Xarxes de zombis

Joaquin Garcia Alfaro

PID_00180824

Universitat Oberta de Catalunya
www.uoc.edu

Índex

Introducció

Una xarxa de zombis consisteix en una xarxa d'equips informàtics infectats per un atacant remot, que els controla de manera distribuïda amb finalitats tant malintencionades com lucratives. Aquests equips infectats componen una xarxa de robots (agents de programari) al servei de l'atacant. L'atacant es converteix així, doncs, en operador d'una complexa i potent xarxa els serveis de la qual seran finalment venuts a organitzacions de tot tipus. Per exemple, els serveis de la xarxa podran ser venuts a organitzacions criminals per a l'execució d'atacs coordinats a gran escala, com ara denegacions de servei distribuïdes, campanyes de correu brossa, venda de productes il·legals, etc.

En aquest mòdul, presentem l'origen i les tècniques actuals que fan possible l'existència d'aquestes xarxes. Introduirem les fases necessàries per a construir-les, estudiarem les arquitectures, els protocols i els models de comunicació que les fan possibles. Mostrarem també algunes de les tècniques empleades pels operadors de les xarxes de zombis perquè els equips infectats passin desapercebuts i les seves xarxes no siguin, per tant, desarticulades. Finalment, veurem alguns exemples concrets de xarxes de zombis que han estat descobertes i mostrarem algunes dades sobre el model econòmic que en va garantir l'existència.

Objectius

Els objectius que l'estudiant ha d'haver aconseguit després d'estudiar els continguts d'aquest mòdul són els següents:

1. Entendre què són les xarxes de zombis i saber com van sorgir.
2. Comprendre el model de propagació d'una xarxa de zombis tradicional.
3. Conèixer el model de comunicació i col·laboració entre robots i operadors.
4. Veure algunes de les tècniques utilitzades pels operadors d'una xarxa de zombis per a protegir els seus equips i evitar que la xarxa de robots sigui desarticulada.
5. Conèixer el model econòmic que promou la creació i el manteniment d'una xarxa de zombis, i també les activitats associades.

1. Antecedents i inicis de l'amenaça

Origen del terme

El terme *botnet* prové de la superposició de dues paraules angleses: *robot* i *network*. Una traducció al català seria, per tant, xarxa de robots.

Una xarxa de zombis (també coneguda com a xarxa d'equips robot) és entesa, avui dia, com un conjunt d'equips informàtics connectats a Internet, els recursos dels quals (com ara memòria, execució de processos, sistema de fitxers i connexions de xarxa) són controlats, a distància, sense que els seus usuaris o propietaris en siguin conscients. Els operadors d'una xarxa de zombis (sovint coneguts com a *botmasters* o *botherders*) creen la xarxa mitjançant la propagació de codi maliciós, que infecta els recursos dels futurs equips de la xarxa de zombis i en garanteix el control permanent.

Una vegada infectats, els equips de la xarxa de zombis són vistos pels seus operadors com un conjunt de robots de programari al servei dels clients de la xarxa de zombis. Aquests clients podran llogar els equips per fer activitats com ara campanyes de correu brossa, denegacions de servei distribuïdes, emmagatzematge de continguts multimèdia il·lícits, etc. La majoria dels equips infectats, i futurs robots de la xarxa de zombis, solen ser ordinadors domèstics, sovint activament connectats a Internet durant llargs períodes de temps (hores, dies, setmanes) i amb uns nivells de protecció (pel que fa a seguretat) bastant baixos.

L'operador de la xarxa de zombis (generalment, qui es va encarregar de trobar i infectar els equips) enviarà periòdicament missatges de control via protocols tradicionals com, per exemple, IRC (*Internet relay chat*) o HTTP (*hypertext transfer protocol*). Els robots de la xarxa de zombis poden fins i tot ser reprogramats per terceres parts (de vegades, faccions de comunitats malicioses diferents) amb l'objectiu d'ampliar els seus dominis o reprendre els recursos de xarxes de zombis ja existents.

Actualment, una xarxa de zombis és considerada una xarxa d'equips infectats que ofereix serveis fraudulents. Aquests equips, sovint citats com a *robots*, *zombis*, o simplement *agents* de la xarxa de zombis, són controlats a distància, de manera distribuïda, per un o diversos operadors (esmentats en la bibliografia com a *botmasters* o *botherders*).

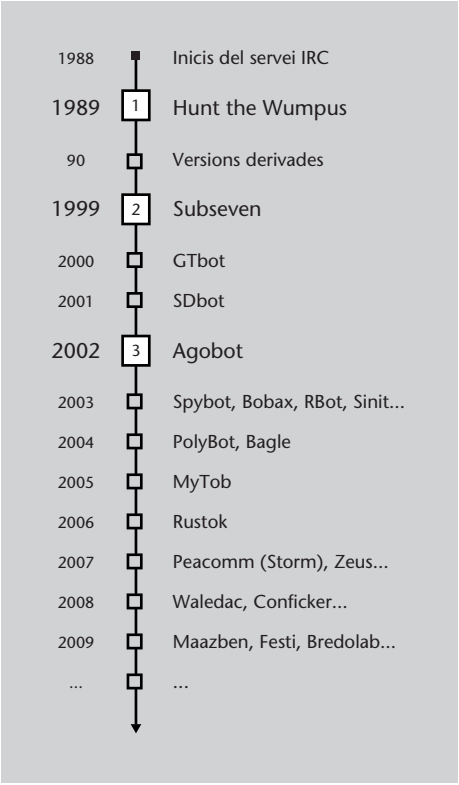
No obstant això, les xarxes de zombis no sempre han estat lligades a serveis il·lícits. En el subapartat següent, veurem quins van ser els inicis d'aquestes xarxes fraudulentes. Tractarem, encara que de manera no exhaustiva, l'evolució que han tingut els seus serveis al llarg dels últims anys. Descobrirem que

les xarxes de zombis no sempre han tingut la connotació negativa atribuïda actualment. Veurem que, en realitat, les xarxes de zombis van ser concebudes per a automatitzar el manteniment i l'actualització d'alguns serveis pioners d'Internet.

1.1. Breu historial sobre xarxes de zombis conegudes

Les xarxes de zombis apareixen a la fi de la dècada dels vuitanta. La figura 1 resumeix, de manera no exhaustiva, el nom i la data (aproximada) d'aparició d'alguns dels desplegaments de xarxes de zombis que més repercussió han tingut des de llavors.

Figura 1



Hunt the Wumpus

Relacionat amb la primera xarxa de zombis de la història, *Hunt the Wumpus* és un videojoc també famós per contenir algunes de les tècniques pioneres en matèria d'intel·ligència artificial. Es tracta d'una aventura conversacional en xarxa per mitjà d'una consola d'instruccions que permet llançar les accions de l'usuari en el joc. La versió original del joc, programada en Basic, es remunta a la dècada dels setanta. El jugador ha de recórrer una estructura geomètrica (similar a un dodecaedre) composta per habitacions i túnels. Similar al mite del Minotaure, dins de l'estructura s'amaga un misteriós monstre, Wumpus, que té l'objectiu de trobar els jugadors i devorar-los. Addicionalment, algunes de les habitacions contenen paranys mortals (pous sense fons, ratapinyades gegants, etc.).

L'aparició de la primera xarxa de zombis està íntimament relacionada amb la invenció del protocol IRC (*Internet relay chat*) i amb la versió en xarxa de *Hunt the Wumpus* per mitjà de canals IRC. De fet, i com succeeix amb moltes altres tecnologies fraudulentes associades a Internet, l'origen d'aquesta primera xarxa de zombis, totalment lícita i inofensiva, va ser concebuda per a l'automatització de tasques de gestió virtuals de canals IRC. Els equips d'aquesta primera xarxa de zombis tenien per objectiu la construcció i el manteniment de processos associats a jocs per a usuaris IRC. Els robots de la plataforma havien d'estar disponibles les 24 h del dia per a oferir als usuaris la possibilitat de jugar amb ells. Ràpidament, i de manera espontània, xarxes similars van ser desplegades per a donar suport a operadors d'altres serveis.

Un aspecte important en el desenvolupament d'aquests precursors de les xarxes de zombis actuals és la capacitat de crear un canal de comunicació entre els operadors i els robots, i també la inclusió de mecanismes de control d'accés per a evitar que terceres parts puguin prendre el control dels equips de la xarxa de gestió. Per això, trobem en aquesta època una arquitectura basada en canals de control, per mitjà dels quals l'operador podrà comunicar instruccions de gestió, com ara inicialització de serveis, represa de tasques, operacions d'actualització i manteniment de versions. Aquests robots, així doncs, van evolucionant des de simples programes autònoms capaços de fer jugar i entretenir internautes, envers gestors automatitzats de tasques i llançament de noves aplicacions al servei de terceres parts. És comú trobar en el codi font d'aquests robots del final dels noranta la possibilitat de creació de comptes d'usuaris amb privilegis estratificats, i també la inclusió de consoles d'ordres i la possibilitat d'execució de macros i *scripts* per part d'usuaris amb prou privilegis.

Lectura recomanada

Una de les millors lectures per a entendre l'evolució de les xarxes de zombis és l'article "The Evolution of Malicious IRC Bots", publicat per Symantec i escrit per John Canavan. Hi podreu trobar un segon cas semblant al desplegament de Subseven, conegut sota l'àlies de **Pretty Park**. Igual que el cas relacionat amb el desplegament a gran escala de Subseven, Pretty Park es caracteritza per la instal·lació de programari maliciós de tipus troià, que permetrà a l'operador de la infecció un control total sobre els equips que compondran la futura xarxa de zombis.

La primera utilització del terme *botnet* es remunta a 1993, basant-se en la construcció de xarxes repetidores del servei IRC mitjançant el control d'equips informàtics ordinaris, connectats a Internet. El control d'aquests equips per a formar la xarxa de servidors d'IRC es basava en la utilització de les ordres del protocol mateix. Des d'aquesta primera utilització el 1993, les xarxes de zombis han evolucionat avui dia envers completes xarxes d'equips informàtics infectats i controlats pels operadors que van propagar la infecció.

Fins al final de la dècada dels noranta no podem trobar l'aparició de les primeres xarxes de zombis amb connotacions fraudulentes o malvades. Un dels primers casos rellevants que hem de destacar és el desplegament de robots basat en la infecció a gran escala del cuc IRC/Jobbo i la instal·lació posterior en les màquines infectades de l'eina **SubSeven**. El cuc IRC/Jobbo va tenir com a vector de transmissió l'explotació remota d'errors de programació en clients d'IRC de l'època (majoritàriament, el client mIRC per a sistemes MS Windows). Mitjançant l'explotació de vulnerabilitats, i l'escalada posterior de privilegis, el resultat va ser la construcció d'una xarxa d'equips controlats mitjançant la injecció en les víctimes de programari maliciós de tipus troià. L'eina instal·lada en aquests equips, Subseven, oferirà a l'operador de la xarxa de zombis un control d'administració total sobre cada màquina infectada.

A més d'eines tradicionals que podem trobar en altres troians i *rootkits* de l'època (com ara l'ocultació de processos en execució), el cas Subseven també es va caracteritzar per la instal·lació de noves funcionalitats per al robatori de contrasenyes de correu emmagatzemades en els equips infectats (utilitzades posteriorment per a propagar la infecció, o en campanyes de correu brossa), robatori dels noms d'usuari i contrasenyes de serveis de missatgeria instantà-

nia, capacitat de reconfiguració dels paràmetres de xarxa, emmagatzematge de fitxers, descàrrega automàtica d'aplicacions, incorporació d'eines d'encaminament per a readreçar aplicacions i incorporació de nous servidors i clients IRC en les víctimes (ocults, naturalment, de l'espai de gestió dels administradors dels equips infectats). Una altra de les característiques importants que cal destacar del cas de Subseven és la instal·lació d'eines per a la construcció i el manteniment de canals de control per a l'execució d'atacs posteriors distribuïts de denegació de servei. Aquests atacs requereixen un model distribuït d'equips disposats a ser sincronitzats per part d'un o més atacants per a l'enviament conjunt d'atacs DoS contra un mateix objectiu. L'objectiu de la xarxa de zombis resultant era, així doncs, la utilització d'equips armats amb suficients eines d'atac, amb suficients privilegis d'administració i, si pot ser, amb accés a xarxes amb una gran amplada de banda. L'objectiu era igualment esborrar les petjades originals de l'origen de l'atac, fent que el trànsit de control que desencadenava els atacs passés desapercebut entre centenars o milers de sistemes executant de manera sincronitzada les diferents etapes de l'atac des de diferents xarxes.

Atac DoS

Un atac de **denegació de servei** (de l'anglès, *denial of service* o DoS) agredeix la disponibilitat d'accés de la víctima a un recurs (en el cas de ser un usuari final); o dels usuaris que pretenen accedir als recursos oferts per la víctima (en el cas de tractar-se d'un servidor de serveis). És, per tant, l'apropiació exclusiva d'un recurs o servei amb la intenció d'evitar qualsevol accés a terceres parts.

El cas important següent que cal destacar és **Agobot** (també coneguda sota el nom Gaobot). Aquesta xarxa de zombis es basa, de fet, en una millora de dos desplegaments anteriors (possiblement entre el 2000 i el 2001) batejats sota l'àlies de GTbot i SDbot. La xarxa de zombis Agobot, el desplegament de la qual va ser possiblement a mitjan any 2002, senta les bases definitives en el desenvolupament i cicle de vida actual de les xarxes de zombis. Agobot introdueix un disseny modular i la majoria de les funcionalitats que es troben encara avui en les xarxes de zombis més recents. Les eines relacionades amb la gestió d'Agobot es componen de tres mòduls independents: un primer mòdul encarregat de garantir comunicacions IRC de control i la gestió de portes del darrere; un segon mòdul encarregat de gestionar les tasques i serveis (per exemple, atacs DDoS) proporcionats pels robots de la xarxa de zombis, i un tercer mòdul per a garantir la seguretat del programari maliciós instal·lat en les víctimes i evitar una possible desarticulació dels equips de la xarxa de zombis.

Lectura recomanada

L'article "Spamalytics: An Empirical Analysis of Spam Marketing Conversion", publicat per investigadors de la Universitat de Califòrnia (centres de Berkeley i San Diego) tracta els possibles beneficis obtinguts pels operadors de la xarxa de zombis Peacomm (també coneguda com a Storm), especialment gràcies a les campanyes de correu brossa encobertes pels robots d'aquesta xarxa de zombis.

Agobot també va sentar les bases del model econòmic que fa possible l'existència i evolució contínua de les xarxes de zombis. Multitud d'estudis han reportat estimacions sobre els possibles guanys obtinguts per les activitats encobertes per Agobot i altres xarxes de zombis derivades com Peacomm i Conficker. De fet, la resta de les xarxes de zombis aparegudes a partir d'Agobot es caracteritzen per una millora contínua de les tecnologies emprades per al manteniment i la gestió dels robots. Tals evolucions són merament tècniques, però posen de manifest novament el model econòmic que s'amaga darrere del desplegament d'una xarxa de zombis, i que permet a les organitzacions que promouen la construcció d'aquestes xarxes una millora contínua dels seus productes. Al llarg dels apartats següents tractarem algunes de les tècniques i innovacions que han introduït aquestes xarxes de zombis durant aquests últims anys.

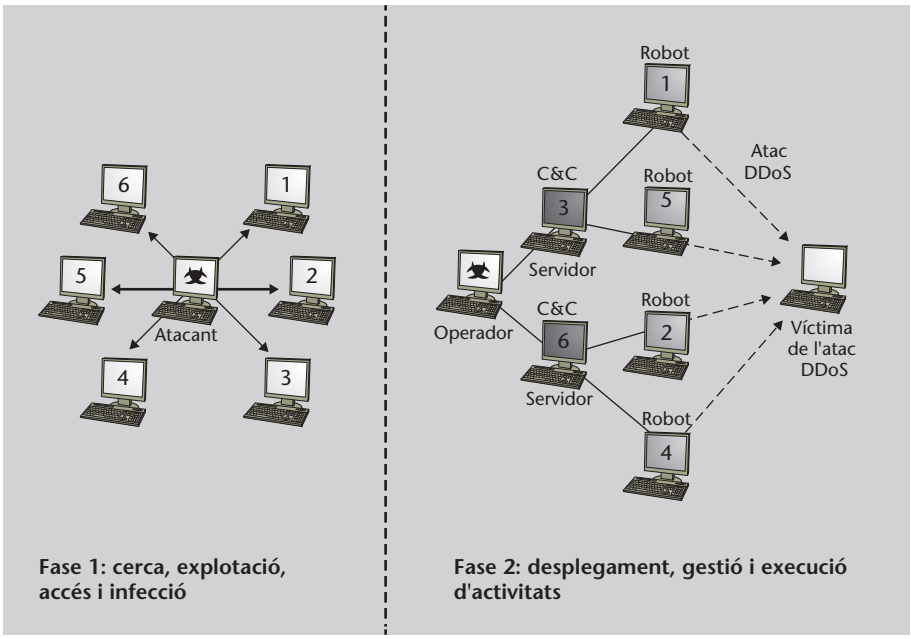
2. Fases prèvies al desplegament d'una xarxa de zombis

La majoria de les xarxes de zombis descobertes avui dia segueixen un patró de desplegament i d'actuació molt similar. La figura 2 mostra de manera esquemàtica la construcció típica d'una xarxa de zombis. L'objectiu de la xarxa de zombis representada en la figura és posar a disposició d'un atacant els recursos de multitud d'equips connectats a Internet per a llançar finalment un atac de denegació de servei contra un equip concret. Podem apreciar dues etapes ben diferenciades:

1) cerca, explotació, accés i infecció dels futurs equips de la xarxa de zombis, i

2) desplegament dels canals de comunicació i execució de tasques.

Figura 2



En aquest apartat, ens centrarem en la primera etapa. Veurem algunes de les tècniques utilitzades per operadors de xarxes de zombis actuals per a garantir una propagació correcta dels futurs equips que compondran la xarxa. Aquestes tècniques comparteixen multitud de semblances amb la majoria del programari maliciós, ja analitzat en mòduls anteriors d'aquest material. Per exemple, realització d'escombratges de ports, de serveis, etc. Aquestes tècniques són necessàries per a inicialitzar el desplegament, alhora que per a classificar les vulnerabilitats que permetran finalment a l'atacant infectar i controlar els seus futurs equips. Com de costum, veurem la utilització i injecció de troians,

de *rootkits* i del codi de control necessari per a convertir els equips en robots de la xarxa de zombis.

La primera fase en el desplegament d'una xarxa de zombis es pot descompondre en els passos següents:

1) **Cerca i identificació de robots.** En aquest primer pas, l'atacant tractarà de recollir informació i aprendre tot el que pugui sobre els equips que tractarà d'infectar i convertir en robots de la xarxa de zombis. Especialment, tractarà de descobrir quins serveis (i les seves versions) són accessibles des de l'exterior, amb l'objectiu d'identificar possibles vulnerabilitats i errors de configuració.
2) **Explotació i accés no autoritzat.** En aquest segon pas, l'atacant tractarà d'aconseguir privilegis d'administrador, abusant d'alguna de les deficiències trobades durant l'etapa anterior.
3) **Infecció i presa de control.** Una vegada ja produïda l'explotació de la vulnerabilitat que va permetre l'accés a l'equip, l'atacant prendrà el control de l'equip i farà la instal·lació d'aquelles eines que permetin que l'atac i les futures accions o tasques passin desapercebudes per al propietari o usuari legítim del sistema.

Dins de la tercera etapa, d'infecció i presa de control, es preveuen activitats com ara l'eliminació d'entrades sospitoses en fitxers de registre, la instal·lació i modificació d'ordres d'administració per a ocultar l'entrada en els sistemes de la xarxa, o l'actualització dels serveis vulnerables que ha utilitzat per a la intrusió (per a evitar que terceres parts s'introdueixin de nou en l'equip), etc. Es preveu també dins d'aquesta fase la realització de connexions necessàries per a descarregar la imatge completa de noves eines o actualitzacions dels binaris associats a la xarxa de zombis. Una vegada feta aquesta fase, l'equip infectat passarà a ser considerat un robot (o agent de la xarxa de zombis) més del sistema controlat per l'atacant. Les eines instal·lades garantiran també l'execució dels futurs serveis associats a la xarxa de zombis.

A continuació, passem a veure amb més detall algunes de les subtasques que acabem de presentar.

2.1. Cerca i identificació de futurs robots

Prèviament a l'explotació de vulnerabilitats i infecció de víctimes, l'atacant requereix trobar i conèixer les característiques dels equips que compondran més endavant la xarxa de zombis. La fase de recollida d'informació pot començar amb la simple utilització d'aplicacions d'administració que permetin

l'obtenció d'informació d'un sistema, com ara *ping*, *traceroute*, *whois*, *finger*, *rusers*, *nslookup*, *rcpinfo*, *telnet*, *dig*, etc.

Per exemple, la utilització de l'ordre *ping* en segons quins dominis, al costat de l'existència d'identificadors especials, podria permetre a l'atacant determinar l'existència d'alguns dels equips connectats a la xarxa d'aquest domini.

Una vegada descoberta l'existència, com a mínim, d'un dels equips del domini, l'atacant tractarà d'obtenir informació relacionada amb la topologia de xarxa de les víctimes. Eines com *traceroute* o *whois* poden ser utilitzades per l'atacant per a esbrinar el sistema operatiu dels diferents equips d'un domini concret, i també de la resta dels equips recorreguts fins al sistema de destinació. D'altres, com *finger* o *rusers*, oferiran informació per a descobrir l'existència d'usuaris vàlids.

L'atacant complementarà les informacions obtingudes amb l'ús d'eines de marcatge que busquen l'obtenció d'empremtes identificatives dels sistemes oposats prèviament. La empremta identificativa que l'atacant tractarà d'obtenir dels sistemes oposats començarà per una referència a les característiques de xarxa, especialment de la pila TCP/IP d'aquests. En primer lloc, aquesta informació li permetrà ajustar o confirmar el sistema operatiu que s'executa en els equips oposats. En segon lloc, facilitarà la classificació de possibles vulnerabilitats per atacar en la propera etapa del desplegament.

Les diferents interpretacions d'un mateix RFC associat a qualsevol protocol, i també les decisions finals per a implementar-lo en un sistema operatiu concret, poden oferir informació molt valuosa per a la identificació de característiques internes d'un equip connectat a Internet. De fet, la probabilitat d'identificar un sistema operatiu mitjançant una simple anàlisi remota de les característiques d'implementació de la seva pila TCP/IP són molt altes.

L'atacant pot, de la mateixa manera, utilitzar eines existents per a la realització d'escombratge de ports, escombratge de serveis o escàners de vulnerabilitats. Així doncs, l'exploració de ports TCP o UDP permetrà el reconeixement de serveis oferts gràcies a associacions preestablertes entre identificadors i serveis estàndard (per exemple, l'associació entre el servei Netbios i l'identificador de port 139). L'atacant podrà utilitzar i combinar més endavant aquesta informació en les etapes posteriors per a afinar l'explotació de vulnerabilitats d'aquells sistemes i serveis que hagin estat oposats. És important tenir present que l'atacant farà part d'aquestes activitats des d'equips que han estat prèviament infectats. És fins i tot probable que l'atacant disposi ja d'una xarxa de zombis existent per a la realització de la seva cerca de víctimes. Pensem que la utilització d'una xarxa de zombis prèvia, composta, aproximadament, de 65.000 robots, seria capaç de fer un escombratge de ports d'una xarxa de classe B mit-

Vegeu també

Per a més informació sobre els escàners de vulnerabilitats podeu consultar l'apartat 5 del mòdul didàctic "Vulnerabilitats en xarxes".

jançant el simple enviament d'un únic paquet per robot. Finalment, no hem d'oblidar la possibilitat de fer la cerca de víctimes dins d'una mateixa xarxa local mitjançant la utilització d'escoltes de xarxa. Les eines de tipus *sniffing* contra xarxes TCP/IP locals són realment efectives, ja que permeten interceptar, emmagatzemar i analitzar gran quantitat d'informació sensible enviada mitjançant protocols que no són protegits mitjançant xifratge. D'aquesta manera, l'atacant pot obtenir novament informació sobre noms d'equips i de domini, comptes d'usuari, claus d'accés o fins i tot adreces d'usuaris de correu electrònic relacionats amb els equips de la xarxa local (víctimes potencials per a les properes etapes d'explotació de vulnerabilitats i infecció complementària d'altres equips).

Vegeu també

Per a més informació sobre les escoltes de xarxa podeu consultar el subapartat 2.1 del mòdul didàctic "Vulnerabilitats en xarxes".

2.2. Explotació de vulnerabilitats i accés no autoritzat

La major part de la informació obtinguda en l'etapa anterior (cerca i identificació de futurs robots) serà utilitzada per a obtenir un accés remot, i no autoritzat, en els equips oposats. Sovint, aquest accés es materialitza mitjançant l'explotació de vulnerabilitats no corregides per part dels propietaris o administradors dels equips en qüestió. La majoria de les vulnerabilitats explotades estan relacionades amb deficiències de programació en aplicacions o serveis de xarxa exposats a Internet. Aquestes deficiències, malgrat trobar-se en el nivell de sistema operatiu o de llenguatge, afecten, en general, la seguretat global d'una xarxa. La majoria del codi víric en forma de cuc, per exemple, aconsegueix introduir-se en nous equips per mitjà de l'explotació d'aquestes deficiències.

Recordem també que la major part de les deficiències de programació explotades durant aquesta fase es deuen a situacions no previstes pels desenvolupadors de l'aplicació. Per exemple:

- entrades no controlades que poden provocar accions malintencionades i execució de codi maliciós;
- ús de caràcters especials que permeten un accés no autoritzat al servidor del servei;
- entrades inesperadament llargues que provoquen desbordaments dins de la pila d'execució i que poden implicar una alteració en el codi per executar, etc.

S'espera, per tant, l'explotació remota de la seguretat per mitjà de tècniques ja vistes en mòduls anteriors, com, per exemple, desbordaments de memòria intermèdia i explotació de cadenes de format. Els atacs que permeten explotar aquest tipus de deficiències es presenten generalment en forma de binaris (programes executables) ja compilats per al sistema operatiu en el qual s'està executant l'aplicació vulnerable, i coneguts amb l'àlies d'*exploits* remots.

Un ***exploit** remot* és un programa, generalment escrit en C o assemblador, que força les condicions necessàries per a aprofitar-se d'un error de seguretat subjacent en una aplicació de xarxa o servei. L'objectiu final sol ser l'obtenció d'un accés remot no autoritzat en l'equip atacat.

La llista següent mostra, de manera no exhaustiva, algunes vulnerabilitats típiques que són analitzades pel codi associat a una xarxa de zombis durant l'etapa d'explotació de vulnerabilitats:

- Serveis RPC (*remote procedure call*) erronis en objectes DCOM (*distributed component object model*) en sistemes operatius Windows XP. L'explotació remota és possible mitjançant l'accés als serveis vulnerables per mitjà de ports TCP (per exemple, els ports 135, 139, 445 i 593, entre altres).

- Serveis web basats en IIS5 WEBDAV. Explotació remota per mitjà de ports TCP (per exemple, el port 80).

- Versions vulnerables del Windows Messenger. Explotació remota per mitjà de ports TCP (per exemple, el port 1025).

- Implementació ASN.1 vulnerable en servei Kerberos per a sistemes operatius Windows. Explotació remota per mitjà de ports UDP (per exemple, el port 88).

- Servei HTTP vulnerable del sistema operatiu CISCO IOS en la seva gamma d'encaminadors (*routers*). Explotació remota per mitjà de ports TCP (per exemple, port 80).

- Versions vulnerables del sistema gestor de bases de dades MSSQL. Explotació remota per mitjà de ports TCP (per exemple, el port 1433).

Es consideren també part d'aquesta etapa l'explotació de deficiències d'autenticació dels serveis oposats durant l'etapa inicial. Per exemple, en el cas que els equips oposats tinguin serveis oberts basats en una autenticació per combinació de nom d'usuari i contrasenya (tipus Netbios, Miscrosoft-DS, FTP, VNC, etc.), un atac manual o automatitzat en forma de cuc pot tractar d'accedir als recursos del servei mitjançant *password cracking*, *rainbow tables*, atacs de diccionari o simplement força bruta. En la majoria dels casos, fins i tot desconeixent els noms d'usuari associats a l'equip per atacar, és normal tractar de forçar l'ús de comptes per defecte, i combinacions conegudes, com ara:

- guest/letmein, invited/client, recovery/temp,
- staff/changeme, faculty/qwerty, student/1234,
- tech/public, ftp/default, manager/friend, ...

Aquestes combinacions, encara que pot ser que ofereixin únicament accessos remots amb privilegis mínims (en general, solament lectura i amb perfil de convidat), poden més endavant donar lloc a la instal·lació local de *exploits* en el sistema operatiu, que permetin una escalada de privilegis final, per obtenir control total sobre l'equip atacat.

Finalment, és en aquesta etapa quan es fan, també, algunes de les parts més crítiques en el desplegament d'una xarxa de zombis: instal·lació de troians i portes del darrere, inicialització de serveis i futurs canals de comunicació/gestió, correcció de vulnerabilitats (per a evitar altres atacants o operadors prendre control sobre els equips), etc. Per això, multitud d'autors consideren que el cicle de vida d'una xarxa de zombis comença precisament durant aquesta part de l'etapa d'explotació, accés i infecció. La llista següent (no exhaustiva) mostra alguns exemples de portes del darrere i troians que són (o han estat) amb freqüència utilitzats per xarxes de zombis durant l'etapa d'infecció d'equips:

Vegeu també

Per a més informació sobre troians, *rootkits* i portes del darrere podeu veure l'apartat 4 del mòdul didàctic "Vulnerabilitats de baix nivell i programari maliciós".

- *Subseven* (port per defecte: 27347)
- *NetDevil* (port per defecte: 903)
- *Optix* (port per defecte: 3140)
- *Bagle* (port per defecte: 2745)
- *Kuang* (port per defecte: 17300)
- *Mydoom* (port per defecte: 3127)

Les eines anteriors solen ser instal·lades de manera automàtica; però, configurades de manera manual per part dels operadors (humans) de la xarxa de zombis. Això és, generalment, necessari per a garantir la configuració apropiada dels equips infectats. També, per evitar errors que podrien ser utilitzats pels propietaris genuïns dels equips per a descobrir i eliminar (per exemple, per mitjà d'eines de detecció de codi víric) parcial o globalment les eines instal·lades. Finalment, pot ser també necessària la interacció directa dels operadors amb l'objectiu d'inicialitzar contrasenyes i llistes de control d'accés per evitar que terceres parts s'apropiïn dels equips recentment infectats. Veurem amb més detall parte d'aquestes accions en els apartats següents, en relació amb les tècniques per a la gestió, coordinació i protecció de recursos d'una xarxa de zombis.

2.3. Atacs i infeccions complementàries

Concloem aquest apartat amb un resum de tècniques complementàries, que se solen fer en paral·lel a les etapes anteriors. Es tracta d'estratègies menys convencionals i menys estudiades des d'un punt de vista acadèmic, però igual d'efectives a l'hora de trobar i infectar víctimes. La majoria propicien, a més, una manera asíncrona i implícita perquè les víctimes es descobreixin i exposin a si mateixes davant els atacs preparats per l'operador de la xarxa de zombis. La majoria són simples vectors de transmissió utilitzats per programari maliciós

Vegeu també

Per a més informació sobre les tècniques d'enginyeria social podeu veure el mòdul didàctic "Enginyeria social".

tradicional (tipus cucs, troians i virus). Ja que la majoria correspon a tècniques relacionades amb l'enginyeria social, veurem un simple resum de les tres tècniques més comunes i representatives:

1) Distribució de correus electrònics que contenen el programari maliciós. Com per a la distribució de molts altres tipus de programari maliciós en general, els operadors d'una xarxa de zombis solen utilitzar equips ja infectats, al costat de tècniques d'enginyeria social, per a la distribució de codi maliciós en correus electrònics (tant per mitjà de serveis SMTP, POP3 o IMAP, com per mitjà de l'ús de nous serveis de missatgeria per a xarxes socials). Un codi maliciós serà associat als missatges amb l'objectiu d'explotar vulnerabilitats de sistema o de xarxa en les aplicacions client de la víctima de l'atac. Per a això, el codi serà associat al missatge com un document o fitxer adjunt (o simplement referenciat en forma d'enllaç en el cos del missatge). A continuació, l'ús de tècniques d'enginyeria social garantirà que la víctima executi el codi (o visiti l'enllaç) des de l'aplicació o el servei vulnerable que l'atacant espera explotar.

Exemples

Els següents són alguns exemples d'atacs relacionats amb aquesta categoria:

- enviament d'enllaços tipus XSS, CSRF o pesca, tractant d'enganyar i robar informació proporcionada per l'usuari (per exemple, noms d'usuari i contrasenyes);
- codi ocult dins del missatge electrònic per a la instal·lació posterior de macros o codi interpretat (imatges o estructures de dades amb contingut maliciós, tipus VBasic, JavaScript, Flash, etc.) que tractarà, més endavant, d'explotar vulnerabilitats locals o remotes en la víctima, i
- propaganda sobre llançadores web (per exemple, falsos noticiaris en línia o llocs web amb continguts il·lícits, que amaguen en el seu codi HTML la injecció i execució en la víctima de codi víric).

Vegeu també

Per a més informació sobre la pesca (o *phising*) podeu veure l'apartat 4 del mòdul didàctic "Enginyeria social".

Sigui quina sigui la tècnica, l'objectiu serà sempre el mateix: bé de manera explícita per part de l'usuari, bé de manera implícita a causa d'errors de programació, que s'executi en el sistema operatiu de la víctima algun procés que acabarà explotant una vulnerabilitat local o remota per a autoinstal·lar el codi (o part del codi) associat amb els binaris de la xarxa de zombis.

2) Infecció per mitjà de missatgeria instantània. De manera similar al correu electrònic tradicional o de xarxes socials, els operadors de xarxes de zombis utilitzen també amb freqüència l'explotació i el desplegament de programari maliciós per comptes de missatgeria instantània. De nou, ens trobem amb la combinació de tècniques d'enginyeria social amb l'objectiu d'enganyar i forçar els usuaris d'equips vulnerables (bé en el nivell d'aplicació o de xarxa) a prémer sobre fitxers adjunts o referències/llançadores malintencionades. És normal, a més, la inundació de múltiples comptes en paral·lel mitjançant SPIM (de l'anglès *spam in instant messaging*).

3) Programari maliciós camuflat en l'intercanvi de fitxers via P2P. Finalment, és normal l'explotació (una vegada més, per mitjà de tècniques d'enginyeria social) de la confiança dels usuaris d'eines per a l'intercanvi de fitxers

via xarxes de parell a parell (de l'anglès *peer-to-peer* o P2P), com l'Emule, el Bittorrent, etc. El codi associat a la xarxa de zombis serà, per norma general, camuflat entre continguts populars d'aquestes xarxes amb l'objectiu de ser transmès i executat en equips vulnerables.

3. Coordinació i gestió bàsica de robots

En aquest apartat tractem sobre la fase de coordinació i gestió dels robots de la xarxa de zombis. En aquesta fase, els operadors de la xarxa de zombis han de desplegar els recursos necessaris per a fer, més endavant, l'execució dels serveis per als quals la xarxa de zombis va ser concebuda (per exemple, venda d'informació fraudulenta, execució coordinada d'atacs o creació d'altres xarxes de zombis). Per tot això, l'operador de la xarxa de zombis desplegarà una sèrie de mecanismes de comunicació, sovint referenciats en la bibliografia com a canals C&C*. Aquests canals permetran a l'operador controlar i coordinar els seus robots. Aquests mateixos canals també han de permetre als robots retornar el resultat de les seves operacions a l'operador de la xarxa de zombis.

*De l'anglès, *command* & *control*

Veurem, en primer lloc, esquemes tradicionals, la majoria construïts sobre arquitectures centralitzades amb el suport de protocols com IRC i HTTP. Aquests primers esquemes es caracteritzen per una gran flexibilitat en el desplegament i manteniment de canals C&C, però sofreixen fortes limitacions lligades a la redundància dels seus serveis i a la dificultat de protecció dels seus nodes centrals. Deixarem per a l'apartat següent l'ús d'esquemes més avançats que tracten de pal·liar aquestes limitacions mitjançant l'ús d'esquemes descentralitzats basats en protocols P2P (de l'anglès *peer-to-peer*) o esquemes preventius que tracten de protegir els servidors de canals C&C amb el suport del protocol DNS.

3.1. Gestió centralitzada basada en serveis IRC

Les primeres xarxes de zombis de la història feien la gestió dels seus equips per mitjà de canals C&C basats en el protocol IRC. Per a això, el codi associat a la xarxa de zombis requereix que cada robot (una vegada finalitzada l'explotació de vulnerabilitats i la injecció de codi víric) se subscrigui de manera automàtica a un, o diversos, canals específics de servidors IRC. Aquests servidors estaran, per descomptat, controlats pels operadors de la xarxa de zombis. Els temes (o *topics*) d'aquests canals IRC són utilitzats per a emmagatzemar i intercanviar ordres amb els robots. L'intèrpret associat al codi del robot simplement requereix anar analitzant i identificant les temàtiques dels canals subscrits per a anar obtenint noves ordres.

La utilització de la tecnologia IRC per a la construcció de canals C&C ofereix multitud d'avantatges. En primer lloc, ofereix un alt nivell d'interacció a partir d'un protocol relativament senzill. Possibilita, a més, la utilització de comunicacions de tipus dúplex i una alta eficiència de resposta en totes dues parts

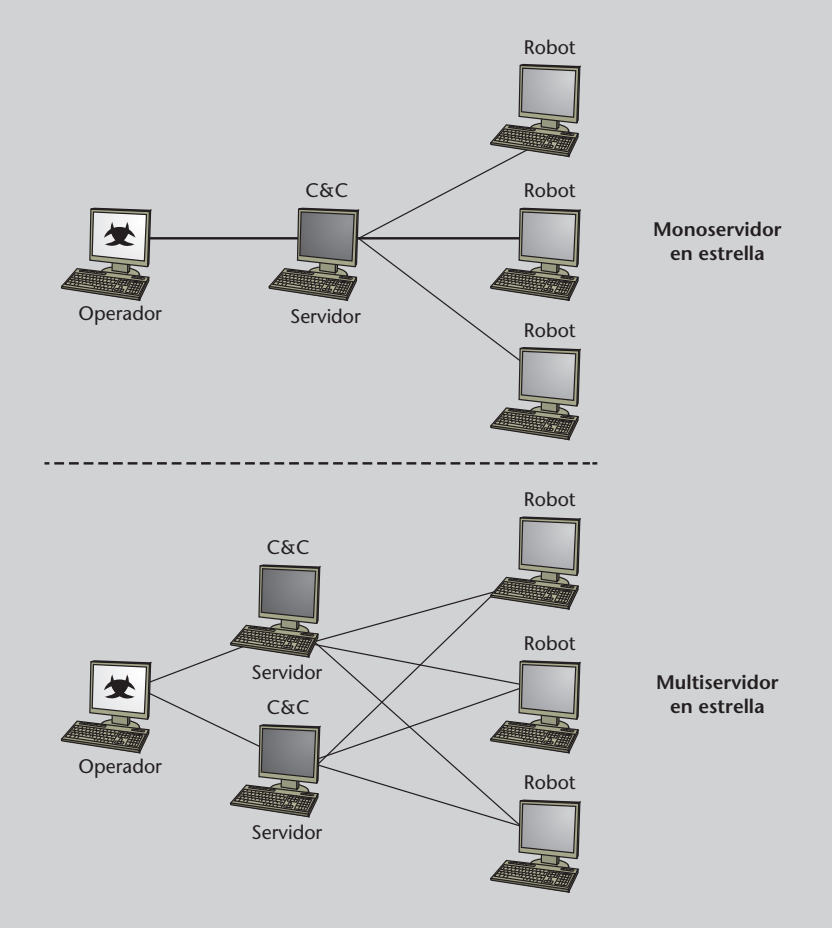
de la comunicació (tant clients com servidors). El desplegament i la gestió del manteniment dels servidors és també relativament senzilla, ja que existeixen des dels seus inicis multitud d'implementacions per a un vast ventall de llenguatges i plataformes. El protocol IRC ofereix, a més, solucions per a garantir un mínim de seguretat en el servei. De fet, el protocol IRC ofereix de manera nativa el concepte d'usuari, àlies d'usuari, gestió de contrasenyes, etc.

Quant a la redundància i robustesa dels models C&C basats en IRC, és important destacar que es basen en arquitectures centralitzades, caracteritzades per l'existència d'un o diversos nodes centrals, encarregats de redirigir els missatges de l'operador entre els robots. El principal desavantatge d'aquesta centralització és la facilitat de detectar i atacar aquests nodes centrals amb l'objectiu de desarticular el sistema de comunicació que garanteix la gestió de la xarxa de zombis. Veurem més endavant algunes de les estratègies de redundància utilitzades sovint entre servidors i clients C&C de xarxes de zombis actuals amb l'objectiu de remeiar aquest problema.

Exemple

La figura 3 destaca dues topologies d'exemple que són, o han estat, comunament utilitzades en arquitectures centralitzades per a la gestió de robots a partir de tecnologies IRC. Totes dues topologies es caracteritzen per utilitzar servidors IRC que s'encarreguen de centralitzar la comunicació dels robots cap a l'operador que va desplegar la xarxa de zombis.

Figura 3



Sigui quina sigui la topologia, podem caracteritzar l'intercanvi d'ordres entre robots i operadors mitjançant l'ús de dos tipus de models:

- **Mitjançant models de tipus PUSH**. Amb la utilització d'un model PUSH, l'operador de la xarxa de zombis serà l'encarregat d'enviar (empènyer) la primera ordre de control que requereixen els robots de la xarxa de zombis. Aquesta ordre és emmagatzemada normalment com el tema dels canals del servidor (o servidors) per als quals els robots han estat programats a visitar. Així doncs, i de manera asíncrona, els robots de la xarxa de zombis comprovaran periòdicament (segons com hagi estat programada la seva agenda) per accedir a aquests canals, per descarregar noves ordres emmagatzemades per l'operador. Cada vegada que un nou equip infectat s'uneixi a la xarxa de zombis, recollirà d'aquesta manera l'operació inicial que ha d'executar per a completar la fase de desplegament.

- **Mitjançant models de tipus PULL**. Amb la utilització d'un model PULL, la mateixa ordre serà executada per tots els robots sense necessitat d'interacció directa amb l'operador. En contrapartida, l'operador necessitarà conèixer *a priori* on cal emmagatzemar o fer l'enviament de les ordres per a garantir una inicialització correcta dels robots del sistema. Per a això, codificarà, per exemple, un conjunt d'adreces IP o de nom de domini associat als servidors IRC que els robots han de visitar després de la seva primera execució. Aquestes llistes seran actualitzades periòdicament a cada interacció amb els servidors IRC. En el cas d'utilitzar un model PULL, els robots requereixen iniciar una comunicació directa amb l'operador, a l'espera de rebre noves instruccions o ordres. Aquest model requereix també que els robots obtinguin durant la fase d'infecció una agenda de tasques, programada pels operadors, i emmagatzemada en els fitxers de configuració dels robots. El robot s'encarregarà d'enviar una petició (en anglès *query*) a l'operador, emmagatzemant-la com a comentari en alguns dels canals dels servidors IRC desplegats per l'operador. En descobrir la petició, l'operador respondrà la consulta mitjançant alguna aplicació automàtica amb la finalitat de proveir una resposta instantània als robots.

La comunicació entre robots i operadors, per mitjà dels servidors de canals C&C basats en tecnologies IRC, es caracteritza també per la direcció de les sessions que guien l'intercanvi de les ordres de control, i també per la presència, o absència, de dades retornades pels robots. Podem parlar de comunicacions unidireccionals quan l'operador, seguint un model de tipus PUSH, empeny les ordres cap als robots, sense necessitat que aquests últims proporcionin confirmació o dades associades a l'execució de l'ordre sol·licitada. Aquest tipus de comunicació està relacionat, en general, amb l'execució d'atacs per part dels robots, per als quals l'operador no requereix confirmació directa de l'execució de les ordres sol·licitades. D'altra banda, el model PULL sol estar lligat a la necessitat de comunicacions bidireccionals que permeten als robots retornar els resultats associats a les ordres executades. Aquest segon tipus està íntimament lligat amb la necessitat de confirmació per part dels operadors (per exemple, per a informar de l'estat de les operacions iniciades), i també en serveis de recollida d'informació per part dels robots (per exemple, operacions relaci-

onades amb campanyes de robatori d'identitats o d'intercanvi de materials il·lícits).

3.2. Gestió centralitzada basada en connexions HTTP

L'ús de canals C&C basats en HTTP és actualment (el 2011) el segon tipus més comú per darrere d'IRC. HTTP ofereix als operadors un ús més intensiu de comunicacions de tipus PULL. Com en el cas IRC, els robots sol·licitaran informació de l'operador enviant peticions, i l'operador s'encarregarà de recollir, tractar i respondre aquestes peticions. En el cas IRC és normal la utilització de servidors desplegats directament per l'operador de la xarxa de zombis. No obstant això, en el cas HTTP, és normal l'ús de servidors web desplegats per terceres parts que, de manera inconscient, es converteixen en punts d'emmagatzematge de peticions i respostes entre robots i operadors. Per exemple, llocs web que permetin als usuaris enviar i consultar informació (com fòrums, blocs, xarxes socials i gestors web de correu electrònic) poden ser utilitzats per a l'intercanvi d'informació. Robots i operadors simplement hauran de definir un codi i lloc on han de dipositar tant peticions com respostes. A continuació, els robots emmagatzemaran les seves peticions codificades apropiadament, per exemple, en algun servidor web accessible públicament per a qualsevol usuari.

És possible també esquemes indirectes de comunicació entre operadors i robots mitjançant connexions HTTP unidireccionals. En aquest cas, els robots faran una connexió, sense necessitat d'obtenir resposta immediata. Més endavant, l'operador de la xarxa de zombis tractarà de recollir aquestes connexions (per exemple, per mitjà de registres reportats pels servidors d'aquests serveis) i descobrir, per exemple, les adreces IP associades a cadascun dels robots. L'operador no sempre requerirà un control directe sobre els servidors web accedits pels robots. La possibilitat de trobar aquesta informació publicada inconscientment pels administradors dels serveis accedits (per exemple, historials de visites o estadístiques similars accessibles des de l'exterior) serà suficient. L'operador s'encarregarà, més endavant, de proporcionar les ordres als robots que s'hagin donat a conèixer per aquesta via.

Els canals C&C implementats mitjançant HTTP corresponen, en general, a models de comunicació de tipus PULL, per mitjà dels quals els operadors descobreixen peticions i actuen en conseqüència. No obstant això, és possible també utilitzar HTTP per a la construcció de canals C&C de tipus PUSH, per mitjà dels quals l'operador (que controlarà en tot moment els servidors del servei) s'encarregarà de subministrar les ordres als robots. Aquests últims seran programats per a consultar periòdicament els serveis web proporcionats pels operadors, amb la finalitat d'obtenir les ordres.

Esquemes més avançats preveuen la possibilitat d'intercanviar informació codificada en forma d'URL que contindrà, per exemple, credencials necessàries perquè l'operador es connecti a les portes del darrere instal·lades pels robots. Novament, l'intercanvi d'informació es farà de manera indirecta per mitjà de connexions HTTP en servidors web controlats per l'operador o als quals pot accedir. Aquestes URL codificaran la informació de la manera següent:

```
http://mybotnet.canal.to/get?puerto=2001&clave=1234
```

La URL anterior haurà de ser interpretada per l'operador per a extreure la informació rellevant (port i contrasenya, per exemple). Posteriorment, serà utilitzada per a connectar-se als robots i proporcionar-los les instruccions o respostes corresponents.

3.3. Gestió centralitzada basada en protocols d'aplicació similars

Encara que IRC i HTTP són els dos protocols més comuns a l'hora d'implementar arquitectures centralitzades per a controlar i gestionar els robots, és possible trobar també l'ús d'altres protocols d'aplicació. La majoria, en la seva versió PULL, ofereixen maneres interactives i indirectes per a l'intercanvi de peticions i respostes entre robots i operadors, per mitjà de fitxers emmagatzemats en servidors FTP segrestats pels operadors, o públics en general, i també segrestos d'identitats de serveis públics de missatgeria instantània. No obstant això, avui dia, són molt poques les xarxes de zombis que han estat descobertes fent ús de tecnologies com FTP o missatgeria instantània per a la comunicació per mitjà d'arquitectures centralitzades. Possiblement, aquest fet es troba en la necessitat de crear i controlar comptes associats a aquests serveis.

4. Més redundància i protecció en les comunicacions

A mesura que les xarxes de zombis han anat avançant, especialment cap a xarxes per a l'automatització de tasques il·lícites, el rendiment i la protecció de recursos en el desplegament de canals C&C comença a agafar més importància. L'ús d'esquemes centralitzats incrementa les amenaces de segrest o desarticulació d'una xarxa de zombis per part de terceres parts (en general, pels operadors legítims dels recursos de la xarxa de zombis, encara que també són possibles atacs provinents d'altres comunitats d'atacants). Encara que els protocols usats en arquitectures centralitzades permeten un mínim de seguretat (per exemple, mitjançant llistes de control d'accés per perfils d'usuari i protecció de canals mitjançant contrasenyes), no és possible garantir la resistència contra localització i desarticulació de servidors C&C.

Mostrarem en aquest apartat dues alternatives, amb l'objectiu de millorar la redundància dels recursos oferts pels robots, i també la seguretat dels seus servidors C&C. Això últim, per a evitar la localització final dels operadors i la desarticulació total de la xarxa de zombis. Veurem, en primer lloc, l'ús d'esquemes totalment descentralitzats, la major part inspirats en l'ús d'estructures de parell a parell (P2P, de l'anglès *peer-to-peer*) ja existents per a l'intercanvi de fitxers a escala global; i, en segon lloc, l'ús d'esquemes jeràrquics que combinin estratègies híbrides entre centralització i descentralització total. Aquest últim cas tractarà d'explotar al màxim les possibilitats que ofereix el protocol DNS per a renovar periòdicament l'enllaç entre referències de domini lògiques i físiques de servidors intermedis.

Les primeres xarxes de zombis utilitzaven robots de programari per a l'automatització de tasques legítimes. Els canals de control d'aquestes primeres xarxes de zombis, basats en general tant en IRC com en HTTP, tenien com a objectiu millores en la funcionalitat de les seves xarxes. No obstant això, la seguretat dels serveis oferts, o la facilitat de desarticulació d'aquests serveis, no és ni molt menys un dels objectius principals de tals dissenys. Les xarxes de zombis actuals, en general desplegades per a l'execució de tasques il·lícites, presenten una evolució contínua respecte als seus canals de comunicació i gestió, a la recerca de noves alternatives que garanteixin una gestió més redundant i segura.

4.1. Necessitat d'estratègies alternatives

Abans de passar a presentar les alternatives que sembla que s'obren camí quant a la construcció de nous canals C&C per a xarxes de zombis, repassarem una vegada més les deficiències d'esquemes anteriors, majoritàriament basats en

tecnologies com IRC i HTTP, que poden ser utilitzades per a comprometre la seguretat d'una xarxa de zombis. En primer lloc, hi ha el problema de centralització de les comunicacions entre operadors, servidors de canals C&C i robots. Per definició, la xarxa de zombis tracta de distribuir un conjunt d'operacions entre un gran exèrcit d'equips remots. Al mateix temps, es pretén que el control estigui, com més millor, en mans d'uns pocs usuaris (ja que les activitats són, en general, il·lícites). Una centralització exposa la seguretat de l'operador, o operadors, ja que pot ser reportada a les autoritats pertinents perquè procedeixin a la denúncia i desarticulació dels recursos associats. La majoria de les xarxes de zombis conegudes avui dia han estat ja desarticulades. Per a això, és imprescindible localitzar el centre d'operacions de la xarxa de zombis i reportar-lo a les autoritats i proveïdors de servei pertinents, els quals buscaran i bloquejaran el trànsit generat tant pels servidors C&C com pels robots.

Actualment, els proveïdors de servei d'Internet dediquen grans pressupostos per a rastrejar i detectar operacions sospitoses a les seves xarxes. Una vegada obtinguin les proves necessàries, seran ajudats per les autoritats de seguretat competents per a tractar finalment d'interrompre les operacions d'una xarxa de zombis, fer les denúncies oportunes i empresonar els responsables que van promoure o van desplegar la xarxa de zombis. En la majoria dels països, les activitats associades a una xarxa de zombis es troben ja tipificades apropiadament per a poder fer les intervencions policials i els procediments judicials necessaris per a perseguir i detenir aquestes activitats.

Des d'una perspectiva purament tècnica, l'ús de protocols com IRC i HTTP, sense protecció criptogràfica d'origen, facilitarà també el treball a les autoritats que tracten de desarticular una xarxa de zombis. Aquells servidors de canals C&C que no disposin de proteccions criptogràfiques seran susceptibles d'escoltes digitals, per mitjà de *detectors de xarxa*, la qual cosa permetria analitzar i rastrejar les ordres proporcionades, per exemple, per mitjà d'un simple canal IRC compartit entre operadors i robots per al llançament de tasques, i el lliurament de resultats. No solament la intercepció d'aquestes informacions posa en risc els operadors de la xarxa de zombis, sinó que també possibilita que terceres parts puguin emular els robots o prendre'n el control, bé amb finalitats benintencionades, per part de les autoritats que tractaran de desarticular la xarxa de zombis, o bé per part d'altres comunitats d'atacants, amb la finalitat d'ampliar el nombre de robots de les seves xarxes de zombis.

Lectura recomanada

B. Stone-Gross; M. Cova; B. Gilbert; R. Kemmerer; C. Kruegel; G. Vigna (2011, gener-febrer) "Analysis of a Botnet Takeover". *IEEE Security & Privacy* (vol. 9, núm. 1, pàg. 64-72

Tots aquests elements dificulten les tasques de control dels operadors de xarxes de zombis, que busquen diàriament nous esquemes que garanteixin la supervivència dels seus sistemes, evitant al màxim el risc de ser descoberts i perseguits per les autoritats (de la mateixa manera que la desinfecció dels robots que estan sota el control d'una xarxa de zombis). En el passat, servidors de canals C&C basats en IRC van permetre a les autoritats interceptar les actualitzacions de programari maliciós sol·licitades pels robots amb l'objectiu de restablir les operacions normals dels equips infectats. Avui dia, els nous esque-

mes busquen també detectar el risc de falsos robots, potencialment controlats per investigadors o forces de seguretat, amb l'objectiu d'introduir-se en una xarxa de zombis per recollir informació que més endavant pugui servir per a desarticular la infraestructura al complet.

Els esquemes estudiats en l'apartat anterior són potencialment vulnerables a aquestes activitats lícites (però perilloses a ulls dels operadors d'una xarxa de zombis). Tots aquests motius han estat, amb certesa, estudiats i analitzats per les organitzacions que s'amaguen darrere del programari maliciós disseminat pels controladors de les xarxes de zombis, i explica el nivell de perfecció en les comunicacions C&C de les xarxes de zombis actuals.

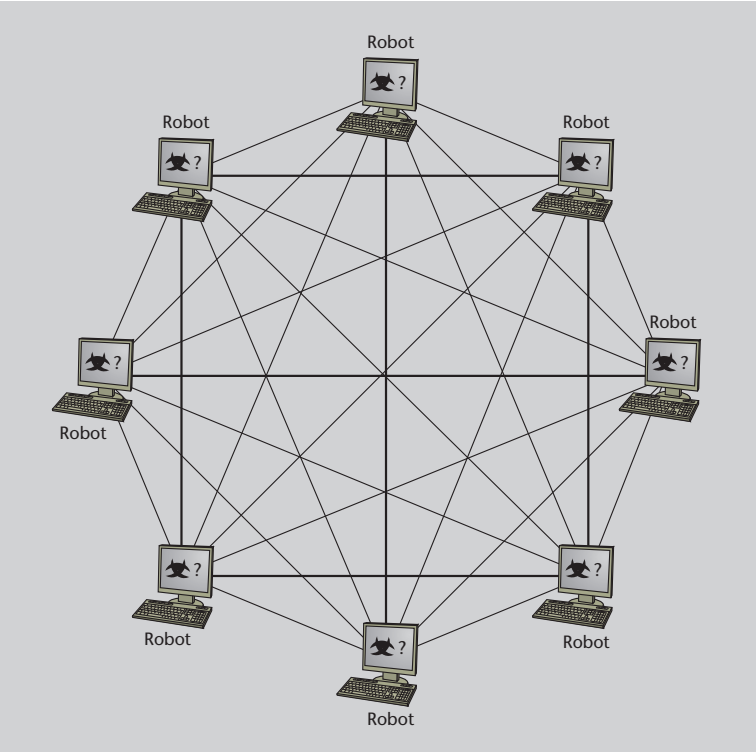
4.2. Comunicació descentralitzada mitjançant xarxes P2P

Un primer esquema que busca solucionar les limitacions vistes anteriorment és la descentralització total en les comunicacions entre robots i operadors. Un exemple pràctic és l'adaptació de xarxes P2P, utilitzades amb èxit per a l'intercanvi de fitxers, i que ha estat ja experimentat en xarxes de zombis recents.

Exemple

La figura 4 mostra un exemple senzill de l'aspecte que tindria una arquitectura basada en P2P per a la comunicació entre robots i operadors.

Figura 4



La figura mostra una xarxa de zombis amb estructura descentralitzada sense servidors C&C pròpiament dits. L'operador (o operadors) de la xarxa de zombis triarà un dels robots (equip compromès) a l'atzar i l'utilitzarà temporalment com a servidor C&C. De manera dinàmica, anirà canviant i repetint aquest procés, la qual cosa li permetrà millorar la protecció de la localització real, sempre pivotat per part d'un dels equips que haurà compromès durant la fase d'explotació. Podem també apreciar en la figura que cap de les màquines no té, *a priori*, un paper crític en l'arquitectura. Per tant, no és possible detenir o desarticular la xarxa per mitjà de la localització d'un conjunt d'equips particulars. Cada equip, durant la fase d'explotació i accés, rebrà una llista (inicialment bastant limitada) d'adreces IP d'altres robots de la xarxa de zombis.

La utilització del model P2P per a la gestió de recursos d'una xarxa de zombis fa desaparèixer el concepte de centralisme. Tots els nodes tindran les mateixes responsabilitats de fer passar peticions i respostes cap als operadors de la xarxa de zombis, els quals, a més, canviaran amb periodicitat la seva posició (lògica) en l'estructura desplegada de manera aleatòria. Si l'esquema és implementat de manera apropiada, les tasques de localització i desarticulació són extremadament complexes. D'una banda, els operadors augmentaran el seu anonimat, en poder amagar-se darrere de qualsevol robot amb igual probabilitat. D'altra banda, cap equip de la xarxa de zombis no exerceix, *a priori*, un paper prou important per a desarticular la xarxa després de desconnectar-lo.

Peacomm

Peacomm és normalment presentada en els mitjans com **Storm**, a causa del nom del cuc que s'encarregava de desplegar la infecció associada a la xarxa de zombis.

Una de les xarxes de zombis amb més repercussió mediàtica, i que estructurava les seves comunicacions per mitjà de tecnologies P2P, va ser Peacomm. La comunicació entre els equips de la xarxa de zombis es va basar en el protocol Overnet, adaptat al seu torn de Kademlia, un protocol P2P de gran importància en aplicacions P2P per a intercanvi de fitxers. A més de descentralitzar les seves comunicacions, Peacomm les protegia també mitjançant tècniques de xifratge. Això va permetre protegir la confidencialitat de les ordres i resultats intercanviats entre operadors i robots. Altres xarxes potser amb menys ressonància, però que també van aplicar el model P2P amb anterioritat a Peacomm, van ser Sinit i Nigache. De nou, els seus protocols per a comunicar els parells es van inspirar en protocols com BitTorrent i Waste. El resultat final, i en comparació de dissenys centralitzats vistos anteriorment, va ser més protecció per als operadors de la xarxa de zombis o, el que és el mateix, més dificultat en les tasques de localització i desarticulació dels servidors de comunicació C&C utilitzats pels operadors per a gestionar els robots de la xarxa de zombis.

Malgrat els avantatges inherents d'una estructura P2P per a la gestió de xarxes de zombis, sense complements addicionals també presentarà deficiències. El motiu principal és la complexitat i dificultat de desplegar els serveis, la qual cosa està íntimament lligada amb problemes de latència i de pèrdua d'ordres o respostes, ja que no sempre serà possible garantir el lliurament dels missatges entre els equips que compondran la xarxa de zombis.

Una de les primeres xarxes de zombis amb un model de comunicacions descentralitzat basat en P2P va ser **Sinit** (entorn de l'any 2003). Sinit utilitzava tècniques d'escombratge aleatòries per a trobar la resta dels parells de la xarxa de zombis. Aquest escombratge d'adreces provoca un volum de trànsit fàcilment caracteritzable, que permetia detectar i aïllar amb facilitat equips infectats per Sinit. Com a conseqüència, la xarxa va ser desarticulada amb relativa facilitat.

La cerca de parells també pot entorpir, i fins i tot reduir, l'eficiència de protecció de la tecnologia P2P. Una mala implementació del protocol d'inicialització de parells, basat en escanejos aleatoris, pot ser identificat amb facilitat per equips de detecció de xarxes de zombis i codi víric, i ser utilitzat pels proveïdors d'accés a Internet per a aïllar aquests equips per a desarticular la xarxa. Per tant, la utilització de P2P per si sola, sense mecanismes addicionals de protecció, continuarà sense solucionar les principals limitacions ja reportades en esquemes centralitzats.

4.3. Protecció basada en renovació cíclica de referències DNS

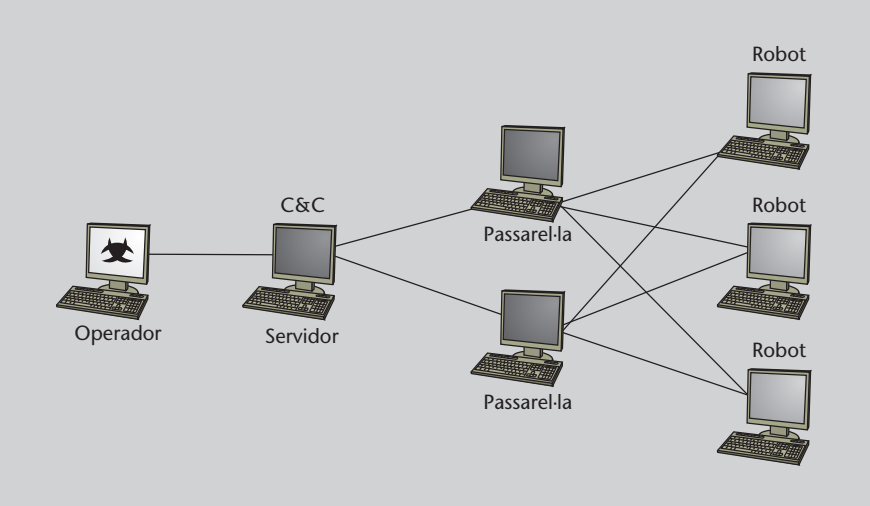
Com vam veure a l'inici d'aquest apartat, una centralització de les comunicacions facilita el desplegament de la xarxa de zombis, però pot també facilitar la localització dels servidors C&C i agilitar la desarticulació de la xarxa de zombis. D'altra banda, una descentralització total del sistema de comunicacions pot ajudar inicialment a protegir els recursos de la xarxa de zombis, però complica el desplegament i l'eficiència de les comunicacions. A més, si no és utilitzada correctament, pot acabar essent utilitzada per a caracteritzar el comportament dels robots de la xarxa de zombis i, novament, facilitar la desarticulació. Operadors de xarxes de zombis han estat treballant aquests últims anys en estructures que combinen el millor de totes dues opcions amb l'objectiu de trobar un compromís híbrid que flexibilitzi tant el desplegament de robots com la protecció dels servidors C&C. L'ús de topologies jeràrquiques basades en federació de servidors C&C per mitjà de passarel·les d'aplicació (en anglès, *proxies*) sembla la clau per a trobar aquest compromís.

Un exemple de xarxa de zombis amb un sistema de comunicacions basat en topologia jeràrquica és **Waledac** (entorn de l'any 2008). Els robots de Waledac comuniquen directament amb un conjunt de nodes repetidors que es comporten com a passarel·les. Aquests repetidors reexpediran les peticions i respostes dels robots a servidors de nivell superior mitjançant comunicacions xifrades amb el protocol TSL (*transport security layer*). Els nodes arrel de la jerarquia actuaran finalment com a servidors C&C per a respondre les peticions dels robots, o recollir-ne els resultats.

Exemple

La figura 5 mostra un exemple senzill de topologia jeràrquica. En la figura podem veure una estructura multiservidor que utilitza comunicacions estratificades en diferents nivells i enllaçats amb els robots per mitjà de passarel·les. Els robots comunicaran en primera instància amb les passarel·les, que redirigiran els missatges cap als nivells superiors, on es trobaran protegits els nodes que actuen com a servidors C&C (en última instància, en comunicació directa amb l'operador de la xarxa de zombis). Generalment, les comunicacions entre passarel·les i servidors de nivell superior utilitzaran tècniques criptogràfiques per a protegir les seves comunicacions.

Figura 5



Recordem que tots els esquemes vistos fins al moment es poden beneficiar de l'ús del protocol DNS per a obtenir comunicacions de tipus *multihoming*. El concepte de *multihoming* és utilitzat per serveis tradicionals (i legítims) per a assignar múltiples adreces IP a un mateix nom associat amb DNS. Per exemple, la configuració d'un servidor DNS pot assignar una configuració com la següent:

```
acmeBotnet.servers.com pointing to 10.0.0.1
acmeBotnet.servers.com pointing to 10.0.0.2
acmeBotnet.servers.com pointing to 10.0.0.3
...
```

Al mateix temps, l'ús de DNS també facilita que una sèrie d'equips principals gestionin aquests localitzadors de referències, fins i tot abans que la connexió amb el servidor C&C que els posarà en contacte es faci efectiva. El fet de descobrir dominis inexistents o compromesos pels operadors d'una xarxa de zombis i informar-ne implica un risc molt menor (per als operadors) que, per exemple, descobrir les adreces IP finals dels servidors C&C. Aquesta característica presenta grans avantatges i sembla l'estratègia comuna en xarxes de zombis actuals per a aconseguir la màxima protecció dels equips més propers als operadors de la xarxa de zombis, tant els servidors finals com els equips intermediaris entre l'operador i els robots. Per a beneficiar-se d'aquesta protecció, els robots dirigiran les seves peticions cap a un conjunt de servidors DNS establerts *a priori* per l'operador de la xarxa de zombis, i rebran com a resposta el conjunt d'adreces IP associades als servidors C&C. Combinat amb l'ús de tècniques com FastFlux, el sistema final millorarà la redundància i re-

sistència enfront d'una possible desarticulació per part dels proveïdors d'accés a Internet on es troben localitzats els robots. D'aquesta manera, cada robot rebrà un conjunt de referències per resoldre, les adreces IP de les quals s'aniran alternant al llarg del temps.

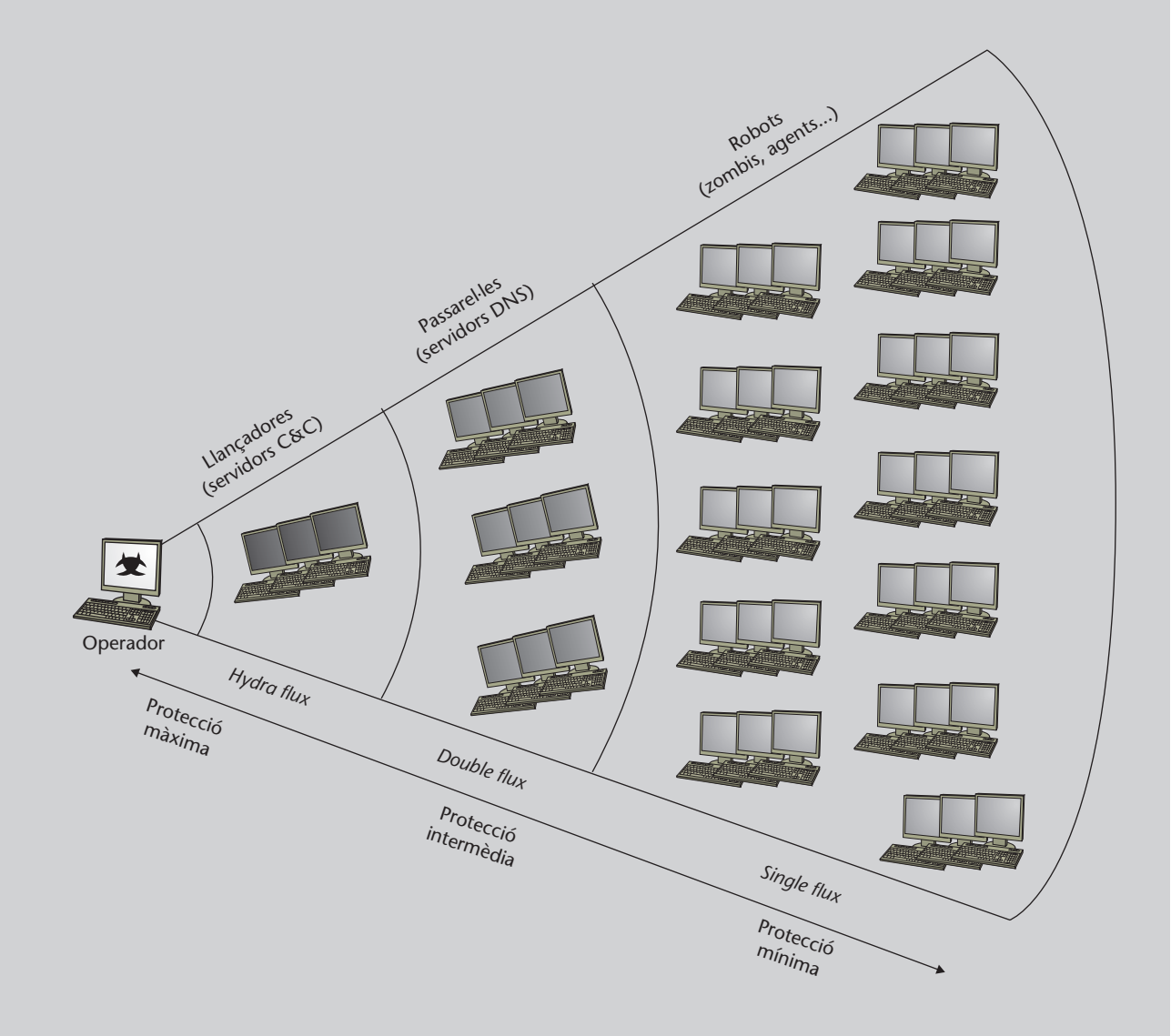
Variants i millores del FastFlux tradicional poden ajudar a complicar encara més el rastreig i la desarticulació de les infraestructures C&C d'una xarxa de zombis. L'ús de FastFlux avançat, àlies amb el qual es refereix sovint en la bibliografia a la composició jeràrquica de FastFlux encadenat, recull la majoria d'aquestes variants. L'estratègia consisteix a col·locar els recursos més propers a l'operador (com ara la consola d'operacions i els servidors C&C) en la part més alta de la jerarquia, reanomenats ara amb l'etiqueta de llançadores (de l'anglès *motherships*). A continuació, es col·locaran en la segona part de la jerarquia els servidors de DNS, etiquetats en general com a passarel·les, i que faran l'enllaç final entre robots i llançadores.

La figura 6 mostra els diferents nivells de protecció que es poden obtenir amb l'ús de FastFlux avançat.

Els servidors C&C, ara amb més responsabilitats que en esquemes anteriors, continuen en contacte directe amb l'operador de la xarxa de zombis. Entre les seves noves responsabilitats, els servidors C&C hauran de gestionar també la infraestructura de servidors DNS i fer efectiva la protecció que FastFlux avançat ofereix a la infraestructura global de la xarxa de zombis. La gestió de servidors DNS correspon a tasques de registre, actualització de noms de domini i manteniment dels servidors de nom de cada domini. El registre i l'actualització de noms de domini és fet, en general, en forma de registres DNS de tipus NS (*name server*), que emmagatzemaran l'enllaç del servidor (o servidors) encarregats de respondre a les peticions DNS dels robots per a cada tipus de domini establert pels operadors de la xarxa de zombis. És necessari gestionar, també, els fitxers de configuració de les diferents zones existents en cada domini establert per l'operador. Aquests fitxers contenen la llista dels equips existents en un domini, i també l'enllaç corresponent entre nom i adreça IP (en forma de registres d'adreça).

La xarxa de zombis **Conficker** (entorn de l'any 2008) va basar la seva estratègia de protecció en la combinació de FastFlux i la introducció d'algorismes propis per a la generació aleatòria de noms de domini associats als servidors C&C. De manera simplificada, els robots de Conficker requerien generar una llista de possibles dominis DNS associats als seus servidors C&C. Més endavant, l'operador s'encarregaria de registrar aquesta llista de dominis per a associar-los a la localització final dels servidors C&C. Periòdicament, la localització (adreça IP) dels servidors C&C s'adaptava per a reduir el risc d'una desarticulació de la xarxa de zombis.

Figura 6



Els fitxers de configuració de cada zona contindran també el valor TTL (temps de vida, de l'anglès *time-to-live*) associat amb cada registre d'adreça. Aquest valor estableix el temps (en general, en segons) durant el qual l'associació és emmagatzemada pel client en la seva memòria cau. Transcorreguts els TTL segons, el client donarà per caducada aquesta associació i tornarà a sol·licitar al seu servidor de DNS que interrogui novament als servidors arrel la nova adreça IP. Mitjançant la utilització de valors TTL petits, els operadors asseguraran que tots els equips de la xarxa de zombis refresquin els seus enllaços de manera periòdica. De nou, l'objectiu final és trobar el millor compromís perquè cap punt de la xarxa no tingui dependències directes amb nodes principals. En conseqüència, el descobriment de qualsevol node de la xarxa triat a l'atzar tindrà el mateix efecte per a la xarxa de zombis, i n'augmentarà la robustesa contra una possible desarticulació.

Lectura recomanada

És interessant la lectura de l'article "Know Your Enemy: Fast-Flux Service Networks, An Ever Changing Enemy", dels autors del projecte Honeynet, on es pot veure la utilització de FastFlux bàsic i avançat. L'article està disponible en aquesta adreça: http://honeynet.org/papers/ff/

5. Model econòmic associat a les xarxes de zombis

De manera molt breu, conclourem aquest mòdul mostrant alguns detalls sobre el model econòmic que explica l'existència actual dels desplegaments de xarxes de zombis. Aquest model és també clau per a entendre la progressiva evolució d'aquestes xarxes envers noves tècniques que dificultin les investigacions que tant proveïdors de serveis d'Internet, com autoritats i forces policials de diferents països, duen a terme diàriament en la seva guerra particular contra les organitzacions que promouen l'existència de les xarxes de zombis (i els seus clients potencials).

5.1. Primeres generacions

Com ja hem vist en els primers apartats, les xarxes de zombis inicials es van construir sobre esquemes molt bàsics, generalment basats en un codi executat per part de robots que contenien multitud d'errors de programació (és a dir, replets d'errades de programari) i que presentaven facilitat de detecció i desarticulació dels servidors C&C. També, hem vist que l'ús d'arquitectures centralitzades, comuna en les primeres xarxes de zombis, facilitava el treball a investigacions policials amb l'objectiu de trobar l'origen dels operadors i desarticular les xarxes de zombis.

Els anys 2002 i 2003 van ser els anys de més auge de les xarxes de zombis. Especialment, amb el desplegament de Gaobot i successors. Encara que el descobriment i la desarticulació van ser relativament ràpids, va assentar les bases respecte a nous mètodes de reproducció, cerca i explotació de vulnerabilitats d'equips poc protegits (però localitzats en xarxes amb grans capacitats). Aquestes tècniques permetran als seus operadors l'expansió d'activitats típiques d'economies submergides del món real sobre el pla digital (per mitjà d'Internet). Aquestes primeres generacions no es caracteritzen per una alta qualitat de productes, sinó per la força potencial dels seus recursos. Efectivament, la possibilitat de gestionar a distància xarxes de més de 65.000 robots permet recórrer amb facilitat gran part dels equips connectats a Internet, i es genera per a cada robot un volum relativament baix de trànsit.

Les tendències actuals es caracteritzen per uns operadors de xarxes de zombis cada vegada més ben formats, amb amplis coneixements en construcció de protocols robustos i utilització de comunicacions xifrades. De fet, les xarxes de zombis amaguen actualment enginyers amb gran experiència tant en xarxes com en seguretat. Estudis recents mostren millores constants de canals C&C i incorporació de tècniques d'anonimat per a continuar dificultant la detecció i desarticulació de robots i servidors associats.

A mesura que les tècniques de detecció de robots o servidors C&C avancen, els operadors de xarxes de zombis tracten també d'adoptar noves mesures que dificultin la detecció de signatures o patrons que liderin la desarticulació dels seus equips.

Però passem a repassar a continuació, abans de concloure aquest mòdul, algunes de les activitats principals que s'amaguen darrere d'una xarxa de zombis, i també les previsions de futur que expliquen la millora constant de les xarxes de zombis.

5.2. Activitats associades a xarxes de zombis actuals

Hem destacat en el primer apartat d'aquest mòdul que una de les primeres activitats que van donar a conèixer les xarxes de zombis va ser precisament l'execució d'atacs. Més concretament, atacs de tipus DDoS. Es tracta d'atacs a la disponibilitat de serveis oferts per equips o xarxes de tercers, que exerciran el paper de víctimes de la xarxa de zombis. El total, o un gran nombre, dels robots de la xarxa de zombis, tractaran de consumir els recursos de les víctimes de manera simultània, anonimitzant, a més, l'origen real de l'atac. En efecte, les ordres i les peticions originals de l'operador de la xarxa de zombis passaran desapercebudes a ulls de la víctima i de les investigacions posteriors a l'atac.

També és conegut per tots l'ús de les xarxes de zombis per a la posada en pràctica de campanyes de correu brossa per a la disseminació d'anuncis deshonestos. Com la majoria de les amenaces a Internet, les campanyes de correu brossa se solen llançar des de xarxes de zombis controlades per operadors anònims. Novament, les ordres i les peticions originades per l'operador passaran desapercebudes per a les víctimes d'aquests atacs de venda il·lícita d'informació, i es garanteix una disseminació anònima de productes en línia, a la recerca de compradors potencials. Com en el cas anterior, els robots actuen com a repetidors o passarel·les dels missatges originals orquestrats pels operadors de la xarxa de zombis.

Potser, menys conegut pel públic en general, és l'ús de les xarxes de zombis com a llançadora de disseminació de codi maliciós per a xarxes de zombis ja existents, o per a noves xarxes de zombis que s'estan desplegant encara. De manera paral·lela a la disseminació de missatges considerats per les víctimes com a correu brossa, els robots són utilitzats amb freqüència per a disseminar codi maliciós. L'objectiu és contaminar i continuar el desplegament de la xarxa de zombis mateixa, o de terceres parts, garantint l'existència de bases de codi maliciós distribuït al llarg d'Internet. Multitud d'atacs relacionats amb vulnerabilitats de serveis web, com ara XSS, CSFR, la pesca, etc., dependran en gran mesura de l'existència de xarxes de zombis paral·leles encarregades de garantir el desplegament correcte del codi final dels atacs corresponents.

Vegeu també

Per a més informació sobre vulnerabilitats web podeu veure l'apartat *Atacs a aplicacions web* del mòdul didàctic "Seguretat en aplicacions web".

Un altre exemple, fins fa poc desconegut pel públic en general, és l'ús de xarxes de zombis per a espionatge, tant de sectors públics i governamentals com dins de sectors privats (indústries de sectors com el de l'automòbil, l'aeronàutic i el de les noves tecnologies). Ja que els robots de la xarxa de zombis solen estar allotjats en aquests sectors (pensem en ordinadors o equips de sobretaula de treballadors i executius associats), és freqüent el desplegament d'atacs sobre vulnerabilitats de xarxa, que permetran l'execució d'escoltes de xarxa per a recollir i reexpedir als operadors de la xarxa de zombis qualsevol informació que passi per aquests equips sense la protecció adequada (per exemple, sense capacitats de protecció criptogràfica).

Finalment, és important tenir també present que les xarxes de zombis són utilitzades actualment per a l'emmagatzematge i la distribució de continguts audiovisuals. De fet, la falta de maduresa d'un model econòmic real basat en la distribució de continguts audiovisuals per mitjà d'Internet obre als operadors de xarxes de zombis un nínxol perfecte per a emmagatzemar i distribuir continguts audiovisuals obtinguts de manera il·lícita. Es tracta, per tant, de l'emmagatzematge i de la distribució de pel·lícules, sèries televisives, llibres electrònics i música, sense el consentiment d'autors o institucions que en tenen de manera legal el dret de còpia. Podríem incloure també en aquesta categoria la utilització de recursos per a allotjar servidors de jocs il·lícits, com casinos en línia i serveis d'apostes il·legals. L'ús de sistemes de fitxers de gran capacitat per part dels robots d'una xarxa de zombis, i també l'accés a recursos de xarxa amb grans amplades de banda i baixa latència, facilita la distribució d'aquests elements i dificulta les investigacions posteriors sobre l'origen real dels equips que allotgen els fitxers.

5.3. Perspectives i garanties de millores contínues

Podem afirmar que l'època en la qual aficionats de la informàtica es dedicaven a programar codi maliciós per simple diversió, o per donar a conèixer les seves habilitats tècniques, ha acabat. Avui dia, la programació de codi per a la construcció de xarxes de zombis és un autèntic negoci. Organitzacions de tot tipus (governamentals, comercials i fins i tot criminals) es dediquen a buscar i contractar especialistes en la matèria perquè desenvolupin nous esquemes i estratègies.

Actualment, la motivació principal dels operadors d'una xarxa de zombis sol ser de tipus econòmic. A diferència d'activitats similars al món real, com per exemple el robatori o atracament a persones o institucions físiques, el robatori de recursos electrònics i la utilització amb finalitats deshonestes, a més de comportar molts menys riscos físics i jurídics, és automatitzable i paral·lelitzable. Una vegada construïda la xarxa, aquests recursos poden ser llogats a terceres parts. Aquests ingressos econòmics expliquen l'evolució i millora tècnica contínua dels productes associats a les xarxes de zombis actuals.

La majoria dels estudis actuals sobre els guanys econòmics associats amb el manteniment d'una xarxa de zombis no deixa lloc a dubtes sobre la viabilitat del seu model econòmic. Algunes de les xifres que descrivim a continuació, basades en un estudi fet el 2004 per Peter Haag i Alain Hugentobler, ajuden a entendre la contínua evolució i millora de les tecnologies associades:

- El lloguer d'un compte d'usuari, amb accés no exclusiu als recursos del robot, ascendeix als 15 cèntims d'euro mensuals.

- El lloguer d'un compte d'usuari, amb accés exclusiu als recursos d'un robot de la xarxa de zombis, ascendeix als 30 cèntims d'euro mensuals.

- El lloguer d'una zona parcial d'una xarxa de zombis, fins a 500 robots, pot assolir els 380 euros mensuals.

- La utilització puntual d'un volum major de robots, per exemple, per a la realització d'un atac de tipus DDoS contra una víctima per determinar, pot assolir entre 40 i 700 euros.

- El lloguer de volums majors (d'un ordre superior als vint mil robots), per exemple, per a fer una campanya de publicitat mitjançant l'ús de correu brossa es comercialitza a uns 75 euros per setmana.

Informes elaborats per criminalistes i especialistes en delinqüència, tant al món real com en la seva versió electrònica, llancen a la llum xifres similars. La majoria d'aquests estudis es basen, a més, en resultats i prediccions de més de 5 anys d'antiguitat, per la qual cosa les xifres actuals poden ser molt més elevades i inquietants. La majoria dels especialistes en la matèria semblen estar d'acord sobre la gravetat de la situació, i també l'estat de maduresa dels fonaments sobre els quals es recolzen avui dia les xarxes de zombis.

En relació amb les organitzacions que hi ha darrere d'aquestes xarxes (tant avui dia, com potencialment les que les usaran en el futur) es parla sovint d'organitzacions criminals relacionades amb màfies de l'est d'Europa, igual que càrtels relacionats amb contraban de productes des de països africans i americans (tant del nord com del sud). També es parla sovint d'organitzacions governamentals en països asiàtics, que es podrien valer dels recursos de les xarxes de zombis per a obtenir avantatges industrials en relació amb les indústries occidentals. Possiblement, la realitat amaga molts altres actors que financen, directament o indirectament, millores substancials perquè futurs operadors de xarxes de zombis puguin passar desapercebuts i els seus recursos difícilment desarticulats.

Casos recents de criminals, comercials, enginyers i desenvolupadors associats amb les xarxes de zombis estan començant a sortir a la llum, i han donat a conèixer al públic general la realitat i potència d'aquesta gran amenaça. Tots aquests casos demostren una vegada més que l'objectiu final de les xarxes de

zombis, i el codi maliciós associat a aquestes xarxes, no és la destrucció massiva d'equips o recursos informàtics, o el simple acte de persones aïllades amb pretensions deshonestes, sinó l'obtenció de beneficis. L'associació dels primers serveis, la majoria relacionats amb simples atacs, juntament amb les tendències actuals de disseminar publicitat, campanyes de venda de productes, i intercanvi de transaccions financeres, mostren que no són activitats ingènues, ni a l'atzar, sinó més aviat negocis ben organitzats i reflexionats.

Resum

Les xarxes de zombis constitueixen actualment l'amenaça més gran coneguda contra Internet. Les xarxes de zombis són el resultat d'una infecció a gran escala d'equips informàtics que, una vegada infectats, passen a ser controlats per un mateix atacant (o per una mateixa organització d'atacants), sense que els propietaris autèntics ho descobreixin i, en general, amb finalitats tant malintencionades com lucratives. Així doncs, els equips infectats componen la xarxa de zombis resultant, que pot ser finalment definida com una xarxa de robots al servei de l'atacant. L'atacant es converteix en operador d'una complexa i potent xarxa, els serveis de la qual seran finalment venuts a organitzacions de tot tipus. La taula següent resumeix la major part dels aspectes que han estat tractats en aquest mòdul.

Xarxes de zombis		
Descobriment, explotació i infecció	Cerca de víctimes	Escombratge de ports + escàner de vulnerabilitats Distribució de missatges corruptes, P2P, IM... Enginyeria social, serveis secrets...
	Explotació de vulnerabilitats	Desbordaments de pila Condicions de cursa Robatori de contrasenyes, força bruta...
	Presa de control dels equips	Modificació de serveis interns Instal·lació de codi maliciós Obertura de portes del darrere
Coordinació i gestió dels robots	Desplegament de recursos i canals C&C	Arquitectures centralitzades - Topologia monoservidor en estel - Topologia multiservidor en estel Arquitectures descentralitzades - Topologia aleatòria Arquitectures híbrides - Topologia jeràrquica
	Protocols majoritàriament utilitzats	IRC, HTTP, IM, FTP... P2P (Bittorrent, Kademlia, Waste...) DNS (resolució i protecció de recursos)
	Inicialització i característiques de la comunicació	Model PUSH monodireccional Model PULL monodireccional Model PULL bidireccional
	Tècniques de redundància i protecció	Descentralització total dels servidors C&C Federació de servidors C&C Ús de FastFlux i FastFlux avançat
Serveis i activitats associades al model econòmic de les xarxes de zombis actuals	Denegacions de servei distribuïdes Campanyes de venda il·lícita Serveis d'espionatge Allotjament d'aplicacions il·lícites Disseminació d'aplicacions il·lícites	Serveis de correu brossa Allotjament de continguts il·legals ...

Exercicis d'autoavaluació

1. Quina de les afirmacions següents és correcta?

a) Les primeres xarxes de zombis de la història van ser utilitzades per administradors d'operadores de serveis il·lícits per a protegir les seves campanyes de venda de productes il·legals i per a agilitar els seus serveis d'espionatge i de control de companyies de la competència.

b) Els atacs d'una xarxa de zombis són controlats per l'operador per mitjà dels servidors C&C. Una vegada seleccionada una víctima, els robots es limitaran a seguir ordres i dirigir les accions cap a l'equip o les xarxes seleccionades per l'operador.

c) La utilització de protocols de tipus P2P per part dels robots d'una xarxa de zombis facilita la identificació dels seus servidors C&C, i assegura un desplegament de recursos més senzill i flexible per als operadors de la xarxa.

d) Les xarxes de zombis actuals són operades per amateurs amb l'objectiu de mostrar a amics i coneguts les seves habilitats tècniques a l'hora de programar codi maliciós.

2. Com garanteix l'operador que els robots continuïn sota el seu control?

a) Mitjançant la modificació dels registres o guions d'inicialització dels equips infectats, assegurant que el codi maliciós s'engegui després de cada nova reinicialització.

b) Amb l'ús d'enginyeria social, fent que els usuaris dels equips infectats continuïn executant les aplicacions relacionades amb la xarxa de zombis en cada reinicialització.

c) Mitjançant l'ús d'incentius econòmics, oferint una participació de la xarxa de zombis als usuaris legítims dels equips infectats.

d) Per mitjà de l'ús d'aplicacions P2P i estructures aleatòries per a la gestió de canals C&C que mantenen els usuaris mateixos.

3. Quin tipus d'equip informàtic és infectat i transformat amb més facilitat en forma de robot d'una xarxa de zombis

a) Els telèfons mòbils, especialment aquells que es caracteritzen per tenir més autonomia i llibertat de moviment.

b) Qualsevol equip informàtic connectat a Internet que presenti vulnerabilitats o deficiències de seguretat no corregides.

c) En general, tots aquells equips informàtics amb sistema operatiu de la família Windows.

d) Qualsevol equip que ofereixi extensions de programació basades en codi lliure.

4. Per què tots els protocols per a la gestió de robots d'una xarxa de zombis requereixen connexions transportades sobre TCP?

a) Perquè TCP ofereix els mecanismes de redundància i protecció necessaris per a evitar una desarticulació total de la xarxa de zombis.

b) Perquè les primeres xarxes de zombis de la història ho van fer així, i les xarxes de zombis actuals es limiten a estendre altres funcionalitats, però no canvien els protocols de transport originals.

c) Perquè els operadors de les xarxes de zombis requereixen l'ús de sessions de tipus TCP per a codificar les ordres de control.

d) No és cert. També hi ha casos de xarxes de zombis els canals C&C dels quals es construeixen sobre altres protocols de transport com, per exemple, UDP.

Solucionari

1. b; **2.** a; **3.** b; **4.** d;

Glossari

bug *m* Error de programació que pot desencadenar una deficiència de seguretat.

cavall de Troia *m* Programa, aparentment inofensiu, que conté en el seu interior un atac contra una vulnerabilitat no corregida.
sin **troià**

denegació de servei *f* Atac que tractarà de saturar recursos de la víctima, com ara memòria o capacitat de càlcul i processament.

denial of service f Denegació de servei.
sigla **DoS**

detector *m* Aplicació que intercepta tota la informació que passi per la interfície de xarxa a la qual estigui associada.

distributed denial of service f Denegació de servei distribuïda.
sigla **DDoS**

empremta identificativa *f* Informació precisa que permet identificar un equip o una xarxa en concret.
en fingerprinting.

escàner de vulnerabilitats *m* Aplicació que permet comprovar si un sistema és vulnerable a un conjunt de deficiències de seguretat.

exploit *m* Tècnica (en general, de tipus programari) que permet utilitzar una vulnerabilitat, encara no corregida, amb finalitats deshonestes.

exploració de ports *f* Tècnica utilitzada per a identificar els serveis que ofereix un sistema o un equip en particular.

programari maliciós *m* Programa amb finalitats malintencionades.

requests for comments *m* Conjunt de documents tècnics i notes organitzatives sobre Internet.
sigla **RFC**

robot *m* Programa deshonest que permet a l'operador d'una xarxa de zombis controlar a distància els recursos d'un equip infectat.

rootkit *m* Conjunt d'eines utilitzades per un intrús per a l'ocultació d'empremtes, garantir futures entrades a un equip, fer altres atacs al sistema, etc.

Bibliografia

Filiol, E. (2009). *Les virus informatiques: théorie, pratique et applications*. (2a. ed.). Paris: Springer-Verlag France.

Graham, J. i altres (2011). *Cyber Security Essentials*. Boca Ratón: Taylor & Francis Group.

Paget, F. (2005). *Vers & Virus. Classification, lutte anti-virale et perspectives*. Paris: DUNOD.

Schiller, C. A. i altres (2007). *Botnets: the killer web app*. Waltham: Syngress Publishing.