Malware

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Malware

https://doi.org/10.5281/zenodo.4302267

https://github.com/mikel-egana-aranguren/EHU-ISSKS-31

Definizioak

Malware: beste programei edo erabiltzaileari kalteak sortzen dizkion programa

Malware klasikoak: Virusak, harrak, troianoak, bonba logikoak, ...

Malware berriak: Spyware, backdoors, keyloggers, rootkits, exploits, ...

Definizioak

Malware motak ez daude beti ondo zehaztuak

Hitz generikoak erabiltzen dira (birusa, troianoa), beraien ezaugarriak kontutan hartu gabe

Birus

Artxiboak aldatzeko, datuak ezabatzeko, bikoizteko eta hedatzeko gaitasuna duen programa

Birus

Chernobyl:

- Taiwan-en sortua 1998-an
- Windows 9x sistemetako artxibo exekutagarriak infektatzen ditu
- Memorian dago, data zehatz batean aktibatzen da
- Dokumentuak gain-idazten ditu, MBR (Master Boot Record) formateatzen du
- BIOS-a flasheatzen du, PC-a erabilezin utziz

Harrak

Helburu nagusitzat bere burua ugaltzea duen programa

Birus-ekiko desberdintasun nagusia: ez ditu beste artxibo batzuk infektatzen

Harrak

Netsky:

- Emaila edo P2P sareak erabiltzen hedatzen da. Ordenagailua infektatu duenean, aurkitzen dituen kontaktu guztietara hedatzen da
- Igortzailearen helbidea faltsuztatzen du
- Infektatzeko artxiboa exekutatu behar da

Harrak

I love U (2000)

Emailean jasotzen zen, atxikitutako "maitasun gutuna" bezala

Gutun hori VBS makro bat zen, irekitzerakoan harra kontaktu guztiei birbidaltzen ziena

Artxiboak ezabatu eta ezkutatzen zuen Birus bat aktibatzen zuen

Aste batean 50 miloi makina infektatu zituen

Harrak

Sasser (2004)

Ez du erabiltzailearekin elkarekintza behar infekzioa burutzeko

FTP zerbitzaria sortzen du beste makina batzuk konektatu daitezen infektatzeko

Ordenagailua berrabiatzen du

Harrak

WannaCry (2017)

Windows-en ahulezia aprobetxatzen du, Microsoft-ek hilabeteak lehenago partxea argitaratu zuena

Gezurrezko artxibo batean heldu daiteke makinara

Exekutatzen denean saretik hedatzen da

Edukiak zifratzen ditu eta bahisari bat eskatzen du edukiaren truke (**Ransomware**)

Troianoak

Itxura ez kaltegarria dauka, baina beste funtzionalitate ezkutua dauka

(Troiako zaldia)

Ez ditu beste artxiboak infektatzen, ez da ugaltzen ezta hedatzen ere

Troianoak

AIDS: 1989-an, IHES-ari buruzko informazioa duen programa baten 10.000 kopia banatu ziren

Erabilpen baldintzetan lizentzia apurtzeak ondorio larriak ekarriko zituela jartzen zuen

Exekuzio zenbaki batera heltzean, disko gogorraren edukia zifratzen zuen

Gakoa lortzeko ordaindu beharra zegoen (**Ransomware**)

Bonba logikoak

Aplikazio latentea, aktibatzeko baldintza gertatu arte

Bonba logikoak

Friday 13 (Jerusalem)

.com eta .exe artxiboak infektatzen ditu

Ostirala 13 heltzen denean, infektaturiko artxibo guztiak ezabatzen ditu

Israel sortu zeneko data oroitzen du

Backdoors

Atzeko atea, sarbidea eta kontrola baimentzen du kautotze zilegi barik

Backdoors

Backdoor BackOrifice

Zerbitzari bezero aplikazioak dauzka

Zerbitzari aplikazioa instalatzean, ordenagailuaren kontrol totala lortzen da

Artxiboak irakurri eta idatzi, aplikazioak exekutatu, sistema berabiarazi, pantaila ikusi, arratoia eta teklatua erabili, pasahitzak lapurtu, ...

Malware mota gehiago

Spyware: informazio pribatu eskuratu eta bidaltzen du, erabiltzailearen ezagutza edo/eta baimena barik

Keylogger: erabiltzaileak sakatutako teklak grabatzen ditu, pasahitzak eta horrelakoak lapurtzeko

Adware: Iragarkiak erakutsi edo eskatu gabeko web orrialdeak irekitzen ditu

Malware mota gehiago

Coinminer: makinaren konputazio ahalmena erabiltzen du kriptodirua minatzeko erabiltzaileak jakin barik

Malware motak

Gaur egun malwarea normalean ez dago kategoria bakarrean, kategoria desberdinen ezaugarriak aurkezten ditu

Adibidez Emotet (2019):

- Birus polimorfikoa
- Emailez hedatzen den har polimorfikoa
- Keylogger funtzioa dauka
- Bankuko kredentzialak lapurtzen dituen troianoa

Malware motak

Ezaugarria nagusia kontutan izanda kategorizatzen dira

Adibidez Lamin.B atzeko atedun Birus-a da:

- Birus polimorfikoa, Windows-en exekutableak erasotzen dituena
- Sare lokaletik hedatzen den harra
- Keylogger funtzioa dauka
- Makinaren urruneko kontrolerako atzeko atea

Malware motak

Zeus

- Botnet-a sortzen duten troianoa. Botnet-a: infektaturiko makinek osatutako sarea, norbaitek kontrolatua
- Bankuetarako sarrerak kontrolatzen ditu
- Web orrialdeak klonatzen ditu eta datuak kontrolatzaileari bidaltzen dizkio
- Gaur egungo troiano finantziero askoren aitzindaria

Malware motak

SpyEye

- Zeus-en eboluzioa
- Banku datuen lapurketarako ordaintzeko plataforma

Malware izendegia

Ohitura bezala hurrengo egitura jarraitzen da: Aurrizkia + Izena + Aldaera + Atzizkia (Computer antibirus Research Organization)-ek ezarria

Malware izendegia

Adibidez **W32/Klez.H@MM**

- **W32** Aurrizkia: Windows 32 bits sistemei eragiten die
- **Klez** izena: identifikatzeko izena
- **H** aldaera
- **@MM** atzizkia: emailez masiboki hedatzen den harra

Malware izendegia

Aurrizki erabilienak:

- **W32**: Windows 32bit
- **W95**: Windows 9X/Me
- **WM**: Word Macro
- **XM**: Excel Macro
- **Worm**: Harra
- **Troj**: Troianoak
- **Bck**: Backdoor

Birus batean faseak

1.- Sistemara heltzea (beti kanpoaldetik), apropos edo nahigabe sartua

2.- Instalazioa (Infekzioa): Birus-aren kodea lehenengo aldiz exekutatzean ematen da

Birus baten instalazioa

Gehitzea: Birus-aren kodea infektatu behar den artxiboaren amaieran gehitzen da. Artxiboaren tamaina handitzen da

Txertaketa: Birus-aren kodea infektaturiko artxiboaren leku "libre"-tan txertatzen da. Infektaturiko artxiboaren tamaina ez da aldatzen

Birus baten instalazioa

Birbideratzea: infektaturiko artxiboan Birus-aren kodearen zati txiki bat soilik instalatzen da. Gainerako sisteman zehar banatua dago. Exekutatzean Birus-a bir-eraikitzen da eta bere funtzioa betetzen du

Ordezkapena: Birus-ak infektaturiko artxiboaren kodea zuzenean ordezkatzen du

Birus batean faseak

3.- Aktibazioa eta sistemaren kontrola:

- Zuzena: infektaturiko artxiboa exekutatzen den bakoitzean Birus-a exekutatzen da
- Zeharkakoa: Birus-a memorian dago eta erregularki exekutatzen da

4.- Ezkutaketa: antibirus-arekiko eta erabiltzailearekiko

Ezkutaketa

Dispertsioa: Birus-a zatitzen da eta bere zatiak ezkutatzen ditu

- Artxiboak ezkutu bezala markatzen ditu
- Diskoaren zati libreetan ezkutatzen da eta akastun bezala markatzen ditu
- Sistema eragileak irakurri ezin dituen formatuetan gordetzen da

Ezkutaketa

Konpresioa: birusak infektaturiko programa konprimatzen du eta libre geratzen den lekuan instalatzen da, tamaina ez aldatzeko

Kamuflajea: birusak antibirusa eta sistema eragilea engainatzen ditu artxiboaren atributoak konprobatzerakoan (tamaina, aldaketa data, ...)

Ezkutaketa

Gainigarotzea: birusak sistemaren zerbitzuen rutinen gainean eragina dauka, zerbitzuak konprobatzen dituen antibirusa engainatzen

Autozifratua: birusak bere burua zifratu eta deszifratzen du, bere beharren arabera, gako desberdina erabiliz. Horrela, antibirusak ezin du birusaren edukia ikusi eta detektatu

Ezkutaketa

Polimorfismoa: hedatzen une oro birusak forma eta jokaera aldatzen ditu

Blindatzea: birusa desensanblatzea ezinezkoa egiten du eta beraz ezinezkoa da bere kodera sartu

Birus batean faseak

5.- Ugalketa:

- Ostalariak bilatu
- Ostalariak lehendik infektatuak izan ez direla konprobatu
- Birus-aren ber-konposizioa
- Ostalarian kopiatu

Birus batean faseak

6.- Agerpena: birusak bere ekintzak egiten ditu, kaltegarri edo kaltegarriagoak:

... interfazarekin jolastu (Birus Cascade)

... hardwarea apurtu (Chernobyl)

Antibirus teknikak

Sinadura bidezko detekzioa: birusaren kodea analizatzen da kate zehatza bilatuz, besteengandik desberdinduko duena

Antibirusak kate hori aurkitzen duenean, infekzioa dagoela konfirmatzen du

EICAR Anti Malware test file:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-antibirus-TEST-FILE!$H+H*

Sinadura bidezko detekzioa

Antibirusen artean teknika hedatuena da

Malware-a modu zehatzean identifikatzea baimentzen du

Ez ditu Birus berriak ezta aldaerak detektatzen

Filosofia erreaktiboa da, eguneratze jarraia behar du

Birus-a enkriptatzen bada, ezin da katea aurkitu

Antibirus teknikak

Artxibo izena eta kokapena bidezko detekzioa: Birusak sortzen dituen arxiboak bilatzen ditu

Artxiboa aurkitzen badu, antibirusak infekzioa dagoela determinatzen du

Ez ditu Birus berriak ezta aldaerak detektatzen

Filosofia erreaktiboa da, eguneratze jarraia behar du

Antibirus teknikak

Detekzio heuristikoa: kodea analizatzen da malwarean ohikoak diren instrukzioak eta jokaerak bilatzeko

Ez ditu hainbeste eguneraketa behar

Malware berria detektatu ahal du

Positibo faltsuak detektatzeko joera

Analisien errendimendua ez da hain ona

Ezaugarri berridun Malwarea ez du detektatzen

Antibirus teknikak

Jokaera bidezko detekzioa: kodea analizatu beharrean, aplikazioen ekintzak analizatzen dituzte, eta arriskutsuak direnak detektatu

Ez ditu hainbeste eguneraketa behar

Malware berria detektatu ahal du

Positibo faltsuak detektatzeko joera

Sistemaren errendimendua txarra

Ezaugarri berridun Malwarea ez du detektatzen

Antibirus teknikak

Emulazio bidezko detekzioa: aplikazioak simulazio batetan exekutatzen dira (sandbox), arrisku maila ebaluatzeko

Ez ditu hainbeste eguneraketa behar

Malware berria detektatu ahal du

Positibo faltsuak detektatzeko joera

Analisien errendimendua ez da hain ona (heuristikoekin baino okerrago)

Ezaugarri berridun Malwarea ez du detektatzen

Beste antibirus teknika batzuk

Osotasuna konprobatzea: artxiboen osotasuna konprobatu datu base baten kontra (checksums)

Artxibo garbi batetik hasi behar da

Ekiditeko errazak (spoofing)

Beste antibirus teknika batzuk

Sarbide kontrola: administratzaileak onartutako aplikazioak soilik exekutatu daitezke, baimen eta profil batzuen arabera

Kudeatzeko zailak, eta banakoentzako ez oso praktikoak

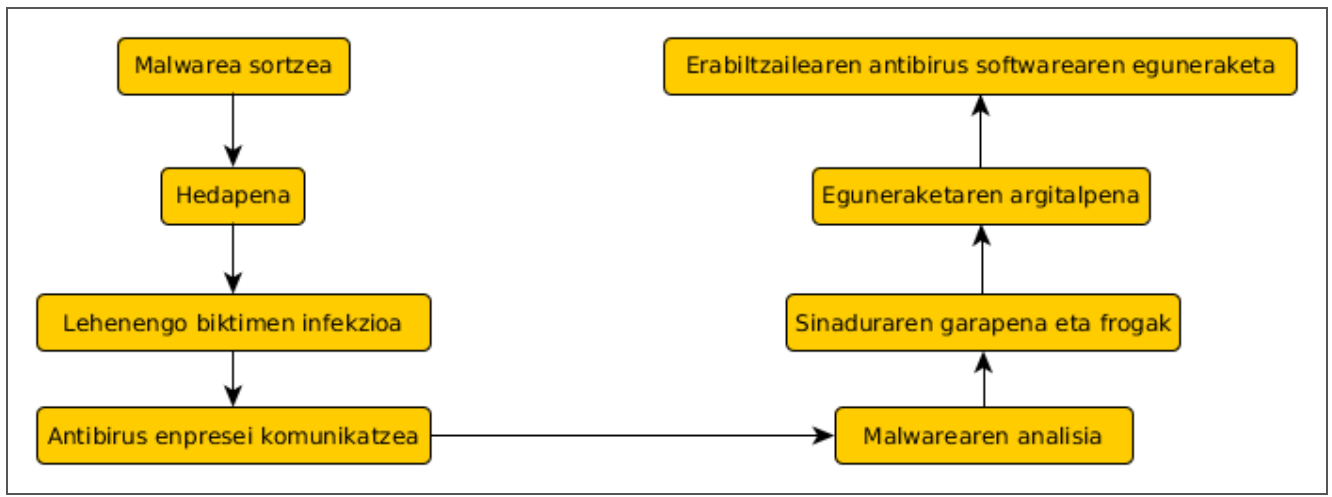
Antibirus tekniken mugak

Detekzio metodoak ekiditea erraza da

Eskema erreaktiboa, soluzioa a posteriori

Ahultasun-leihoa, ez dira garaiz heltzen

Ahultasun-leihoa



Antibirus tekniken mugak

Segurtasun sentsazio faltsua (perimetralak adibidez)

Analizatu ezin diren protokoloak (HTTPS, ...)

Perimetroko analisiaren zailtasuna (posta elektronikoa, web, ...)

Pakete eta konpresio formatuak

Malwarearen eboluzio eta dibertsifikazioa

Malwarearen kontrako defentsa

Infekzioen jatorria:

Artxibo zilegiak ireki (Birusak)

Eskatu ez diren artxiboak ireki, email atxikiak, P2P, deskargak (harrak, troianoak)

Besteek nahita bidalitako artxiboak ireki (Ingenieritza soziala)

Malwarearen kontrako defentsa

Infekzioen jatorria:

Sistema eragilearen konfigurazio ahula (Harrak, Birus, backdoors, ...)

Interneteko aplikazioen konfigurazio ahula (nabigatzailea, email bezeroa)

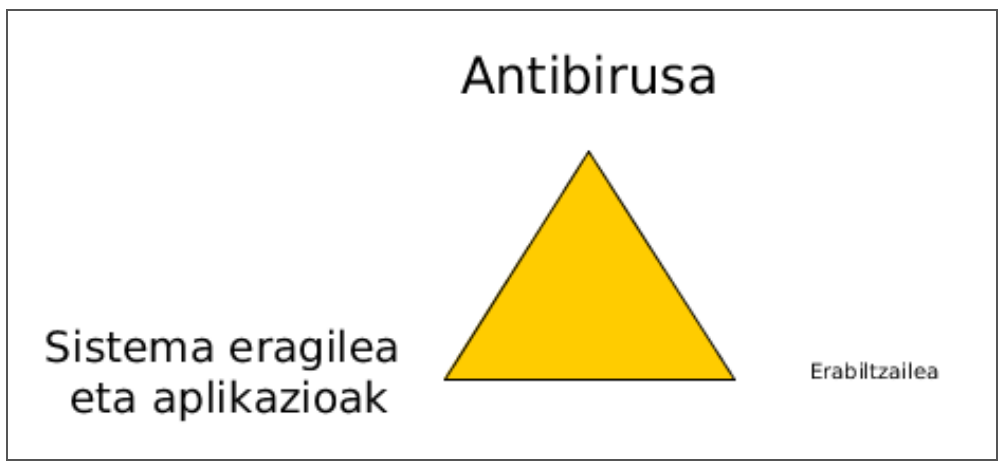
(spyware, harrak)

Sistema eragilearen eta interneteko aplikazioen ahultasunak (harrak,

spyware, backdoors)

Malwarearen kontrako defentsa

Prebentzioaren ohiko ikuspegia



Malwarearen kontrako defentsa

Zeinen kontra egiten du bakoitzak?

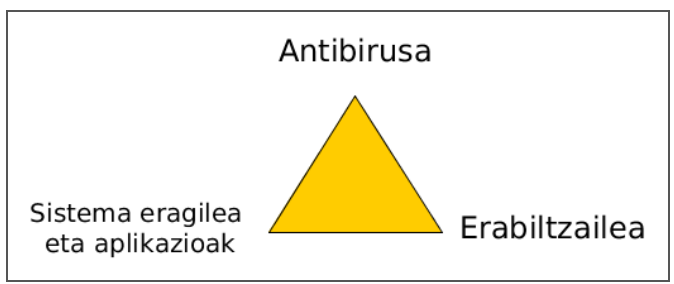
Antibirus: artxibo zilegiak ireki

Erabiltzailea: ez eskatutako artxiboak ireki, ingenieritza soziala, sistema eragilearen konfigurazio ahula, interneteko aplikazioen konfigurazio ahula

Sistema eragilea eta aplikazioak: Sistema eragilearen konfigurazio ahula, interneteko aplikazioen konfigurazio ahula, Sistema Eragilearen eta aplikazioen ahuleziak

Malwarearen kontrako defentsa

Antibirusak gutxien egin ahala duena bada, zergatik ematen diogu garrantzi handiena? Oreka bilatu behar da



Malwarearen kontrako defentsa

Erabiltzailea hezi

Segurtasun kultura

Formatu arriskutsuak

Ez ireki aurretik eskatu ez diren artxiboak

Nabigazio segurua

Pasahitzen kudeaketa

Babes-kopiak

Malwarearen kontrako defentsa

Sistema eragilea eta internet aplikazioak

Beharrezkoak ez diren zerbitzu guztiak desaktibatu

Eguneraketa automatikoak aplikatu (WSUS, SCCM)

Nabigatzailea eta posta ondo konfiguratu

USB eta eramangarrien sarbidearen kudeaketa

Sarearen segmentazio logikoa

Erabiltzaileen eta aplikazioen araberako baimenen kudeaketa

Babes kopiak

Malwarearen kontrako defentsa

Antibirus eta antimalware tresnak

Tresna ezberdinak eta osagarriak geruzen arabera (perimetroa, artxibo zerbitzaria, host).

Firewall perimetralak eta host-ean

Edukien baheketa

Sarerako sarbidearen kudeaketa

Segurtasunaren kudeaketa zentralizatua

Auditoriak eta kontingentzia planak

Malwarearen kontrako defentsa

Malwarearekiko bereziki ahulak diren aplikazioak

Posta elektroniko aplikazioak

Idazmahai aplikazioak

Berehalako mezularitzako aplikazioak

Web nabigatzaileak

P2P aplikazioak

Malwarearen kontrako defentsa

Baimendu gabeko aplikazioen blokeoa: baimena lehenetsia edo blokeoa lehenetsia

- Birus-en kontra
- Sinatutako komando sekuentziak bakarrik exekutatu
- Baimendutako aplikazioak soilik instalatzen direla bermatu
- Makinak blokeatu

Antibirusa aukeratu

Ez fidatzekoak

Marketing-a (100% babesa, birus ezagun eta ezezegaun guztiak detektatzen ditu, hoberena, ...)

Detektatzen dituen Malware kopurua

“Kontsultoreak” (Kontsultoreak edo banatzaileak?)

Sariak, zertifikazioak

Konparaketak

Antibirusa aukeratu

Kontuan hartzekoak

Behar dituen baliabideak, errendimendua eta egonkortasuna

Erabiltzeko erraztasuna eta konfiguratzeko aukera

Malware motak

Eguneraketak

Antibirusa aukeratu

Kontuan hartzekoak

Eskainitako laguntza

Konparatibak

Kudeaketa zentralizatua

Antibirusa aukeratu

Ez dago antimalware perfektorik

Hoberena konbinazioa erabiltzea da: antibirus, antiexploit, firewall, antispyware