubtosa o que no ens generen prou confiança.

Connector

Un connector és un programa que afegeix noves funcions a un determinat programa ja existent. En el cas que ens ocupa, un connector sol afegir funcionalitats al navegador web.

2. Tipus d'atacs

És tal el nombre de les diferents tipologies d'intrusos o atacants de sistemes informàtics –furoners, pirates, detectors, pirates telefònics (*phreakers*), emissors de correu brossa (*spammers*), etc.– que la realització d'una classificació, o simplement la selecció dels atacs informàtics principals existents actualment, es converteix en una tasca àrdua.

Com en la vida real, són diversos els motius pels quals un individu o grup d'individus duen a terme actes il·lícits contra sistemes d'informació, sigui un ordinador personal, el sistema informàtic d'una empresa o organització o fins i tot el d'un estament governamental.

A títol informatiu, a continuació s'enumeren i descriuen les fases principals d'un atac informàtic:

- **Reconeixement**. Encara que no es pot considerar pròpiament un atac, atès que no provoca cap dany, l'atacant busca lucrar-se d'informació com poden ser les versions de programari instal·lades a l'ordinador, el sistema operatiu o el disseny de la xarxa a la qual està connectat, tot això mitjançant mètodes d'escaneig de xarxes i/o sistemes.

- **Escaneig**. En aquesta fase es duu a terme la detecció de les vulnerabilitats que li presentin l'oportunitat d'accedir al sistema. Aquestes vulnerabilitats poden sorgir del programari instal·lat però desactualitzat, és a dir, en el qual no s'han instal·lat els pegats adequats, o bé serveis o ports oberts innecessaris o mal configurats oferts pel sistema.

- **Accés**. És pròpiament en aquesta fase en la qual l'atacant intenta aconseguir l'accés no autoritzat al sistema. Per a això, utilitzarà l'explotació d'alguna de les vulnerabilitats localitzades en el punt anterior. Òbviament, depenent de la gravetat de la vulnerabilitat l'accés tindrà més o menys repercussió en el sentit que l'atacant rebrà un privilegi o altre en el sistema atacat.

- **Manteniment**. Una vegada l'atacant accedeix al sistema, buscarà poder mantenir-s'hi, ja que un simple reinici del sistema per part de l'usuari legítim o simplement pel mateix dispositiu infectat podria fer perdre el privilegi aconseguit per l'atacant. Per a dur a terme la permanència en el dispositiu, se sol introduir un altre programari maliciós o modificar arxius del sistema per a garantir la persistència de l'atac.

- **Eliminació**. Encara que no sempre es duu a terme, en molts casos el furoner o atacant decideix esborrar les proves que puguin relacionar-lo amb

l'acte il·lícit. A aquest efecte, l'atacant sol prendre nota de les accions dutes a terme durant l'explotació per a poder fer reversible l'acte amb posterioritat, evidentment amb la intenció d'evitar possibles accions legals contra ell.

En els subapartats següents veurem quins són els principals atacs informàtics als quals podem haver de fer front actualment. Com s'ha dit anteriorment, no pretén ser una explicació complexa de terminologia informàtica de difícil comprensió, sinó una breu anotació dels atacs més comuns per a poder entendre la terminologia bàsica del món de la seguretat dels sistemes informàtics interconnectats, denominada *ciberseguretat*.

2.1. Falsejament d'identitat

El falsejament d'identitat consisteix, per definició, en la generació de tràfic utilitzant un origen falsejat. Això vol dir que, abans de res, es parteix del falsejament o suplantació d'algun dels actors participants en la comunicació en xarxa, la qual cosa dóna lloc als diferents tipus de falsejament d'identitat existents.

Els tipus de falsejament d'identitat més comuns són els IP, ARP i DNS, encara que en aquest subapartat també veurem el falsejament web i el falsejament de correu.

Encara que queda fora d'estudi d'aquest mòdul, és important saber que existeix un model en informàtica, anomenat TCP/IP, format per diferents protocols, que regeix, per norma general, les comunicacions a les xarxes. Un dels protocols usats és el protocol IP o protocol d'internet, que assigna una adreça IP, que és un nombre que identifica lògicament i jeràrquicament un dispositiu dins d'una xarxa que utilitzi aquest protocol. Podem dir llavors que qualsevol dispositiu connectat a la xarxa disposa d'una adreça IP que l'identifica inequívocament.

Dit això, el falsejament d'identitat IP consisteix a ocultar l'origen de l'atac suplantant o falsejant l'adreça IP.

Així, un intrús ataca canviant l'adreça IP del paquet que conté informació que es transmet per la xarxa, fent veure que s'ha originat en un altre lloc. D'aquesta manera, si modifiquem un paquet posant-hi una adreça IP d'un dels ordinadors autoritzat a accedir a un sistema, podrem fer arribar a aquest sistema els paquets que vulguem enviar des d'un dispositiu en principi no autoritzat.

A títol d'exemple, mitjançant el falsejament d'identitat IP es podrien executar accions en un sistema informàtic en nom d'un usuari que hi manté una sessió activa i lícita suplantant la seva IP, com per exemple transferències bancàries o compres en línia.

Per a comprendre el falsejament d'identitat ARP hem d'introduir breument el protocol ARP. El protocol ARP és un protocol de comunicació que s'encarrega de resoldre i mantenir la taula d'equivalències entre les adreces MAC i les adreces IP de les màquines que es comuniquen en una xarxa. Cal recordar que en l'entorn Ethernet, per a poder enviar els paquets de dades cal conèixer l'adreça MAC del destinatari amb independència de la seva IP.

MAC

L'adreça MAC (en anglès *media access control*) és una adreça que identifica una interfície de xarxa de maquinari de manera única. L'adreça MAC es compon de 48 bits.

Atès que totes les màquines d'una mateixa xarxa local comparteixen el mateix mitjà i que, per tant, són capaces de veure tot el tràfic originat a la xarxa, les targetes Ethernet incorporen un filtre que ignora tot el tràfic que no està destinat a elles mateixes. Això s'aconsegueix ignorant els paquets l'adreça MAC dels quals no coincideix amb la seva.

Ethernet

Ethernet és una família de tecnologies basades en el marc de les xarxes d'ordinadors per a xarxes d'àrea local (LAN).

Dit això, no és difícil imaginar l'objectiu del falsejament d'identitat ARP. L'autenticació ARP està basada, igual que el falsejament d'identitat IP, en l'adreça font, és a dir, l'adreça d'on provenen els paquets.

El procés de falsejament d'identitat ARP consisteix a manipular la taula ARP de les dues màquines a les quals es vol suplantar.

D'aquesta manera, una vegada modificades les taules ARP de totes dues màquines, aquestes començaran a comunicar-se sense adonar-se que tota la informació és prèviament obtinguda i analitzada per una màquina intermèdia que quan l'obté, la reenvia a la màquina destinació de la comunicació per a evitar ser detectada. Així, la comunicació és transparent per als dos dispositius. Òbviament, la detecció és molt senzilla: només hem d'analitzar la nostra taula ARP (se sol utilitzar l'ordre `arp -a`) i observar que no tinguem dues màquines amb la mateixa adreça MAC.

El falsejament d'identitat DNS va una mica més enllà. A diferència del cas anterior, en aquest cas utilitzarem un dispositiu de xarxa normalment situat fora de les nostres xarxes: el DNS.

Sense entrar en gaires detalls, direm que el DNS (*domain name server*, 'sistema de noms de domini') és el cor de la internet actual, en el sentit que és l'encarregat de traduir els noms de dominis de les webs a la IP de l'ordinador on està allotjada la pàgina que estem buscant per internet. És a dir, imaginem que volem visitar la pàgina de la UOC: www.uoc.edu. Nosaltres escrivim aquesta pàgina en el navegador i aquest ens hi porta. Però enmig d'aquest procés hi

ha hagut un element de xarxa, el servidor DNS, que ha traduït *www.uoc.edu* (nom de domini) a l'adreça 213.73.40.242 (IP), atès que com a humans que som, ens resulta molt més senzill recordar el nom de domini abans que la IP.

Els falsejaments d'identitat DNS provoquen una direcció errònia en els equips afectats a causa d'una traducció errònia dels noms de domini a adreces IP, cosa que facilita la redirecció dels usuaris dels sistemes afectats cap a pàgines web falses.

Per a poder dur a terme aquest atac, un atacant dirigeix la nostra petició web (el nom de domini que hem escrit) a un servidor DNS il·legítim que ens porta a una pàgina web que no es correspon amb la sol·licitada. Perquè no ho detectem serem enviats a un lloc web erroni que simularà ser el lloc web real. A partir d'aquí, en aquest web fals introduirem les nostres dades d'usuari, que òbviament seran emmagatzemades i analitzades per l'atacant. Podem imaginar les conseqüències si aquest web és el de la nostra entitat bancària?

Amb una finalitat similar a la del cas anterior, el falsejament d'identitat web consisteix que l'atacant crea un lloc web (fals) similar al que la víctima vol visitar.

Els accessos a aquest lloc estan dirigits per l'atacant (potser utilitzant el falsejament d'identitat DNS, esmentat anteriorment), fet que li permet monitorar totes les accions de la víctima: dades, contrasenyes, números de targeta de crèdit, etc. Com podem veure, els falsejaments d'identitat DNS i web es complementen a la perfecció per a culminar un dels atacs compostos més perillosos de la xarxa.

Però no només l'ús d'un falsejament d'identitat DNS ens pot portar a executar una web falsa. Hi ha altres mètodes molt més senzills que permeten la infecció de la nostra màquina a partir de la qual dur a terme activitats il·lícites. Un dels més senzills però alhora més perillosos és utilitzar un virus perquè desviï la connexió d'una víctima i les seves dades mitjançant una pàgina falsa amb aspecte de veritable.

El falsejament d'identitat SMTP pot tenir lloc de maneres diferents, però totes tenen un resultat similar: un usuari rep correu electrònic que sembla haver-se originat d'un emissor lícit quan, en realitat, ha estat enviat des d'un emissor fals.

SMTP

El protocol SMTP (*simple mail transfer protocol*, 'protocol simple de transferència de correu') és el protocol estàndard d'internet per a l'intercanvi de correu electrònic.

El falsejament d'identitat SMTP és sovint un intent d'enganyar l'usuari per a la divulgació d'informació confidencial, com els noms d'usuari i les seves contrasenyes.

Són diversos els exemples de correus electrònics falsos que podrien ser utilitzats per a enganyar un usuari. Vegem-ne un parell:

- Un correu electrònic que diu que és d'un administrador del sistema que sol·licita als usuaris que canviïn les seves contrasenyes en una cadena especificada i que amenaça de suspendre el seu compte si no ho fa.

- Un correu electrònic que afirma que prové d'una persona amb autoritat que sol·licita als usuaris que els enviï una còpia d'un arxiu de contrasenyes o una altra informació sensible.

A partir d'aquest punt, i de la mateixa manera que passava en els casos estudiats anteriorment, l'atacant ja disposa de les claus d'accés necessàries per a poder dur a terme les activitats il·lícites que vulgui.

2.2. *Sniffing*

Conceptualment, l'*sniffing* és una cosa molt senzilla d'entendre: és la captura del tràfic que circula per una xarxa.

Els detectors, també anomenats *packet sniffers*, són programes que permeten capturar els paquets que viatgen per una xarxa i poden ser usats per a propòsits legítims i il·legítims. Per exemple, un administrador de xarxa pot usar-los per a monitorar el flux de tràfic a la xarxa i assegurar-se que la xarxa funciona adequadament. Però d'altra banda els detectors també poden ser utilitzats per usuaris maliciosos per a obtenir informació personal valuosa.

Per dur a terme les seves finalitats, els detectors solen utilitzar un equip connectat a la xarxa amb la seva targeta de xarxa configurada en «mode promiscu», per a poder processar tot el tràfic que rep encara que vagi dirigit a altres equips.

Com hem vist en el cas del falsejament d'identitat ARP, cal modificar les taules ARP, que contenen les adreces MAC de les màquines que mantenen una comunicació, per a poder obtenir els paquets de dades que s'envien. Les adreces MAC que es modifiquen vénen imposades de fàbrica en cada targeta de xarxa dels nostres dispositius.

Conservar la confidencialitat de la nostra informació és un dels punts clau per a mantenir la seguretat de les nostres dades. Per això, i fent front a possibles atacs en xarxa com l'*sniffing*, que permetria la lectura de les nostres dades com

si es tractés d'un llibre obert, es recomana l'ús de protocols de xifratge que xifrin totes les dades confidencials que s'envien per internet o de la nostra xarxa (per exemple, els correus electrònics).

És per aquest motiu que actualment són poques les pàgines web que utilitzen el protocol HTTP (*hyper text transfer protocol*, 'protocol de transferència d'hipertext'). Aquest protocol és utilitzat pels navegadors per a comunicar-se amb els servidors web i els permet veure les pàgines web. El problema d'aquest protocol és que les dades circulen en «text pla», és a dir, sense xifrar.

Per aquest motiu, va néixer el protocol HTTPS (*hyper text transfer protocol secure*, 'protocol de transferència d'hipertext segur'). En si mateix, l'HTTPS no és més que l'HTTP sobre SSL / TLS (*secure sockets layer*, 'capa de sòcol segur' / *transmission layer security*, 'seguretat de la capa de transport'), que són dos protocols per a enviar paquets xifrats per internet.

D'aquesta manera, i atès que es xifren totes les dades d'HTTP –no només la pàgina web, sinó també adreça d'una pàgina a internet, els paràmetres enviats o les galetes–, encara que un usuari estigués escoltant les nostres comunicacions, no entendria les dades que n'estigués capturant i veient. Aquestes dades resulten totalment il·legibles.

2.3. Pesca (*phishing*)

La pesca consisteix bàsicament en el robatori d'informació a un usuari suplantant o falsejant una entitat legítima en la qual aquest a priori confia.

Un exemple de pesca podria consistir que un atacant repliqui la pàgina web d'una entitat bancària amb la qual normalment treballem. En el moment en què accedim a la web falsa (que creiem que és la veritable) amb el nostre usuari i la nostra clau, l'atacant disposarà de les nostres dades d'accés a rampells, de manera que només haurà d'accedir a la veritable web de l'entitat bancària i operar amb els nostres comptes lliurement.

En aquests casos tan senzills l'atacant tan sols s'ha de preocupar de dues coses. Primer, trobar un domini web molt semblant al que vol falsejar; per exemple, si vol suplantar www.elbanc.com, pot substituir la *l* del nom per un *1*, amb la qual cosa quedaria de la manera següent: www.e1banc.com. Això dificultaria enormement veure el canvi en l'URL.

Segon, fer un enviament massiu de correu brossa esperant que coincideixi que algun dels receptors dels missatges creguin que «el seu banc», amb aquest correu electrònic, els sol·licita accedir-hi, mitjançant un enllaç incorporat en aquest missatge, per a dur a terme qualsevol operació (és igual el motiu; és una

excusa per a introduir l'usuari i la contrasenya). Per descomptat que aquest correu electrònic buscarà semblar igual que la correspondència legal enviada per l'entitat bancària original.

Els primers casos de pesca coneguts solien ser bastants toscs en el sentit que les pàgines web utilitzades per a falsejar les webs originals estaven bastant mal elaborades i s'hi veien errors ortogràfics per tot arreu. Solien elaborar-les ciberdelinqüents estrangers que utilitzaven traductors en línia les traduccions dels quals estaven força mal fetes o que donaven missatges d'error molt sospitosos una vegada introduïts l'usuari i la contrasenya.

Però actualment el seu desenvolupament ha evolucionat enormement. La ciberdelinqüència ha millorat les seves traduccions, ja que hi ha ciberdelinqüents a tots els països, alhora que els traductors automàtics en línia també ho han fet. A més, s'ha depurat la interacció amb l'usuari per a no aixecar sospites. Així, una vegada hem introduït el nostre usuari i la contrasenya, la pàgina falsa acostuma a reenviar la petició a la pàgina veritable, fet que genera un procés transparent per a l'usuari enganyat i que no aixeca cap tipus de sospita.

Per aquest motiu, no ens han de sorprendre notícies com que els casos de pesca als Estats Units augmenten un 400% durant la declaració d'impostos, o que PayPal o eBay són algunes de les companyies que més casos de pesca acumulen any rere any.

Encara que queda fora del contingut d'aquest mòdul, actualment se sol parlar també del descaminament (*pharming*). A títol informatiu, cal tenir present que el descaminament es tracta d'una tàctica fraudulenta que consisteix a canviar els continguts del DNS, sigui mitjançant la configuració del protocol TCP/IP o l'arxiu corresponent en cada sistema operatiu, per a redirigir els navegadors a pàgines falses.

És important recordar que, com en la majoria dels atacs vistos, les persones solen ser la baula més feble de la cadena, susceptibles a atacs com la pesca, per la qual cosa la conscienciació en l'àmbit de la seguretat resulta fonamental.

2.4. Injecció SQL

Abans d'entrar pròpiament en matèria, és important entendre a què ens referim quan parlem de SQL.

Una base de dades és un conjunt de fitxers que contenen dades i els programes que gestionen l'estructura i la forma en què s'emmagatzemen, així com la manera en la qual s'han de relacionar entre si. Alguns exemples de sistemes de bases de dades són Access, Oracle, SQL, etc.

L'SQL o *structured query language* ('llenguatge d'interrogació estructurat') és, per tant, un llenguatge de programació estàndard destinat a la gestió, administració i comunicació de bases de dades, utilitzat per a interactuar amb bases de dades relacionals. La unitat típica d'execució de SQL és la consulta, que és el conjunt d'instruccions que permeten modificar l'estructura de la base de dades. És a dir, mitjançant una consulta interactuem amb una base de dades per a consultar-hi, modificar-hi, afegir-hi o esborrar-hi informació.

L'atac per injecció de codi SQL consisteix en un atac d'introducció de consultes en el qual un atacant pot executar sentències SQL malicioses en un servidor de base de dades.

Es produeix perquè no es filtra adequadament la informació enviada per l'usuari. Des d'una vulnerabilitat d'injecció SQL es pot arribar a afectar qualsevol aplicació que faci ús d'una base de dades basada en aquest llenguatge de programació. Aquesta vulnerabilitat és una de les més antigues, més freqüent i més perillosa de les diferents vulnerabilitats que se solen executar sobre aplicacions web.

En aprofitar una vulnerabilitat d'injecció SQL, i amb les circumstàncies adequades, un atacant pot recuperar el contingut d'una base de dades completa. La injecció SQL també es pot fer servir per a afegir, modificar i eliminar registres en una base de dades, fet que n'afecta la integritat.

Com a conseqüència d'aquests atacs, i depenent dels privilegis de l'usuari de base de dades que executa les consultes, es podria accedir no només a les taules relacionades amb l'operació de l'aplicació del servidor web, sinó també a les taules d'altres bases de dades allotjades en el mateix servidor web.

Atès que l'SQL és un llenguatge de programació, la manera d'evitar aquest tipus d'atacs consisteix a programar adequadament la base de dades i depurar el codi per a evitar-ne la corresponent explotació o bretxa de seguretat.

2.5. *Cross-site scripting* (XSS)

Un atac de *cross-site scripting* (XSS) consisteix bàsicament en l'execució de codi script, o un petit programa arbitrari en un navegador, en el context de seguretat de la connexió a un determinat servidor web.

Script

El terme *script* fa referència a tots els fitxers o seccions de codi escrits en algun llenguatge de programació, com ara Visual Basic Script (VBScript), JavaScript, etc.

Els atacs XSS tenen lloc quan un atacant utilitza una aplicació web per a enviar codi maliciós, generalment en forma d'un script del costat del navegador, a un usuari final. Aquesta injecció de codi HTML o JavaScript on no n'hi hauria d'haver fa obtenir a l'atacant algun profit, com per exemple el robatori de galetes, la redirecció a una pàgina falsa, etc.

JavaScript

El JavaScript és un llenguatge de programació que aporta característiques dinàmiques (dades variables en funció del temps i el mode d'accés, interactivitat amb l'usuari, personalització, etc.) a les pàgines web escrites en llenguatge HTML.

Un atacant pot usar XSS per a enviar un script maliciós a un usuari desprevingut. El navegador de l'usuari final no té manera de saber que les seves accions no són confiables, així que executarà la seqüència d'ordres perquè creu que l'escriptura ha vingut d'una font de confiança. Així, l'script maliciós pot accedir a les claus de sessió o alguna altra informació sensible retinguda pel navegador i utilitzada en aquest lloc.

Atès que en aquest tipus de vulnerabilitats els atacants exploten la confiança que un usuari té en un lloc en particular, en primer lloc és fonamental disposar d'una solució de seguretat instal·lada i actualitzada. Això és important, ja que l'execució d'alguna aplicació maliciosa sense el nostre consentiment, com ara programari maliciós o *exploits*, automàticament serà bloquejada. A més, si es tracta d'una redirecció a algun lloc de pesca, es té la protecció de l'antivirus i el bloqueig proactiu per part dels navegadors.

En segon lloc, és important observar l'URL als quals accedim. Com s'ha comentat, un dels mètodes d'engany consisteix en la redirecció a pàgines web falses o de l'interès de l'atacant, per la qual cosa, observant la barra d'adreces del navegador veurem si estem movent-nos pel domini correcte o no.

2.6. DOS i DDOS

Un DOS o *denial of service* és un atac contra un recurs amb l'objectiu de degradar totalment o parcialment els serveis prestats per aquest recurs als seus usuaris legítims.

Error de programació

Un error de programació indica una fallada o error en un programa informàtic.

Dit d'una altra manera, consisteix a inutilitzar un dispositiu de xarxa, normalment essencial, amb la intenció d'anul·lar o reduir la funcionalitat del servei ofert per aquest dispositiu. Mitjançant aquests tipus d'atac, la persona que el duu a terme pot arribar a obtenir accés a un sistema, ja que l'atac dispara altres tipus d'errors de programació en un sistema.

Imaginem, per exemple, una pàgina web d'una organització a la qual fem milers de peticions de connexió alhora. Si el servidor de la pàgina o un dispositiu de xarxa intermedi no estan preparats per a fer front a la gestió d'un nombre de peticions tan elevat, el més probable és que aquest servidor quedi fora de servei.

Algunes de les oportunitats que ofereix l'atac DOS són:

- Una execució que elevi el consum dels recursos de les màquines afectades: processador, memòria, disc dur, etc., i provoqui una caiguda en el seu rendiment. Per a executar-lo cal establir múltiples connexions simultànies o atacs llançats contra els ports de configuració dels encaminadors, entre altres.

- Col·lapsar xarxes d'ordinadors mitjançant la generació de grans quantitats de tràfic, generalment des de múltiples equips.

Ping de la mort

A manera d'exemple, parlarem d'un dels casos coneguts de DOS més importants: el «ping de la mort». L'ordre `ping` (*packet internet groper*) s'utilitza per a comprovar si hi ha errors de xarxa. El funcionament del mecanisme és molt simple i treballa mitjançant l'enviament de sèries d'informació a una adreça IP, màquina o servidor. Així, la màquina font envia una sol·licitud d'eco, és a dir, una petició de contestació, a una màquina destinació. La màquina destinació rep la sol·licitud i envia una resposta a la màquina font i una altra informació d'interès. L'ordre d'execució és `ping` *`adreça_IP_equip_a_avaluar`*.

Mitjançant l'ordre `ping -l 65510` *`adreça_IP_equip_víctima`*, l'atacant envia un paquet IP d'una grandària superior als 65.535 bytes amb la finalitat de col·lapsar el sistema atacat. Òbviament, actualment la majoria de sistemes estan protegits contra un atac tan senzill de fer, però va arribar a afectar la majoria de sistemes operatius, com Unix, Linux, Mac, Windows, les impressores i els encaminadors.

D'altra banda, un DDOS o *distributed denial of service* és una denegació de serveis distribuïda, és a dir, un atac de denegació de serveis (DOS) fet al mateix temps des de diversos ordinadors.

Un DDOS és causat per un atac massiu i simultani a un únic objectiu real, i actualment és un dels atacs més estesos. És lògic pensar que si en comptes d'una sola màquina atacant en disposem de centenars o potser milers, les probabilitats d'èxit augmenten quantiosament.

Per a dur-lo a terme, en primer lloc hem de comprometre un nombre de màquines prou elevat per a poder executar l'atac sense problemes. Atès que no tothom està disposat a facilitar la seva màquina per a aquestes finalitats, resulta obvi que l'atacant intentarà infectar com més màquines li sigui possible millor amb un «exèrcit» de màquines zombis. Aquests equips zombis seran equips infectats per algun virus o troià que permetrà el control remot per part de l'usuari atacant.

Zombi

Un zombi és un ordinador controlat mitjançant la utilització de *bots*. Un *bot* és el programari maliciós utilitzat per l'atacant per al control de l'ordinador infectat. Així, la xarxa d'ordinadors infectats s'anomena *xarxa de zombis*.

Per aquest motiu, no només és important la protecció davant un DDOS, sinó també la seguretat dels nostres ordinadors com a usuaris connectats a internet, ja que sense adonar-nos-en podem convertir-nos en còmplices col·laboradors d'un atac massiu contra qualsevol organització a la xarxa.

Casos de DDOS

Són nombrosos els casos de DOS o DDOS executats anualment al món. Així podem trobar notícies com ara «Diversos ciberatacs massius inutilitzen les webs de grans companyies», publicada al diari espanyol *El País* el 22 d'octubre de 2016, on es comentava el següent:

«Una onada de ciberatacs massius contra el proveïdor d'internet Dyn han interromput aquest divendres el servei de pàgines web de grans companyies i mitjans de comunicació internacionals, com Twitter, Spotify, Amazon, Netflix o *The New York Times*. L'atac, planejat en diverses fases, ha durat gairebé 11 hores.

El Departament de Seguretat Nacional dels Estats Units ja va avisar la setmana passada que els furoners estaven utilitzant un nou enfocament "molt poderós" per a llançar aquestes campanyes. Aquest nou sistema consisteix a infectar encaminadors, impressores, televisors intel·ligents i tot tipus d'objectes connectats amb un programari maliciós que els converteix en una espècie d'"exèrcit robot" que pot llançar els anomenats atacs DDOS.

Aquest tipus d'atacs de denegació de servei saturen amb dades inservibles els servidors –en aquest cas, els de Dyn– de manera que impedeix als usuaris reals accedir a les pàgines per la sobrecàrrega de l'amplada de banda provocada per l'acció dels furoners. El servidor no pot atendre la quantitat enorme de sol·licituds.»

Resum

En la primera part d'aquest mòdul s'han mostrat els tipus principals de programari maliciós amb què ens podem trobar. S'han estudiat les portes posteriors, els troians, els virus, els cucs, els enregistradors de teclat, les eines d'intrusió, el programari espia i el programari de publicitat. Hem vist que en alguns casos aquest programari maliciós treballa conjuntament, bo i incrementant la seva capacitat maliciosa.

En la segona part del mòdul s'han enumerat i descrit les fases principals d'un atac informàtic, que són: reconeixement, escaneig, accés, manteniment i eliminació.

També hem vist els diferents atacs amb què ens podem trobar. Els principals atacs estudiats han estat el falsejament d'identitat, l'*sniffing*, la pesca (fent referència al descaminament), la injecció SQL, el *cross-site scripting* (XSS) i el DOS i DDOS.

S'han posat exemples per a alguns d'ells amb l'objectiu de mostrar l'actual permanència i constància en el del dia a dia d'aquests atacs, l'activitat dels quals no es redueix, sinó que s'incrementa a mesura que les organitzacions criminals s'adonen dels beneficis econòmics que suposen els seus actes il·lícits.

Activitats

1. Actualment, una de les amenaces més grans quant a programari maliciós a la qual està exposada una organització, govern o empresa és l'anomenada *amenaça persistent avançada*, les sigles de la qual en anglès són APT (*advanced persistent threat*). En què consisteix aquest tipus de programari maliciós? Per què es caracteritza principalment? Coneixes algun cas d'APT que es fes públic?

2. En el subapartat 2.3 hem definit la pesca (*phishing*) com el robatori d'informació a un usuari suplantant o falsejant una entitat legítima en la qual confia a priori. Què és l'*spear phishing*? Quina semblança té amb les APT del primer enunciat? Coneixes algun cas de *spear phishing* que es fes públic?

Bibliografia

Abliz, M. (2011). *Internet Denial of Service Attacks and Defense Mechanisms*. Department of Computer Science, University of Pittsburgh.

Arbor Networks, Inc. (2016). *Worldwide Infrastructure Security Report*. Arbor Networks.

Aycock, J. (2005). *Computer Viruses and Malware*. Springer.

Cole, E.; Krutz, R.; Conley, J. (2005). *Network Security Bible*. John Wiley & Sons.

Richardson, R. (2010). *2010/2011 CSI Computer Crime and Security Survey*. Computer Security Institute.

Enllaços d'internet

https://www.symantec.com/connect/articles/introduction-spyware-keyloggers

https://ecrimeresearch.org/

https://apwg.org/report-phishing/

http://virusattack.blogspot.com.es/2007/08/qu-es-un-keylogger-leccin-9.html

http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

https://www.nist.gov/publications