eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea

Informatikan Ingeniaritza

Karrera Bukaerako Proiektua

Botnet-en azterketa eta analisia

Egilea
Ekaitz Astiz

informatika fakultatea
facultad de informática

2013

Laburpena

Egun sare informatikoak ezinbesteko tresna bilakatu dira eguneroko eginkizun askotarako. Horren ondorioz, mota guztietako informazio mordoa garraiatzen da sarean barna. Sarearen erabilerak hainbat abantaila ekarri ditu, baina baita arriskuak ere. Sareko informazio horri guztiari etekina atera nahian zenbait informazio lapur eta *zibergaizkilek* tresnak garatzen dituzte etengabe. Arazo horri aurre egiteko babes mekanismo ugari garatu dituzte segurtasun aditu eta eragileek. Baina era berean, mekanismo horiek gainditzeko erasoak automatizatzeko eta indartzeko gai diren tresnak berriak agertu dira. Azken hauen artean kokatzen dira *botnet*ak, gaur egungo mehatxu handienetako bat segurtasun aditu askoren iritziz.

Botnetak kontroladore baten edo batzuen agindupean egon daitezkeen makina multzoak dira. Makina horiek, *bot* edo *zombie* izenez ezagunak, ezkutuan martxan dagoen software bati esker kontrolatu ohi dira. Jatorrian *bot*en mekanismoa atazak automatizatzeko erabiltzen bazen ere, gaur egun ezaugarri hori aprobetxatuz erasoak eta beste motako ekintza ez-zilegi batzuk egiteko erabiltzen dira.

Botneten tamaina milaka makinakoa izatera irits daiteke. Horri esker egin ditzaketen erasoen ahalmena handitu egiten da eta, ondorioz, etekin handiagoa ateratzeko aukerak handitzen dira ere. Beste ezaugarri nagusienetako bat *malware*ren bati esker kontrolpean dauden makinen jabeak ohartu gabe funtzionatzea da.

Azken urteotan botneten hazkundea nabarmena izan da eta izugarrizko mehatxua bilakatu dira sarearen funtzionamendurako eta sareko sistemen segurtasunerako. Horrek motibatuta garatu da proiektu hau. Funtsean botnetak zer diren, hauen bilakaera eta nola funtzionatzen duten azaldu nahi da. Segurtasun neurri batzuk ere aztertzen dira. Azkenik, azterketa praktikoa ere lantzen da, *Zeus* eta *Flu* izeneko botnetak modu lokalean probatuz.

Gaien aurkibidea

Irudien aurkibidea

Taulen aurkibidea

1. KAPITULUA

Sarrera

Gaur egun bitarteko informatikoak ezinbesteko tresna bilakatu dira gure gizartean. Geroz eta gehiago erabiltzen ditugu egunerokoan, hala nola, hezkuntzan, administrazioan, lanean, baita aisialdian eta harreman pertsonaletan ere. Erabilera handitu eta esparru gehienetara hedatu izanak, gailu informatikoetan geroz eta informazio garrantzitsuagoa biltegiratzera eraman gaitu. Sarritan informazio pertsonala izaten da, hala nola, bankuko kontuak, nortasun agiriak... Hortaz, informazio hori eskuratzeko edo eta aktibo horiek guztiak baliatzeko tresna berriak sortu dira, horien artean botnetak.

Botneta pertsona batek edo talde batek kontrolpean dituen ordenagailu multzoa da. Ordenagailu horiek erabiltzailea ohartu gabe zenbait programekin kutsatuta bihurtzen dira *bot*, gerora erasoak egiteko erabiltzen direnak, hala nola, informazioa lapurtzeko, zerbitzuak eteteko, spama bidaltzeko. Azken urteetan kontrolpean milaka, baita milioika makina dituzten botnetak atzeman dira, hala nola, *Zeus* eta *Mariposa* izenekoak.

Ordea, erabiltzaileek arruntek, informatikari askok, ez dute boteneten berri, ezta sortzen dituzten kalteen berri ere. Hori horrela, proiektu honetan, botnet bat zer den, nola funtzionatzen duten, zein egiturako botnetak dauden (zentralizatua: HTTP, IRC eta banatua: P2P) eta zein motako erasotarako erabili ohi diren azaltzen da (DoS/DDoS, *spamming*a...). Botneten atzean eratu den industriaren berri ere ematen da, botnet gehienen atzean ongi antolatutako taldeak daude, horregatik, botneten komertzializazioa eta ematen duten dirutza ere aztertzen dira. Bestetik, botnet berriek erabiltzen dituzten teknika batzuen berri ere ematen da, hala nola, *fast-flux* eta *domain-flux* teknikak.

Funtzionamenduaren inguruko informazioa emanda eta botnetek sortzen duten kalte-aren dimentsioa ikusita, zenbait segurtasun irizpide eta neurri azaltzen dira, gehienak edozein erabiltzailek ulertu eta aplikatzeko moduan.

Bukaeran, *Flu* eta *Zeus* botnetarekin proba batzuk egiten dira, aurretik azaltzen dena hobetu ulertzeko balio du eta zenbait eraso egiten dira. Simulazio horiei esker egungo botnetek dituzten dituzten kontrol panelak aztertzen dira eta eskaintzen dituzten agindu multzoak nolakoak diren eta nola exekutatzen diren aztertzen da.

Botneten inguruko informazioa eta azalpenak eman eta gero, aurrera begira botneten mehatxuari aurre egiteko egin beharko liratekeen zenbait gogoeta eta neurri aurki daitezke. Kalteak eta kutsatua izatea saihesteko neurriak eta teknikak batetik, eta kalteak konpontzekoak bestetik. Antibirusak, *firewall*ak, *honeypot*ak, *sinkhole*ak ...

2. KAPITULUA

Proiektuaren Helburuen Dokumentua

2.1 Proiektuaren helburua

Sarreran aipatu den bezala, proiektu honen helburua botnetak zer diren azaldu, nola funtzionatzen duten eta sareetarako nolako mehatxua diren aztertzea da. Era berean, mehatxu horri aurre egiteko gako nagusiak ere aurkeztuko dira.

Botneten azterketa honetan ondorengo hurbilpena jarraituko da:

- *Aurkezpena* Botnet bat zer den eta nola dagoen osatuta aztertuko da, parte hartzen duten makinei nola eragiten dion azalduz.
- *Mehatxuaren garrantzia* Tresna hauen mehatxua zein dimentsiotakoa den argi izateko, orain arteko bilakaera aurkeztuko da, datuak agertuz. Hau da, azken urteetan egondako botnet kopurua, kutsatuak izan diren makinak... Azken urteetako zenbait kasu erreal ere aipatu eta deskribatuko dira gaiaren gaurkotasuna adierazteko besteak beste.
- *Funtzionamendua* Puntu honetan aztertuko da nola hedatzen diren eta zer nolako egitura izaten duten. Ondoren sistema hauek detektatzeko eta aurre egiteko neurriak ere aztertuko dira.
- Botnetei aurre egiteko planteatuko diren neurriek erakutsi behar dute zer dagoen erabiltzaileen esku eta zer ez. Proben helburua ez da neurri hauek nola aplikatzen

diren eta nola konfiguratzen diren ikastea, baizik eta, bete beharreko irizpide edo gako orokorrak zeintzuk diren identifikatzea eta soluzio posibleen berri izatea.

- Zenbait botneten funtzionamenduaren eta deskribapenen inguruan emango den informazioa hobe aztertu eta ulertu ahal izateko, hauetako batzuk frogatuko dira modu lokalean.

- Botneten inguruko informazioa ulertzeko erabiliko diren terminoen hiztegi edo glosategi bat osatuko da.

2.2 Atazen zerrenda

Proiektua ataza ezberdinetan banatu da. Hona hemen atazen zerrenda:

Lan bibliografikoa: Ataza honen betekizuna botnetekin zerikusia duen informazioa biltzea da.

Informazioa ongi aukeratu eta sailkatu behar da, informazio ongi egituratu eta errepikatua ez izateko. Kontutan hartu behar da botneten inguruko liburu gutxi daudela eta termino ezberdinak erabiltzen direla erreferentzia batzuetan eta besteetan. Horrek informazioa kontrastatzeko beharra sortzen du eta bestetik, ezinbestean iragazki edo irizpide batzuk ezartzea. Hona hemen informazioa biltzeko erabili behar diren iturburu motak:

- Botneten eta sareko segurtasunaren inguruko ikerkuntza lan eta liburuetatik. Kontuz ibili behar da serioak ez diren erreferentzia asko baitago.

- Datuak informatika munduko erakundeen webgune eta txosten teknikoetatik, eta segurtasun informatikoaren inguruko liburuetatik jasoko dira.

- Gaiari gaurkotasuna emateko erabiliko diren adibide eta informazioa, informatikaren inguruko erakunde eta alor honetako albisteak jasotzen dituzten aldizkari eta webguneetatik jasoko dira.

Azpi-ataza hauek banatu dira:

- Botnetei buruzko informazioa aztertu

- Botneten eraginaren inguruko datuak jaso
- Botnetei buruzko erreportaje eta albisteak aztertu
- Segurtasun neurriak aztertu

Garapen teorikoa: Bildutako, irakurritako eta kontrastatutako informazio guztitik azaldu: botnetak zer diren, nola funtzionatzen duten, nola hedatzen diren, baita haietatik nola babestu eta haiei nola aurre egin. Informazioa ulerterrazago egiteko irudiak egin edo aurkitutako irudiak erabili. Beraz, horretarako ondorengoa egingo da:

- Eskema egituratu eta honi jarraitu
- Jasotako informaziotik azalpenak idatzi
- Segurtasun neurriak proposatu
- Botneten eraginen datuak aztertu eta baliatu

Frogak botnetekin: Gutxienez botnet bat aztertuko da eta botneten hedapena ahalbidetzen duten tresnak aurkitu eta probatuko dira. Proba honen bitartez egungo botnetek eskaintzen dituzten kontrol panelak eta tresnak eta agindu motak aztertuko dira, zenbait eraso ulertzeko simulazioa egingo da eta aurretik azaldutako kontzeptuak hobe azaltzeko erabiliko dira frogak. Frogak modu lokalean egingo dira legea ez urratzeko. Frogak aurrera eramateko ondorengo azpi-atazak proposatzen dira:

- Botnet eta Malwarearen dokumentazio aztertu
- Botnetak eta *malwarea* aukeratu eta eskuratu
- Probak zehaztu eta planifikatu
- Ingurunea prestatu eta probak egin
- Emaitzak eta ondorioak dokumentatu
- Proba eta garapen teorikotik ondorioak atera (aurrera begira)

Proiektuaren kudeaketa: Ataza hau da proiektua kontrolatu eta aurrera eramateko egin behar diren azpi-atazak barnebiltzen dituena. Ataza hau proiektuak irauten duen bitartean etengabe egin beharreko zerbait da. Proiektua nola doan begiratu beharko da, helburua betetzeko ongi bideratuta doala kontrolatu beharko da, estimatutako denboretatik ahalik hurbilen ibiltzea ere kontrolatu beharko da eta azkenik proiektua bera aurkezteko baldintzak eta prestakuntza batzuk bete beharko dira. Ondorengoak dira jarraitu beharreko azpi-atazak:

- Bilerak egin: Proiektua definitzeko, zalantzak argitzeko eta zuzenketak egiteko.
- Proiektua kontrolatu: Atazak betetzen direla eta helburuei begira iparra galdu ez dela ziurtatu, epeak kontrolatu eta arazoen aurrean soluzioak aztertu.
- Dokumentazioa egin: PHDa idatzi, botneten inguruan idatzitakoa zuzendu, ondorioak idatzi eta guztia dokumentu batean jaso.
- Aurkezpena prestatu

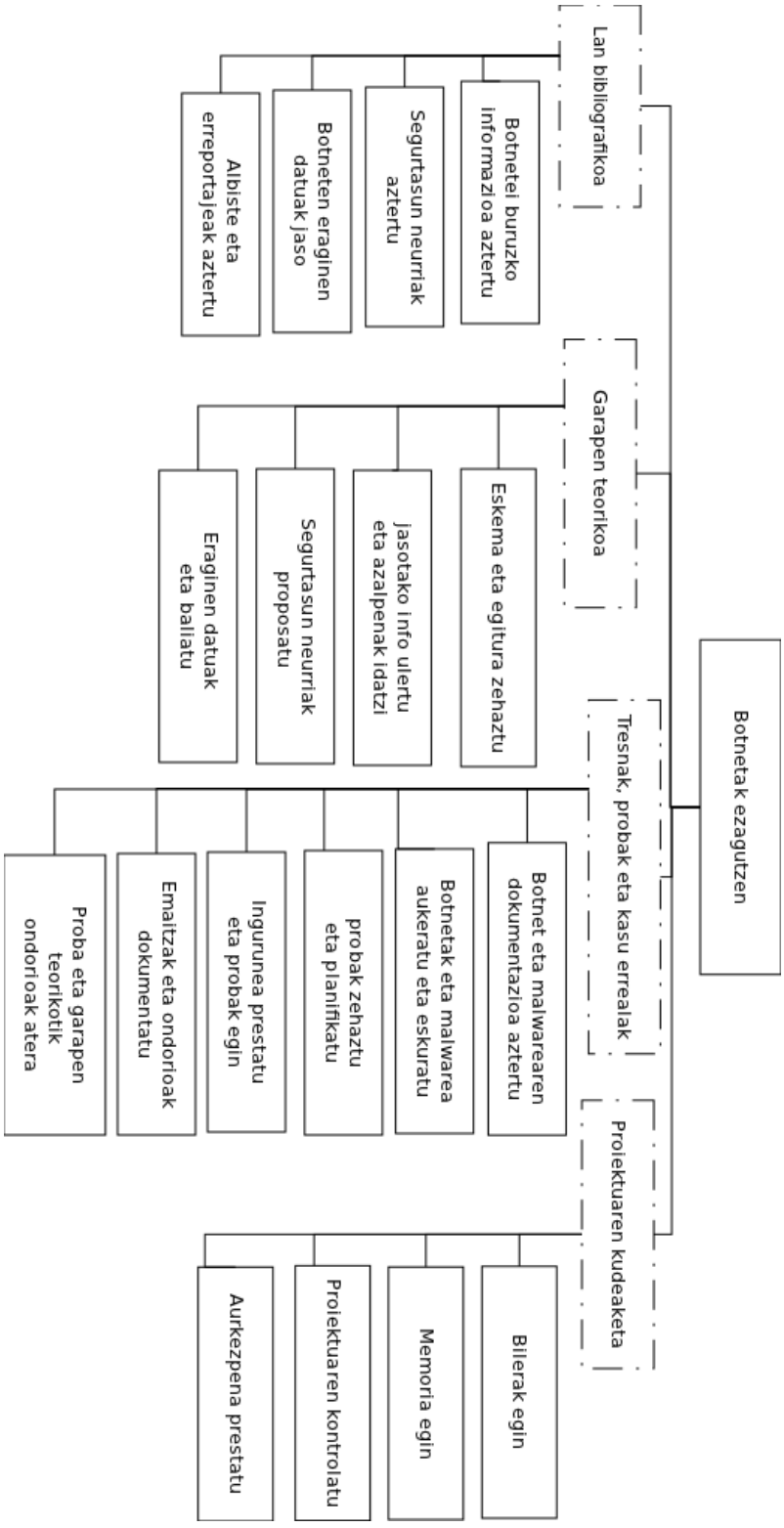
2.1 irudian ikus dezakezue LDE diagrama.

2.3 Denbora-estimazioak

2.1 taulan lan-pakete bakoitzari eskaini beharreko denbora azaltzen da, baina lan-pakete asko zeudenez, batzuk multzokatu egin dira modu argiagoan ikusteko.

2.4 Planifikazioa

Ondoren, lehen aipatutako atazak proiektuaren hasieratik amaitu arte nola nola banatu agertzen da, alegia, maiatzetik azaro erdi bitarte. 2.3 irudian soilik ataza nagusiak ageri dira aipatutako epeetan. Aldiz, Gantt diagrama baten bitartez 2.2 irudian ageri da proiektuko atazak eta azpi-atazak zerrendatuta. Zenbait ataza paraleloan egingo dira. Data zehatzak jarri badira ere, malgutasuna dago, ez dago bete beharreko epe zehatzik, planifikazioan datak jarri dira hobe lan egiteko eta ardura gehiago izateko. Esan bezala, ez dago data zehatzik baina abendurako amaituta izatea aurreikusten da.

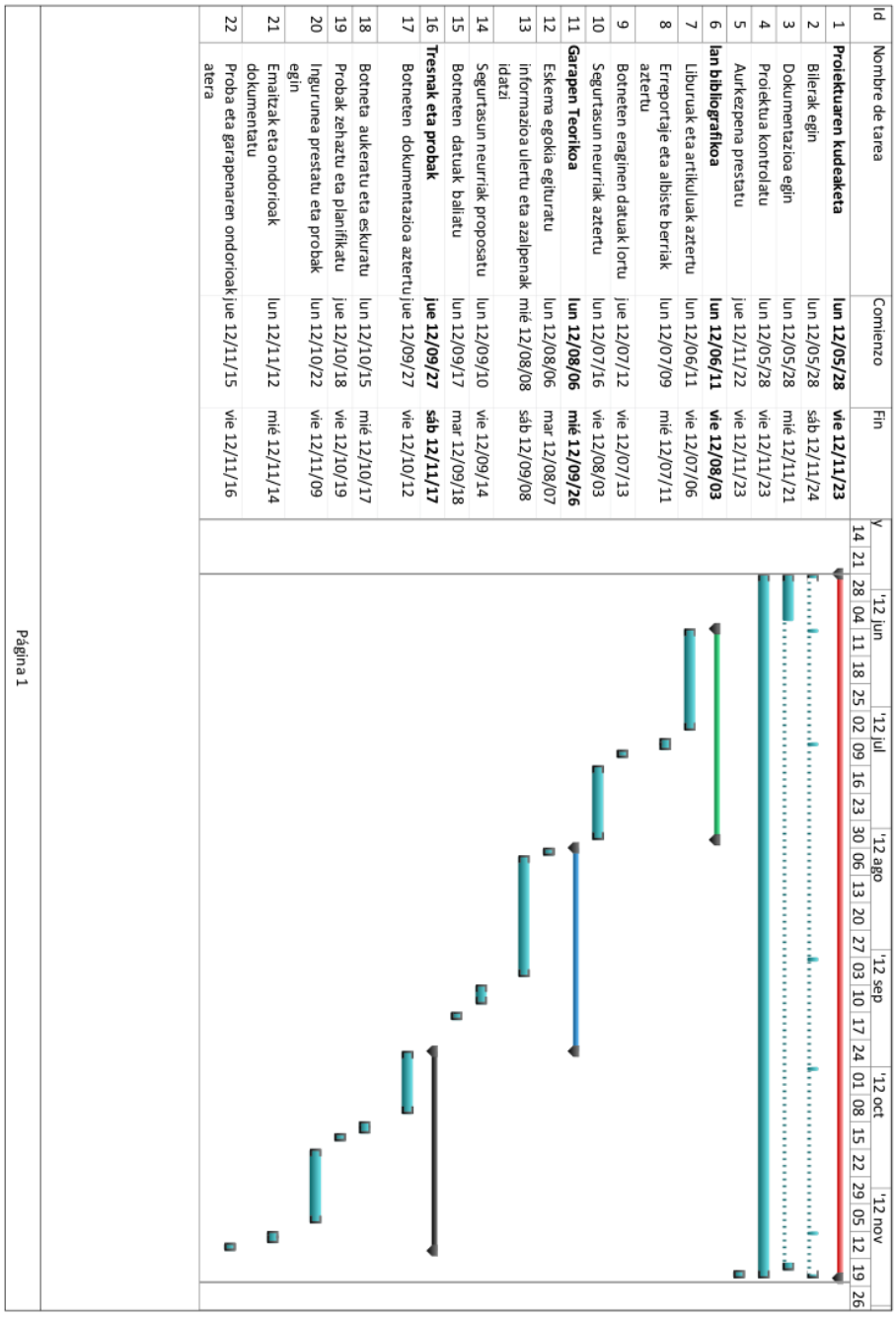


2.1 Irudia: Atazen Deskonposaketa Egitura

Atazak	Orduak
1 Proiektuaren kudeaketa	64
2 Bilerak egin	12
3 Proiektua kontrolatu	12
4 Dokumentazioa egin	28
5 Aurkezpena prestatu	12
6 Ian bibliografikoa	96
7 Liburuak eta ikerkuntza artikuluak aztertu	56
8 Erreportaje eta albiste berriak aztertu	6
9 Botneten eraginen datuak jaso	6
10 Segurtasun neurriak aztertu	28
11 Garapen teorikoa	90
12 Eskema egokia egituratu	5
13 Jasotako informazioa ulertu eta azalpenak idatzi	65
14 Segurtasun neurriak proposatu	15
15 Botneten eraginen datuak baliatu	5
16 Tresnak eta probak	85
17 Botneten dokumentazioa aztertu	22
18 Botnet eta *malwarea* aukeratu eta eskuratu	10
19 Probak zehaztu eta planifikatu	10
20 Ingurunea prestatu eta probak egin	23
21 Emaitzak eta ondorioak dokumentatu	12
22 Proba eta garapenaren ondorioak atera	8
BATURA	335

2.1 Taula: Denbora estimazioak

2.2 Irudia: Atazen planifikazioa



2.3 Irudia: Atazen planifikazioa Gantt diagrama erabilita

Maiatzean bilera bat egingo da, proiektuaren helburuak zehaztuko da eta behin hori zehaztu eta gero ekingo zaio PHD dokumentua garatzeari. Behin hori osatuta eta lanerako planifikazioa eginda, ikerketa lanari ekingo zaio.

Proiektua garatuko den denboraldi osoan, eguneko 3-4 ordu sartu beharko dira, esan bezala, hasiera batean astegunak bakarrik izango dira lanerako. Halere, behar izanez gero larunbatetan ere egingo da lan, aurretik egin gabe utzi den zerbait eguneratzeko. Planifikazioak tartea ematen du ere egunen batzuetan pixka bat gutxiago sartzeko.

Uztailean eta abuztuan lan karga txikiagoa izango da, hala ere lan bibliografikoa irailerako bukatuta egotea aurreikusten da.

7 bilera egitea aurreikusten da, hala ere datak ez dira zehatzak, aurreikuspen bat da, gero beharren arabera gehiago izan daitezke.

Proiektuaren kontrola proiektu osoan zehar egin beharreko ataza bat da, hala nola, sartzen diren orduak apuntatzea eta planifikatutakoarekin bat datorren ikustea. Ez badatoz bat, birplanifikatzea ere ataza honen parte da. Kudeaketaren parte da PHD dokumentua baita ere, eta horren barruan dago memoria egitea, beraz, proiektuaren amaieran proiektuari buruz idatzi beharreko ondorio eta azalpenak izango dira egin beharreko azkena, horregatik azken aurreko ataza *Gantt diagrama*n dokumentazioa egin da. Eta paraleloan egingo dira azken atazak proiektuari itxiera emateko, zuzendariarekin *bilera egin*, *proiektua kontrolatu* eta *aurkezpena prestu* dira egingo diren aztek atazak.

2.5 Arriskuak eta aurreikusitako soluzioak

Proiektu guztietan lana egin bitartean hainbat arrisku daude. Horiek aurreikusiz gero soluzioak ere proposatu eta planifika daitezke.

Hauek dira proiektu honek dituen arrisku nagusiak eta ez beharrak gertatzekotan proposatzen diren soluzioak:

- 2012ko maiatzean hasiko denez eta uda igaro eta gero berriro 2012 kurtsoan jarraitu, proiektua zuzentzen duen irakaslea oporretan egonen da, liburutegia eta bestelako baliabide batzuen ordutegia ere mugatuagoa da. Udan ere lana egin behar izanez gero, ordu gutxiago daude proiektua egiteko. Hori horrela, planifikazioa ez litzateke zehatz mehatz beteko.

Soluzio modura, lana atzeratzen ari dela ikusiz gero, birplanifikazio bat egingo da, udan edo udako epe jakinen batean sar ezin daitezkeen orduak uda pasatakoan sartu beharreko orduan nola banatu azalduz.

- Proiektuaren informazioa galtzea.

  Datuak gal ez daitezen, segurtasun kopiak egin lanaldia bukatzen den aldiro, horretarako Dropbox tresna erabiliko da eta bestetik, 10 egunean behin beste disko batean ere gordeko da segurtasun kopia bat.

- Botnet kodeak aurkitzeko zailtasuna izatea eta ez probak ezin egin izatea.

  Hori horrela, proiektuaren hedapen modura planteamendu bat egingo da egin nahi ziren probak dokumentatuz eta proba horietan lortu nahi zena azalduz.

3. KAPITULUA

Proiektuaren garapena

3.1 Zer da botnet bat

Hasierako atal honetan botneten jatorria zein den azalduko da, bere osagai nagusiak zein diren aipatuko da eta lehenengo botnetak azaldu zirenetik gaur arte izan duten bilakaera ikertuko da.

3.1.1 Jatorria

Botnet ingelesezko izenak dioen moduan roboten edo *bot*en sare (*net*) bat da. Konputagailu multzo batek osatzen du, eta makina horiek guztiak aldibereko atazak burutzeko erabil daitezke. Gaur egun ordea, ordenagailu multzo hori ekintza ez-zilegi edo legez kanpokoak diren erasoak eta kalteak egin eta etekin ekonomikoak zein politikoak lortzeko erabili ohi da. Botneta kontrolatzen duenari *botmaster*ra edo *herder*ra esaten zaio, eta kontrolpean dauden makinak bot izenaz ezagutzen dira. Kontrola edukitzeaz hitz egiten denean, funtsean bot horiekin guztiekin komunikatzeko aukera duela eta besteak beste, uneoro bot horien egoera ikus dezakeela eta mota guztietako ataza exekutatu aukera izan dezakeela esan nahi da, makinak bereak izango balira bezalaxe, hau da, konputagailu horietara mugarik gabe nahi duena egitera iris daitekeela.

3.1.2 Bilakaera

Hasiera batean botak atazak automatizatzeko erabiltzen ziren, elkarrizketa edo joko kanal bat babesteko (IRC[1], IM[2], MUDS[3] motako kanaletan), elkarrizketak mantentzeko, sareko jokoen ataza automatikoak egikaritzeko... [Schiller and Harley, 2007].

IRC protokoloa asmatu zuen Jarkko Oikarinenek 1988an. IRC-aren funtzionamenduan oinarritu ziren lehen botnetak, azken finean talde kanalak kudeatzen zituen kudeatzaile bat zuelako eta komunikazio protokolo horren bidez bezeroak gehitu eta ken zitezkeelako. IRC bot zaharrena, Greg Lindahl izenekoa, 1989an asmatu zen, GM (Game Manager, Hunt the Wumpus jokorako) izena jarri zioten.[4] IRC-ko erabiltzaileekin jolasteko balio zuen. Denborarekin aipaturiko atazak automatikoki egiteko baliatu zuten, taldeak eta kanalak sortu, baimenak esleitu, etab.

1999an Prettypark atzeman zuten [Canavan, 2005]. Lehen bota dela esan daiteke, nahiz eta ondorengo ezaugarriak zituen har bat izan, gerora agertutako boten oinarri izan baitzen [David et al., 2002]:

- Sistemaren informazioa eskuratzeko ahalmena, besteak beste, ordenagailuaren izena, SE bertsioa eta erabiltzailearen informazioa.
- Fitxategiak jaitsi eta igotzeko gaitasuna
- DoS/DDoS erasoak egiteko tresnak
- Pasahitzak, erabiltzaile izenak eta dial-up konexioak eskuratzeko ahalmena.
- Bere IRC bezeroa instalatu eta haren bitartez kutsatutako makinara sarbidea izateko aukera

Gaur egungo bot gehienek aipatu berri den zerrendako ezaugarriak dituzte besteak beste.

1990ean har batzuk, besteak beste IRC/Jobbo-k, IRC-ren ahuleziez baliatu ziren zenbait IRC bezerotan, mIRC-n batik bat, Backdoor bidez urruneko kontrola ahalbidetzeko. 1990eko ekainean, SubSeven Trojan/Bot 2.1 bertsioa zabaldu zen, inflexio puntu bat

[1] http://en.wikipedia.org/wiki/Internet_Relay_Chat
[2] http://en.wikipedia.org/wiki/Instant_messaging
[3] http://en.wikipedia.org/wiki/MUD
[4] http://en.wikipedia.org/wiki/Internet_Relay_Chat_bot

izan zen botneten bilakaeran, (SubSeven) zerbitzari bat kontrolatu baitzitekeen, bertan IRC zerbitzari batera konektatuko zen bot bat instalatuz. Botmasterrak kutsatutako makinaren kontrol osoa har zezakeen.

Denbora joan ahala, helburu suntsitzaileak nagusitu ziren, hala nola, spamaren zabaltzea, ordenagailuak kontrolatzea, zerbitzuak etetea, informazioa lapurtzea...

Zerbitzuak eteteko erasoei DoS eta DDoS izana eman zaie ingelesez, Denial Of Service eta Distributed Denial of Service-ren akronimoak izanik.

Esate baterako, *DoS-DDoS* erasoak 1999 urtean erabili ziren lehen aldiz, besteak beste Stacheldraht[5] bezalako programak erabiliz [Daniel Plohmann, 2011]. Stacheldraht DoS erasoak egiteko sistema banatu gisa jokatzen duen Solariserako eta Linuxerako software bat da. Finean, TFN[6] (DoS erasoentzako tresna multzo bat) eta Trinooren[7] (DoS egiteko tresna multzo bat) ezaugarriak konbinatzen ditu, eta gainera komunikazioaren zifratzea ahalbidetzen du.

Arkitekturari dagokionez ere, denboraren poderioz geroz eta egitura konplexuagoak eta ahaltsuagoak erabiltzen ari dira erasotzaileak. Hasieran botneten C&C (komando eta kontrola) azpiegitura deritzona IRC protokoloan oinarritutakoa zen ohikoena, gaur egun ordea, geroz eta gehiago ikus daitezke HTTP (*HyperText Transfer Protocol*) protokoloa erabiltzen duten botnetak, baita egitura banatuko P2P (*Peer-to-Peer*) sareetan oinarritutakoak ere. Azken hauek diseinatu eta eraikitzea konplexuagoa bada ere, sendotasun maila handiagoa dute, hortaz zailagoak dira suntsitu eta atzemateko. Honen inguruko xehetasun gehiago ematen dira 3.3 atalean.

Tresna hauen bidez jende eta erakunde askok diru asko lortzen du [ESET, 2010]. Diru iturri handia dira eta horrek askoren arreta erakarri du. Hori horrela izanik, geroz eta botnet konplexuago eta ahaltsuagoak agertzen ari dira.

Horrekin lotuta, ezagutzen diren lehen erasoak 1999. urtean izan baziren ere, gobernuek ez zuten horren serio hartzen afera hau. Baina 2005. urtean Erresuma Batuko National Infrastructure Security Coordination Centre (NISCC) erakundea jabetu zen Erresuma Batuko Gobernuaren sarean bertan botnet bat zegoela [NISCC, 2005]. Horrelako gertakizunek adi jarri dituzte gobernuak.

3.1 taula aztertuz gero, ikus daiteke 1998 urtetik aurrera agertu diren botnet esanguratsuenak haien protokoloak, egitura, eta tamainak kontutan hartuta. Gainera geroz eta

[5] http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt
[6] http://en.wikipedia.org/wiki/Tribe_Flood_Network
[7] http://en.wikipedia.org/wiki/Trinoo

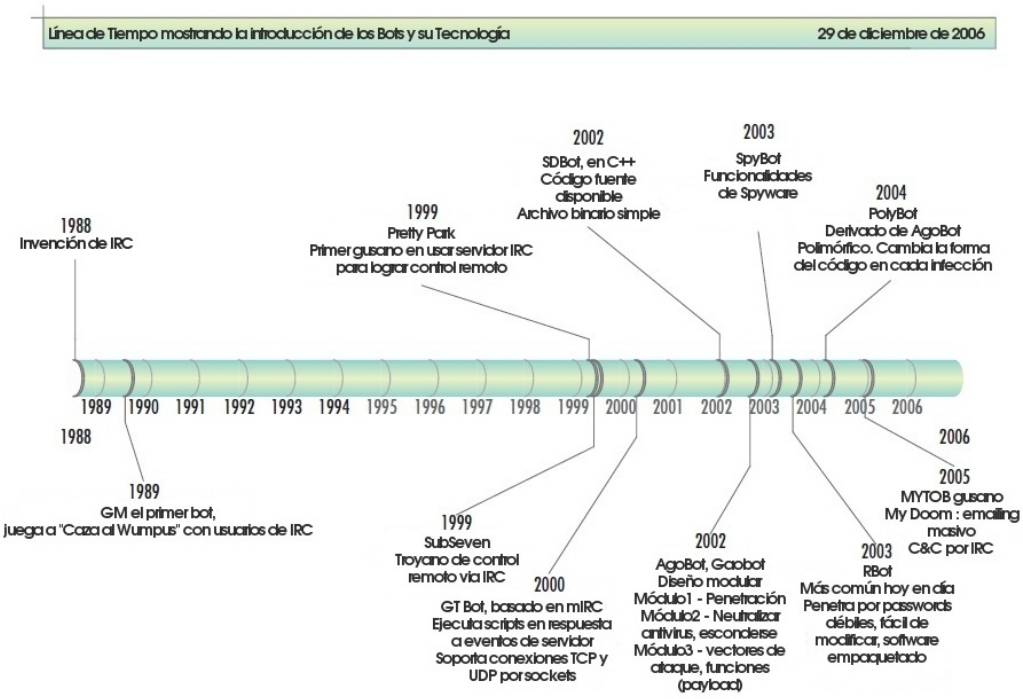
Urtea	Izena	Arkitektura/protok.	Est. Tam.
1998	**GTbot**	Zentr.	-
2002	**SDbot**	Zentr./IRC	-
	Agobot	Zentr./IRC	-
2003	**Spybot**	Zentr.	-
	Synit	P2P	-
2004	Bagle	Zentr.	230.000
	Forbot	Zentr.	-
	Fhatbot	P2P	-
2006	SpamThru	P2P	12.000
	Nugache	P2P	160.000
	Jrbot	Zentr.	-
	Rxbot	Zentr./IRC	-
	Rustock	Zentr./HTTP	150.000
2007	Storm	Zentr.	160.000
	Pushdo	Zentr./HTTP	175.000
	Srizbi	Zentr./HTTP	400.000
	Zeus/Zbot	Zentr./HTTP	3.600.000
	Mega-D	P2P	500.000
2008	Lethic	Zentr.	260.000
	Asprox	Zentr./HTTP	15.000
	Bobax	Zentr./HTTP/UDP	185.000
	Kraken	Zentr.	400.000
	Torpig	Zentr.	180.000
	Conficker	P2P	10.500.000
2009	Waledac	P2P	80.000
	Donbot	Zentr./TCP	125.000
2010	Festi	Zentr./HTTP	-
2011	TDL-4	P2P	4.500.000

3.1 Taula: Botnet-en bilakaera [Silva et al., 2013]

botnet gehiago agertu direla ere ikus daiteke argi eta gabi eta hasieran zentralizatuak zirela gehienak eta gerora mota ezberdinetakoak agertu direla. Taula horretan ageri diren batzuk (GTbot, SDbot, Agobot, Rbot, Spybot) aztertuko dira 3.3.2 atalean, hain zuzen ere horiek direlako beste botnet gehienen oinarri ere. Bestetik, taulan horretan ere ageri diren beste batzuk, atalean kasu esanguratsueenetan aipatzen dira eragin duten kalteen dimentsiogatik eta tamainagatik ere.

3.2 Nork eta zertarako erabiltzen dira

Botnetak erabiltzearen arrazoi nagusia ekonomikoa da. Dirua lotzerko botneten bitartez aurrerago azalduko diren ondorengo ekintza hauek dira ohikoenak: nortasun lapurreta edo ordezkapena, internet zerbitzuen etetea, spama bidali eta klik iruzurrak egitea [Lashkari et al., 2011].

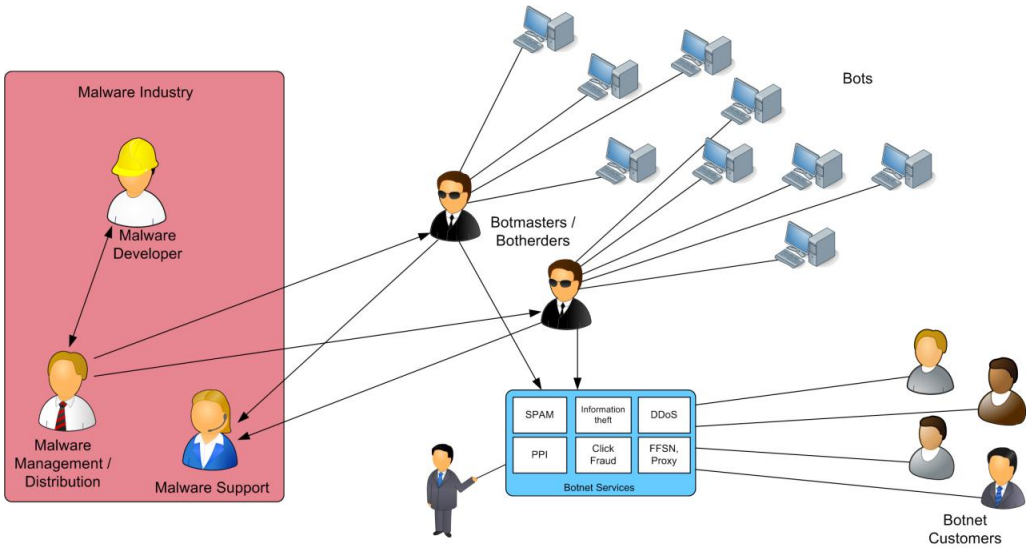


3.1 Irudia: Botneten bilakaera

Interes politikoek eragindako kasuak ere badira, batzuetan gobernu erakundeen partetik, beste batzuetan mugimendu ezberdinen partetik [Gómez Vieites, 2006]. Esate baterako, Israelen arrazoi politikoek bultzatuta informatikari talde batzuek botnet bitartez erasoak egin izan dituzte [Constantin, 2009]. Mugimendu sozialetako kideek eta ziberaktibistek ere protesta ekintzak egiteko erabili izan dituzte botnetak, hala nola, Anonymous[8] taldeak. Estatuek ere erabiltzen dituztela esaten dute zenbait ikerkuntza lanetan, S2 Grupo espainiako segurtasun enpresa bateko kide den Rafael Perez-ek bere artikulu batean dio ECHELON eta Carnivore (gaur egun NarusInsight) izeneko proiektuetan ziberespiotzarako botnetak erabiltzen dituztela [Rafael, 2011]. Hala ere, oso zaila da horrelako tresnen erabileran estatuen parte hartzea frogatzen duten datuak edo eta txosten ofizialak aurkitzea, gehienetan aipatu den moduko blogetan irakur daitezke horrelakoak.

Hori aipatuta, makina multzo hauen atzean dagoen jendeaz hitz egiterako orduan argi eduki behar da ez dela ia inoiz pertsona bakar bat izaten. Helburu lortzeko taldeak osatzen dituzte, antolaturiko zibrekrimena deitzen diote batzuek. Adibide gisa, 3.2 irudiak erakusten du talde horiek duten antolamendu maila altua. Normalean talde horiek bes-

[8] http://en.wikipedia.org/wiki/Anonymous_%28group%29



3.2 Irudia: Botneten atzean dauden taldeak eta erabiltzaileak

te talde, erakunde edo pertsonei alokatu egiten dizkiete botnetaren zerbitzuak edo eta erabilera. Beraz, batetik komertzializatzen dutenak daude [Franklin and Perrig, 2007] eta hortik zuzenean bere erabilera aplikatu gabe dirua lortzen dute, eta bestetik, alokatu egiten dutenek ere, botnetaren erasoak baliatuz helburu ekonomikoak dituzten ekintzak eramaten dituzte aurrera: espioitza industriala, konpetentziaren deuseztatzea, spam bidezko iragarkien zabalpena...

Laburbilduz, gehienetan, alde batetik botnetak erabiltzen dituztenak daude eta bestetik, nolabait, botneten eskaera hori asetzeko industria bat eta zerbitzu bat garatu dituztenak. Horren harira egunkarietan azken urteotan honen inguruko albisteak atera izan dira [El-Pais, 2010].

Esan bezala 3.2 irudia adibide bat besterik ez da, modu ezberdinetan egon daitezke antolatuta taldeak, baina irudi horrek ongi erakusten du noraino iris daitekeen afera. Hau da, botneta sortzeko beharrezko Malwarea diseinatu eta sortzen dutenak egongo lirateke, gerora botmasterrak edo botherderrak botneta kontrolatzeko, eta azkenik, botnetak eskaintzen dituen aukerak zerbitzu gisa merkataratzen dituen jendea. DDoS erasoen deskribapenaren 3.2.2 atalean ikus daiteke sarean eskaintzen diren zerbitzuen bi erreferentzia.

Hona hemen, helburu ekonomikoak, sozialak zein politikoak lortzeko atal honen hasieran aipatu diren zenbat modu. Nortasun lapurreta, klik iruzurrak, spama eta zerbitzu eteteak zer diren eta nolako etekinak ematen dituzten azalduko dira. Aipatuko diren ekintza hauek, sarri bata bestearekin lotuta doaz, edo eta askotan batek bestea

elikatzen du edo beharrezkoa du. Hau da, spama bidaltzeko e-mail zerrendak behar dira, eta hortaz lehenik informazioa lapurtu beharra edo eskuratu beharra dago. Botenetetan tresna multzoak datozenez, asko errazten du hori guztia egin ahal izatea. Argi eduki ondoren aipatzen diren ekintzak legez kanpokoak direla [9].

3.2.1 Nortasun lapurreta

Hau da botneten bidez gehien egiten den gauzetariko bat [Tyagi and G.Aghila, 2011]. *nortasun lapurreta* esaten zaio nortasuna ordezkatzeko balio duen informazioaren eskuratzeari, hau da, e-maileko eta sare sozialetako pasahitza, Paypal eta bestelako ordainketa zerbitzuetarako sarbide datuak lortzeari. Erasotzaileari oso baliagarria izan dakioke e-maileko sarbidea lortzea, bertan informazio pertsonal asko aurki baitezake, adibidez, kontaktuak eta beste zerbitzu batzuetarako pasahitzak eskuratzeko aukera [Daniel Plohmann, 2011]. segurtasun informatikoaren munduan *phissing* izenaz ezagutzen den teknika da hori, alegia, password fishing edo euskaraz pasahitz arrantza litzatekeenarekin.

Datu horiek lapurtzeko botnetek tresna asko eskaintzen dituzte: Snifferrak, pasahitzak hausteko eta igartzeko tresnak... Sarri spam eta *gizarte ingeniaritzari* esker gauzatzen da nortasun lapurreta.

3.7.3 atalean aztertzen den ZEUS (ZBot) botnetari esker 70 milioi dolar eskuratu zituzten 2010ean [Marissa, 2010]

E-mailetan dauden helbideekin edo eta helbideetara spama bidaltzeko erabiltzen dira ere.

3.2.2 Zerbitzu etetea: DoS/DDoS

Erasoen bitartez zerbitzuak etetea da DoS (Denial of Service) eta DDoS (Distributed Denial of Service). Hori egiteko modu bat konexioa itotzea edo trafiko uholdeak sortzea da.

Bot multzo handi bati esker banda zabalera handia lor daiteke igoera trafikoan, segundoko gigabyte kopuru handiak lortuz. Hortaz, horrek aukera ematen die botmasterrei zerbitzarien aurkako erasoak egiteko, hau da sarea edo zerbitzaria trafiko uholde baten

[9] https://www.inteco.es/Formacion_gl/Legislacion_gl/

bitartez itotzeko. Une berean botek eskaera asko egiten dituzte eta azkenik zerbitzaria edo eta zerbitzarira doan sarea ito egiten da. Esaro hauei DoS (Denial of Service) eta DDoS (Distributed Denial of Service) esaten zaie. Teknika asko daude eraso hauek aurrera eramateko, besteak beste, UDP uholdea, ICMP uholdea edo *smurf* izeneko erasoak. Argibide gehiago ematen dira 3.4.3 atalean.

Orain arte nagusiki, konpetentzia edo eta etsaiaren zerbitzuak eteteko erabili ohi izan dira eraso mota hauek.

DDoS erasoak izugarri hazi dira, horren erakusle da Youtuben bertan dauden iragarkiak,[10] baita sarean aurki daitezkeen webguneak ere[11]. Gaur egun, horrelako guneetan DDoS erasoak egiteko zerbitzuak alokatzeko aukera eskaintzen da. DDoS erasoei esker 2008an 20 milioi dolar eskuratu zituzten erasotzaileek [Namestnikov, 2009].

Argi dago DoS eta DDoS erasoak oso ahaltsuak direla eta kalteak eragin ditzaketela. Hain dira garrantzitsuak zenbait erakundek protestetan, estatuk edo eta gerra antolakundek ere erabili izan ohi dituztela 3.2 atalaren hasieran aipatu den moduan. Etsairen sareko zenbait zerbitzu desaktibatzeko erabili izan dira botneten bidez egiten diren eraso hauek. Kasu nabarmena da 2009an Georgiako Gobernuak jasandako erasoak izan ziren, gerran zeudela Gobernua internet zerbitzu gabe geratu zen DDoS erasoen eraginez [Korns and Kastenberg, 2008]. 2004ean Ipar Koreak ere jakinarazi zuen 500 bat informatiko prestatu zituela zibergudetarako, gerora, 2011an Hego Koreak DDoS erasoak jasan behar izan zituelarik [Labs, 2011]. *Ziberprotesta* modura lehen kasu nabarmena Tallinn (Estonia) hirian errusiar gerrako estatua bat kendu zutenean jazotako da. Ondorioz, bi astez instituzio, banku zein albiste webguneak erasotuak izan ziren DDoS teknikak erabiliz [Daniel Plohmann, 2011]. Azken urteotan eraso hauek ezagunak egin dira interneteko Anonymous izeneko taldeak erabili dituelako besteak beste WikiLeaks-en kasuaren harira [Pras et al., 2010].

3.2.3 Bisita eta klik bidezko iruzurra

Botneten bidez dirua egiteko beste ohiko modu bat dira bisitak, instalazioak eta klik kopuruetan oinarritutako iruzurrak. Interneten iragarkietan jasotzen den klik kopuruaren arabera, edo eta iragartzen den software baten deskarga kopuruan oinarrituta dirua irabaz daiteke. Alegia, norbaitek webgune batean iragarkia jartzen du eta iragarki

[10] Esaterako http://www.youtube.com/watch?v=c9MuuW0HfSA&feature=relmfu
[11] http://www.ddosservice.co/

horretan klik egiten duen IP helbide ezberdin bakoitzeko ordaindu behar izaten du adibidez. Dena den, akordio mota horretaz gain, beste aukera eta mota askotako akordioak daude ere badaude.

Baina aurreko adibidearekin jarraituz, botnet bat duen norbaitek, lehenik, sarean iragarki bat jarri nahi duen norbaitekin akordio bat egiten du eta webgunean jarritako iragarkian ordenagailu ezberdinetatik egindako klik bakoitzeko diru kopuru bat kobratzen dio, beraz, klik kopuru hori handitzeko botmasterrak aginduta botek ataza hori egiten dute. Esan bezala, bestelako akordioak ere badira, finean, klik kopurua handitzearen bidez diru gehiago lortzea da helburua.

Software jaitsiera kopuruagatik edo eta ordenagailuetan software gehigarria (adware) instalatzearren ere dirua lor dezakete botneten erabiltzaileek [Hernando, 2006].

Argi eduki behar da ekintza mota hau ez dela legezkoa, iruzur egitea baita.[12]

3.2.4 SPAM

Gehienetan produktuak iragartzeko erabili ohi da spama. E-mailen zerrenda handietara bidali ohi den e-maila da, zabor posta ere esan ohi zaio. Masiboki bidali ohi da, horren helburua portzentajetan oinarritutako negozioa besterik ez da, alegia, milaka eta milaka e-mailetara bidaliz gero, azkenean, portzentaje txiki batek bada ere, iragarkian klik egingo du eta produktuaren salmenta webgunera joko du. Beste batzuetan, portzentajeen hari horretatik tiraka ere, bigarren helburu bat izan ohi du, malwarea hedatzea edo eta nortasun lapurreta egitea esate baterako, 3.2.1 atalean aipatu dena. Lehenago ere azaldu da, eraso batzuk edo helburu batzuk beste helburu batzuk lortzeko erdibideko pausuak direla eta elkar elikatu ohi dutela maiz.

Beraz, portzentajeak kontutan hartuta asko erabiltzen dira botnetak spama bidaltzeko. Garai batean spammerrak behar ziren, bakandutako ordenagailuak erabiltzen zituzten eta gainera atzemateko errazak ziren. Orain ordea, botnetei esker spamaren hedapena izugarri hazi da, aldi berean harrapatua izateko arriskua jaitsi egin delarik.

Malwarea hedatzeko kasuetan fitxategiak atxikitzen dizkiote sarritan edo eta Phishing (password fishing) teknika erabiliko duen guneren baten ezkutuko loturaren bat eransten diote. Hau da, *gizarte ingeniaritzari* lotuta *nortasun lapurreta* egiteko erabili ohi

[12] http://www.inteco.es/wikiAction/Seguridad/Observatorio/area_juridica_seguridad/Enciclopedia/Articulos_1/fraudclick

da [Internautas, 2010]. Gizarte ingeniaritzarekin lotutako gako nagusiak eta zenbait teknika 3.4.1 atalean.

Spama bidaliz urtean 3,5 milioi dolar eskuratzen dituzte [Marissa, 2010].

3.3 Egitura eta ezaugarriak

Atal honetan botnetek eduki ohi duten egitura azaltzen da. Horrekin batera, egitura bakoitzaren arabera zein sendotasun eta zein ahulezia dituzten azaltzen da. Botnetek erabiltzen dituzten protokoloaren arabera zein abantaila eta desabantaila lortzen dituzten ere aipatzen da.

3.3.1 Egitura, protokoloak eta C&C

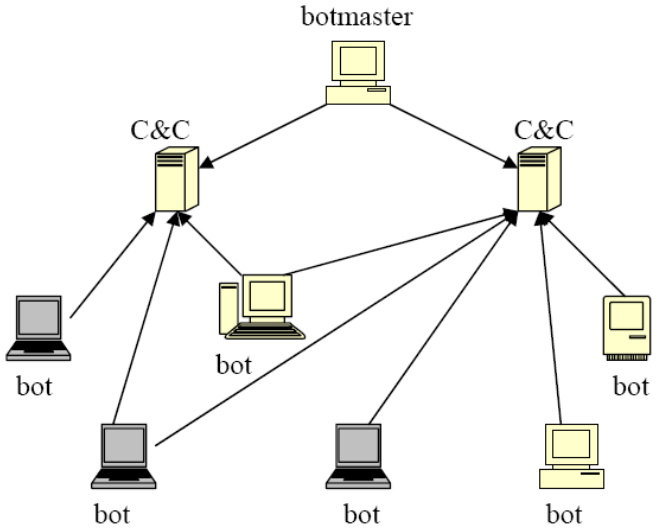
3.1.1 atalean aipatu dugu botnet batean botmasterrak agindu behar duela zer egiten duten kutsatutako makinek, hots, botek. Agindu horien transmisio modu ezberdinengatik sailkatu ohi dira botnetak, hau da, erabiltzen duten protokolo eta sare egituraren arabera. Batzuetan egitura zentralizatua dute eta beste batzuetan banatua (P2P sareak); Botnet batzuk HTTP protokoloa baliatzen dute, beste batzuetan IRC.

C&C egitura

Botnetaren oinarrizko elementua C&C azpiegitura deitzen zaiona da, alegia, 3.3.1 atalean aipatu berri duguna, botmaster batek botei aginduak bidaltzen dizkie eta transmisio hori bideragarria izan dadin C&C zerbitzari bat behar da gutxienez. Egiturari dagokionez batzuetan banatua, besteetan zentralizatua izango da. C&C egituraren araberakoa izango da botnetaren sendotasuna, erantzun denbora eta egonkortasuna.

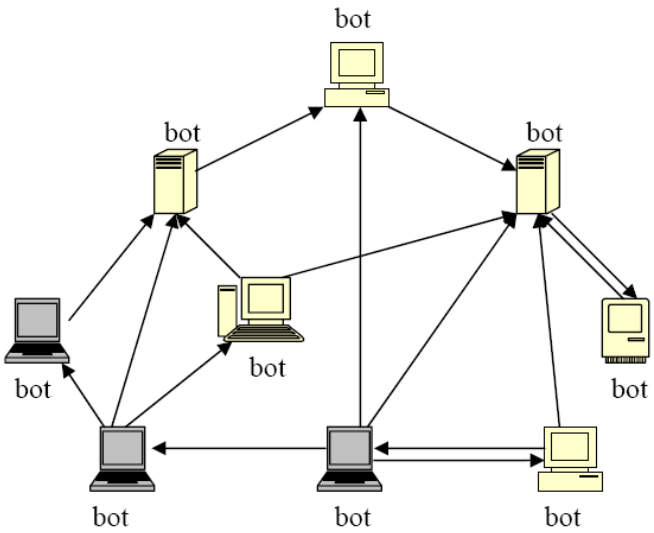
Egitura zentralizatua denean botmasterra, bota eta C&C bereizita daude. Botak zerbitzarira konektatzen dira haren bitartez aginduak jasotzeko, komunikazio hori nola ematen den xehetasun gehiagorekin azalduko da 3.3.1 atalean. 3.3 irudian ikus daiteke zentralizatutako egitura duen botnet batean C&C zerbitzariaren bitartez botmasterrak botekin komunikatzeko duen egitura.

Egitura banatuetako botnetetan botak beste bot batzuekin egongo dira konektatuta, botmasterra beste bot bat bailitzan egongo da botnetaren barruan, makina bat bot bat



3.3 Irudia: *Command & Control* zerbitzaria botnet zentralizatu batean [Wang et al., 2011]

eta C&C zerbitzari bat izan daiteke aldi berean. 3.4 irudian ikus daiteke P2P egitura banatua duen botnet bat. 3.3.1 atalean aztertuko da xehetasun gehiagorekin.



3.4 Irudia: P2P botnet bat, bot-ek zerbitzari papera dute ere [Wang et al., 2011]

Egitura zentralizatua

Egitura zentralizatutako botnetak bezero-zerbitzari ereduan oinarritu ohi dira. Botek puntu bat edo gutxi batzuekin konektatzen dira, alegia, zerbitzari finko bat edo gutxi

batzuk egoten dira. Era horretakoak ziren ezagutu ziren lehen botnetak, IRC protokoloa erabiltzen zuten botnetak ziren.

IRC taldekako bat bateko mezularitza ahalbidetzen duen protokoloa da. IRC botnetek *pull*mekanismoa erabiltzen dute, hots, botak IRC kanal batera konektatzen dira botmasterrak agindurik bidali duen egiaztatzeko. IRC-aren abantaila kanal batean eduki dezakeen kide kopurua mugagabea dela da [Daniel Plohmann, 2011]. Gainera, botmasterrak aldi berean bidaltzen ahal dizkie aginduak bot guztiei (multicast esaten zaio horri) eta erraz monitorizatu ditzake konektatuta dauden botak. Mota honetako botnetak ez dira zailak inplementatzeko, aipatuta berri diren ezaugarriak IRC-ak makinekin komunikatzeko eskaintzen dituen aukeretan oinarritzen baitira.

2010eko *Symantec Internet Security Threat Report* txostenaren arabera 2009ko C&C zentralizatuen %31k IRC protokoloa erabiltzen zuen [C. et al., 2010]. Datu horien araberan, oraindik asko erabiltzen dira IRC botnetak, nahiz eta zaharrenak eta atzematen errazenak izan [Tyagi and G.Aghila, 2011]. Alde txarrena hori dute, errazenak direla atzematen, IRC motako trafikoa ez delako asko erabiltzen eta beraz, sare gehienetan susmoa pizteko nahikoa izan daiteke hori. Hala ere, kode irekiko IRC zerbitzariak erraz aurki daitezke, hortaz, botmasterrak bere neurriko IRC botnet bat eraikitzeko beharra ase dezake, adibidez, 3.5.2 atalean azaltzen den moduan zifratzea gehi diezaioke botnetaren atzematea zailtzeko. 3.5.1 atalean azalduko den firewall tresnei esker adibidez IRC trafikoa galarazi edo blokatu daiteke.

IRC botnetak atzematea nahiko erraza dela kontutan hartuta, botnetetan HTTP protokoloa erabiltzeari ekin zitzaion. HTTP interneten datuak garraiatzeko gehien erabiltzen den protokoloa da, hala nola, webguneak, irudiak, fitxategi bitarrak eta bestelakoak garraiatzeko. Hori horrela izanik, Internetera konektatutako ia sare guztietan onartzen da HTTP. Erasotzaileak horren jakitun dira eta horregatik, geroz eta gehiago dira HTTP bidezko C&C azpiegitura duten botnetak [Daniel Plohmann, 2011]. 2009an zentralizatutako botneten %69 HTTP botnetak dira [C. et al., 2010].

Botak zerbitzariekin konektatzeko, askotan botmasterrek domeinuak erosi eta hosting edo zerbitzariak erosten dituzte. Hutsune legalak dituzten herrialdeetan jartzea izan daiteke aukera ba, herrialde horietan *bulletproof hosting* izenaz ezagutzen den aurki daiteke, alegia, gauza ez zilegietarako edo legez kanpokoetarako zerbitzariak alokatzen ahal izatea herrialde horietan legez kanpokoa ez dela jakinda [SSAC, 2008], beraz, modu horretan edukien inguruko baldintzarik jarriko ez duen hosting bat lor daiteke. Beste batzutan C&C zerbitzari doako ostalaritza (free hosting) dituzten zerbitzuetan

ezartzea da.

Aipatu den moduan, botnet zentralizatuek lotura puntu bakarra edo gutxi izaten dituzte, haustura puntu bakarra (zerbitzaria etenez gero nahikoa botneta hausteko) gainditzeko, batzuetan geruza edo maila ezberdinetan egituratzen dituzte bostmasterrek. Batzuk zerbitzari bat baino gehiago izaten dute eta egitura hauek mailakatuak edo eta hierarkikoak izan ohi dira, batetik bot azpimultzoak sortzen dituzte karga banaketa bat egiteko, beste zerbitzari batzuen bitartez edukia zabaltzen dute, hala nola, spam txantiloiak [Cho et al., 2010]. Egitura horren barruan ere ezberdindu egiten dira internetetik zuzenean eskuragarri dauden botak, sarri proxy lana egiten dutenak, eta beste sareen barruan daudenak. Geroz eta mailaketa konplexuagoa, zailagoa da inplementatzeko eta eratzeko baina zailagoa da atzemateko eta suntsitzeko ere.

Zentralizatutako botnetek duten abantaila nagusiak bi dira, batetik botak kontrolatzeko erraztasuna, eta bestetik, komunikazioetan lor daitekeen erantzun denbora azkarra, bi abantailak botekin daukaten lotura zuzenagatik lortzen dira.

Egitura banatua: P2P peer-to-peer

Botnet hauen egitura banatua da. P2P mota ezberdinak daude, baina oinarrian, botneta aztertzerakoan, azpimarratu beharrekoa egitura banatu bat izateak ematen dizkion ezaugarriak eta baldintzak dira. 3.4 irudian ikus daitekeen moduan boten arteko loturen bitartez osatzen da botneta.

Egitura banatua denez, botnetaren informazio osoa ezin da zuzenean eskuratu, eta aginduak ere bot edo puntu (*peer*) baten bidez sartu behar dira sarera. Puntu horretatik abiatuta gainontzeko botetara hedatuko da inplementatutako edo ezarritako protokoloari jarraituz. Gehienetan botmasterrek bot ezberdin baten bitartez sartzen dituzte aginduak eta horrek botmasterraren atzematea ia ezinezkoa egiten du. Baina botnet banatuen alde txarra erantzun denbora handia dela da; zentralizatutako botnetetan baino handiagoa [Daniel Plohmann, 2011].

C&C mekanismoa bi kategoriatan banatu daiteke sare hauetan, pull edo push. Pull mekanismoari *command publishing/subscribing* ere esaten zaio eta kasu honetan botak botmasterrak publikatutako komandoa aktiboki leku batetik jasotzeko moduari egiten dio erreferentzia. Aldiz, push mekanismokoetan, botak pasiboki komandoen zain geratzen dira, eta gerora beste botei pasatzen dizkiete aginduak. Normalean botnet

zentralizatuek pull erabiltzen dute. Aldiz banatuetan push ere erabil daiteke, biak erabil daitezke, push eta pull.

Fitxategien trukerako ohiko P2P sareetan (Ares, eDonkey, Gnutella...), nodo batek kontsulta bat bidaltzen du sarera fitxategi jakin baten bila, mezua sarean hedatuko da bideratze protokolo bati esker. Fitxategi hori duen nodo batera heltzen denean, "arrakasta" mezu batekin erantzungo dio fitxategiaren transmisioa has dadin. Pull mekanismoko P2P botnetetan funtzionatzeko era hori erabili da. Hau da, botmasterrak ausaz hartutako bot baten bitartez komandoak publikatzen ditu fitxategi bat duela "arrakasta" adierazteko egiten duen moduan. Fitxategi horren izena aurrez definitu behar da, edo boteko kodean algoritmo baten bitartez kalkula daitekeen izen bat izan behar da, horrela botek fitxategi hori bilatuko dute. Behin fitxategia aurkitu dela erantzuten denean, erantzun horretan bertan bidaliko da komando bat edo beste batzuetan helbide bat pasako zaio beste leku batera jo dezan agindu bila. Behin horra iritsita, kasu horretarako bereziki kodetutako kontsulta berezien bitartez, botek aginduak eskuratuko dituzte fitxategien ordez.

P2P motaren arabera badaude pull mekanismoa bestelako modu batean inplementatzen duten botentak , baina funtsean aipatu berri dugun ideia erabiltzen dute.

Bestetik, push mekanismoa darabilten botnetak daude. Botmasterrak aginduak bidaliko dizkie botei eta hauengana iristean beste batzuei bidaliko dizkiete. Horrela botak ez dira etengabe agindu bila eskaerak egiten aritu behar, gainera horrek txikitu egiten du botneta atzemateko aukera. Hala ere zailtasunak egon ohi dira aginduak beste bot batzuei bideratzeko, P2P sarean makina guztiak ez baitira botak eta hortaz, nola jakin zein den bot bat. Normalean aurrez fitxategi ezagun batzuk definitzen dira, botak fitxategi horien bila ibiliko dira, hortaz beste botek badakite makina hori ere bot bat dela. Horrek ordea, agerian utz ditzake botak [Wang et al., 2011].

Beste motako botnetekin alderatuz gero, P2P botnet bat deuseztatzea zailagoa da, ez baita haustura puntu bakarreko egitura, hau da, zentralizatuan zerbitzaria botaz gero nahiko da. Aldiz, arestian aipatu dugun bezala, erantzun denbora motelagoa da, aginduak beraien kabuz hedatzen uztea mantsoagoa da eta. P2P egiturako botnet baten tamaina ere ez da besteetan bezain handia izaten [Lashkari et al., 2011].

Botnetak mugikorretan

Gaur egun interneterako konexioa duten mugikorrak aurki daitezke. Wifi edo eta mugikorren komunikaziorako zenbait protokoloren bitartez konektatu daitezke Internetera, hala nola, *High-Speed Downlink Packet Access* (HSDPA), *Evolution-Data Optimized* (EVDO), *Universal Mobile Telecommunication System* (UMTS)...

Mugikorrez osatutako botnetak C&C mekanismoaren menpe dauden kutsatutako mugikor edo smartphone multzo bat dira. Aipaturiko HTTP botneten antzera jokatzen dute. Hala ere, zenbait baliabide arazorengatik ez dira ordenagailuetakoak bezain eraginkorrak, besteak beste, bateriaren iraupen laburragatik eta interneten atzigarritasuna mugatua delako [Rajiv, 2012]. Hala ere, smartphonen merkatua handituz doan heinean smartphonen baliabide ahalmena handituz doa. Horrek erabiltzaileei gauza gehiago egiteko aukera ematen die, baina era berean, botnet diseinatzaileen arreta ere piztu du. Gainera erabiltzaileek geroz eta informazio gehiago gordetzen dute mugikorretan.

Mugikorretako lehen botneta 2009an atzeman zen, SymbOS.Yxes. Symbian sistema eragilea zuten mugikorrentzako egin zuten eta HTTP botnet bat zen [Apvrille, 2012]. 2009an ere, pixka bat beranduago, Ikee.B agertu zen, *jailbreaking*[13] egina zuten Iphone mugikorrei eragiten ziena eta *SymbOS.Yxes*-en antzeko funtzionamendua zuena [Porras et al., 2010]. 2010eko Abenduan Android sistemarako lehen botneta atzeman zen, Geinimi.

Hala ere, oraindik ez da mugikorretako botnet kopuru edo multzo handirik ezagutzen, baina aurrera begira segurtasun mehatxu handia izan daitekeela aurreikusten da [Traynor et al., 2009]. Argi dago egunez egun, mugikorretan geroz eta informazio gehiago izanik, jo puntu erakargarria direla.

Aipatu diren botnet egitura ezberdinek dituzten ezaugarriak kontutan hartuta, 3.2 taulan zenbait parametro baloratu dira, atzemateko erraza edo zaila den, inplementatzeko konplexutasuna, eta haien ahulezia nagusiak.

Lehen hiru kasuetan etetea erraza da behin atzemanda, hau da, esan dugun moduan zerbitzaria bota behar da bakarrik, zentralizatutako egiturak direlako (HTTP kasuan salbuespenak daudela aipatu dugu, egitura hierarkikoa ere izan daiteke ...).

[13] http://en.wikipedia.org/wiki/IOS_jailbreaking/

Botnet egitura	Protok.	Konplex.	Atzematea	Gabeziak
Zentralizatua	IRC	Baxua	ertaina, IRC ez ohiko trafikoa	Eteteko erraza, IRC sarri blokeatuta. Haustura puntu bat edo gutxi
Zentralizatua	HTTP	Baxua	zaila (80 ohiko portu onartua)	Eteteko erraza, haustura puntu bat edo gutxi
Banatua	P2P	altua	oso zaila	denbora erantzun handia, bot kop. txikia

3.2 Taula: Botneten konparaketa

3.3.2 Bot familiak

Botnet motak bereizteaz gain, bot familiak ere sailkatu daitezke. Hedatzeko modua, egitura, kodearen inplementazioa, kontrol mekanismoa eta diseinua kontutan hartuz sailka daitezke bot familiak. Desberdintasunak badaude ere, Agobot, Spybot eta bestelako bot batzuk iturri kode bera dutela frogatzen du esate baterako Symantec-en ikerkuntza batek [Canavan, 2005]. Hauek dira botnetak agertu zirenetik orain arte oinarri edo eredu gisa gehien erabili izan diren botak.

Agobot

2002koak dira ezagutzen diren lehen erreferentziak [Barford and Yegneswaran, 2007, Schiller and Harley, 2007]. Gaur egun kode horren ehunka bertsio daude eta Phatbot izena ere eman ohi zaie. C/C++ lengoaian idatzitako iturburu kodea 20.000 lerrokoa da. IRC botnet bat eraikitzeko osagaiak ditu. DoS erasoak egiteko aukera ematen du. Pasahitzak (Paypal, AOL) bilatzeko tresnak, Keyloggerrak eta *sniffer*rak ere eskaintzen ditu. Antimalwarea blokeatzeko tresnak ere baditu. Agobotak diseinu bereziko arkitektura monolitikoa duen kodea du. Kodea dokumentatuta dago eta modularizatutako kodea da.

Bot honek bere burua zein direktoriotan sistemako zein direktoriotan kopiatu ohi duen azaltzen dute Shophosen webgunean[14]

[14] http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Agobot-A/detailed-analysis.aspx

SDBot

Honen berri ere 2002an izan zuten segurtasun adituek [Barford and Yegneswaran, 2007, Schiller and Harley, 2007]. Agobota baino xumeagoa da bere kodea eta C lengoaiaz 2000 bat lerrotan idatzitako kodea da. GNU General Public License (GPL) lizentziapean dago argitaratua. Ez ditu Agobotak adina tresna eskaintzen. IRC botnet bat da. Bere kode xumea dela eta erraz gehitzen ahal zaizkio bestelako tresnak, DoS3.2.2 erasoak egiteko tresnak, sniffer, keylogger eta bestelako tresnen moduluak aurki daitezke prest. 80 bat hedapen aurki daitezke sarean.

GT Bot

Paul Barfordek 1998an agertu zela jasotzen du [Barford and Yegneswaran, 2007]. Aristoteles izenaz ere ezagutzen da. Botak berak, kutsatutako makinan bere burua ezkutatzeko, HideWindow programa du. mIRC [15] bidez kontrolatzeko aukera ematen du, funtsean pertsonalizatutako script batzuk dituen mIRC pakete bat da [Parolli, 2011]. DoS erasoak egiteko aukera ematen du. NetBIOS eta RPC ahuleziak probesteko tresnak ere baditu.

SpyBot

2003an izan zen bere berri [Barford and Yegneswaran, 2007]. Dagoeneko ehunka bertsio ditu honek ere. C-z idatzitako 3000 bat lerro ditu. SDBot-etik eratorritako kodea du, C&C mekanismorako lerro asko berdinak dira. Esan daiteke SDBot-en eboluzioa dela [Parolli, 2011, Canavan, 2005], informazioa lapurtzeko aukerak aurreratuagoak eskaintzen dituena, *spyware* ere esaten zaie tresna mota horiei. SpyBotaren bertsio batzuk NetBIOS/Kuang/Netdevil/KaZaa Exploit tresnak, Scanning tresnak eta uholde erasoak egiteko tresnak dituzte. P2P sareetan barrena heda daiteke eta bestelako *malware*ak irekita utzitako *backdoor* eta ahulezietatik sar daiteke sistema berrietan.

Beste berezitasun bat, uneko mezularitza sistema baliatuz spama zabaltzea da, hau da, *Spam over Instant Messaging* (SPIM) baliatuz [Schiller and Harley, 2007]. MSN, AIM eta Yahoo IM mezularitza programen leiho irekiak bilatzen ditu, bat edo beste irekita badago mezu bat bidaltzeko aukera ematen du [Canavan, 2005]. Windows XP SP2

[15] mIRC Windowserako IRC bezero bat da, aukera bereziak eskaintzen ditu,besteak beste zifraketa, eta bestetik scripting lengoaia bat eskaintzen du mIRC automatizatu ahal izateko. http://www.mirc.com/

instalatzea ere galarazi dezake erregistroa aldatuz, edo eta *Windows XP Security Center* babes zentroa desgaitu dezake.

RBot

2003an sortu zuten eta bot familien artean konplexuena da [Schiller and Harley, 2007]. Hau izan zen zifraketa eta trinkotzea (konpresioa) erabili zituen bota [Parolli, 2011]. Behin sistema kutsatuta dagoela, besteek egiten dituzten gauza gehienak egin ditzake, hala nola, DDoS erasoetan parte hartu, internetetik fitxategiak jaitsi edo exekutatu, e-mailak bidali, zapaldutako teklak gorde, baita webcam bat konektatuta edukiz gero bertatik irudiak jaso. Hedatzeko pasahitz ahulak hausten ditu edo eta sarean konpartitutako direktorioak dituzten sistemetatik sartzen saiatzen da.

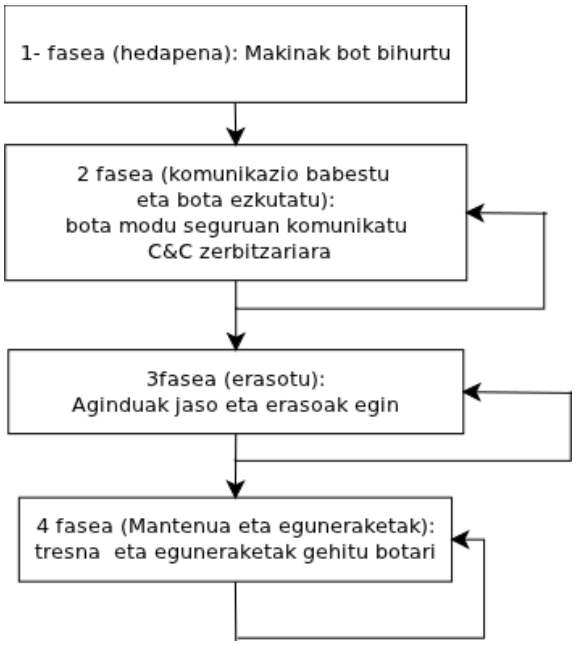
3.4 Botnet baten eratze faseak

Orain arte botnetak nork erabiltzen dituen eta zein erabilera eta aukera ematen dituzten azaldu da. Boneten eraketan ezinbestekoak diren pausu batzuk daude, botnet guztiek jarraitzen diete pausu horiei. Bonetak bizia du, edo botnet bat dela esan daiteke gutxienez botmasterraren menpeko sare horretara bot bat gehitu denean eta erabiltzen hasten denean.

Bot bat edukitzetik gehiago izatera izango da hasierako helburua, eta hortaz, botnetaren hedapen fasea osatuko da. Era berean, botnetaren parte diren botekin segurtasun neurri batzuk jarri behar ditu martxan botmasterrak botnetaren biziraupenerako baita bere segurtasunerako ere, hau da, atzematea eta botnetaren etetea zailduko dituzten neurriak.

Behin hori eginda, esan liteke botneta segurua dela,kasu askotan komunikazioak zifratuta daudela eta bot-aren prozesuak kutsatutako makinan ezkutatuta daudela adibidez. Beraz C&C bidez aginduak jasotzeko prest egongo dira botak. Egingo den lehen gauzetako bat behar dituen tresnak kargatzea izango da, hots, bota nahi duen ataza burutzeko baliatu nahi badu tresna gehiago instalatu beharko dizkio C&C bidez pasatako aginduekin. Azkenik egin nahi dituen erasoak egiteko tresnak baliatu ahal izango ditu eta botak erantzunak itzuliko edo bideratuko dizkio botmasterrari.

Aipatutako atazak errepikatu egin daitezke baita paraleloki egin ere, hau da, bot gehiago gehitu, zerbitzariarekin modu seguruan komunikatu, aginduak jaso eta erasoak



3.5 Irudia: Botnet bat eratzeko eta erabiltzeko pausuak

egin eta azkenik bot horien lotura ez galtzeko eguneraketak aplikatzea eta mantenua egitea. Aipatutako atazen sekuentzia hori 3.5 eskeman ikus dateke.

Botnet baten sorkuntza bi multzo orokorretan banatzen da zenbait ikerkuntzatan, lehena makinak kutsatzea eta lotzea, bigarrena, makina horiek kontrolatzea eta bidalitako aginduak aurrera eramatea [Wang et al., 2011].

Botneta eratzea botmasterraren eta botneta diseinatu dutenen arabera teknika ezberdinen bidez gauza daiteke,esate baterako metodo ezberdinak erabil daitezke makina bat kutsatu eta bot bihurtzeko, 3.4.1 atalean aipatuko dira zenbait aukera ezberdin. Hala ere guztiek beteko dituzte aipatutako pausu horiek.[Schiller and Harley, 2007, Tyagi and G.Aghila, 2011].

Ondorengo zerrenda botnet bat martxan jartzeko jarraitu behar diren pausuen adibide bat da (adibidearen irudia 3.6), ematen diren pausuetan aipatutako lehen faseak ikus daitezke:

1. Botmasterrak bitarteko eta teknika bereziren baten bidez bere menpe daukan makina batetik lehen biktima kutsatzen ahaleginduko da, esaterako berea ez den ordenagailu batetik bidalitako e-mail faltsu baten bidez. 3.4.1 atalean aipatuko dira kutsatze horiek egiteko teknika ezberdinak. Adibidez e-mail bidez bidaliko dion fitxategi kutsatu batekin.

2. Biktima horrek atxikitutako fitxategia jaistean edo eta irekitzean bere makina kutsatuko du.

3. Instalatutako malware horren bitartez, zenbait portu irekiko dira karga handiagoko fitxategi bat jaitsi eta erabiltzailea ohartu gabe instalatzeko. Bigarren hau erasoak egiteko bot bat edo boterako modulu gehigarri bat (sniffer, keylogger ...) izango da. (Zentzua du bigarren batean egitea, dagoeneko makina kutsatuta dagonean eta antimalwareak saihestu direnean. Bestela lehen saiakeran botaren fitxategia harrapatuz gero, botneta arriskuan jar dezake C&C zerbitzaria zein den agerian utziz.)

4. Esan bezala URL batetik jaitsitako fitxategi bat instalatuko da makinan, botnetaren lehen makina prest egongo da, alegia, lehen bota. Dagoeneko bot horren bitartez erasoak egin ahalko ditu. (Hala ere bot gehiago lortzea da normalena, lehengo prozesua errepikatuz edo antzeko zerbait eginez.)

5. Bota, kontrolatzaile batekin, zerbitzari (demagun IRC zerbitzari bat) batekin, komunikatuko da bere egoeraren berri emateko.

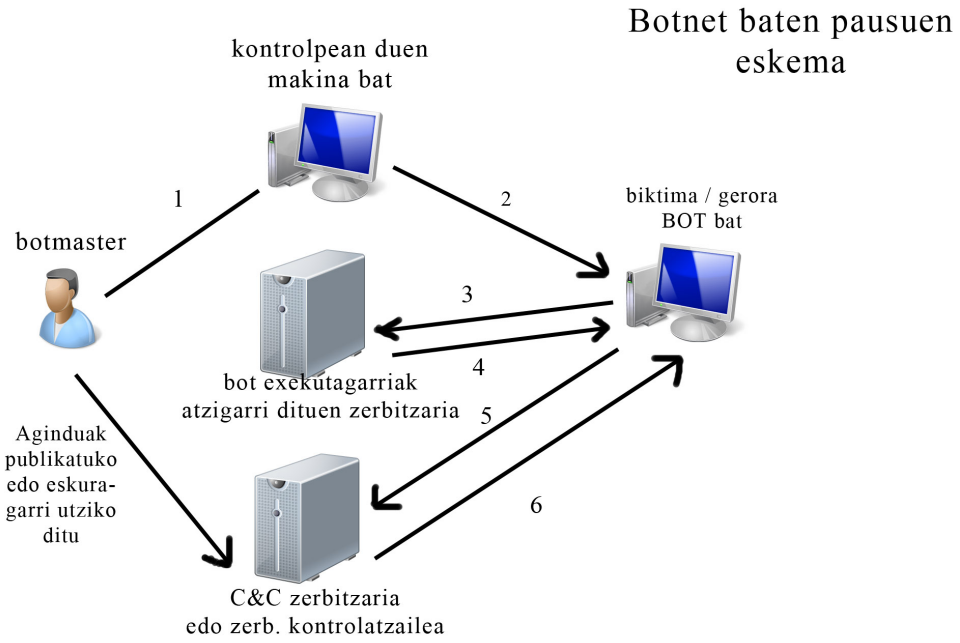
6. Zerbitzari horren bitartez erantzuna itzuliko zaio baita agindu gehiago bidali ere. Hau da, botmasterrak aginduak publikatuko ditu botak zerbitzaritik jaso ditzan. Hortik, C&C izena, aginduak eta kontrola.

Jarrain, kapitulu honen hasieran eta 3.5 irudian agertzen diren faseei buruz azterketa sakonago bat egiten da. Esan bezala, fase horiek metodo eta tresnak ezberdinak erabiliz gauza daitezke eta jarraian horietako batzuk azalduko dira.

3.4.1 1. Fasea: Hedatu

Hedapen fasea Botnet baten eraketaren fase garrantzitsuena da, botneta zenbait eta handiagoa izan orduan eta ahaltsuagoa izango baita; hori da botneten funtsa.

Hedapenaz hitz egiterakoan, bi atal bereiziko dira, batetik teknika informatikoak soilik erabiliz egiten dena azalduko da, hau da, botnetak zein ahulezia informatiko eta tresna baliatzen dituen eta zein baldintza aprobetxatzen dituzten bot gehiago lortzeko, horietako batzuk 3.4.1 azpiatalean ikus ditzakezue. Bestetik, botnet baten zabalpenerako giza faktorearen menpe dauden teknikak daude, gizarte ingeniaritza esaten zaiona. Oinarria pertsonak engainatzea da.



3.6 Irudia: Botnet bat martxan jartzearen adibidea

Esan daiteke hedapenaren eta kutsatzearen arrakasta abilezia teknikoen, trikimailuen eta ideien uztarketaren ondorioa dela. Botmaster gehienek gizarte ingeniaritza erabiliz eta sareei eraso zuzenak eginez lortzen dute botneta hedatzea. Adibidez, horrela izan zen Nugache botnetaren kasuan [Dittrich and Dietrich, 2008].

Ahulezia eta ezaugarri teknikoak

3.3.1 atalean azaldu dugu zein egitura eta protokolo baliatzen diren botneten funtzionamendurako. Baina hemen botnetek zein ahulezia eta segurtasun gabezia baliatzen dituzten landuko da, hau da, nola lortzen duten makina berri batera sartu eta hau botnetaren parte izatera pasatzea.

Gaur egun, etxeko makinak edo erabiltzaile arrunten makinak jo puntu erakargarriak dira erasotzaileentzat. Erasotuenak Microsoft Windows sistema duten ordenagailuak dira. Symantec-ek 2009an jasotako datuetatik ondoriozta daiteke hori [C. et al., 2010]. Hori aipatzen dute ere Honeynet proiektuko Paul Bacher eta bere kideek [Bacher et al., 2008] baita Yuanyuan Zeng-ek ere [Zeng, 2012]. Microsoften txostenean aipatzen du berezi-ki erasotuena Windows XP SP2 dela [Dennis et al., 2011]. Askotan erabiltzaileek ez dituzte eguneraketa paketeak (patch) instalatu edo eta ez dute firewallik martxan edo eta gaizki konfiguratuta eduki ohi dute, horrek segurtasun ahuleziak agerian uzten

ditu.

Argi eduki behar da erasotzaileek oso gustuko dituztela ere uneoro piztuta dauden eta banda zabalera handia duten makinak, baldintza horiek betetzen dituzten makinak kutsatzeko saiakerak egiten dituzte nagusiki. Baldintza horietako makinak kutsatuz botnetari ahalmen handiagoa gehituko diote. Banda zabalera handiko konexioa duten makinak geroz eta gehiago direnez, biktima potentzialen sorta geroz eta handiagoa da. Teknika automatizatuak erabiliz, sarea eskaneatzen (scan) dute ahulezia ezagunak dituzten sistemen bila. Sarritan B klaseko IP helbideak dituzten sareak aukeratzen dituzte edo IP tarte txikiagoko sareak.

Beraz, erasotzaileek bilaketak egin ditzakete IPak eskaneatuz, eskaneatzeko eta zerrendatzeko tresnen bitartez makinen ezaugarriak ezagutu (sistema eragilea, bertsioa, martxan dituzten programa edo zerbitzuak) eta haien ahulezia ezagunenak bilatzen dituzte, hala nola portu irekiak, software akatsak eta gabeziak, firewalla duen ala ez... [Schiller and Harley, 2007].

Esan bezala, sarritan ahulezia horiek erabiltzaileek beharrezko neurriak hartu ez dituztelako nabarmentzen dira, gainera hackerrak adi daude Microsoften "patch tuesday" eguneraketei, berriro ahuleziak aurkitzeko. Baina askotan beste malware batzuk eragindako kalteetatik eratortzen dira, hau da, Birusaek, Troiar:rek, Harrek eta bestelakoek eragindako kalteetatik. Horiei esker itxita egon beharko luketen portuak irekita aurki daitezke. Edo beste batzuetan, erabiltzailea jabetu gabe sistemara sartzeko aukera ematen duten programak instalatzen dituzte. Beraz, askotan botmasterrek badakite malware hedatu behar dutela hauen kalteak aprobetxatzeko. Software gabezia edo ahuleziak badituzte, horiei esker erabiltzailea ohartu gabe instalatu daitezke behar diren tresnak.

Kutsatzeko bide bat ere *backdoor* izenekoak dira, *trapdoor* izena ere ematen zaie, euskaraz *atzeko atea* esango genieke. Ezkutuko sarrera bat da, urruneko exekuzioa eta kontrola ahalbidetzen du makinako erabiltzailea ohartu gabe. Sartzeko ohiko prozedurak erabili behar izan gabe baimentzen du programara sartzea. Malware askok backdoor sarbideak irekitzen dituzte, baina beste askotan inteligentzia zerbitzuek edo eta software garatzaileek beraiek txertatzen dituzte programetan beraiek sistemetara sartu ahal izateko, besteak beste NSA erakundeak eta Microsoftek [Gómez Vieites, 2006]. Gerora noski, sarbide hori bai beraiek bai beste batzuek erabil dezakete. Beraz, backdoorrak sarbide ezin hobeak dira botneten hedapenerako, hona hemen zenbait backdoor ezagun [Kola, 2008]:

- Optix backdoor (3140 portua)
- Bagle backdoor (2745 portua)
- Kuang backdoor (17300 portua)
- Mydoom backdoor (3127 portua)
- NetDevil backdoor (903 portua)
- SubSeven backdoor (27347 portua)

Hala ere webguneetatik jaisten diren script, *cookie* eta programatxoak sarritan malwarez josita daude eta horiei esker aipaturiko sarbideak irekitzen dira, sarbide horretatik makinarekin konektatu eta bertara jaisten dira botak instalatzeko exekutagarriak.

Esan bezala botnet gehienek urrutiko *exploit*ak erabiltzen dituzte makinak kutsatzeko eta ondorengoak dira gehien erabiltzen dituzten portuak [Bacher et al., 2008]:

- 445/TCP (Microsoft-DS Service). Windows 2000, XP, edo 2003 sistemetan baliabideak konpartitzeko portuak. Esate baterako fitxategiak elkarbanatzeko.
- 139/TCP (NetBIOS Session Service) Windows 9x, ME and NT sistemetan baliabideak eta fitxategiak konpartitzeko.
- 137/UDP (NetBIOS Name Service) Windows makinatan erabiltzen da beste ekipo batek eskainitako sareko ezaugarriak jakiteko. Esate baterako sistemaren izena, konpartitzen dituen fitxategien izenak...
- 135/TCP Microsoftek erabiltzen du RPC (Remote Procedure Call) zerbitzuak inplementatzeko. RPC zerbitzua makina batean exekutatzen dagoen programa bat beste sistema batean exekutatzea ahalbidetzen duen protokoloa da.
- 80/TCP web zerbitzutara konektatzeko balio du.

Sarritan ere *0-day-exploits* izeneko ahuleziak bilatzen dituzte erasotzaileek, hots, ezezagunak diren ahuleziak edo ezagunak direnak baina oraindik haientzako eguneraketa paketeak sortu ez dituztenak.

Rbot-ek Brute-force teknika erabiltzen du pasahitzak asmatzeko fitxategi konpartituak dituzten Windows sistemetan. Beraz, 139 eta 445 portuak eskaneatzen ditu.

Beste batzutan *hijacking* eginez, hau da, beste botmaster batzuen botneteko botak bereganatuz, lortzen dituzte bot gehiago botneterako. Horretarako snifferrak baliatzen dituzte, askotan C&C komunikazioa zifratu gabe doa, eta ez denez arraroa sare edo makina batek botnet batean baino gehiagotan parte hartzea, xurgatutako trafikotik ez da zaila beste botneta atzeman eta bere egitea. Beste batzuetan bere burua birbikoizten du, horretarako makinan dauden fitxategiak kutsatzen ditu erabiltzaileak beste makina batzuetara heda ditzan [Cert/cc and Cert/cc, 2005].

Ondoren ikus dezakezue lehen aipaturiko bot familiak (3.3.2 atala) nola hedatu ohi diren, hau da, hedapenerako gehien erabili izan diren teknikak.

- **SDbot:** Lehen bertsioak, jatorrizko bertsioak, ez zuenez helburu erasokorrik ez dauka hedapenerako tresnarik, ordea, bere ondorengoek badituzte hedapenerako bitartekoak [Barford and Yegneswaran, 2007]. Ohikoa da fitxategiak konpartitzeko sare ahuleziak baliatzea sistemak kutsatzeko, baita aipatutako backdoor sarbideak. Behin sistema horretara konektatuta, gai da script bat jaitsi eta sistemaren kontrola bereganatzeko daukan RAT (Remote Access Tool) motako osagaiari esker eta IRC zerbitzari batera konektatzeko [Martínez, 2011]. Ezaguna da ere Microsoft SQL Server ahuleziak probestea.

- **Rbot:** SDbotaren antzera sarean barna baliabide konpartituen ahuleziak bilatu ohi ditu. Pasahitz errazak edo eta pasahitz hutsak dituzten sare makinak jo puntu erraza izan ohi dira, esan bezala brute-force teknika erabiltzen baitu [Martínez, 2011]. Aipatu berri diren malwareek sortutako backdoor sarbideak eta portu irekiak (139 eta 445)ere probestu ohi ditu [Kola, 2008].

- **Agobot:** SDbotak erabiltzen dituen antzeko teknikez gain, P2P sareetan barna hedatzeko gaitasuna ere badu, hala nola, Kazaa, Grokster, BearShare bidez. Gai da ausazko fitxategi izenak sortzeko, horrela horien bitartez sare horietako erabiltzaileek fitxategi kutsatu horiek jaitsiko dituzte [Schiller and Harley, 2007].

- **SpyBot:** Agobotaren antzekoa aukerak ditu hedatzeko, baina ezaugarri berezi bat badu, uneko mezularitza bidez Broadcast eginez spama zabaltzekoa gaitasuna (SPIM Spam over Instant Message). Ohikoa da *Microsoft Plug and Play* ahulezia (MS 05-039) baliatzea [Kola, 2008].

Gizarte ingenieritza

Informatikako segurtasun adituek diote makinaren faktore arriskutsuena eta mailarik ahulena erabiltzailea dela, [Hadnagy, 2010, Mitnick and Simon, 2002]. Sistemetan gertatzen diren segurtasun arazo gehienak erabiltzaileen akatsetatik datoz. Sarri erabiltzaileek ez dituzte hartzen behar adina neurri edo arduragabe jokatzen dute adi egotea eta segurtasun neurriak hartzearen garrantzia albo batera utzita [Gómez Vieites, 2006].

Horregatik, gaur egun, gizarte ingeniaritza izenaz ezagutzen dena mehatxu handienetako bat da makinen segurtasunerako. Gizarte ingeniaritza eta informatika jakinduria uztartuz gero erasotzaileak arrakasta izateko aukera handiak ditu.

Teknika ezberdinak daude, hala ere, helburu bera dute, erabiltzailea engainatzea informazioa lortzeko eta makina kutsatzeko. Hau da, geroz eta informazio gehiago eduki, erabiltzaileak amua jateko aukera gehiago egongo dira. Erasoak geroz eta orokorragoak izan, orduan eta errazagoak dira atzemateko. Geroz eta zehatzagoak izan, orduan eta eraginkorragoak dira, baina aldi berean hedapen txikiagoa izango dute. Beraz, automatizatuz gero ez dira horren eraginkorrak.

Adibidez, erabiltzailearen zaletasun bat ezagutuz gero, e-mail bat bidali diezaioke norbaitek zaletasun horren inguruan, erabiltzaileak jakin minak jota e-maila irekiko du eta esteka bat sakatu edo programa faltsuren bat jaitsi ordenagailura. Esan bezala, geroz eta pertsonalizatuago izan orduan eta hobe, baina egia esan, gehienetan bot masterrari ez zaio asko inportako nor den botnetaren parte egin nahi duen makina hori duena,azken finean bot-a beste eraso batzuenganako erasoak bideratzeko osagaia da, hortaz eraso masiboak egiten dituzte eta azkenik probabilitate hutsagatik beti dago amua jango duen pertsona bat edo beste.

Horrela hedatzen dira botnetak gehienetan. Bestalde, IRC kanaletan ere sarri erabiltzen dira trikimailuak beste erabiltzaileek amua eror daitezen. Sarri IRC eta IM programak erabiltzen dituzte erasotzaileek erantzungailu automatikoen bidez erabiltzaileei interesa dakiekeen programak eskaintzeko, horiek jaistean eta exekutatzean troianoak, backdoorrak edo eta DDoS erasoak egiteko tresnak instalatzen dira. Hona hemen erabiltzen diren mezuen adibide bat:

> You are infected with a virus that lets hackers get into your machine and read your files, etc. I suggest you to download [malicious url] and clean your infected machine. Otherwise you will be banned from IRC network

Hala ere, gaur egun posta elektronikoa da gizarte ingeniaritzaren bitartez makinak kutsatzeko erabiltzen den baliabide ohikoen, mezu horiek ez dira erabiltzaileak nahi edo eskatuak zituen e-mailak, spam mezuen multzoan sartzen dira, eta kalkulatzen da mezuen %75 edo %80 spam direla [Mallery et al., 2005]. Lehen aipatu diren teknika informatikoak baino gehiago erabiltzen direla esan daiteke. Egunero iristen dira e-mailak eskaintza bereziekin (sariak, sendagaiak, bitaminak, pornografia eta sexua, kreditu txartelak eta bankuak...) edo eta interesa sor dezaketen bestelako gai afektiboekin (ospetsuak, maitasunezko gaiak, injustizia sozialak), dena den, norberak eskatu ez dituen e-mailak dira baina gaiaren tituluagatik edo erakargarritasuna edo une batez gure arreta deitzen dutenak, hurbilak izan daitezkeenak edo eta konfiantza eman dezaketenak [Mitnick and Simon, 2002].

Behin makinara sartuta ordea, sarbidea irekita mantentzea, bertan gauzak egitea eta kontrol hori mantentzea lortu behar du erasotzaileak kutsatutakoaren susmoa edo arreta deitu gabe. Hurrengo atalean ikusiko da hori.

3.4.2 2. Fasea: Ezkutatu eta komunikazioa babestu

Botnetaren biziraupenerako ezinbestekoa da bota bera sistemaren barruan ezkutuan mantentzea eta komunikazioak ere seguru eta susmo handiegirik piztu gabe egitea.

Ondoren botnetak eta botak ezkutatu eta modu seguru edo babestuan komunikatzeko hedatuen dauden teknikak azalduko dira.

Fast-flux eta *Domain-Flux*

Botnet berrietan atzematea zailtzeko erabiltzen ari diren bi teknika dira *fast-flux* eta *domain-flux*.

Fast-flux sareak etengabe aldatzen ari diren domeinu baten DNS erregistroek apuntatzen duten kontrolpeko makinaz osatutako sareak dira. Proxy modura jokatzen dute edukia dagon zerbitzariaren eta bezeroaren artean.

Fast-flux teknikaren bitartez domeinu batek, IP asko edukiko ditu esleituta (A motako erregistroa), adibidez adibide honetarako asmatutako *www.dominioa.com* domeinuak 30 IP helbide dituela esleituta. Esleipen horiek etengabe joango dira aldatzen DNS RRri (*Resource Record*) lotutako TTL (*time-to-live*) txiki bat ezarriz. IP helbideen etengabeko aldaketa *Round Robin* bezalako algoritmo xumeen bitartez egin daiteke. Adibidez,

dominioa.com 5 minuturo IP helbide multzo ezberdin batera egongo da lotuta, hau da, erabiltzaile bat domeinu baten bidez webgune batera badoa, eta hortik 5 minutura berriro domeinu hori bisitatzen badu, webgune berdina ikusiko du baina makina ezberdin batean egon da, hots, beste IP helbide bat ariko da atzitzen. Sarri Round Robin ordez, bestelako algoritmo batzuk garatzen dituzte banda zabalera eta sare ezaugarriak kontutan hartuz. Gainera, batzuetan makina horiek ez dira edukia dutenak, baizik eta berbiderapena egiteko beste geruza bat besterik ez. IP helbide bat erabiltzeari uzten zaion bakoitzean *out of flux* dagola esan daiteke [W. and R., 2007].

Fast-flux teknikaren barruan *single-flux* eta *double-flux* daude.

Single-fluxen proxy moduko bat dago, *fluxing agentea* deritzona, (M) makina batek DNS zerbitzariari galdegingo dio *dominioa.com* non dagon,(A) xx.xx.xx.xx IP helbidearekin erantzungo dio, horrekin A makinara joko du, fluxing agentea dena, eta hark "mothership" izenekora, hau da edukia edo helburu zerbitzaria duen makinara, M makina. Hurrengo atzipenean TTL txikia denez, lan berdina egingo da baina DNS zerbitzariak (B)yy.yy.yy.yy IP itzuliko dio, hori izango da orain fluxing agentea.

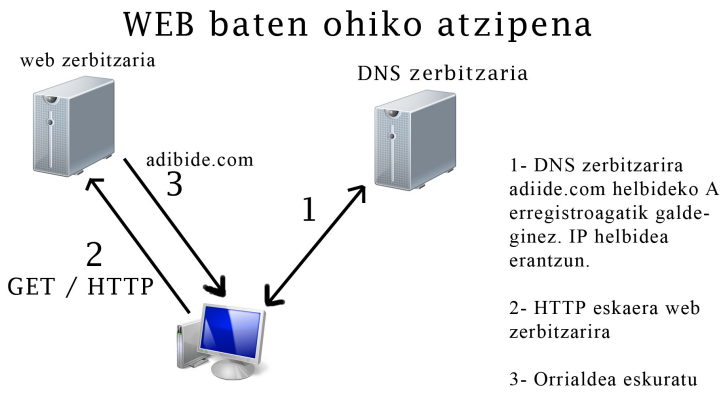
Double-fluxean ere single fluxean antzera jokatzen da baina DNS zerbitzari ugari daude, hau da, NS erregistroak editatzen dira ere. Datuen erredundantzia egiten da. DNS zerbitzariak botnetaren parte izaten dira edo botmasterraren menpe daude, ez dira hornitzaileren batenak. Horretarako *authoritative* DNS zerbitzaria ere kontrolpean izan behar da [Zhang et al., 2011].

Aipatutakoaren ikus dezakezue 3.8 eta 3.9 irudietan, eta atzipen normala erakusten duen 3.7 irudiarekin konparatu.

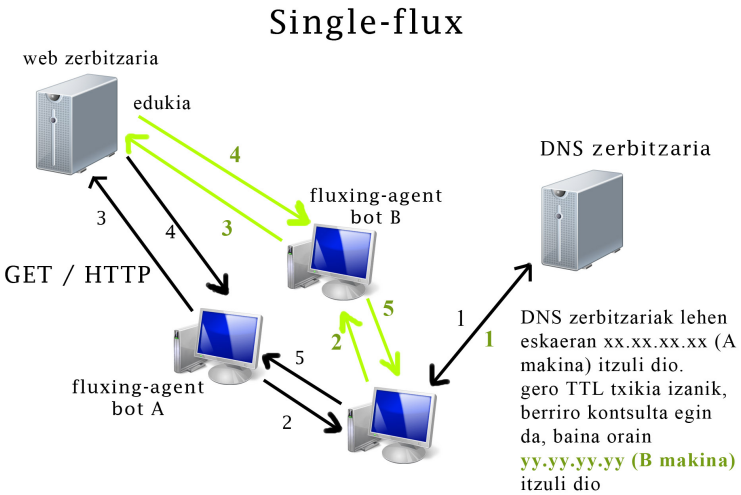
Beraz, fast-flux teknikaren bitartez aginduak makina ezberdinetatik (IP ezberdinetatik) igaro eta gero jasotzeko aukera dago, horrek zaildu egiten du zerbitzari kontrolatzailea (fluxing teknikan *mothership* izenekoa) atzematea. Hau da, zerbitzari ezberdinak eduki daitezke, eta horiek flux agente moduan erabili, botak horietara konektatzeko.

Fast-Fluxek domeinu bakarra izanez gero badu haustura edo hutsegite puntu zehatz bat. Biziraupen luzeagoa izateko domain-flux teknika hobea da. Automatikoki eta periodikoki domeinu multzo bat sortzen da IP bat esleitzen zaiona. Domeinuak sortzeko algoritmo bat inplementatzen dute.

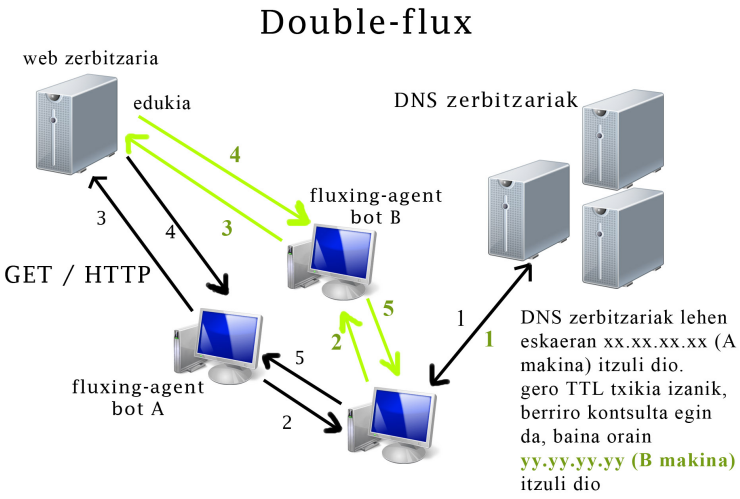
Torpig izeneko botnetak bere botetan algoritmo bat du uneko astea eta urtea erabiliz domeinuak sortzeko, *asteaurtea.com* eta *asteaurtea.biz* izeneko domeinuak ditu adibidez. Botek gerora sortu dituzten domeinu horiek erabiliko dituzte zerbitzari kon-



3.7 Irudia: Sareko webgune baten ohiko atzipena



3.8 Irudia: Single-Flux eskema



3.9 Irudia: Double-flux eskema

trolatzailera konektatzeko. Konektatzea lortu ezean, *eguna.com* edo *eguna.info* eta horrelakoekin saiatuko dira, eta horiek ere hutsegitekotan fitxategi batean dituzten domeinu batzuk erabiliz saiatuko dira zerbitzarira konektatzen [Zhang et al., 2011].

Aipatutako teknikek asko zailtzen dute atzematea.

IP spoofing eta DNS spoofing

Bi teknika hauei esker erasoen jatorria ezkuta daiteke. Hau da, makina batetik egindako erasoari IP faltsu bat edo beste makina baten IP bat esleitu ohi zaio askotan, honekin ezkutatzeaz gain erasoak ere arrakasta izan dezake segurtasun neurrien aurrean baimendutako IP bat aukeratzen badu. DNS-arekin berdin antzekoa da, faltsifikatu egiten dituzte bestelako IP batera jo dezaten.

Hori eginez bot-ak eta zerbitzariak ere ezkutatu ditzakete.

Zifraketa

Lehenago aipatu da RBot izan zela komunikazioei zifraketa ezarri zien lehen bota [Parolli, 2011]. Zifraketaren bidez bidaltzen diren aginduak ezkutatzeaz gain, hijackinga saihesteko ere balio du.

Prozesuak eta aplikazioak ezkutatzen

Aplikazioak eta prozesuak ezkutatzeko Rootkit izeneko tresnak erabiltzen dira. Sistemaren kudeaketa tresnak ordezkatzen dituzte eta horrela mantentzen dira ezkutuan sistemaren kontrola hartzea ahalbidetuz. Sistemaren inguruko informazioa ere truka dezake. Rootkitei esker backdoor sarbideak eraiki daitezke.[INTECO, 2006].

[Kola, 2008]-k nabarmentzen du Hidden32.exe. Tresna hau erabiltzen da interfaze grafikoa duten aplikazioak ezkutatzeko. HideUserv2 izenekoak aldiz erabiltzaile ezkutu bat gehitzen dio talde administratzaileari. Spybotaren kasuan geroz eta gehiago dira FU Rootkit delakoaren bertsioak dakartzaten botak. Rootkit horrek prozesuak ezkutatu eta baimen altuagoak eskaintzen dizkiot bot-ari [Canavan, 2005].

Beraz tresna horiei esker boten kontrola hein handi batean iztukuan egin daitekeela esan daiteke.

Anti-A/V

Botek duten biziraupenerako duten tresna ahaltsuenetako bat antibirusen aurkako tresnak dira. Askok antibirusa eten egiten dute eta ezin da eguneraketarik egin, antibirus ezagun gehienak atzeman eta desaktibatu egiten dituzte, antibirusekin zerikusia duten webguneak ere blokeatzen dituzte batzuek, esaterako Agobotak hori egin dezake. Beste askok, ez dituzte desaktibatzen, hau da, badirudi martxan segitzen dutela baina berez ez dute ezer egiten. Beraz, horri esker ezkutatu egiten dira eta bestetik ordenagailuan zerbait arraroa dagola pentsatuz gero, antibirusak ez duenez ezeren berri eman normalean erabiltzaileak ez du pentsatzen kutsatuta dagoenik. [Kola, 2008]

SpyBotak adibidez `kill_av()` funtzioa erabiltzen du, horren bidez eta antibirus eta segurtasun aplikazioen zerrenda bat erabiliz, segurtasun neurriak indargabetzen ditu [Canavan, 2005].

3.4.3 3. Fasea: Erasotu

Behin botari aginduak bidaltzeko ezarritako bidea segurua denean, hau da, 2. fasea eta gero, bota prest dago erasoak egiteko. Botak aginduak jaso, exekutatu eta emaitzak itzuliko ditu zerbitzarira botmasterrak emaitzak jaso ahal izateko. Aginduak jasotzeko

eta emaitzak itzultzeko modua ez da beti berdina, C&C egituraren araberakoa izaten da, botnet mota bakoitzean komunikazio hori nolakoa den 3.2 atalean azaldu da.

Bot familiaren araberakoa da aurrez prestatuta dauden agindu multzoa, baina agindu berriak gehitzeko aukera ere izaten da, beraz, eraso berriak egiteko aginduak gehi daitezke edo eta urrunetik botean bertan tresna berriak jaitsi eta instalatu.

Erasoen artean azpimarratzekoa da, 3.4.1 atalean aipatutako teknika eta eraso asko egiten direla, egindako erasoaren arrakasta bot kopuruaren arabera hazi egingo baita, esate baterako, bot guztiek ahuleziak eskaneatuz gero errazago aurkituko dituzte makina ahulak. Era berean pasahitzak hausterakoan eta horrela hedatzeko beste metodoekin ere.

3.2 atalean aipatu dira erasoen helburuak zeintzuk diren. Baina hemen helburua baino, eraso horien zenbait adibide eta eraso horiek egiteko zenbat modu azalduko dira, era berean erraz ikusiko da botneten bitartez egindako eraso batek botnetik gabe egindakoak baino askoz ahalmen handiagoa izateaz gain, ezkutatzeko aukerak ere handitu egiten dituela.

DoS/DDoS egiteko moduak

Zerbitzuak eteteko eraso ezberdinak daude, baliabideak gainkargatzea esate batera, hala nola, banda zabalera, CPU, memoria, diskoko espazioa... Adibidez, banda zabalera gainkargatzen duten erasoek TCP/IP konexioa gainkargatzen dute. Izugarrizko pakete pila bidaltzen dute zerbitzarira sareko trafikoa handitzeko eta sarea itotzeko. Aldiz, sistemaren baliabideak gainkargatzen dituzten erasoek, sarea trafikoz gainezka jarri beharrean, makinak sarera konektatzeko dituen baliabidea erosotu ohi dituzte normalean. Hala nola, pakete iritsierarako bufferrak, irekitako konexioen taula eta antzeko memoria egiturak.

Botneten bitartez ahalmen handiagoa dago hori egiteko, azken finean bot askotatik egiten baita erasoa eta eskaera, trafiko edo dena delakoei ezin izaten diote erantzun baliabideek. Ondorengo zerrendan egin ohi diren eraso batzuk dira ondorengoak:

- **Uholde erasoa: flooding**

  Eraso honen helburua jo puntu den edo erasoa jasango duen antolakundearen sare konexioa itotzea da. Erasotzaileak ahalmen handiagoko sare konexioa

edukita ahalmen txikiagoa duen bat erasotzen du, bigarren horrek jasa ezin duen trafiko kopurua sortuz. Nahikoa da *ping* komandoa erabiltzea uholdea sortzeko.

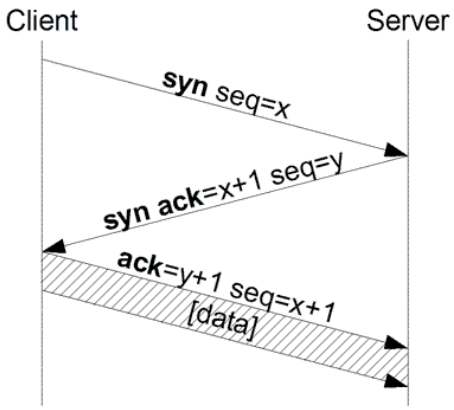
Adibidez ping bidez egindako uholdeak erasotzailearen ikuspuntutik bi desabantaila nagusi ditu. ICMP paketeetan jatorrizko makinaren helbidea agertzen da. Horrek, batetik erasotzailea identifikatzen du. Bestetik, erasotua den makinak ICMP echo eskaera paketeak erantzungo ditu eta erasoa erasotzailearen makinan islatuko da, hau da, ispilu bat izanen da, berak sortu duen trafikoari eginiko erantzunen eragina jasango duelako. Hala ere, erasoa botnet bidez eginda, erasotzailearen helbidea atzematea ez da izanen horren erraza eta ispilu efektuak ere ez dio botmasterrari eragingo, botari baizik. Gainera, jatorriko helbidea ezkutatzeko aipatu den IP spoofing teknika erabil dezakete esate baterako 3.4.2 eta bidenabar, ispilu efektua desagertu egingo da, erantzunak jatorriko helbide faltsura bideratuko direlako.

Badago uholdea ICMP bidez egiterik, hau da, **ICMP uholdea**. Lehenago ere aipatu da ICMP *echo* erantzun paketeen bidez eginiko erasoa. Zerbitzari batzuetan firewallen bidez ping egiteko aukera saihesten hasi dira. Horren ondorioz, erasotzaileak bestelako ICMP paketeak hasi dira erabiltzen. Horiek ezin dira firewallaren bidez galarazi, edo ez da inondik ere komeni, TCP/IP sareen funtzionamendurako ezinbestean erabiltzen direlako eta hauek iragaztearen ondorioz sarearen portaera aldatuko litzatekeelako.

ICMP peketeak erabiltzearen alternatiba izan daiteke **UDP** paketeak bidaltzea portu jakin batera (zerbitzu garrantzitsu bat izan daiteke) biratuta. Eraso hauetan ere jatorrizko helbide faltsua erabiltzen da ICMP paketeekin egiten diren erasoetan bezala. Eraso honetan jatorriko helbide faltsuaren bitartez ere *Smurf* erasoa egin daiteke. Hau da, erasotua ez da eskaerak jasotzen dituena, eskaeren erantzunak baizik. Horregatik eskaerak Broadcast helbide batera bidalita, sare horretako makina guztiek jatorrizko helbide faltsuari erantzungo diote, izan daiteke web zerbitzari bat. *Anplifikatutako* eraso bat dela esaten da, hau da, makina bakoitzak N erantzun eragiten ditu, 1:N eskaera-erantzun sortuz [Mirkovic et al., 2004].

- **TCP SYN uholdea: SYN Flood**

  Eraso mota hau ulertzeko, TCP konexioak ezartzeko erabiltzen den *3 urratseko akordioa* deritzon prozesua gogoratu behar dugu. Bezeroak TCP konexio baterako eskaera egiten du SYN paketea zerbitzariari bidaliz. Honek, bezeroaren helbidea eta portu zenbakia gordetzen ditu besteak beste TCP konexiotarako taula batean,



3.10 Irudia: 3 urratseko akordioa

hasierako sekuentzia zenbaki bat ezartzen du eta eskaerari erantzuten dio SYN-ACK pakete batekin. Bezeroak hau jasotzean, ACK pakete bat itzultzen dio zerbitzariari sekuentzia zenbakia inkrementatuta. Zerbitzariak azken pakete hori jasotzean TCP konexioa ezarrita geratzen da. Ikusi 3.10 irudia.

Esate baterako eraso hauetan sareko zerbitzari batek TCP konexio eskaerei erantzuteko duen ahalmena gainkargatzen dute, konexio horiek kudeatzeko erabiltzen diren taulak betetzea da erasoen helburua. Taula betez gero, hurrengo TCP konexio eskaerek huts egingo dute. Nahikoa da oso denbora motzean helburuko konputagailuari TCP konexio eskaera asko bidaltzea zerbitzaria kolapsatu arte Horri horrela, iristen diren benetako bezeroen konexio-eskaerek Denial of Service erantzuna jasoko dute, hau da, konexioa ukatuko zaie [Rivadeneyra, 2004]. TCP konexioa eskaera gehiago ireki ezin ahal izateak sareko aplikazio gehienez eragiten die, FTP, SMTP, Telnet... Eraso hau eraginkorra izateko, konputagailu askok parte hartu behar dute, era koordinatuan beren konexio-eskaerak jomugara bidaltzeko. Horregatik eraso hau aurreko egiteko ezin hobeak dira botnetak.

Eraso hauek guztiak egiteko esan bezala botetan tresna bereziak instalatu daitezke edo eta batzuek dagoeneko badituzte eraso horiek egiteko zenbait agindu berezi.

Bista eta klik iruzurra

Nahikoa da webgune jakin bateko iragarki batean klik egingo duen script xume bat programatzea, gero hori bot bakoitzetik exekutatu behar izaten da IP helbide ezberdinetatik egin dadin bisita. Egia da ere denbora tarte laburrean kolpe batez edo

bat batean bisita edo klik asko badaude susmagarria dela ere, beraz, hori zaintzea komeni zaio ere botmasterrari.

Nortasun lapurreta

Modu zuzenena botei sniffer bat jartzea da, modu horretan makina horietan sartzen diren datuak eskura daitezke. Beste tresna bat keyloggerrak dira.

Datuak lortzeko beste modu bat erasoa webgune faltsu baten bitartez egitea da, alegia, phishinga egiteko webgune bat edo formulario bat, eta normalean benetazko zerbaiten antza izan behar du, hau da, banku baten webgune batena, administrazioarena, denda batena edo dena delakoarena. Beraz, gizarte ingeniaritzak bere paper oso garrantzitsua du horretan. Eta botnetak aldiz, lagun dezake webgune faltsu hori bizirik mantentzen (adibidez aurretik aipatutako fast-flux eta domain-flux tekniken bitartes), edo webgune horren itxura duen bat abiarazten makinetan, edo lagun dezake jendeak webgune horiek bisita ditzan spam bidez kanpaina bat egiten ...

Spybot familiako bot guztiek dituzte snifferrak edo eta keyloggerrak, baita pantailaren irudiak eskuratzeko komandoak. Zeus botak esate baterako baditu mota horretako tresnak, nahikoa da agindu bat bidaltzea eta botak emaitza itzultzen du informazioarekin, botnet berriek *man in the browser* teknika erabiltzen dute, honek webgune faltsu bat edo webgune originalaren formularioko eremuaren gainean bikoitutako eremu batzuk aplikatzen ditu. `webinjects.txt` fitxategia irekiz gero ikus daiteke banku eta denden webguneetan injektatzen dituen eremuak, adibidez:

```
set_url https://www.e-gold.com/acct/li.asp
data_before
e-mail:</font>
data_end
data_inject
data_end
data_after
</font>
data_end
```

3.4.4 4. Fasea: Mantenua eta eguneraketak

Fase honen helburua ere botnetaren biziraupena da, komunikazioa ezkutatzearen aldetik ordez, botak berak behar dituen tresnei dagokienean, eguneraketak eta mo-

duluak kutsatutako makinara pasa eta instalatzea, botaren bertsio berriak instalatzea. Adibidez, erabiltzaileak antivirus berri bat jartzearen arriskupean, edo adibidez, atera berri den Windows-eko eguneraketa bat instalatu baino lehen, horri aurre egiteko botari zenbait tresna berri eta eguneraketa egitea izan liteke fase honetako ataza bat.

3.5 Nola aurre egin

Botnetei aurre egiteko zenbait babes neurri azalduko dira Batzuk kalteak saihesteko neurriak dira eta beste batzuk dagoeneko jasandako kalteak eta eraginak konpontzera bideratutakoak.

3.5.1 Nola babestu eta saihestu

Atal honetan babesteaz ari denean, botnetaren parte ez bilakatzeaz ari da, hau da, makina bot bat ez bihurtzea galarazteaz.

Hortaz, lehen botnetek hedatzeko dituzten teknikei nola aurre egin eta hauen aurkako neurri batzuk proposatuko dira hemen. Hala ere, argi eduki behar da makina bat ez dela inoiz 100% seguru egongo, are gutxiago Internetera konektaturik badago. Batetik, egunero agertzen direlako mehatxu berriak eta egunero eboluzionatzen delako,eta bestetik, beti zirrikitu txikiren bat dagoelako, alegia,adibidez lehen aipatu bezala, gizakiak nola jokatuko duen ere ezin da ziurtatu %100ean.

Hori horrela, ondoren aipatuko diren neurrien artean [INTECO, 2007, Daniel Plohmann, 2011, Mallery et al., 2005, Rajiv, 2012, Dunham, 2009, Leder et al., 2009], neurri zehatzak baino, zein esparru kontutan hartu behar diren aipatuko da. Ez du zentzu handirik esparru batzuetan neurri zehatzik gomendatzea, finean, bakoitzak segurtasun neurriak bere behar eta aukeretara tekniko zein ekonomikoetara egokitu behar baititu. (Kontutan hartu neurriak smartphone eta tablet makinetarako ere)

- Kudeatu erabiltzaile kontuak eta baimenak. Hau da, erabiltzaileei beharrezko baimenak esleitu bakarrik. Berrizendatu administratzaile erabiltzailea eta ezgaitu erabiltzaile gonbidatua.
- Zaindu aplikazioek eta zerbitzuek duten sarera eta sistemara duten sarbidea, zaindu zein portu dauden irekita eta barrurako zein kanporako trafikoa. Hori

firewall baten bitartez egin daiteke. Adibidez, hein handi batean IRC trafikoa blokeatuz gero IRC botnet baten parte izatea saihestuko daiteke.

- Bot-en pasahitzak hausteko tresnei zailtasunak jarri. Horretarako pasahitzen sendotasuna bermatu eta aldatu aldian behin, hau da, ez jarri pasahitz errazak. Hona gomendio batzuk: gutxienez 8 karaktere erabili, ez erabili informazio pertsonala (izena, jaiotze data...) pasahitza sortzeko, erabili karaktere alfanumerikoak eta ikur bereziak. Horiek dira leku gehienetan ezartzen diren gutxieneko baldintzak [Microsoft, , SANS, , INTECO, b].

- Pasahitzak eta datu pertsonalak sartu behar diren lekuetan erabili protokolo seguruak, https, ssh...

- Esan dugu birusek, bestelako troiarrek edo eta harrek utzitako ahuleziak probestu ohi dituztela askotan botnetek. Horri aurre egiteko antibirus eta anti-malware bat jarri. Anti-malware edo eta antibirus produktu batzuek anti-spam eta suhesia(firewall) ere eskaintzen dute.

- IE baino nabigatzaile seguruago bat erabiltzea gomendatzen da. Firefox edo Chrome esate baterako.

- Aldatu pasahitza wifi sareari, erabili WEP baino zifraketa sendoagoak eta konektatu behar dituzun makina kopurua bakarrik baimendu.

- Sistemaren eguneraketak instalatu.

- Ez instalatu erabiliko ez diren edo behar ez diren aplikazioak.

- Ez instalatu, jaitsi fidagarriak ez diren aplikazioak.

- Ez bisitatu fidagarriak ez diren webguneak

- Ez ireki e-mail arraroak edo eta spam deritzona. Anti-spama izanez gero hobe.

- Ezgaitu bluetooth eta infragorriak ez bada beharrezkoa. Ez ireki SMS eta MMS arraro eta ezezagunak.

Aipatu diren neurriak gomendio orokorrak dira, etxeko zein erakundeetako makinetan hartu beharrekoak, gerora bakoitzak bere modura konfiguratu beharko dituenak esan bezala. Hala ere, aipatutako neurri batzuk, ikus daitekeen bezala oso lotuak doaz

gizakiaren erabakietara, hau da, ez ireki e-mail *arraroak* bezalako neurriak, horrelako neurriak norberaren esku daude eta kontzientziazio maila bat eskatzen dute.

Bestetik, badira bestelako neurri batzuk, zenbait zerbitzarietarako gomendagarriak direnak aipatutakoaz gain.

- Pasahitzak hausteko ahaleginak zailtzearren, ez erabili berezko SSH portua (22). Ezgaitu *root* erabiltzailearekin sartzea, hau da, bestelako erabiltzaile batekin sartu eta gerora root bihurtu. *Door-knocking* teknika ere egokia izan daiteke eta ez du atzigarritasuna mugatzen.
- Root erabiltzailearekin sartzen saiatzen denaren eta saiakera oker asko egiten dituenaren IP helbidea blokeatu, lista beltzak erabili. Hori egiteko zerbitzu asko daude, hala nola, *denyhosts*[16].
- Ez desaktibatu log fitxategiak. Hauek gainbegiratzea gomendagarria da, horrela jakin daiteke ea zerbitzariaren aurkako sartze saiakerak egon diren ala ez eta bestelako erasorik egon ote den ere.
- Erabili IDS (Intrusion Detection System) bat, esate baterako *snort*[17].
- Zerbitzariko firewall batean, galarazi guztia eta gero joan baimentzen beharrezkoa dena bakarrik. Politika hori jarraitzea gomendatzen da.

Aipatutako neurri batzuek atzigarritasuna muga dezakete, baina ez asko, aipatutakoak baino neurri zorrotzagoak eta konplexuagoak ere har daitezke, hala ere, botneten kutsatzea zailtzea eta erabileraren erosotasunaren artean oreka bat bilatu behar da, baliabidearen atzigarritasuna bermatu behar da. Kontutan hartu, orduan eta konfidentzialtasun eta osotasun gehiago, atzigarritasuna orduan eta mugatuagoa izango dela.

3.5.2 Nola atzeman eta suntsitu

Nola atzeman esaten denean bi aukera aztertuko ditugu, bat nola jakin makina bot bat dela eta bestetik, nola atzeman botnetak sarean, bigarren hau, interneten orokorrean aurki daitezkeen botnetak atzemateko sarean eta munduan aurki daitezkeen proiektuekin lotuta dago.

[16] http://denyhosts.sourceforge.net/
[17] http://www.snort.org/

Makina bot bat da?

3.5.1 atalean aipatu da %100ean ezin dela makina bat babestu, hortaz, makina bat botnet baten parte izatekotan nola atzeman? Batzuetan oso nabarmena da jasan den kalteagatik birus edo bot edo eta malwareren batek makina kaltetu duela, esatera, mezu bat ateratzen delako, makinan ezin direlako gauza asko egin... Hala ere, bot bat izanik, normalena da makina hori beste makina batzuk erasotzeko baliatzea, beraz, ezkutuan eta susmorik piztu gabe mantenduko da makinan.

Hala ere, badira botnet bat makinak bot bat izan eta botnet baten parte izan daitekeenaren susmoa izateko aztarnak edo zantzuak.

Bot gehienek exekutagarriak kokatzen dituzte `C:\Windows\System32` direktorioan [Schiller and Harley, 2007]. Hala ere, erabiltzaile arrunt batentzat hauen berri izatea eta horietaz jabetzea ez da erraza, hau da, fitxategi konkretu batzuk bilatu beharko lirateke, eta ezin aldiro begiratzen ibili ezta ere. Beraz, noiz edo zeri esker jakin daiteke makina bot bat dela?

Esan daiteke ez dela hain erraza, aipatu ditugun ezkutatzeko teknikak nahiko konplexuak direlako, hau da, antibirusa desaktibatzea, tresna bera ezkutatzea etab.

Adibide batzuk jar daitezke bot batek makina hartzean askotan agertu eta gertau ohi direnak, erabiltzaile arruntentzat hauek dira gutxi gora behera nabaritu ditzakeenak:

- Internet oso mantso joatea (oso probablea da botneta ez den beste zerbaitengatik izatea ere).
- Antibirusa desagertu izana.
- Antibirusa ezin eguneratu ahal izatea edo eta antimalwareen webguneetara ezin sartu ahal izatea.
- Iragarkiz josita egotea, baita nabigatzailea ireki gabe iragarki leihoak irekitzea.
- Prozesu arraroak ikustea Windowseko atazen administratzailean. (honetarako ordea gutxieneko prozesu batzuk ezagutu behar dira).

Hala ere, aipatutakoak malware ezberdinek sor ditzaketen ondorioak dira, edo eta kudeaketa txar batek ere, beraz, susmo hartzeko bakarrik balio dezake, horrekin ezin da ziurtatu makina botnet baten parte denik.

Aukera bat izan daiteke, makina DoS, spam edo antzeko ekintzetarako erabiltzen bada *abuse e-mail* izeneko e-maila itxarotea, horrelako e-mailen bitartez jakinarazi ohi da makina sarearen erabilpen txar bat ari dela egiten, trafiko gehiegi sortzen duela, sarea itotzen duela etab.[Schiller and Harley, 2007]. Horrelako mezuak zerbitzaria dutenek jaso ohi dituzte. Horrelako zerbait jasoz gero, lehen bait lehen internetetik deskonektatu eta garbitu makina.

Beste aukera bat etxeko erabiltzaile edo erabiltzaile arrunten artean ohikoa ez bada ere, bestelako esparru batzuetan, IDS sistemak dira, Snorti esker esate baterako, sarkinak atzeman daitezke eta horrek lagundu dezake. Hala ere, Snort tresna konplexua da.

Ez da erraza erraza makina botnet baten parte den jakitea, horregatik, gehienetan hobe da babestu sendatu edo konpondu baino. Tresna asko daude eta teknika asko botnetak atzemateko baina oso konplexuak dira. Ongi babestea da konponbide onena.

Botnet ehiza

Badira ikerlari taldeak, aditu taldeak, sarean eta munduan barna, botneten sare portaeran edo eta ondorioetan oinarrituta batik bat botnetak atzeman eta hauek suntsitzeko tresnak eta proiektuak garatu dituztenak eta etengabe teknika berrien bila dihardutenak.

Haien lanari esker, botnetak atzematen dira eta botneten inguruko informazioa jasotzen da. Horrek, batetik, martxan dauden zenbait botnet suntsitzeko balio du, bestetik, hartu behar diren babes neurrien inguruko gomendio gehiago egiteko informazioa ematen die adituei.

Beraz, teknika, tresna eta proiektu ezagunenak aztertu eta haien helburuak azalduko dira ondoren, teknika gehienak nahiko konplexuak dira orain arte etengabe azpimarratu ditugun botneten ezaugarriengatik.

- *Honeypot*ak ahuleziak dituzten sistemak simulatzen dituzten sistemak dira. Mota ezberdineko honeypotak daude, zerbitzariak, bezeroak... Haien helburua erasotzaileen arreta deitu eta egiten dizkieten erasoen bitartez erasotzaileek erabiltzen dituzten teknikak eta ezaugarrien informazioa biltzea da. Askotan ere, uzten duten arrastoagatik infektatutako sistemak atzematera iris daitezke. Honeypotek erasotzaileen ekintzak gordetzeko eta monitorizatzeko tresnak dituzte.

- *Honeynet*ak honeypot bereziak dira, hau da, honeypot ezberdinez eraturik dauden sareak dira, horrela aldi berean aztertu daitezke botnetak baina sare batean duten portaera aztertzeko aukera ere ematen du.

Honeypotak eta honeynetak erabiltzen dituzten erakunde eta proiektu ezagunenak:

- *honeynet.org*[18]
- *shadowserver.org*[19]
- ATLAS[20] (*Arbor Networks*)
- GHH[21] (Google Hack Honeypot)
- *HoneyBot*[22]
- *Dionea*[23]

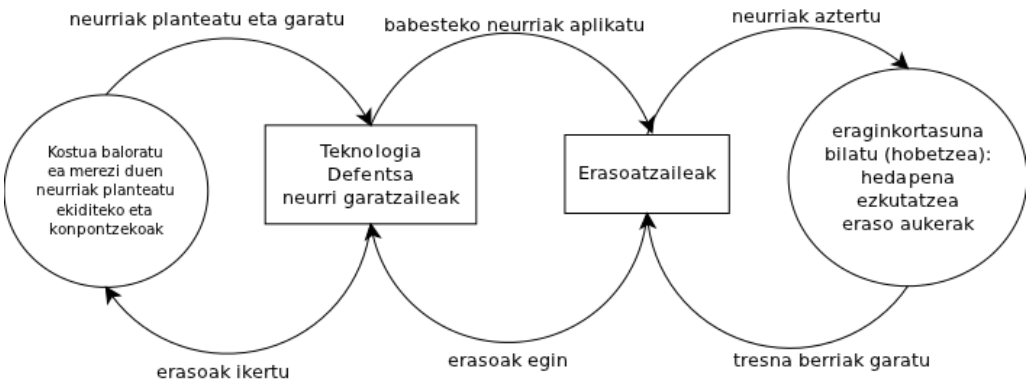
Denbora errealean,mapa batean, munduan zehar banatutako honeypotei esker erasoak ikus daitezke `http://map.honeynet.org/` helbidean, baita `http://atlas.arbor.net/worldmap/index` helbidean ere.

Honeypotez gain, IDS eta snifferrei esker ere jakiten dira botnet baten ezaugarriak [Gu et al., 2008].

DNS Sinkhole teknika ere gero ezta ezagunagoa da da botnetak osorik suntsitzeko. Botak konektatzeko puntua kontrolatzen saiatuko da. Hau da, botak zerbitzari batera konektatzen badira, sinkhole bitartez beste leku batera (ikertzaile edo anti-malware antolakundeen zerbitzari batera) konektatzea lortuko dute DNS-aren konfigurazioetan aldaketak eginez. Horrela jakingo dute gainera botnetak zenbat bot dituen, zein motatakoa den... Hau ISPek egin ohi dute bezeroren batek botnet edo bestelako malwareren bat erabiltzen duenaren susmoa dutenean [David, 2004].

Darknet edo *blackhole* izeneko teknika ere erabili ohi da trafiko susmagarria klasifikatzeko. Makina bateri ere ez dagokion IP multzo bat da, baina birbideratze taulan

[18] `http://honeynet.org/`
[19] `http://www.shadowserver.org`
[20] `http://www.arbornetworks.com/es/atlas.html`
[21] `http://ghh.sourceforge.net/`
[22] `http://www.atomicsoftwaresolutions.com/honeybot.php`
[23] `http://dionaea.carnivore.it/`



3.11 Irudia: Teknologia garapena, defentsa neurriak eta eraso berriak

erregistroak ditu. IP helbide multzo horretara bideratuta doan trafiko oro susmagarritzat jo ohi da [David, 2004].

Batzuetan zenbait ikerlari botnetetan infiltratzen dira [Cho et al., 2010], hau da, botnet baten parte bilakatzen dira bere portaera barrutik aztertu eta kontrola eskuratu eta botneta suntsitzeko [Daniel Plohmann, 2011].

Sare trafikotik jasotako datu multzo handiei datu meatzaritza aplikatuz aurrerapenak egin dira ere, makina bat botnet baten parte den edo ez jakiteko sailkatzaileak garatu dituzte [Strayer et al., 2008].

Beraz, botnetei aurre egiteko geroz eta baliabide eta teknika gehiago garatzen dira, geroz eta inplikazio handiagoa dago erakunde zein adituen partetik. Hala ere, esan daiteke botneten eboluzioa oso azkarra dela ere eta botnet garatzaileen eta botneten aurkako taldeen arteko lasterketa bat dagola martxan, alde batetik aurrerapen bat dagonean bestetik ahalegin osoa egiten da hori gainditzeko, beraz, batak bestearen aurrerapenei hobekuntza eta trikimailu gehiagorekin erantzuten dio. Arma lasterketa bat dagola esan daiteke, ingelesez *arms race* izenarekin ezagutzen dena. 3.11 irudian duzue lehia horren eskema bat. Garestiagoa da defentsa garatzea erasoa baino, azken finean erasotzaileek dagoeneko garatuta dagon teknologian bilatu ohi dituzte zirrikituak eta dauden tresnei bestelako erabilpen bat emanez kalteak sortzeko tresna bihurtzen dituzte. Argi izan behar da, defentsa mekanismo on bat izan behar du ahalik eta kostu txikienarekin erasoa geratzeko gai dena, kasu batzuetan merkeagoa da kaltea konpontzea erasoa saihestea baino, normalean botneten kasuan ez, kalteak handiak izaten baitira. Erasotzaileek ere berdina bilatzen dute, kostu gutxienarekin kalte handiak edo etekin handiak lortzea. Beraz, teknologia eta neurriak garatzen diren heinean mehatxu berriak azaltzen dira.

3.6 Arazoaren dimentsioa

Atal honetan azaltzen diren datuek erakusten dute arazoa izugarri handia dela, herrialde guztietako erabiltzaileei eragiten diela, milaka eta milaka daudela kutsatuta, batzuetan milioika ere, milioika spam sortzen dela boteneten bitartez...

Bestetik, orain arte egin diren botneten aurkako operazio esanguratsuenak aipatzen dira, operazio horiek ez dira batere xumeak, talde eta erakunde ezberdinen elkarlana ezinbestekoa izaten da.

3.6.1 Azken urteetako datuak

2006an Symantecek urtarriletik uztaila bitarte eguneko 57.717 bot aktibo atzeman zituen, ikusi 3.13[24] grafikoa. Kontutan hartu benetako zenbakia askoz handiagoa dela, ezin baitira munduko botnet guztiak atzeman.

2010ean *threatsense.net Early Warning System* sistemaren datuen arabera, 200 erabiltzailetik batek baino gehiok IRC/SDBot bota zuen, 2009ko kopuruaren bikoitza. Hauek dira ESET produktuen bidez atzemandako malwarean aurkitutako bot portzentajeak 2009 eta 2010ean [ESET, 2010]:

ESET produktuen datuak	**2009**	**2010**
IRC/SDBot	%0.24	%0.49
Win32/IRCBOT	%0.15	%0.24
Win32/ZBot	%0.09	%0.18

2010eko Symantecen segurtasun txostenak dio 2009an AEB zela botnet aktibitate gehien zuena, bigarren Txina, hirugarren Brasil eta laugarren Alemania [C. et al., 2010]. AEB azken urteetan lehen hiruen artean egon da, hala ere, 2011an Taiwan eta Brasilek bot gehiago zituzten, %17 eta %13 hurrenez hurren, ikusi 3.12.

Badirudi AEB eta Alemaniaren beherakada Rustock izeneko botnetaren suntsitzearen ondorio izan zela. Horrekin lotutako datu bat aipatzearren, Rustock botnetak sareko spamaren %60 sortu zuen 2010eko abuztuan [Symantec, 2011].

Etengabe botneten inguruko estatistikak eguneratzen dituzte `http://www.shadowserver.org/` helbidean ere. Interesgarria da ere denbora errealean atzematen diren botneten

[24] `http://www.symantec.com/threatreport/archive.jsp` helbidetik aterata

Source	Rank	Percentage
Taiwan	1	17%
Brazil	2	13%
United States	3	10%
Italy	4	9%
Hungary	5	7%
China	6	7%
Poland	7	6%
Germany	8	5%
Japan	9	5%
Argentina	10	3%

3.12 Irudia: Bot aktiboak 2011an [Symantec, 2011]

inguruko irudia ikusteko ematen den aukera `http://map.honeynet.org/` helbidean, baita `http://atlas.arbor.net/worldmap/index` helbidean ere.

Bestelako datu esanguratsuen artean, botneten hedapen teknikak dira interneteko *bigarren mailako soinu* (ingelesez *background noise*) eragileak, bereziki TCP 135 eta TCP 445 portuetan `honeynet`.

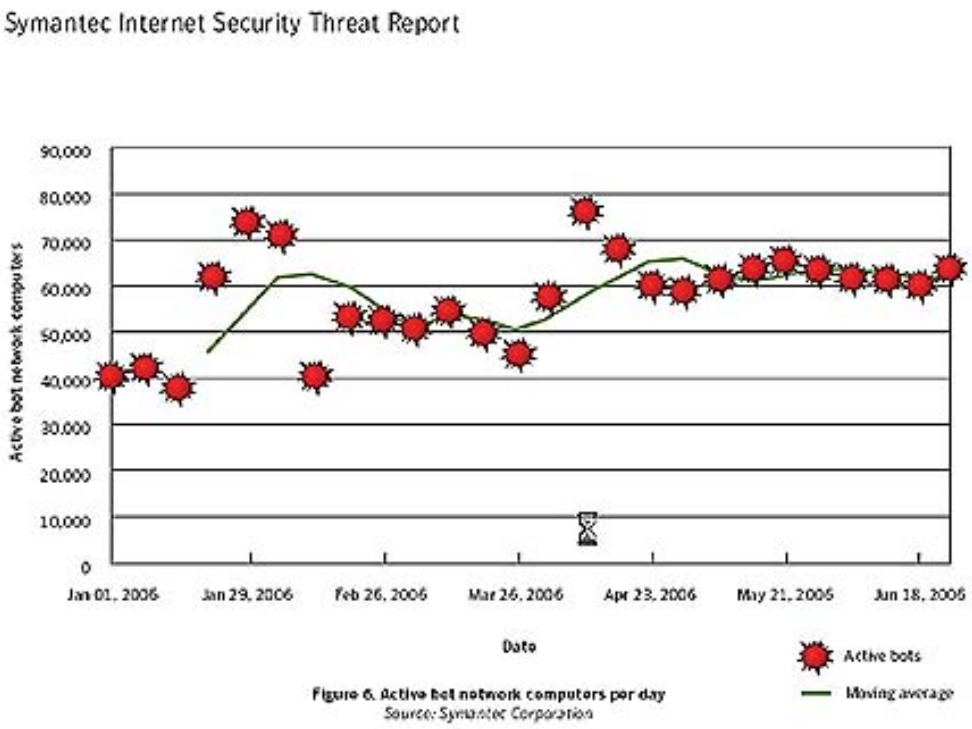
Argi dago botnetak direla malware ahaltsuenak eta eraso gehien sortzen dituztenak gaur egun, kalte handiak eragiten dituztela ordenagailuetan eta eragina dutela sarearen funtzionamenduan. Azken urteetan botneten gorakada izugarria izan da, eta adituek diotenez oraindik kopurua hazi egingo da.

Bestetik, nabarmendu behar da Rustock botnetaren kasuak erakusten duela botnet bat eteteak zenbat jaisten duen spam edo eta bestelako malware batzuen eragina.

3.6.2 Botnet ezagunak eta haien aurkako operazioak

Atal honetaraino aipatu da botnetak arriskutsuak direla, botneten ezaugarri nagusiak eta bot familia nagusiak aipatu dira, hori guztia islatzen duten zenbait kasu aipatu eta gaiari gaurkotasuna ematen dioten zenbait kasu aztertuko dira orain.

Jarraian aipatuko diren botnetak azken urteotan ezagutu diren botnet ahaltsuenak dira, bai dimentsio aldetik, bai konplexutasun aldetik, baita eragindako kalteengatik ere.



3.13 Irudia: Bot aktiboak 2006an (Symantec-en datuak)

Zeus Botnet

Helburu ekonomikoak lortzeko botnet bat izan zen, frogetan 3.7.3 erabili den Zeus Bot edo ZBot tresnarekin eraikia. Argi dago hori erabiltzaile kontuetako datuak eskuratzeko dituen ezarpenengatik. Zeus 2007an sortu zen, merkatu beltzean erosi (700USD inguru) edo eta *underground* foroetan aurki daiteke [Falliere and Chien, 2009]. Jatorri errusiarra du eta 2007a geroztik eguneraketak egin dizkiote.

2009an Danballak publikatutako txosten baten arabera botnet handiena ZeusBotnet zen, hau da, kontrolpean makina kopuru handiena zuena, 600.000 baino gehiago. [Ollmann, 2009b]. eta Zeus botetik eratorritako botnetak ziren bigarrenak gehien hedatutakoenen artean [Ollmann, 2009a].

Interesgarria da zeustracker[25] proiektua, Zeus erabiliz eraikitako botneten C&C zerbitzariak atzematen ditu.

[25] https://zeustracker.abuse.ch/

Waledac

2009an agertu zen P2P motako botnet bat da. Storm Worm Botnet izeneko botnetaren ondorengo bat da eta 390,000 bot zituen gutxienez. Waledac botnetak ez zuen hedapenerako mekanismo berezirik, hau da, ez zuen ahuleziak bilatzeko tresnarik. Gizarte ingeniaritza baliatzen zuten bere hedapenerako [Stock et al., 2009]. Windowseko sistema eragileei eragiten zien eta Estatu Batuetan zeuden bot gehienak. Windows XP sistemak ziren gehienak.

Estimatzen da Waledacek eguneko 1.5 bilioi spam e-mail bidaltzeko ahalmena zuela. 2009ko abenduaren 3aren eta 21aren artean 650 milioi spam bidali zituela ondorioztatu zuten [Garza, 2010].

Azkenik Microsoft bere Waledacek bere bezeroengan zuen eragina ikusita, Microsft beraren eta zenbait ISPren (Internet Service Porivider) elkarlanari esker botneta eten zuten *b49* izeneko operazioan. Kutsatutako botak garbitzeko, bezeroei laguntza eskainiko zieten CERT (Computer Emergency Response Team) talde bat jarri zen martxan. Gainera Microsoftek jarritako salaketaren ondorio, Waledacek erabiltzen zituen 276 domeinu Microsfoten esku geratu ziren [Microsoft, 2010].

Rustock

Milioi bat makina inguru zituen bere menpe Rustcok botnetak.

Spam asko zabaltzen zuen botneta zen. Sareko spamaren %60 sortu zuen 2010eko abuztuan [Symantec, 2011].

Botnet askok McColo izeneko enpresan zituzten haien C&C zerbitzariak, Rustocken zerbitzari batzuk ere han zeuden, 2008an enpresaren itxiera kolpe handia izan zen, baina hala ere Rustockek bizirautea lortu zuen [Barroso, 2008].

Hilabete asko pasa zituzten Microsofteko zenbait departamentutan Rustocken aurkako lanean, *b107* operazioa prestatu zuten botneta gelditu eta suntsitzeko, 2011ko martxoan gauzatu zen operazioa. Operazio horretan Pfizer, FireEye eta Washingtoneko Unibertsitateak ere hartu zuten parte. Waledacen aurkako operazioaren antzekoa izan zen eta egun kutsatutako ordenagailuak garbitzeko ISP eta CERT taldeekin lanean dihardu Microsoftek [Williams, 2011].

Hain da handia botnet honek eragin zuen kaltea uztailean Mircosoftek 250000 Dolar eskaini zituela botmasterrak harrapatzen zituenarentzako [Boscovich, 2011].

Mariposa

2009an eman zuen bere berri Defence Intelligencek[26].Zerbitzariekin konektatzeko domeinu dezente zituzten, 30 gutxienez atzeman zituzten eta 12 milioi makina kutsatu zituela ikusi zuten botneta gelditzea lortu zutenean,inoiz ezagutu den handiena. 2009ko maiatzean atzeman zuten eta urte bereko abenduan deuseztatzea lortu zuten Mariposa Working Group taldekoek [Thompson, 2010]. MWG taldean Defence Intelligence, Georgia Institute of Technology eta Panda Security enpresek, gehi herrialde ezberdinetako polizia taldeek parte hartzen zuten. Azpimarratu behar da atzeman zutenetik deuseztatzera horrelako botnet handia izateko ez zela denbora asko pasa.

Mariposa botnetaren atzean antolaturiko taldeak zeuden, DDP (Dias de Pesadilla Team) izena zeukan taldeak eta botneta alokatzen zuten. VPN (Virtual Private Network) erabiltzen zuten zerbitzariekin konektatzeko eta horrek zaildu egiten zuen botmasterren jatorria ezagutzea. Botmasterrak espainiarrak ziren eta 2010ean atxilotu zituzten, zerbitzariarekin egindako konexio guztien artean, konexio bat VPN erabili gabe egin baitzuen haietako batek [Corrons, 2010].

3.7 Probak

Atal honetan tresna ezberdinak aztertuko dira, azken urteetan ezagutu diren botnet ahaltsuenen portaera ulertzeko lagungarriak diren proba batzuk azalduko dira eta haien ezaugarri eta arrakastaren zenbait arrazoi aipatuko dira. Bestetik, probetan zehar, orain arte ikertutakoan oinarrituz, zenbait ohar eta behaketa egingo dira.

Tresnen frogak modu lokalean egingo dira, nahiz eta horrek arazo batzuk sor ditzakeen, horrela egingo da. Bestetik, kasu erreal baten dimentsioak dituen botnet baten simulazioa egin nahi balitz argi dago izugarrizko baliabideak beharko liratekeela eta hori martxan jartzea ere izugarrizko lana dela. Horren erakusle da 3000 nodoko botnet bat simulatzeko zenbait unibertsitate eta erakunderen artean egindako lana [Calvet et al., 2010]. Kontutan hartu ere, probatuko diren tresnen erabilpenak legea urratu dezakeela[27], beraz, modu lokalean eta beste inoren datuak arriskuan jarri gabe ez dago arazorik.

Argi utzi behar da egingo diren probak urrun daudela botnet baten ahalmen eta

[26] http://defintel.com
[27] http://cert.inteco.es/Formacion/Legislacion/

dimentsiotik, baina botnetak diren eraketa handi horren osagai txiki bat zer den ulertzeko balioko dute.

3.7.1 Ingurunea eta tresnak

Frogak egiteko bi bot aztertuko dira, bat *flu-project* izeneko proiektuak sortutako *Flu* bota, ikerkuntzarako eta modu didaktikoan erabiltzeko bota. *Flu* oso egokia da egungo botnet askoren portaera ulertzeko. Bestetik *Zeus* edo ZBOT izeneko botneta erabiliko da.

Frogak egiteko beraz, ondorengo softwarea erabili eta aztertuko da:

- Vmware Player[28]
- Windows XP SP3[29]
- Ubuntu 11.10[30]
- Appserv[31] edo XAMPP[32] (apache, php, mysql, phpmyadmin)
- Zeus
- Flu[33]
- Mozilla Firefox[34]
- Wireshark[35]
- Microsoft Security Essentials[36] eta Panda Cloud Antivirus[37]

Frogetarako ingurunea Ubuntu sistemaren gainean exekutatuko diren bi makina birtualek osatzen dute:

[28] http://www.vmware.com/products/player/
[29] http://windows.microsoft.com/es-ES/windows/products/windows-xp
[30] http://www.ubuntu.com/
[31] http://www.appservnetwork.com/
[32] http://www.apachefriends.org/es/xampp.html
[33] http://www.flu-project.com/downloadflu/flu
[34] http://www.mozilla.org/eu/firefox/new/
[35] http://www.wireshark.org/
[36] http://windows.microsoft.com/en-US/windows/products/security-essentials
[37] http://www.cloudantivirus.com/

- Ubuntu 11.10 (host) (botmasterraren ordenagailua)
- Makina birtuala 1: Windows XP SP3 (guest) (bot)
- Makina birtuala 2: Windows XP SP3 (guest) (C&C zerbitzaria)

Direktorio bat partekatuko da lana errazteko, beraz, VM Tools instalatu beharko da makina birtualetan.

VMwareko ezaugarrietan, sarea *bridget* moduan jarri, horrela makinen artean konexioak gauzatzeko ez da arazorik izango, bestela, etxeko ingurunean routerra dela eta arazoak izaten dira.

3.7.2 Flu

Bere sortzaileek Flu-Project-en webgunean[38] dioten moduan Flu *informazioaren segurtasunaren gaia eta malwarearen inguruan edonork bere jakintza konpartitu eta ekarpenak egiteko proiektu ireki eta parte hartzaile bat da*.

Zenbait botneten portaeraren oinarriak ikasten laguntzeko proiektu egokia da, eta horrexegatik, proiektu honetan ere, tresna honen bitartez zenbait kontzeptu ulertu eta aipatu diren zenbait gai praktikan jartzeko ezin hobea da.

Frogak egin aurretik Fluren ezaugarri batzuk aipatzearren, esan behar da Flu HTTP motako botnet bat dela, botmasterra zerbitzarira konektatzean eta Fluk eskaintzen duen panela erabiliz, XML fitxategi batean idazten direla aginduak. Botak zerbitzarira konektatzen denean XML hori irakurriko du agindu bila.

Flurekin egingo diren probetan ondorengoa aztertuko da:

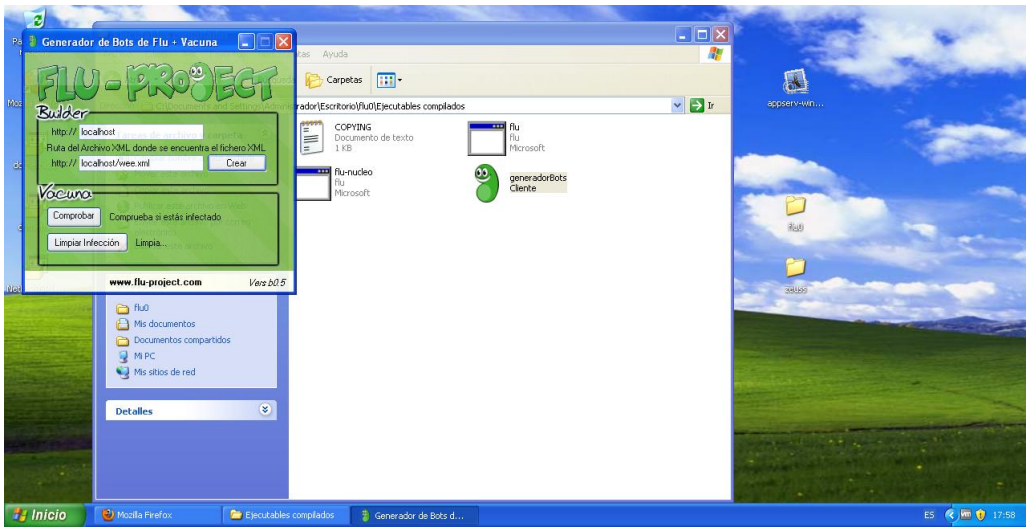
- HTTP botnetek nola funtzionatzen duten, interesgarria da HTTP motako botnetak ikustea, ia firewall guztiek HTTP trafikoa onartu egiten dutelako. Windowseko firewalla aktibatuta frogatuko da ea Fluren kasuan horrela den.
- Flu bidez ikus daiteke nolakoak diren gaur egun aurki daitezkeen botnet askoren kontrol panelak, edo ideia bat egiteko balio du. Eta aztertuko da panel horiek garatzeak zer eragin duen botneten hedapen eta *gizarteratzean*.

[38] http://www.flu-project.com

- Erakutsiko da zein erraza den botnet bat instalatzea, eta non dauden botnet bat sortzearen benetako zailtasunak.
- Eraso ezberdin batzuk egingo dira, 3.2 atalean aipatu diren eraso batzuk izango dira.
- Wireshark bidez aztertuko da zerbitzariaren eta botaren arteko komunikazioa.
- Bota nola ezkutatzen den aipatuko da
- Biktimaren sistema kutsatzeko plan azkar bat diseinatuko da gizarte ingeniaritzaren kontzeptua hobe ulertzeko.
- Ondorio orokor batzuk aterako dira probetatik eta erasoa eta botneta ez balitz simulazio bat, kontutan hartu beharko liratekeen zenbait iradokizun egingo dira.
- Frogak antibirusa jarrita eta jarri gabe, eta firewalla jarrita eta jarri gabe egingo dira. 3.5.1 atalean aipatu diren neurrien puntuetako bat aztertzeko. Eta babesteko aipatu diren beste neurriekin ere erasoa saihesteko nahikoa ote zen hausnartuko da.

Berriro azpimarratu behar da, froga hauek eskala txikian egindako eraso batzuk direla, botnet baten portaera pixka bat gehiago ulertzen lagunduko duten froga batzuk direla. Kontutan eduki egingo diren frogak miloi bat bider gertatzen direla eta botmasterrek ehunka, milaka teknika ezberdin erabiltzen dituztela erasoek arrakasta izan dezaten eta botneta ahalik eta gehien hedatzeko. Finean, ez ahaztu industria bat dagola martxan honen atzean, botnetei esker egiten dutela dirua eta beraz, inbertsioa ere egiten dela erasoak hobetze aldera, alegia, 3.5.2 atalean aipatu den *arms race* edo erasotzaile-defentsa arteko lehia hori.

1. **Flu instalatu eta martxan jarri:** Lehen proba honetan ez da ezer berezirik egingo, besterik gabe, C&C zerbitzaria instalatu, bota sortu, eta zerbitzarira sartu bota ongi konektatzen dela ikusteko. Ez da ezer ezkutatuko, ez da antibirusik jarriko...
   (a) jaitsi Fluren azken bertsioa
   (b) Instalatu Appserv makina birtualetako batean, hori izango da C&C zerbitzaria.



3.14 Irudia: Flu bota sortzeko programa

(c) Ireki Firefox eta `http://localhost/phpmyadmin` helbidearen bitartez sartu phpmyadminera eta inportatu fluren direktorio barruko BBDD direktorioan aurkitzen den datu-basea.

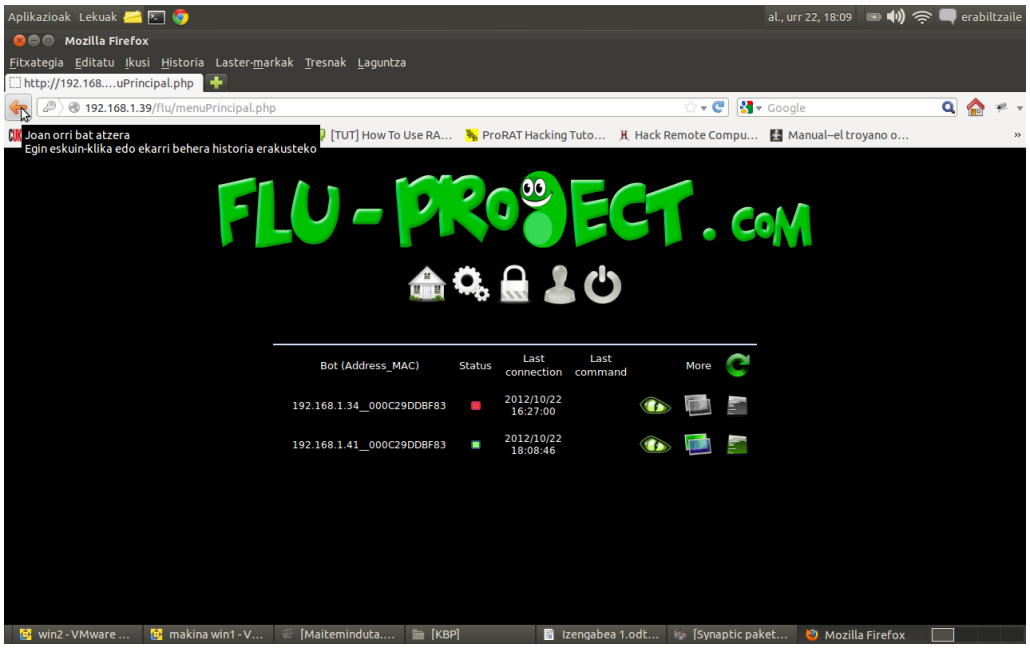
(d) Kopiatu `C:\Appserv\www` direktoriora *servidor web* izeneko direktorioa eta berrizendatu, jarri *flu* izena.

(e) Sortu bota, horretarako *ejecutables compilados* direktorioan *generador de bots* exekutatu, panel bat irekiko da eta bertan, makina birtualari dagokion IP helbidea jarri /flu/ helbidea atxikita (kasu honetan 192.168.1.39. IP ikusteko *cmd* exekutatu makina birtualean eta *ipconfig* agindua exekutatu) Hori izango da botak bisitatuko duen helbidea aginduak jasotzeko. Ikusi 3.14 irudia.

(f) Botaren fitxategia zuzenean beste makina birtualera pasa eta exekutatu partekatutako direktorioa baliatuta.

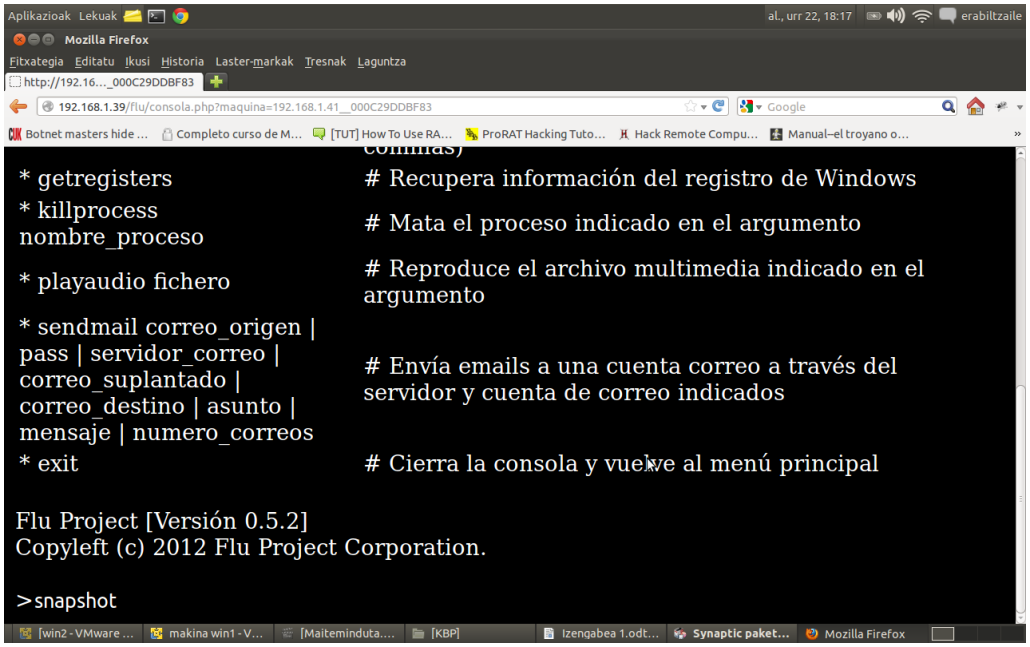
(g) Ubuntu makinan firefoxen sartuta eta zerbitzari gisa dagoen makina birtualeko IP helbidea erabilita (kasu honetan 192.168.1.39) Fluren kontrol panelera sar daiteke, iphelbidea/flu; *admin* erabiltzailea eta *1234* pasahitza dira defektuz daudenak. Beste makina birtuala dagoeneko bot bat dela ikusiko da. Ikusi 3.15 irudia.

2. **1. erasoa: pantaila gorde eta trafikoa aztertu:** Bot asko badaude agindua denei bidaltzen ahal zaie, kasu honetan bakarra dago, beraz horri bidaliko zaio agindua, zerbitzariko paneletik agindu kontsola ireki eta *snapshot* idatzi eta

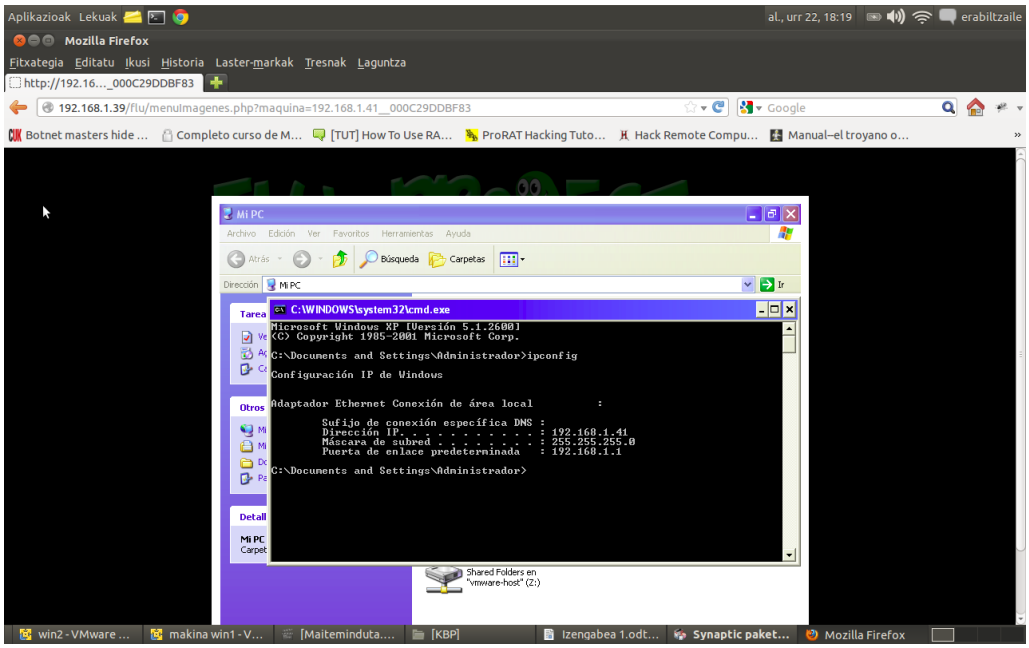


3.15 Irudia: Fluren zerbitzariko kontrol panela eta bot bat konektatuta

intro sakatu behar da, hori nahi adina aldiz egin daiteke.*Keylogger* bidez ere jaso daiteke informazioa. Hau da, egokia da *nortasun lapurreta* (3.2.1 atala) gauzatzeko. Gero bueltatu boten zerrendaren lekura eta hortik pantailazoak ikus daitezke. Ikusi 3.16 eta 3.17 irudiak .



3.16 Irudia: Fluren zerbitzariko kontrol panela aginduentzako konsola irekita



3.17 Irudia: Botaren makina atzituz Fluren zerbitzariko kontrol paneletik

```
1  ===== botmasterra fluren panelera sartu da ======
2  731 28.059636   192.168.1.34    192.168.1.39    HTTP    521 GET /flu/menuPrincipal.php HTTP/1.1
3
4  ====== bot eta zerbitzariaren arteko komunikazioa =====
5  837 33.839955   192.168.1.41    192.168.1.39    HTTP    146 GET /flu/actualizarEstadoMaquina.php?m
       =000C29DDBF83\&s=5.1 HTTP/1.1
6
7  838 33.849941   192.168.1.39    192.168.1.41    HTTP    221 HTTP/1.1 200 OK
8
9  839 33.850487   192.168.1.41    192.168.1.39    HTTP    105 GET /flu/wee.xml HTTP/1.1
```

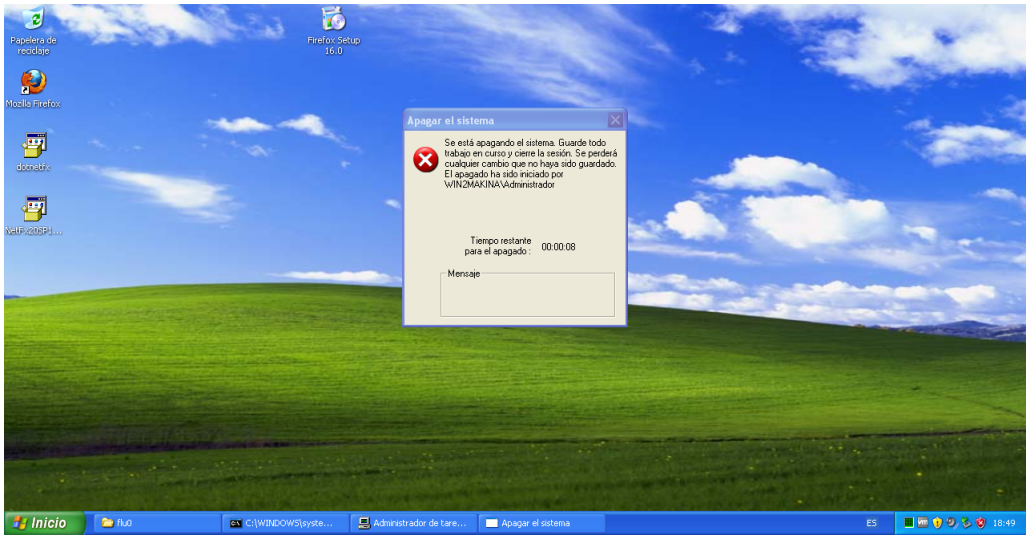
3.18 Irudia: Erasoaren trafikoaren azterketa

Erasoa egin bitartean Wireshark bitartez aztertu da sareko trafikoa.

Whiresark bidez jasotako emaitzetan ikus daiteke 192.168.1.41 makina aginduen bila konektatzen dela GET bat eginez 192.168.1.34 helbidera, hau da, C&C zerbitzarira (3.18 irudia).

Paketak aztertuz gero XML-a irakurtzera konektatzen dela jakin daiteke, baina komunikazioa zifratua doa. Fluren kodea begiratuz gero ere, *flu nucleo* direktorioan ikus daiteke *Crypto* fitxategia eta bertan daude komunikazioa nola zifratzen den argitzen duten azalpenak. Horrek atzematea zailduko luke. Hala ere, bestelako botnetak Fluk baino segurtasun neurri zorrotzagoak dituztela argi da 3.4.2 atala irakurrita.

Bestelako erasoak ere badaude, esan bezala, keyloggerra, Windowseko Segurtasun Zentroa gelditzeko aginduak, botean erabiltzaileak gehitzeko aukera, fitxategiak deskargatzeko aukera, ordenagailua itzaltzeko aukera (errorea ateratzen da ordea)... (3.19 irudia). Fluren bidez ikus daiteke behin botarekin komunikazioa ezarri denean, gainontzeko ia guztia posible dela eta oso modu errazean. Horrelakoak dira gerora ikusiko den moduan egungo botnet kontrolatzaileek dauzkaten panelak.



3.19 Irudia: Fluren zerbitzariko kontrol panelean bitartez bota itzaltzen

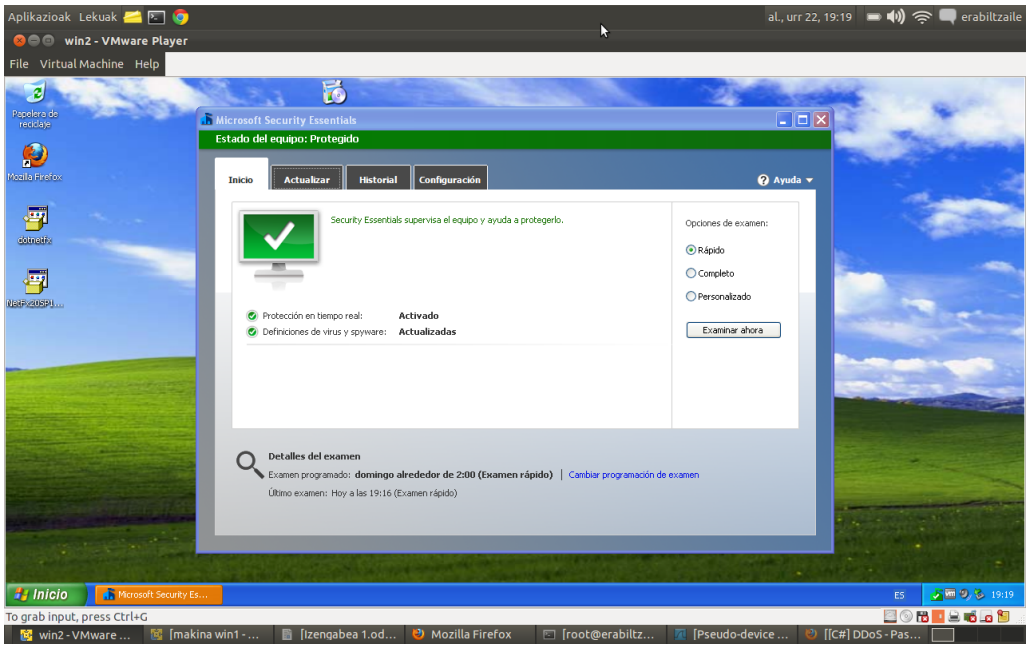
3. **1. proba antibirusa jarrita:** Bi antibirusekin egingo da proba, bat Microsoft Security Essentials (MSE) eta bestea Panda Cloud Antivirus (PCA) erabilita. Eta Windowsen firewalla ere aktibatuko da.

   MSEk ez du ezer atzeman, ez Flu instalatuta ezta instalatu aurretik ere, ordenagailua osorik aztertuta ezta ere, eta firewallak ezta ere, firewallarena ez da arraroa azken finean HTTP trafikoa baita eta gainera zifratuta doa. Ikusi 3.20 irudia.

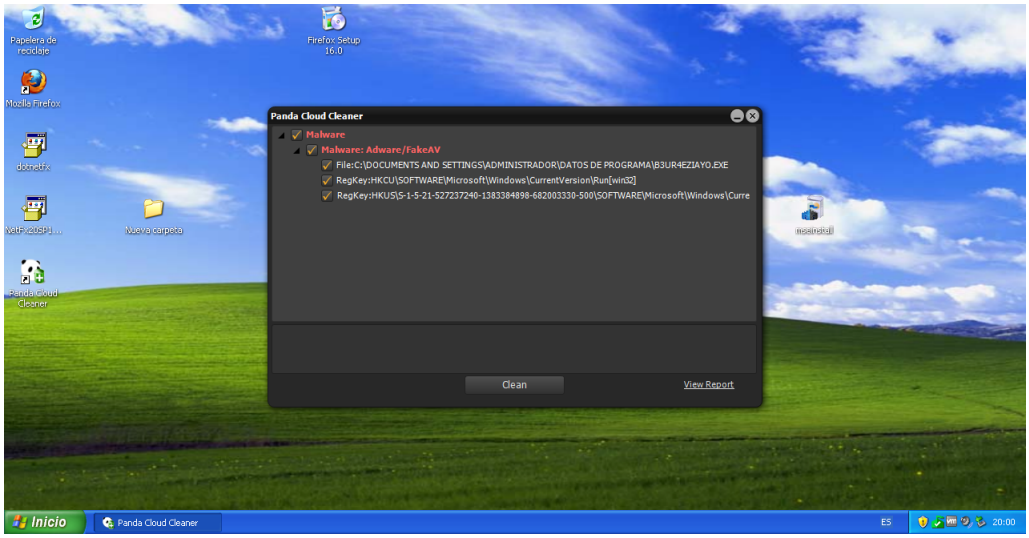
   Aldiz, Panda Cloud Antibirusek malwarea atzeman du eta bestetik flu.exe fitxategia malware modura katalogatu eta ezabatu du ere. Ikusi 3.21 irudia.

   Baliteke Fluren helburua ez denez kalteak eragitea beraien datu-basean sartu ez izana, baina hori albo batera utzita, hori litzateke ere bot berri bat azaltzean gertatuko litzatekeena. Beraz, antibirusaren datu-basean ez bada bota aurkitzen ez du ezertarako balio, beraz, bot berri askorekin hori da gertatzen dena ere.

   Pandak bota garbitu duenean panelean bota deskonektatuta ageri da.3.22



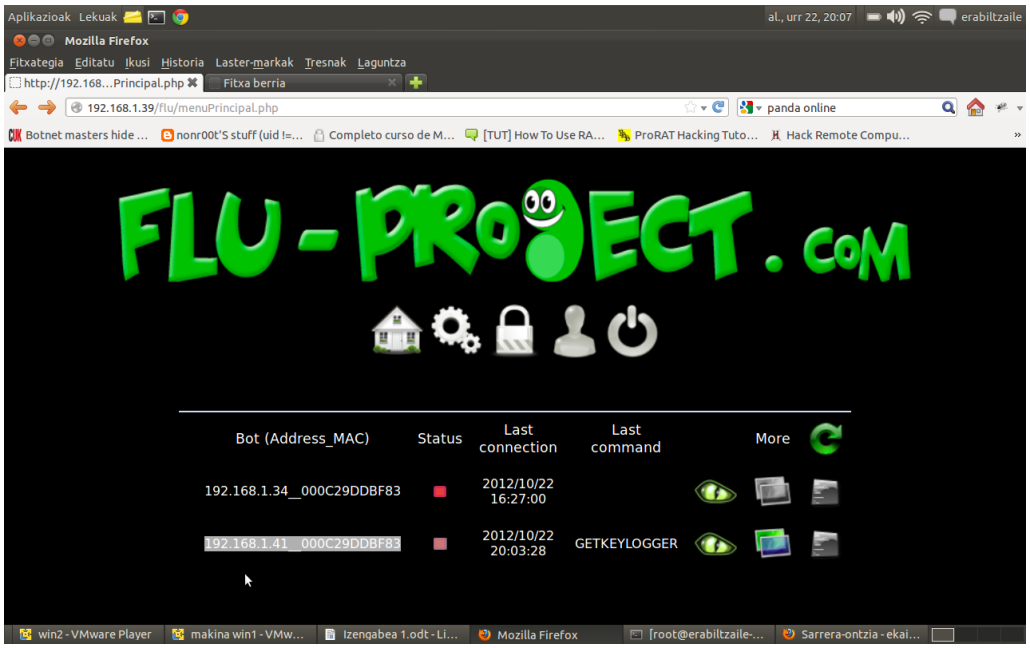
3.20 Irudia: MSEk ez du ezer atzeman



3.21 Irudia: PCAk atzeman du bai bota egin zaion erasoen kaltea eta garbitu egin du

Atazen kudeatzailea aztertuz gero ere, flu.exe prozesua ezkutatu egiten da.

4. **Gizarte ingeniaritza:** Fitxategia biktimaren sisteman sartzea ez da aurreko probetan egin den moduan gertatzen, hau da, ez da horren erraza. Ezezagun baten sistemara exekutagarri bat bidaltzea ez da horren erraza, baina ez da horren zaila ere, eta ezezagun horrek fitxategi hori ireki edo exekutatzea ezta ere. Hau da, nola lortu erabiltzaileak bota exekutatzea?



3.22 Irudia: MSEk ez du ezer atzeman

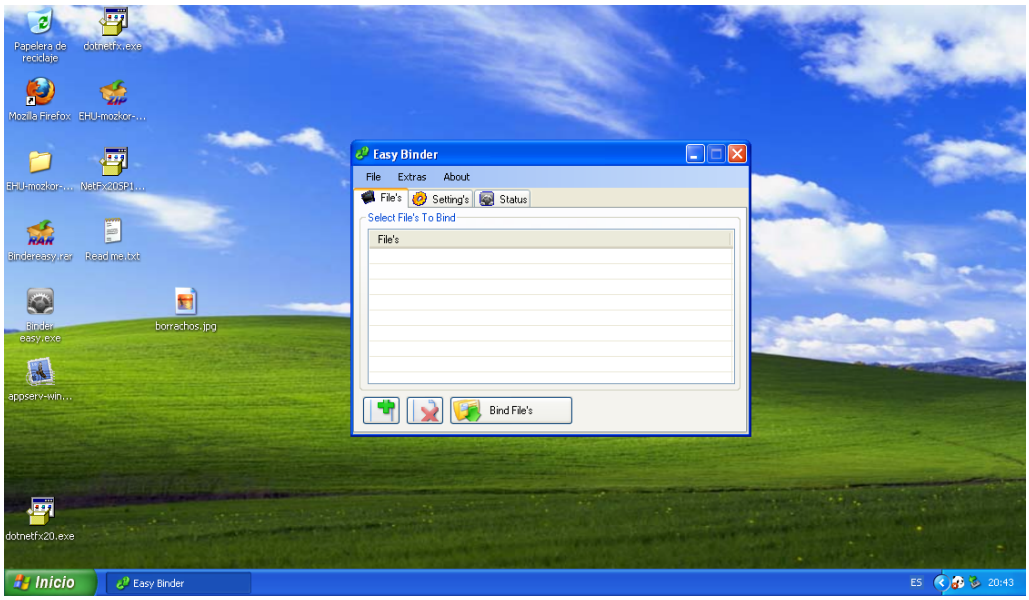
Aipatutako gizarte ingeniaritza (3.4.1 atala) delakoa aplikatuz gero, buruari pixka bat eraginez eta tresna berezi batzuk erabiliz gero, arrakasta izan dezake erasoak.

Esate baterako, UPV-EHU unibertsitateko ikasleei bota bidaltzeko (e-mailak nahiko erraz lor daitezke, bestela sare sozialak ere informazio iturri onak dira jendearen e-mailak lortzeko). EHUko e-mail faltsu baten bitartez egin daiteke oso modu errazean, gainera EHU-koa izanik denei e-mail berdina bidaltzeko aukera dago arrakasta gehiegi jaitsi gabe. Bestetik, pertsonalizatuago bidaliz gero arrakasta izateko probabilitatea ere handiagoa da, baina lan handiagoa da ere.

Aipatutako kasuari jarraitu, adibide posible bat jartzearren, demagun ikasleen e-mail zerrenda batera bidaliko dela e-maila, denen eskura dagon tresna ezagun bat `http://emkei.cz` da (kasu errealetan e-mail bomberrak edo spammerrek bidaltzen dituzte haien zerbitzarietatik), e-mailak bidal daitezke eta kasu askotan ez da spam gisa sailkatzen. Beraz, horren bitartez e-mail bat bidaliko da botaren exekutagarriaren helbidearekin eta *irakasle mozkorrak* edo azterketak izeneko gaiarekin, erakargarria, arreta piztu eta ikusi eta ireki gabe ezinegona sortzen duen zerbaitekin, hau da, guztiz fidatzen ez bada ere irekitzera bultzatuko duen zerbaitekin. EHUko e-maila bada seriotasuna emango dio, konfiantza sor dezake eta gainera spam gisa sailkatzeko aukera gutxiago. Hala ere, EHUko helbide

batetik bada azterketak izeneko e-mailak dauka zentzu gehiago besteak baino.

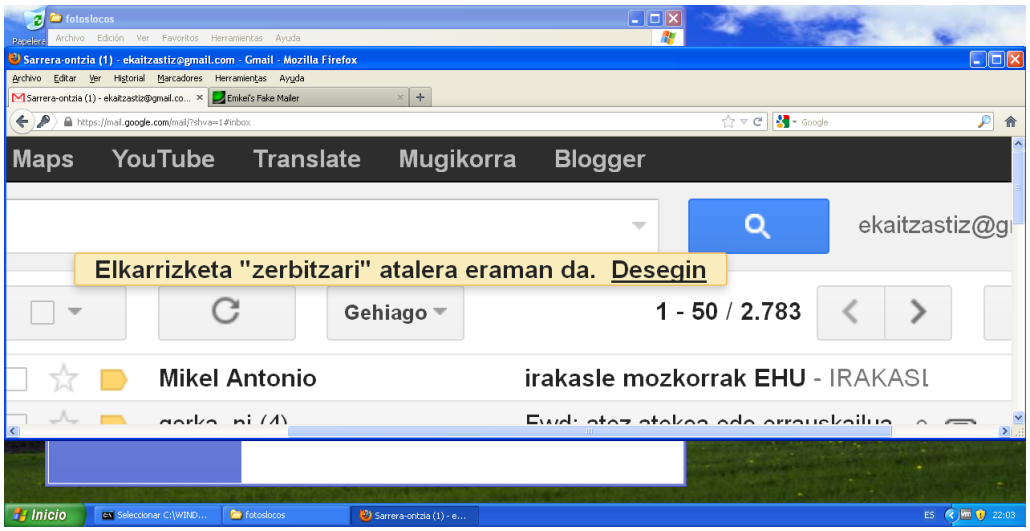
Zerbitzari batean flu.exe fitxategia igoko da, frogen kasuan zerbitzaria den makina birtualera, zip batean sartuta eta beste argazki batzuekin edo dokumentu batzuekin nahasita. Erasoa maila baxukoa da, baina jende askok fitxategien luzapena ezkutatzeko aukera duenaren aukera aprobetxatuko da. Zip horren barruan alfabetikoki lehen fitxategia izan dadin izendatuko da, horrela lehen fitxategia irekiko dela ia ziurra da. Gainera *binder* (programa hauek erraz lortzen dira Interneten) motako programa batekin, hau da, fitxategia irudi batekin fusionatzen duen programa batekin itxura aldatuko zaio, irudi baten itxura izan dezan eta ikonoa ere aldatuko zaio 3.23. Aipatu den helbidera jo eta handik *zerbitzariarenhelbidea/irakaslemozkorrak.zip* fitxategiaren lotura duen e-maila bidaliko da. Hau oso xumea eta oso maila baxuko erasoa da, baina e-mail askotara bidaliz gero bat edo bestek amua jango luke.



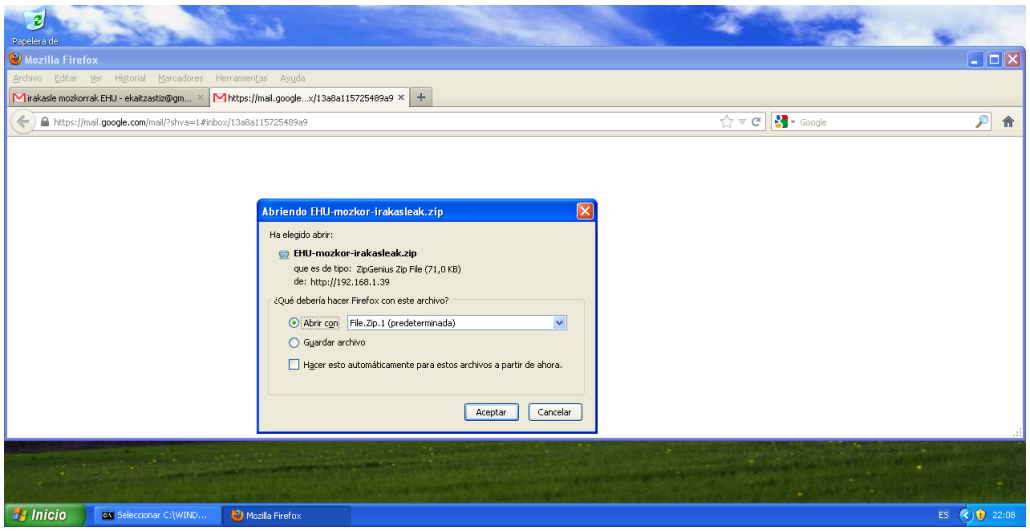
3.23 Irudia: Easy Binder programarekin flu.exe eta irudi bat elkartzen

Esan bezala gainera, kasu askotan ez da spam gisa sailkatzen. Ikusi 3.24 eta 3.25 irudiak. Antibirusarekin berdina pasatzen da zip fitxategia aztertuz gero, PCAk atzematen du, MSEk ez. Eta Gmailek ezta ere, helbidea pasa baitzaio eta ez fitxategia.

5. **Egindako froga eta botneten inguruko informaziotik ateratako ondorioak:** Ikusi den moduan kontrol panelari esker erasoak egitea ez da zaila, eta horrelako bot bat aurkitzea ezta ere. Mota horretako panelak dira merkatu bat

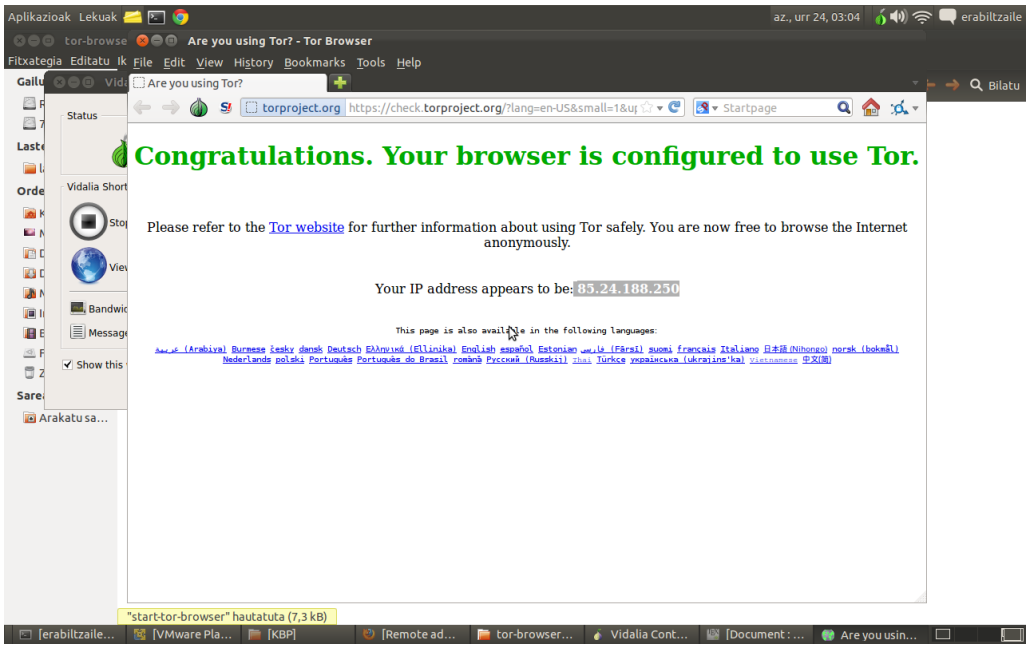


3.24 Irudia: Gmailen fitxategiak dituen helbidea duen e-maila sarrera ontzian



3.25 Irudia: zerbitzaritik flu.exe duen zip fitxategia jaisten

zabaltzea ahalbidetu dutenak hein handi batean, asko erraztu dute botnetaren erabilera. Hala eta guztiz ere, kontutan hartu, Wiresharkekin aztertu den trafikoan zuzenean ikusten zela nondik nora zihoan trafikoa, hau da, helbidetik helbidera. Hori saihesteko 3.4.2 atalean aipatu diren teknikak erabiliko zituzten kasu erreal batean, hau da, fast-flux motako zerbait edo eta domain-flux edo proxyak... Behintzat egin diren frogetan baino egitura konplexuagoak. Kontua da modu lokalean hori ez dela horren erraza egitea, baliabide ahaltsuagoak behar dira makina asko martxan jarri eta benetako botnet baten pareko zerbait simulatzeko edo aipatutako tekniken simulaziorako.



3.26 Irudia: Tor programari esker beste IP helbide bat eskuratzen

Bestetik, botmasterrak ere proxyak, VPN edo Tor izeneko programak eta erabil zitzakeen, edo aurrekoak eta gainera bere menpe duen eta kontrola dezakeen beste makina bat eta gainera bere etxea ez den leku batetik. Hau da, konplexutasun maila nahi adina handitu dezake botmaster batek. Baina hori da zailena ziurrenik, edozein erabiltzaileren esku ez dagoena, arrastorik edo ia arrastorik ez uztea. Probetan Tor eta VPN ez dira erabili ezin baita NAT kanpoko makina batetik makina birtuala atzitu. Hala ere 3.26 irudian ikusten da Tipularen bideraapena teknika inplementatzen duen Torri esker beste IP helbide bat esleitu zaiola makinari.

Beraz, panelak aukera ematen du merkatu bat zabaltzeko, baina botnet ahaltsu bat sortzea antolatutako taldeek egiten dute eta gero zerbitzua alokatu, hau da, konfigurazioa egokituta eta botneta eratuta alokatzen dute. Normala da hori, den dena jendearen esku balego eta erraza baino, *errazegia* balitz, botnetetatik bizi direnak ere ez lukete dirurik lortuko.

Bestetik, argi dago antibirus guztiek ez dutela balio, eta argi dago ere neurri guztiak hartu arren, gizarte ingeniaritzaren bitartez beti dagoela zirrikitu edo tarte bat neurri horien eraginkortasuna bertan behera utz dezakeena, alegia, ekintza bat aurrera eramateko erabiltzaileak konbentzitzea.

Gaineratu behar da botenetaren bizi zikloa azaltzen duen atalean eta gerora

agertzen den 3.5 irudian jarritako adibideak bigarren injekzio bat egiten zuela bota sortzeko, horrela lehenik biktimaren makina bere menpe hartu eta gero sartuko du bota biktima ohartu gabe eta zerbitzariarekin komunikazioa antibirusak eta firewallak geldituta egin ahal izateko.

Hortaz, oso garrantzitsuak dira 3.5.1 atalean aipatutako neurriak baina beti ere erabiltzailea kontzientziatuta baldin badago.

Panelak erraztu egiten du, eta bestetik, imajina daiteke erabiltzaile arruntek horrelako erasoak egiteko tresnak aurki baditzakete, botneten gaian aditua den edo botnetei esker bizi direnek zer nolako tresnak izango dituzten eskura. Gainera Interneten jakina da bilatzen den guzti hori aurkitu daitekeela, eta Flu ikasteko helburuarekin sortutako bot bat bada ere, Googlen denbora bat pasaz gero argi dago instalatzen eta martxan jartzen Flu bezain errazak diren botak aurki daitezkeela, baita eraso konplexuak egiten ikasteko nahikoa material dagoela. Hurrengo atalean ikusiko da nahiko ezaguna den Zeus bota Interneten dagoela eta gainera, gida eta bideotutorial ugari dagoela bere erabilpenerako eta martxan nola jarri azaltzen dutenak ere.

Jarraian datorren atalean Zeusek Flurekin aipatu diren zenbait ezaugarri betetzen ditu, panel bat eskaintzen du, ez da zaila instalatzeko, trafikoa zifratuta doa...

3.7.3 Zeus

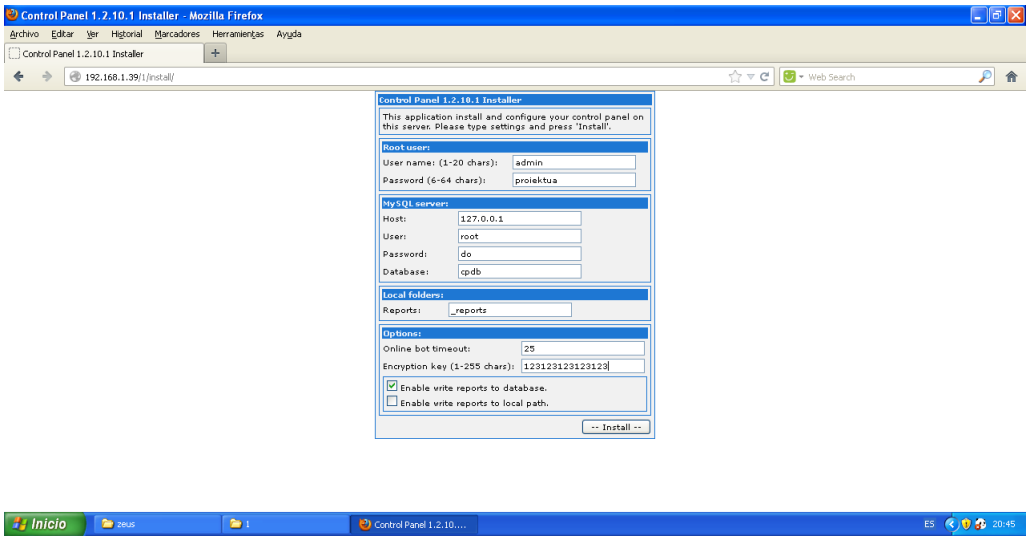
1. **Zeus botneta instalatu eta martxan jarri:** Fluren antzeko prozedura da. Datu basea inportatu eta gerora *1* izeneko direktorioa Appserv/www direktorioan kopiatu. Bertako global.php fitxategian definitu datubasearen datuak.

   Ubuntutik atzitu IPhelbidea/1/install/ helbidea eta instalatu aukerak aktibatuz eta *encryptation key* eremuan komunikazioa zifratzeko erabiliko duen gakoa idatzi. Ikusi 3.27.

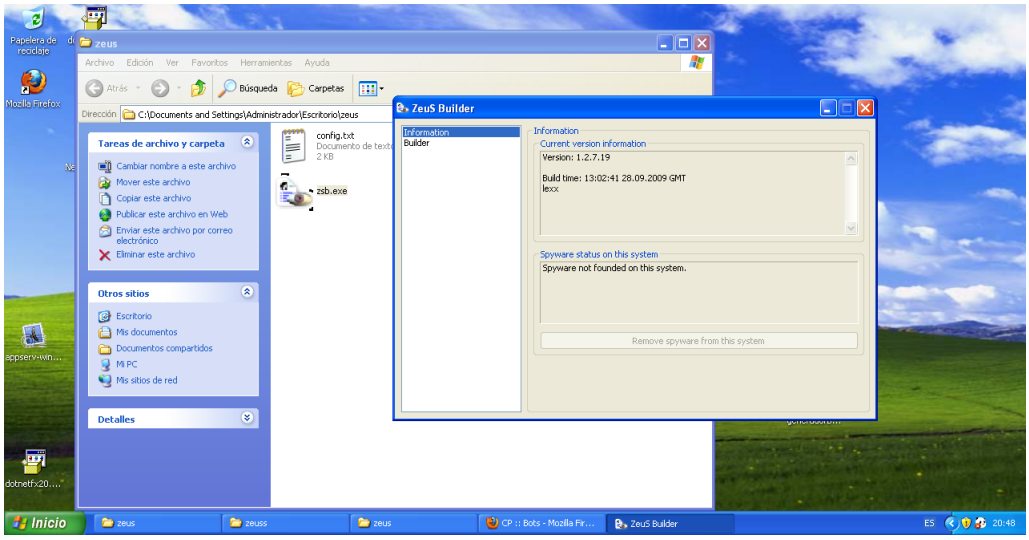
   Horrekin botnetaren panela instalatuta egongo da.

   Bota sortzeko ireki zeus/zeus karpeta barruko config.txt fitxategia eta bertan zerbitzariaren IP helbidea jarri. *Load config* sakatu eta ondoren *build loader*. Kopiatu sortu diren artxiboak Appserv/www/1 barruan. Ikusi 3.28 irudia.

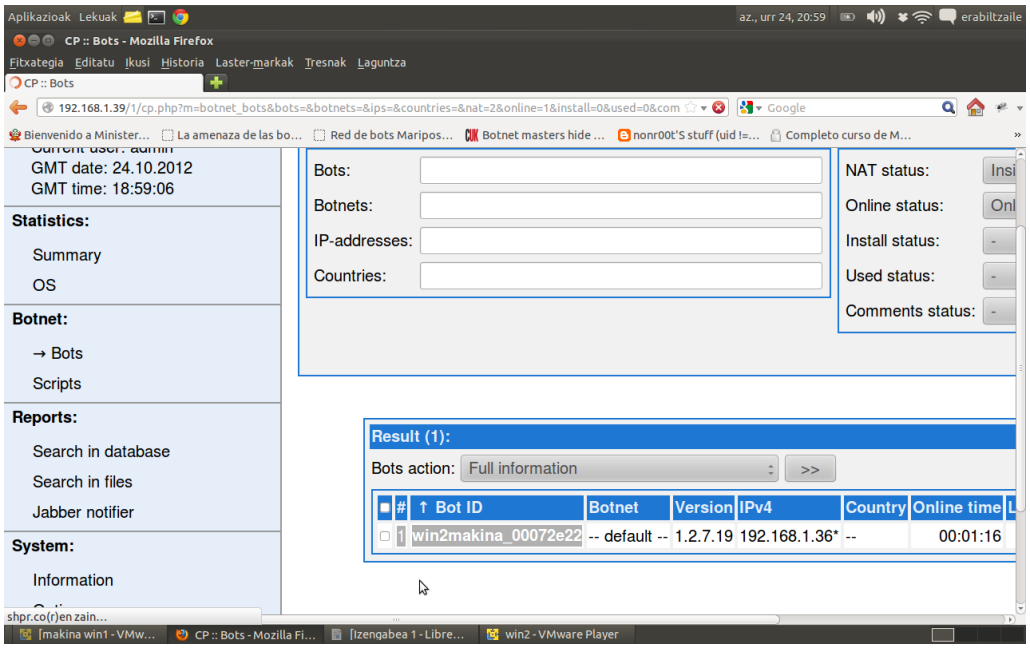
   Exekutagarrian Flurekin egin den moduan biktimari bidali eta exekutatzean bota panelera gehituko zaio. Ikusi 3.29 irudia.



3.27 Irudia: Zeus instalatzeko panela



3.28 Irudia: Zeus instalatzeko panela



3.29 Irudia: Zeusen kontrol panelean win2 makina bot gisa gehituta

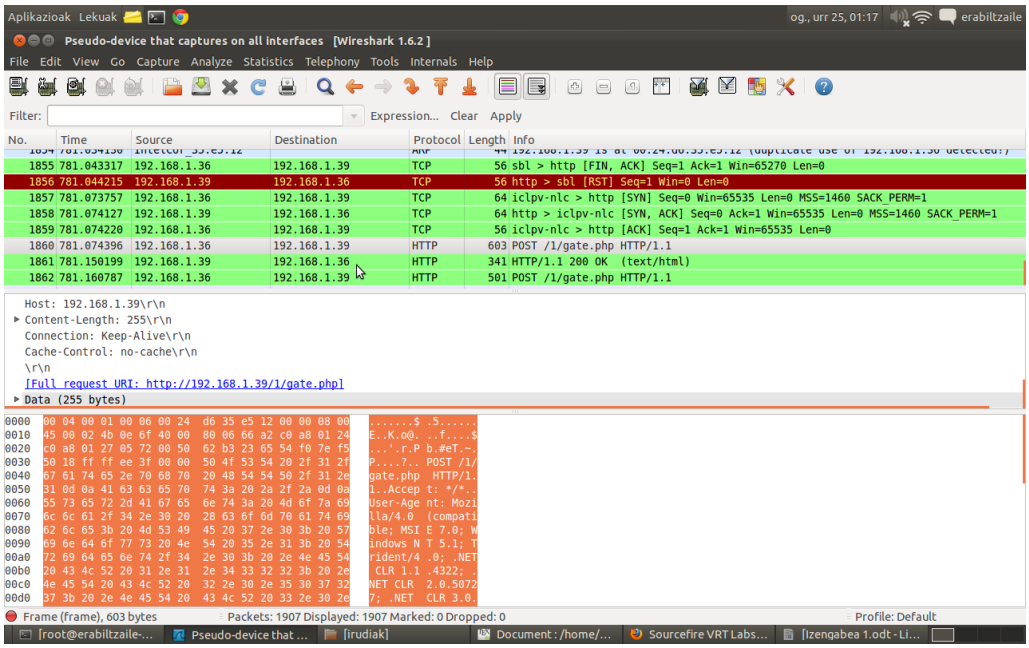
Instalazio hau egiteko fitxategian Interneten bilatuz gero aurki daitezke eta Youtuben bertan ere instalazioa nola egin azaltzen duten bideoak[39] daude, baita bideoen deskribapenean fitxategiak eskuratzeko loturak[40] ere.

2. **Erasoak egin:** Fluren antzekoa da, bota zerbitzarira konektatzen da agindu bila, hau da, pull mekanismoa, trafikoa aztertuz gero GET config.bin eskaera ikus daiteke. Eta emaitzak POST bidez itzultzen dizkio (aipatu den bezala, informazioa zifratuta dago) 3.30:

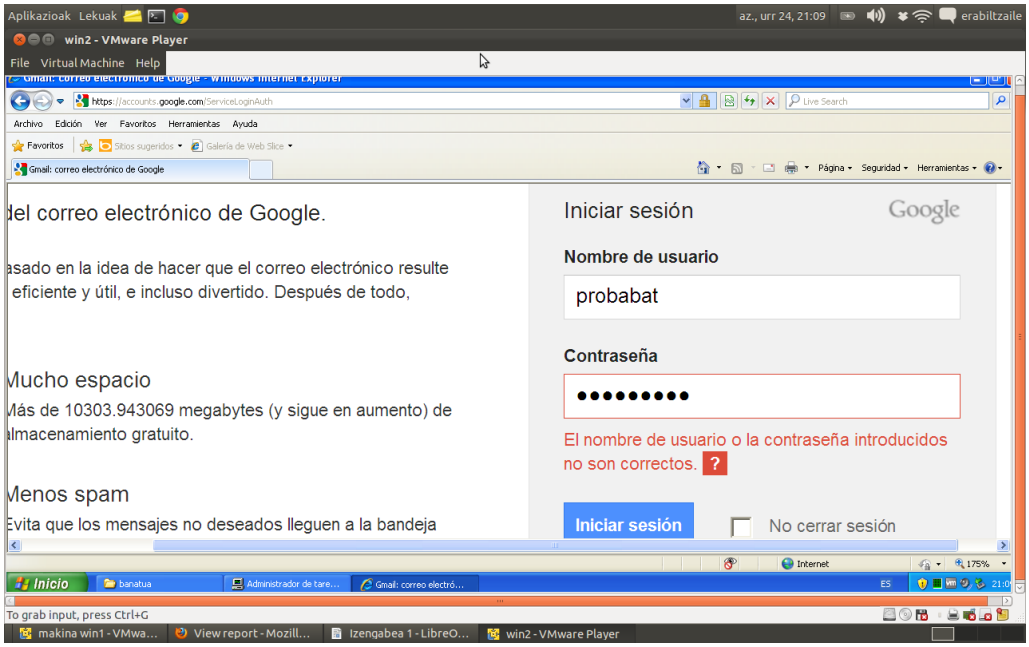
```
1860    781.074396  192.168.1.36    192.168.1.39    HTTP    603 POST /1/gate.php HTTP/1.1
1861    781.150199  192.168.1.39    192.168.1.36    HTTP    341 HTTP/1.1 200 OK  (text/html)
```

Zeus banku datuak lapurtzeko erabili izan da, horregatik ditu horrelako webguneetarako filtro bereziak, hau da, datuen parametroak ezagutzeko webguneen helbideak eta filtroek dauzka konfigurazio fitxategietan gordeta. Egin den erasoan argi ikusten da datuak erraz xurgatzen dituela, esate batera Gmail-en *probabat* erabiltzailearekin eta ausazko pasahitz bat sartuta gero panelean *report* aukera emanda datu guztiak gorde direla ikus daiteke. Ikusi 3.31 eta 3.32 irudiak.

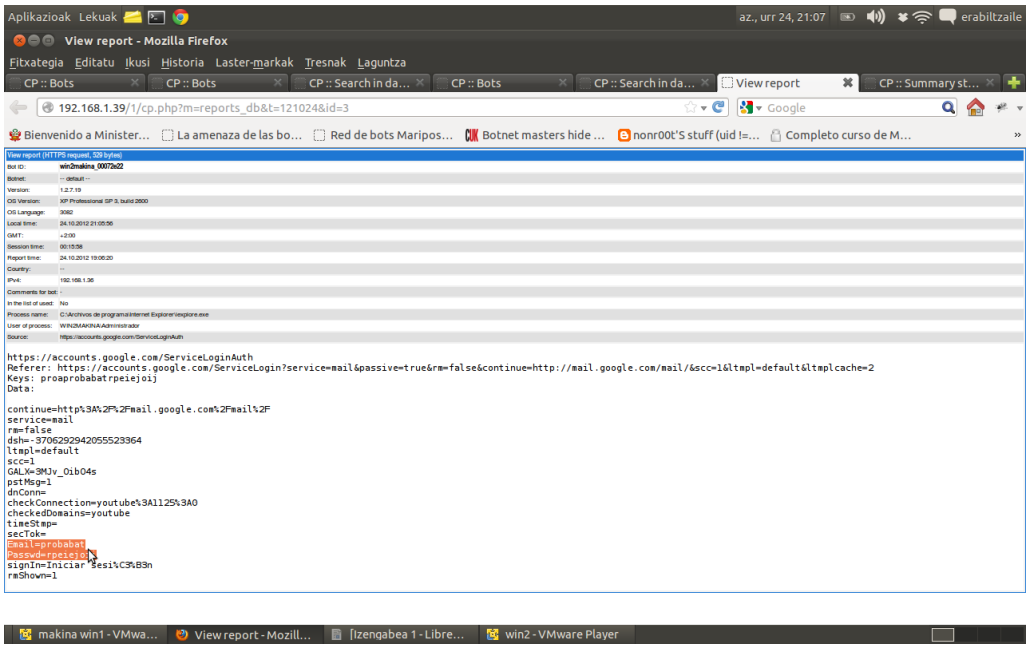
[39] http://www.youtube.com/watch?v=rDZShHU6Rk4
[40] http://www.youtube.com/watch?v=kyyjgp4abhY&feature=related



3.30 Irudia: Wireshark bidez trafikoa aztertzen



3.31 Irudia: Gmailen sartutako datuak



3.32 Irudia: Gmailen sartutako datuak jasota

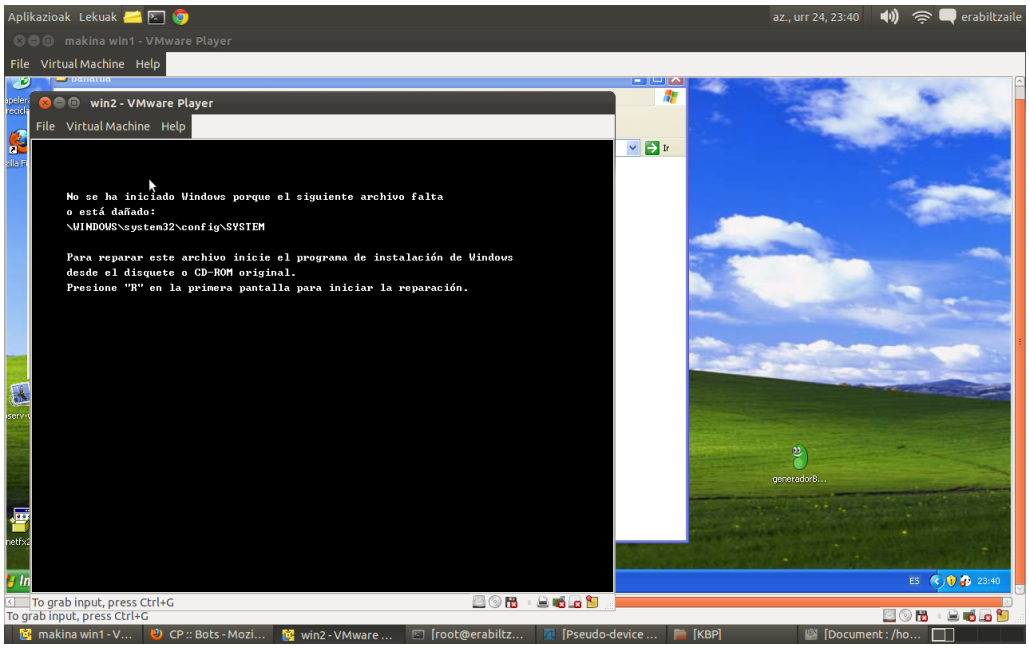
Zeusek ere aurredefinitutako erasoak ditu, pantaila gorde, webguneetako erabiltzaile eta pasahitz datuak xurgatu, sistema eragilea suntsitu, makina berrabiarazi... Eta agindua gauzatu den edo ez ikusteko informazioa ematen du. Ikusi 3.34 eta 3.33 irudiak.

Beraz, orokorrean Flurekin erakutsitakoaren antzekoa da Zeusen funtzionamendua.

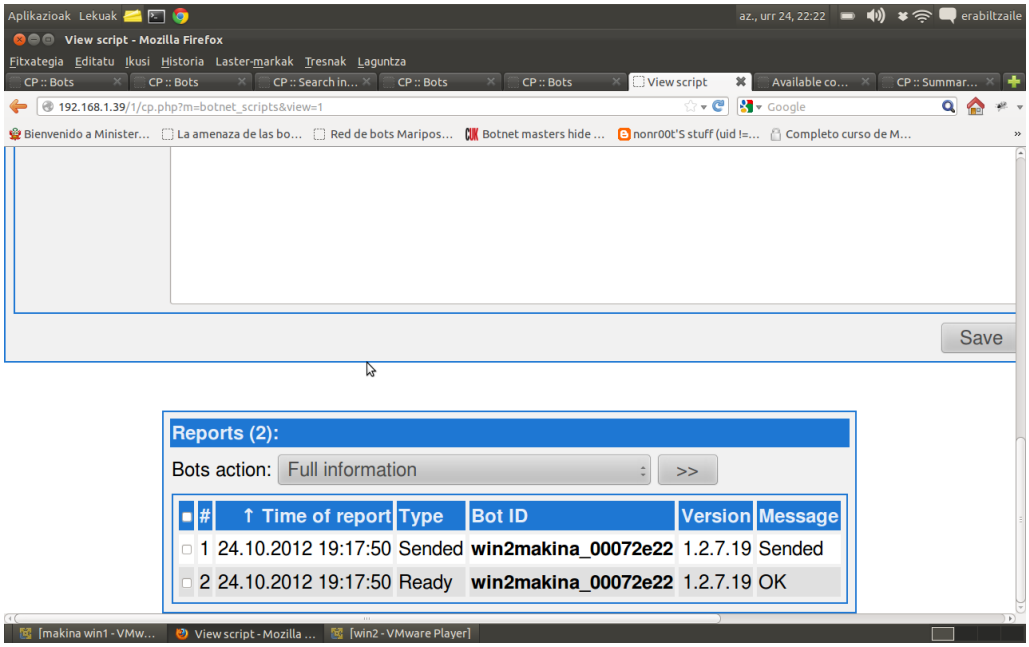
3. **Fluren antzekoa**

Fluren frogen 5 atalean ondorioztatu dena da hemen ere ondorioztatu daitekeena, berriro azpimarratzearren, panela oso intuitiboa eta erraza da erabiltzeko eta interneten informazio ugari dago bere erabilera errazteko. Boten kontrola erraza da, zailagoa da ordea makinak kutsatzea, baina kasu asko eta askotan denbora kontua eta buruari eragitea besterik ez da.

Aztertu diren bi botnetak bot bakarrekoak ziren, baina hori eskala handira eramanda erraz ondoriozta daiteke diru iturri handia izan daitekeela botnet bat eta horregatik garatu direla geroz eta botnet ahaltsuagoak.



3.33 Irudia: Kos agindua bidali eta gero sistema ez da abiarazten



3.34 Irudia: Bidalitako aginduaren informazioa

3.8 Ondorioak

Botneten inguruko lan osotik, nolabait esatearren arlo teorikotik eta egindako probetatik (3.7 atala), ondorio eta ideia nagusi batzuk atera daitezke, horiek ahalik eta labur eta argien jaso nahi dira hurrengo lerroetan.

3.1 atalean azaldu da botnetak kutsatutako makina asko makina batetik edo gutxi batzutatik kontrolatzeko aukera ematen duten sareak direla eta erasoak egiteko erabili ohi direla. Botnetak erakunde antolatuen menpe dauden tresnak dira normalean, eta gero eta ugariagoa da hauen erabilpena. Azken urteetako datuen arabera (3.6 atala) botnetek eragindako kalteak hazi egin dira, hori lotuta dago geroz eta botnet handiago eta konplexuagoen agerpenarekin. Gainera, botneten inguruan merkatu bat garatu dela argi geratu da 3.2 atalean eta probetan, 3.7.3 atalean argi ikusi da sarean dauden botnetek zein motatako panelak dituzten botnetak alokatzen dituztenei hauen erabilpena errazteko, horri esker merkatua erabiltzaile arruntei eskaintzeko aukera lortu da.

3.4 atalean botnet bat eratzeko faseak aztertu direnean ere, argi geratu da botneten arrakasta eskaintzen duten tresna sorta zabalean oinarritzen dela hein handi batean. Ikusi da malware askoren konbinaketa edo fusioaren emaitza moduko bat dela eta kutsatutako milaka eta milaka makinaren ahalmena bereganatuz tresna horiei ahal den etekin handiena ateratzen ahal zaiela botnet baten bitartez. Erasoen eraginkortasuna handitzeko tresna izugarria dira ezbairik gabe, makina bakanaren bitartez horietako eraso askok ez lukete eraginik izango.

Botneten kontrako borroka sarearen funtzionamendu egokirako ezinbesteko erronka bilakatu da. Erronka horretan, 3.6.2 atalean ikus daitekeen moduan, sareko segurtasun aditu taldeak, poliziak eta informatika munduko erakunde garrantzitsuenak geroz eta gehiago inplikatzen ari direnaren erakusle dira azken urteetako operazioak. Era berean, botnetei aurre egiteko 3.5 atalean ikusi da geroz eta teknika aurreratuagoak aurkitzen ari direla eta geroz eta proiektu eta tresna gehiago garatzen ari direla. Baina behin eta berriz aipatu da botneten eboluzioa ere etengabea dela, lehia hori nork irabaziko duen edo noizbait botnetak eraginkor izateari utziko dioten denborak esango du.

Zalantzarik gabe, hori guztia argituta, aurreikus daiteke aurrerantzean ere botnetek zer esan handia emango dutela, hurrengo atalean, 3.9 atalean, lan honetatik ondorioztatu denarekin eta berau osatzeko erabili diren erreferentzietatik etorkizunean botneten

inguruan zer gerta litekeen aipatzen duen atala aurki daiteke.

3.9 Etorkizunean zer?

Aurrera begira botneten industria ez dela gelditukо argi esan daiteke. Aurreikus daiteke botneten industria ere beste esparru batzuetara zabalduko dela, eta orain arte ebolu-zionatu duen bezalaxe laster geroz eta gehiago izango direla mugikorretan hedatuko diren botnetak. Gainera geroz eta datu trafiko eta eragiketa garrantzitsuagoak egiten dira mugikorren bitartez. Hala ere, aipatu den bezala, geroz eta proiektu gehiago daude botneten arazoari aurre egiteko, eta ziurrenik hurrengo urteetan ildo beretik segituko dute segurtasun enpresa handiek, batez ere Internet eta sarea delako une honetan diru gehien mugitzen duen merkatua eta eremua eta bezeroen konfiantza bermatzea ezinbestekoa delako.

Argi dago estatu aurreratuenek ere teknologian aurrerapenak egiten dituzten heinean, geroz eta esfortzu handiagoa ere egin beharko dutela estatu egituren teknologiaren eta azpiegitura kritikoen defentsan teknika berriak bilatzen. Teknologiaren erabilpena esparru guztietara hedatu izanak onura asko ekar diezazkieke bai gizarteari baita estatuei ere, baina gizartearen funtzionamendua teknologiaren menpe jartzeak ere arriskuak ditu eta arrisku horien analisia eta kudeaketa lehentasunezko lana bihurtu da. Aurrerantzean ere horrela izan beharko dela argi dago, egunez egun geroz eta gehiago zabaltzen ari baita zibergudaren kontzeptua, eta zibergudetarako eta ziberes-pioitzarako botnetak tresna baliagarriak direla argi geratu da, beraz, hori izan daiteke hurrengo urteetan gerta litekeen gauzetako bat, botneten erabilpena zibergudetarako ziberkrimenerako adina erabiltzea.

Azkenik, eta batez ere, orain arte zenbait ataletan aipatu denaren harira, ezinbestekoa izango da teknologien erabilpenaren inguruko heziketa, orain artean teknologiaren erabilpena sustatu da eta nola erabiltzen duen gehiegi axola gabe, baina aurreran-tzean kontutan izan behar da belaunaldi berri guztiek txikitatik teknologia gizarteko ezinbesteko elementutzat dutela eta bere erabilpen egokia egiten irakatsi beharko zaiela txikitatik, arau eta balore etikoek barne. Batez ere haiek ez ditzaten botneten edo eta bestelako malwarearen bidez kalteak eragin, jendearen pribatutasuna eta informazioaren trataera egokia egin dezaten, eta bitarteko teknologikoak gizartearen aurrerapenetarako erabil ditzaten.

4. KAPITULUA

Ondorioak eta hobespenak

Atal honetan,zenbait ondorio jasotzen dira proiektuaren bilakaeraren inguruan. Bukatzeko proiektu honi segida eman diezaioketen edo eta proiektu honen osagarri izan daitezkeen proposamen batzuk egiten dira.

4.1 Helburuak vs egindako lana

Hasieran proposatzen ziren helburuak (2.1 atala) bete dira. Ondorengoak hauek ziren planteatutako helburuak:

- Botnetak zer diren azaltzea, nola funtzionatzen duten eta sareetarako nolako mehatxua diren aztertzea.
- Mehatxu horri aurre egiteko gako nagusiak aurkeztea.

Lehena behar bezala bete dela baloratu daiteke. Bigarrenarekin baliteke, gako nagusi bezala planteatu diren neurri, tresna edo eta teknikek egoera guztietarako balio ez izatea eta neurri eta tresna horien inguruan gehiago sakontzeko beharra egotea. Baina egia da ere, gaia oso zabala zela eta ezin zela tresna, babes neurri eta tresna bakoitzean gehiegi sakondu. Horregatik erabili da *gako nagusiak aurkeztea* hitza eta horrek tartea eskaini du denborarekin justu antza ibilita xehetasunetan sartu behar ez izateko. Hala eta guztiz ere, esan bezala pena da xehetasun gehiagotan sartu ahal ez izana eta horregatik aurrera begira egindako lanaren jarraipen bat izan liteke hori egitea.

Horrekin batera, botneten inguruko informazioa dokumentatzeaz gain, proba batzuk egitea proposatzen zen azalpenak ulerterrazagoak izan zitezen. Hasiera batetan zalantza eta arriskuak planteatzen baziren ere, izandako baldintza eta mugak ez dira oztopo handiegia izan (4.3.1 atalean ikus daitezke) botneten inguruko azalpenak argitu ahal izateko.

Aldiz epeei eta sartu beharreko orduei dagokienean ez dira zehatz mehatz bete eta horregatik hurrengo atalean egiten da horren balorazioa ere.

4.2 Estimatutako denbora vs denbora erreala

Estimatutako denbora osotara 335 ordukoa zen. Osotara 350 bat ordu sartu ditut. Pixka bat gehiago izan da azkenean.

Botneten inguruko informazioa eskuratzen hasiera batean estimatutako denbora baino gutxiago izan da, baina frogak egiteko egin beharreko guztiarekin eta suertatutako arazoekin, atal horretarako estimatutako denbora baino gehiago behar izan dut, besteak beste, makina birtual bat izorratu izana eta berriro osagai guztiak instalatu behar izanagatik. Memoria idaztea ere, hau da, ondorioak eta PHDa idatzi eta zenbait zuzenketa egitea, estimatutako denbora baino gehiago kostatu zait.

Epeak malguak izanik ere planifikazioa ez da zehatz mehatz jarraitu datei dagokienez, hortaz, beranduago bukatu da proiektua.

Baina hala eta guztiz ere, epeetan malgutasuna zegoenez, estimazioa baino ordu batzuk sartu izanak ez du bestelako atzerapenik ekarri, atzerapenak aurkezpenaren datari eragiten dio, lan gehiago egin izanaren ondorioz atzeratutako lanak eguberriak harrapatu baititu erdian, ondorioz, eguberriak eta gero egingo da aurkezpena, ahal bada martxoa aldera eta beranduenez ekainerako utziko da.

4.3 Izandako zailtasunak

4.3.1 Frogentzako baliabideak, baldintzak eta mugak

Frogak egiterako orduan, frogen atalean aipatzen den moduan, proiektua planifikatzerako orduan eta helburuak betetzeari begira nahikoa edo ez da motz geratu egindako

froga, baina zenbait eraso eta ezkutatzeko zenbait teknika ezin izan ditut frogatu, modu lokalean ezin baitziren gauzatu. Pena izan da ere neuzkan baliabideekin ezin nituela bot gisa erabiliko nituen zenbait makina martxan jarri. Eta bukatzeko, lokalean ez balitz egin izan malware hori zerbitzariren batean jarrita legea urratu zitekeela edo hosting zerbitzua ematen zuten lekuetakoren batean benetako erasoak egiteko botneta instalatu izan nuenaren susmoa har zezaketela.

4.3.2 Terminologia eta ortotipografia

Botneten inguruan egindako garapen atalean anglizismo ugari eta ingelesezko termino asko erabili dira, esan behar da gainera, ingelesez ere botneten inguruan aurkitutako informazio iturri ezberdinek termino ezberdinak erabiltzen dituztela gauza berdina aipatzeko. Gaztelerazko segurtasun informatikoko liburu eta testuetan ere antzera gertatzen da. Beraz, asko erraztuko luke terminoak normalizatuko balira, hau da, arau batzuk ezarriko balira botneten eta segurtasun informatikoko gaietarako. Aipatutakoaren ondorio, eta terminoak zein modutan idatzi ziurtasun handirik ez nuela, zalantzak argitzeko eta lan osoan ildo berari segitzeko, Eusko Jaurlaritzak argitaratutako Jose Ramon Etxeberriaren *Zientzia eta Teknikako Euskara Arautzeko Gomendioak* liburuxka erabili dut.

4.4 Proiektuaren hedapen aukerak

Atal honetan etorkizunean egin daitezkeen hobekuntzak azaltzen dira.

- Baliabideekin izandako mugak direla eta interesgarria litzateke, dagoeneko martxan dagoen proiekturen batetik abiatuta, edo hasieratik hasita, botneten simulaziorako eta ikerkuntzarako ingurune bereziak aztertzea.
- Bestetik, proiektu honetan botnetak zer diren eta nola funtzionatzen duten ikusi eta gero, egin diren probekin jarraitzea eta proba horietan sakontzea. Hau da, Flu eta Zeus hartu eta proba gehiago egitea. Bestela, beste Zeus edo Flu ez diren beste batzuk erabiltzea ere interesgarria izan liteke.
- Segurtasun neurriak martxan nola jarri eta erabili azalduko duen gida moduko bat geratzea ongi legoke, zerrendatu eta azaldu diren neurri horiek praktikara eraman ahal izateko aukera emanez.

- Botneten eta botnetak erabiltzen dituzten bitarteko guztien erabilpenaren eta garapenaren inguruko ikerketa eta azterketa juridiko bat ere egin daiteke, bai estatu mailan baita nazioarteari begira dauden behar juridikoen inguruan.

Glosarioa

Backdoor Sistemarako edo programa baten ezkutuko sarrera bat da, makinaren jabea ohartu gabe sistemara sartzeko. Askotan *malware*ren batek sortzen du sarrera hau, beste batzuetan programa beraren garatzaileek blokeo egoerak gainditzeko jartzen dituzte eta gerora kentzea ahazten dute. Eta beste askotan inteligentzia zerbitzuek jartzen dizkiete sistema edo programei [Gómez Vieites, 2006]. 14, 93

Birusa Erabiltzailearen baimenik gabe eta automatikoki bere burua kopiatzen duen programa da. Bere helburua konputagailuaren funtzionamendu normala aldatzea da. Laburbilduz birus batek hiru fase ditu [David et al., 2002]: sisteman sartu, bere burua kopiatu edo ugaldu eta kalteak egin. 35, 93

Broadcast Nodo batetik sareko nodo guztitara une berean bidalketa bat egiteko balio du, nodoz nodo bidaltzen ibili gabe. IP helbide batean, Beste aldetik, bere 32 bitak, sarekoak eta interfazekoak, 1-ekoak dituen helbidea ere gordeta dago (255.255.255.255 helbidea, alegia): hori difusio mugatutako helbidea da. Sareko konputagailu guztiak identifikatzeko balio du [Rivadeneyra, 2004]. 37, 45, 93

Brute-force Pasahitzak lortzeko teknika bat da, aukerazko gako guztien konbinaketak egiten ditu pasahitz zuzena lortu arte. Zifratutako pasahitzak igertzeko balio du. 36, 93

DNS Domain Name System domeinu izenen informazioa gordetzeko sistema bat da hierarkizatutako eta banatutako datu-base sare moduko batean, Internet adibidez. Domeinu bati IP helbide bat esleitzen zaio, hau da, domeinu baten bitartez kontsulta eginez makina (normalean zerbitzari bat) baterako helbidea itzultzen digu DNS zerbitzariak. Makinak identifikatzeko IP helbideak erabil daitezke, baina gizakientzat ez da batere erosoa, batere mnemoteknikoak ez direlako.

Horregatik, Interneten izen-sistema bat definitu da, erabiltzaileek makinak izendatzeko. Izenak www.rfc-editor.org, jazzvitoria.com, www.konektazaitez.net, gaia.cs.umass.edu edo mailin.sc.ehu.es bezalakoak dira [Rivadeneyra, 2004]. 93

DNS Spoofing DNS zerbitzariek datu baseak dituzte IP helbidearen eta domeinuaren arteko lotura guztiekin.DNS spoofing egitean IP helbidea aldatzen da, horrela webgune baten helbidea idaztean beste leku batera joko du nabigatzaileak. 93

DoS/DDoS Zerbitzuak eteteko erasoak dira, normalean sarean trafiko uholdeak sortuz egiten dira eta makinak edo sareak ezin dio trafiko horri guztiari erantzun, alegia, edo TCP/IP konexioa gainkargatzen da eta sarera konektatzeko sistemaren baliabideak gainkargatzen dira. DDoS erasoak banatutako DoS erasoak dira, hots, makina ezberdinen bitartez gauzatzen da, botnetak erabiltzen dira horretarako. DDoS eraso ezagunenak *islada* erasoak (*reflector attacks*) eta eraso anplifikatuak (*Amplifier attacks*) dira. 1, 14, 93

Exploit Malware bat da. Programa baten ahulezia batez edo akats batez baliatu nahi duen programa bati deitzen zaio. 30, 93

Gizarte ingeniaritza Bitarteko informatikoak edo eta elektronikoak erabiliz, hala nola, internet eta telefonoa, norbaiti iruzur egitearen teknika da hark informazio baliagarria eman dezan. Kevin Mitnickek, saltzaile lana aipatzen du (bere aita adibidetzat hartuz), norbaitek hauen izate eta jarreraz iruzurrak salduz gero gizarte ingeniaria bilakatzen dela dio [Mitnick and Simon, 2002]. Informazio berezia lortzeko *hacker* eta sarkinek erabiltzen duten teknika eta trikimailu multzoari deitzen zaio [Gómez Vieites, 2006]. 93

GPL GNU General Public License. 29, 93

Har Bere burua hedatzeko gai da bestelako fitxategi edo aplikazio baten beharrik gabe. Makinan egon daitezkeen zenbait bitarteko baliatzen ditu bera bakarrik hedatu ahal izateko. Esate baterako, email kontuak eskuratzen ditu eta bere buruaren kopiak bidaltzen ditu. 35, 93

HTTP *HyperText Transfer Protocol* (Hipertestuaren transferentziarako protokoloa) *World Wide Web*ean datuak elkartrukatzeko erabiltzen den protokoloa da.Arakatzaileen eta web zerbitzarien arteko komunikazioetarako protokoloa. HTTPk web bezeroak web zerbitzariari agiri bat nola eskatuko dion definitzen du, baita zerbi-

tzariak bezeroari eskatutakoa nola bidaliko dion ere [Rivadeneyra, 2004]. 15, 93

ICMP ICMP protokoloak bideratzaileek eta erabiltzaileen konputagailuek erabiltzen dituzte beren sarearte-mailan gertatutakoaren berri emateko. Bidaltzen diren paketeen egoera zein den jakiteko balio du. Sare-kontrolerako aplikazioek askotan erabiltzen dituzte. 45, 93

IP helbidea IP protokoloa erabiltzen duen sare batean gailu bat identifikatzen duen zenbakia da. Erabiltzaile bati, Internetera konektatzean, IP helbide bat esleitzen zaio. Helbide hau aldatu egin daiteke konektatzen den bakoitzean; kasu hauetan IP helbide dinamiko deitzen zaio. Interneteko zerbitzariek, ordea, IP helbide estatikoa izaten dute gehienetan, errazago eskuratu ahal izateko beharrezkoa dutelako [wikipedia, a]. 50, 93

IP Spoofing Spoofinga egiteko modu bat da. Sareko edozein IP edo eta erabiltzaile jakin baten IP-a hartuz eta benetan IP hori dagokion makina delakoan berez sarbiderik ez duen lekuetara lortzen sartzeko teknika da. Makina baten zerbitzua eteteko ere balio dezake, hau da, zerbitzua eteteko teknika zaharrenetakoa. Sarean ezin dira IP berdineko bi makina egon, beraz, IP helbideen arteko talka gertatuko litzateke eta kasu horretan bat kanpoan geratuko litzateke.[María Teresa Jimeno García, 2008]. 93

IRC *Internet Relay Chat* (IETF-RFC #1459) Internet bidez txatean aritzeko bat-bateko mezularitza sistema ezaguna da. Komunikazioa batez ere taldeetara zuzenduta dago, jende askoren arteko solasaldietara, alegia. Dena den, bi solaskideren arteko elkarrizketa ere egin daiteke [wikipedia, b]. 93

Keylogger Teklatuan sakatutako botoiak gordetzen dituen programa bat da. 29, 93

Malware Gaizkia edo kaltea eta software hitzen arteko elkarketatik sortutako terminoa da, *malicious software*. Definizio honek kalteak sortzeko programa multzo zabal bat barnebiltzen ditu: botnetak, birusak, Troiar:rak, Backdoorrak, Harrak, spywarea ... Programa horien guztien helburua bera da, kalteak eragitea [INTECO, a]. 5, 18, 93

NISCC National Infrastructure Security Coordination Centre. 15, 93

P2P Puntutik-punturako (*Peer to peer*) sare mota bat da. P2P sareetan P2P protokolo desberdinak definitu daitezke. P2P sareak soilik definitzen du nodoak nola konektatu eta antolatu behar diren. Nodo guztiak bezero eta zerbitzaria dira aldi berean, honela lan karga nodoen artean banatzen delarik. Banda zabalera optimizatu daiteke P2P erabiliz. P2P aplikazioetan parte-hartzaile guztiek paper bera jokatzen dute, ez daude zerbitzariak alde batetik eta bezeroak beste aldetik. Aplikazio-entitate guztiak dira zerbitzari eta bezero aldi berean. Eredua guztiz deszentralizatua da: edozein partaidek eman ditzake beste partaide batek eskatutako zerbitzuak [Rivadeneyra, 2004]. 15, 93

PHDa Proiektuen Helburuen Dokumentua. 93

Phishing *Password fishing* hitzen elkarketatik dator, hau da, pasahitzak arrantzatzea. Internet bidezko iruzur bitartez norbaiten pasahitzak edo eta norabait sartzeko informazio pertsonala eskuratzeko teknika da. Spoofing mota bat da, hein handi batean, datuak eskuratzeko web spoofing eta mail spoofing arteko konbinazio bat erabiltzen duen eraso bat.[María Teresa Jimeno García, 2008]. 22, 93

Rootkit *Root* edo administratzaile baimenak eskuratzeko malwarea da. Kudeatzaile baimenik ez dituzten erabiltzaileei aukera ematen die baimen horik eskuratzeko, kautotze sistemak trukatzeko eta baimen horiek mantentzeko ezarpenak jartzen [McClure et al., 2003]. 42, 93

Scanning Portu irekiak eta sistemaren ezaugarriak ezagutzeko teknika. Scanner motako tresnen bitartez makinak izan ditzakeen ahuleziak zeintzuk diren ondoriozta daitezke. 30, 93

Sniffer Sareko trafikoa xurgatzeko tresna da, hau da, sareko paketeak aztertzeko edo zelatatzeko. 20, 93

spam Iragarkiak edo eta kalteak sortzeko helburua duten eta jaso nahi ez diren emailak [Mallery et al., 2005]. 1, 15, 93

Spoofing Nortasun ordezkapena egitean oinarritzen den teknika da. Spoofingaren helburua konfiantza lotura mantentzea da. Spoofing teknika sofistikatuenak oinarrian gizarte ingeniaritza teknikak dira. Batzuetan pertsonei iruzur egin edo eta makinei iruzur egitea da helburua. Spoofing tekniken artean aurki daitezke, IP spoofinga, DNS spoofinga, ARP spoofinga, mail spoofinga, web spoofinga... [María Teresa Jimeno García, 2008] . 93

TCP *Transmission Control Protocol* Interneteko oinarrizko protokoloetako bat da, berari esker sarean barrena programa askok haien artean datuak truka ditzakete errorerik gabe eta ordenan iritsiko diren ziurtasunarekin. Garraio-mailako zerbitzu fidagarria TCP protokoloaren bidez ematen da [Rivadeneyra, 2004]. 93

Tipularen biderapena Bideragailu ezberdinen artean ausaz eraikitako zirkuitu birtual baten bidez anonimotasuna bermatzen duen teknika da. *Tor* programak teknika hori erabiltzen du, nodoen arteko komunikazioak zifratzen dituelako. Lehenik azken nodoarekin negoziatzen du paketearen zifraketarako gakoak, ondoren azken aurrekoarekin eta horrela nodoz nodo, beraz, zifratze geruza ezberdinekin babesten da paketea eta horrexegatik ematen zaio *tipularen biderapena* izena. transmisioa seguruagoa da baina mantsoagoa da ere.[Lockhart, 2006]. 75, 93

Troiar: Malware honek ez du bere burua birsortzeko edo auto-hedatzeko gaitasunik, hortaz, erasotzailearen aginduak beharrezkoak dira troiar baten funtzionamendurako. Troiako Zaldiaren istorioan oinarritutako metafora bat da izena, hau da, “opari"edo mezu bat delakoan, erabiltzailearen oharpenik gabe beste kodigo bat exekutatzen da. Gizarte ingeniaritza baliatuz, norbaitek software kaltegarria instala dezake sisteman. Erabiltzailea ohartu gabe, RAT (*Remote Access Transmission*) motak troiar baten bidez portuak ireki eta sistema kontrola daiteke urrunetik.[McClure et al., 2003, David et al., 2002]. 35, 93

UDP TCPren antzekoa da baina protokolo honen helburua azkartasuna da, hau da, helburua datuak azkar iristea da. Garraio-mailak aplikazio-mailari arintasuna eskaintzen dio UDP bitartez. Ez dago transmisioaren kontrolik ez bestelako kontrolik ere. Bere betebehar bakarra jatorrizko eta helburuko aplikazio-entitatea identifikatzea da [Rivadeneyra, 2004]. 21, 93

Bibliografia

[Apvrille, 2012] Apvrille, A. (2012). Symbian worm yxes: towards mobile botnets? *Journal in Computer Virology*.

[Bacher et al., 2008] Bacher, P., Holz, T., Kotter, M., and Wicherski, G. (2008). Know your enemy: Tracking botnets (using honeynets to learn more about bots). Technical report, The Honeynet Project.

[Barford and Yegneswaran, 2007] Barford, P. and Yegneswaran, V. (2007). An inside look at botnets. In *Malware Detection*, pages 171–191. Springer.

[Barroso, 2008] Barroso, D. (2008). Mccolo: bullet-proof hosting in the usa. online.

[Boscovich, 2011] Boscovich, R. (2011). Microsoft offers reward for information on rustock.

[C. et al., 2010] C., W., J., M., D., M., B., G., S., E., J., B., and T., A. (2010). Symantec global internet security threat report trends for 2009. Technical report, Symantec.

[Calvet et al., 2010] Calvet, J., R. Davis, C., Fernandez, J. M., Marion, J.-Y., St-Onge, P.-L., Guizani, W., Bureau, P.-M., and Anil, S. (2010). The case for in-the-lab botnet experimentation: creating and taking down a 3000-node botnet. In *Annual Computer Security Applications Conference*, Austin, Texas, États-Unis.

[Canavan, 2005] Canavan, J. (2005). The evolution of malicious irc bots. Technical report, Symantec.

[Cert/cc and Cert/cc, 2005] Cert/cc, N. I. and Cert/cc, A. H. (2005). Botnets as a vehicle for online crime cert © coordination center.

[Cho et al., 2010] Cho, C. Y., Caballero, J., Grier, C., Paxson, V., and Song, D. (2010). Insights from the inside: a view of botnet management from infiltration. In *Proceedings of the 3rd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more*, LEET'10, pages 2–2, Berkeley, CA, USA. USENIX Association.

[Constantin, 2009] Constantin, L. (2009). Botnet tool to support israel's offensive. Online.

[Corrons, 2010] Corrons, L. (2010). Red de bots mariposa.

[Daniel Plohmann, 2011] Daniel Plohmann, Elmar Gerhards-Padilla, F. L. (2011). Botnets: Detection, measurement, disinfection & defence. Technical report, ENISA.

[David et al., 2002] David, H., Robert, S., and Urs, G. (2002). *Virus Informaticos*. McGraw-Hill/Osborne.

[David, 2004] David, J. (2004). Dns, honeynets y darknets utilizadas en el monitoreo pasivo de red en ambientes académicos. In *DNS, honeynets y darknets utilizadas en el monitoreo pasivo de red en ambientes académicos.* Universidad Nacional Autónoma de México.

[Dennis et al., 2011] Dennis, B., Shah, B., Joe, B., and Eve, B. (2011). Microsoft security intelligence report. Technical report, Microsoft.

[Dittrich and Dietrich, 2008] Dittrich, D. and Dietrich, S. (2008). P2p as botnet command and control: a deeper insight. In *In Proceedings of the 3rd International Conference On Malicious and Unwanted Software (Malware 2008)*, pages 46–63.

[Dunham, 2009] Dunham, K. (2009). *Mobile Malware Attacks and Defense*. Syngress Publishing.

[El-Pais, 2010] El-Pais (2010). Botnets, el lado oscuro de internet. Online.

[ESET, 2010] ESET (2010). Trends for 2011: Botnets and dynamic malware. Technical report, ESET Latin America.

[Falliere and Chien, 2009] Falliere, N. and Chien, E. (2009). Zeus: King of the bots. Technical report, Symantec | Security Response.

[Franklin and Perrig, 2007] Franklin, J. and Perrig, A. (2007). An inquiry into the nature and causes of the wealth of internet miscreants. In *Proceedings of the 14th ACM conference on Computer and communications security*, CCS '07, pages 375–388, New York, NY, USA. ACM.

[Garza, 2010] Garza, G. (2010). Operation b49: Waledac botnet take down.

[Gómez Vieites, 2006] Gómez Vieites, A. (2006). *Enciclopedia de la Seguridad Informática*. RA-MA.

[Gu et al., 2008] Gu, G., Zhang, J., and Lee, W. (2008). Botsniffer: Detecting botnet command and control channels in network traffic. In *BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic*.

[Hadnagy, 2010] Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*. John Wiley & Sons.

[Hernando, 2006] Hernando, S. (2006). Botnets como herramientas de fraude en sistemas de pago por click. Online.

[INTECO, a] INTECO. Malware.

[INTECO, b] INTECO. Recomendaciones para la creación y uso de contraseñas seguras. Online.

[INTECO, 2006] INTECO (2006). Amenazas silenciosas en la red: rootkits y botnets. Technical report, INTECO.

[INTECO, 2007] INTECO (2007). Consejos generales de seguridad. Technical report, INTECO.

[Internautas, 2010] Internautas, A. (2010). Intento de phishing a clientes de banco de valencia.

[Kola, 2008] Kola, M. K. (2008). *Botnets: Overview and Case Study*. PhD thesis, Mercy College.

[Korns and Kastenberg, 2008] Korns, S. W. and Kastenberg, J. E. (2008). Georgia's cyber left hook. *Parameters*, 38(4):60–76.

[Labs, 2011] Labs, M. (2011). Malware in recent korean ddos attacks destroys systems. Online.

[Lashkari et al., 2011] Lashkari, A. H., Ghalebandi, S. G., and Moradhaseli, M. R. (2011). A wide survey on botnet. In Cherifi, H., Zain, J. M., and El-Qawasmeh, E., editors, *DICTAP (1)*, volume 166 of *Communications in Computer and Information Science*, pages 445–454. Springer.

[Leder et al., 2009] Leder, F., Werner, T., and Martini, P. (2009). Proactive botnet countermeasures – an offensive approach. In *!st CCDECEO Conference on Cyber Warfare*.

[Lockhart, 2006] Lockhart, A. (2006). *Network security hacks - tips and tools for protecting your privacy*. O'Reilly.

[Mallery et al., 2005] Mallery, J., Zann, J., amd W.Ñooman, P. K., Seargen, E., Love, P., Kraft, R., and O'Neill, M. (2005). *Blindaje de redes tu red invulnerable a los hackers*. ANAYA MULTIMEDIA.

[Marissa, 2010] Marissa, V. (2010). Four ways cybercriminals profit from botnets. Online.

[Martínez, 2011] Martínez, R. T. (2011). Los botnets.

[María Teresa Jimeno García, 2008] María Teresa Jimeno García, Carlos Míguel Pérez. Abel Mariano Matas García, J. P. A. (2008). *Hacker Edicion 2009*. Grupo Anaya, S.A., 2009 edition.

[McClure et al., 2003] McClure, S., Scambray, J., and Kurtz, G. (2003). *Hacking Exposed: Network Security Secrets and Solutions, Fourth Edition*. McGraw-Hill, Inc., New York, NY, USA, 4 edition.

[Microsoft,] Microsoft. Las contraseñas deben cumplir los requerimientos de complejidad. Online.

[Microsoft, 2010] Microsoft (2010). R.i.p. waledac: Undoing the damage of a botnet.

[Mirkovic et al., 2004] Mirkovic, J., Dietrich, S., Dittrich, D., and Reiher, P. (2004). *Internet Denial of Service: Attack and Defense Mechanisms (Radia Perlman Computer Networking and Security)*. Prentice Hall PTR, Upper Saddle River, NJ, USA.

[Mitnick and Simon, 2002] Mitnick, K. D. and Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons, Inc., New York, NY, USA, 1st edition.

[Namestnikov, 2009] Namestnikov, Y. (2009). The economics of botnets. Technical report, Kaspersky Lab.

[NISCC, 2005] NISCC (2005). Targeted trojan email attacks. Technical report, Centre for the Protection of National Infrastructure.

[Ollmann, 2009a] Ollmann, G. (2009a). Top-10 botnet malware families of 2009. online.

[Ollmann, 2009b] Ollmann, G. (2009b). Top-10 botnet outbreaks in 2009. online.

[Parolli, 2011] Parolli, M. (2011). Botnets: La mafia silenciosa. Master's thesis, Universidad Nacional-Regional Mendoza.

[Porras et al., 2010] Porras, P., Saïdi, H., and Yegneswaran, V. (2010). An Analysis of the iKee.B iPhone Botnet. In Akan, O., Bellavista, P., Cao, J., Dressler, F., Ferrari, D., Gerla, M., Kobayashi, H., Palazzo, S., Sahni, S., Shen, X. S., Stan, M., Xiaohua, J., Zomaya, A., Coulson, G., Schmidt, A. U., Russello, G., Lioy, A., Prasad, N. R., and Lian, S., editors, *Security and Privacy in Mobile Information and Communication Systems*, volume 47 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, chapter 12, pages 141–152. Springer Berlin Heidelberg, Berlin, Heidelberg.

[Pras et al., 2010] Pras, A., Sperotto, A., Moura, G. C., Drago, I., Barbosa, R., Sadre, R., Schmidt, R., and Hofstede, R. (2010). Attacks by "anonymous" wikileaks proponents not anonymous.

[Rafael, 2011] Rafael, P. (2011). Sistemas de monitorización social. Online.

[Rajiv, 2012] Rajiv, V. D., editor (2012). *Study of Mobile Botnets: An Analysis from the Perspective of Efficient Generalized Forensics Framework for Mobile Devices*. International Journal of Computer Applications.

[Rivadeneyra, 2004] Rivadeneyra, J. (2004). *TCP/IP SAREAK 2*. UPV/EHU, 2 edition.

[SANS,] SANS, I. Password policy. Online.

[Schiller and Harley, 2007] Schiller, C. and Harley, D. (2007). *Botnets: The Killer Web App*. Syngress Publishing.

[Silva et al., 2013] Silva, S. S. C., Silva, R. M. P., Pinto, R. C. G., and Salles, R. M. (2013). Botnets: A survey. *Computer Networks*, 57(2):378–403.

[SSAC, 2008] SSAC (2008). Fast and double flux attacks. Technical report, ICANN.

[Stock et al., 2009] Stock, B., Göbel, J., Engelberth, M., Freiling, F. C., and Holz, T. (2009). Walowdac - analysis of a peer-to-peer botnet. In *Proceedings of the 2009 European Conference on Computer Network Defense*, EC2ND '09, pages 13–20, Washington, DC, USA. IEEE Computer Society.

[Strayer et al., 2008] Strayer, W. T., Lapsley, D. E., Walsh, R., and Livadas, C. (2008). Botnet detection based on network behavior. In *Botnet Detection*, pages 1–24. Springer.

[Symantec, 2011] Symantec (2011). Symantec intelligence quarterly. Online.

[Thompson, 2010] Thompson, M. (2010). Mariposa botnet analysis. Technical report, DefenceIntelligence.

[Traynor et al., 2009] Traynor, P., Lin, M., Ongtang, M., Rao, V., Jaeger, T., McDaniel, P., and La Porta, T. (2009). On cellular botnets: measuring the impact of malicious devices on a cellular network core. In *CCS '09: Proceedings of the 16th ACM conference on Computer and communications security*, pages 223–234. ACM.

[Tyagi and G.Aghila, 2011] Tyagi, A. K. and G.Aghila (2011). Article: A wide scale survey on botnet. *International Journal of Computer Applications*, 34(9):10–23. Published by Foundation of Computer Science, New York, USA.

[W. and R., 2007] W., S. and R., D. (2007). Know your enemy: Fast-flux service networks. Online.

[Wang et al., 2011] Wang, P., Aslam, B., and Zou, C. C. (2011). Peer-to-peer botnets: The next generation of botnet attacks.

[wikipedia, a] wikipedia. Ip helbide. Online.

[wikipedia, b] wikipedia. Irc. online.

[Williams, 2011] Williams, J. (2011). Operation b107 - rustock botnet takedown.

[Zeng, 2012] Zeng, Y. (2012). *On Detection of Current and Next-Generation Botnets*. PhD thesis, The University of Michigan.

[Zhang et al., 2011] Zhang, L., Yu, S., Wu, D., and Watters, P. (2011). A survey on latest botnet attack and defense. In *Proceedings of the 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, TRUSTCOM '11, pages 53–60, Washington, DC, USA. IEEE Computer Society.