Sigurnosna inteligencija u korporacijama

Jovanovski, Grga

VISOKO UČILIŠTE ALGEBRA

ZAVRŠNI RAD

SIGURNOSNA INTELIGENCIJA U KORPORACIJAMA

Grga Jovanovski

Zagreb, kolovoz 2017.

Student vlastoručno potpisuje Završni rad na prvoj stranici ispred Predgovora s datumom i oznakom mjesta završetka rada te naznakom:

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor, te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada".

U Zagrebu, 04.09.2017.

Predgovor

Zahvaljujem svojim roditeljima na podršci tijekom studiranja. Također zahvaljujem svome mentoru i svim profesorima koji su podijelili svoje znanje s nama studentima tijekom studija.

Hvala svim kolegama i kolegicama za nezaboravne tri godine studija.

Prilikom uvezivanja rada, Umjesto ove stranice ne zaboravite umetnuti original potvrde o prihvaćanju teme završnog rada koji ste preuzeli u studentskoj referadi

Sažetak

U ovom radu objašnjeno je što je sigurnosna inteligencija te kako ju korporacije koriste za održavanje sigurnosti informacijskog sustava. Objašnjeni su pojmovi koji čine sigurnosnu inteligenciju, sigurnost i inteligencija.

Spomenuti su zakoni i pravne regulative povezane uz sigurnost informacijskih sustava. Prikazani su trendovi računalnog kriminala u Republici Hrvatskoj i broj razriješenih slučajeva.

Objašnjene su najpoznatije prijetnje informacijskom sustavu korporacije te odjeli korporacije kojima je posao obraniti informacijski sustav od prijetnji.

Prikazan je način analize zlonamjernih sadržaja različitim alatima te je analiza podijeljena na statičku i dinamičku analizu. Uz statičku i dinamičku analizu prikazana je i analiza javno dostupnim servisima. U prilogu rada nalaze se primjeri tri izvješća analize zlonamjernih sadržaja.

Opisane su vrste obrane koje korporacija može koristiti.

Ključne riječi: sigurnosna inteligencija, zlonamjerni sadržaj, analiza, prijetnje, računalni kriminal

Summary

This paper explains security intelligence and how corporations use it to maintain the security of information systems. Concepts that compile security intelligence, security and intelligence are explained.

Information security laws and regulations are mentioned. The computer crime trends in the Republic of Croatia and the number of cases resolved are presented.

Most famous threats to corporate information systems and departments that fight against these threats are explained.

The way of analyzing malicious content with different tools is presented and the analysis is divided into static and dynamic analysis. The paper also demonstrates analysis on publicly available malware analysis platforms. Attached to the paper are examples of three reports of malicious content analysis.

Different types of defense against threats are described.

Keywords: security intelligence, malicious content, analysis, threats, cybercrime

Sadržaj

1. Uvod

Današnje korporacije uvelike ovise o informacijskim tehnologijama. Svi dijelovi poslovanja, uključujući i glavne poslovne procese, ovise o dostupnosti informacijskog sustava korporacije.

Takva informatizacija korporacijama olakšava poslovanje, no, s druge strane, otvara niz mogućnosti za ometanje ili prekid poslovanja koje nisu bile moguće prije dvadesetak godina.

Niti jedan sustav nije potpuno siguran. Svaki sustav, bio on poslovni ili osobni, moguće je ugroziti. To dobro opisuje sljedeći citat.

„Jedini uistinu siguran sustav je onaj koji je isključen, bačen u blok betona i zapečaćen u olovnoj prostoriji s naoružanim stražarima.“ (Dewdney, 1989)

To ne znači da bi korporacije trebale odustati od kibernetičke obrane, naprotiv, potrebno je aktivno primjenjivati sigurnost te je uvesti kao jedan od ključnih dijelova svakodnevnog poslovanja.

Efektivna obrana ovisi o prikupljanju i analizi informacija o potencijalnim prijetnjama poslovanju. Ovdje se sigurnosna inteligencija postavlja kao glavni čimbenik informacijske sigurnosti.

2. Sigurnosna inteligencija

Sigurnosna inteligencija podrazumijeva sve analizirane i obrađene informacije koje su korisne za sigurnost neke imovine te obranu te imovine od neke prijetnje ili ugroze.

„Sigurnosna inteligencija se koristi u svim granama korporativne sigurnosti:

- Fizička zaštita imovine
- Fizička zaštita zaposlenika
- Kontinuitet poslovanja
- Upravljanje i odgovor na krize
- Informacijska sigurnost
- Sigurnost informacija i podataka
- Unutarnje istrage
- Sprječavanje prijevara i pranja novca
- Zaštita marke“ (Crump, 2015)

Cilj sigurnosne inteligencije je dati uvid u trenutno stanje sigurnosti korporacije te pomoći pri suzbijanju i eliminaciji prijetnji.

2.1. Sigurnost

„Sigurnost je jedna od osnovnih pretpostavki ljudskog života i jedna od osnovnih ljudskih potreba. Stoga je interes u ovom području za sve aspekte ljudske aktivnosti potpuno prirodni i racionalni fenomen.“ (Bilandžić et al., 2014)

Sigurnost (engl. *security*) u širem smislu riječi je obrana od neke prijetnje. *Institute for Security and Open Methodologies* (skraćeno ISECOM) definira sigurnost kao vrstu obrane gdje se stvara razmak između imovine i prijetnje. Taj razmak predstavlja niz sigurnosnih kontrola koje osiguravaju da prijetnja ne može doći do štićene imovine.

U informacijskoj sigurnosti štićenu imovinu predstavljaju informacije i uređaji koji obrađuju te informacije. Informacije su najčešće zapisi u bazama podataka koji se moraju štititi od neovlaštene izmjene, curenja ili brisanja. Uređaji koji obrađuju informacije su računala, poslužitelji, komunikacijska infrastruktura i aplikacije.

U niti jednoj grani sigurnosti ne postoji stopostotna sigurnost te je svaki sustav ranjiv na neki način.

2.2. Inteligencija

„Inteligencija i informacije su dva različita pojma. Informacije nas okružju, ali uglavnom u obliku sirovih podataka, bez konteksta i koherentnosti. S druge strane, inteligencija je razmatrani i profinjeni proizvod koji daje uvid." (Crump, 2015)

Iz ove definicije može se zaključiti da inteligenciju čine sve sakupljene informacije iz okoline, analizirane kako bi se iz njih izvukli korisni zaključci i odluke. U svijetu informacijske i komunikacijske tehnologije inteligencija može biti široki pojas analiziranih informacija kao što su: dnevnik (engl. *log*), mrežni promet i promet elektroničke pošte.

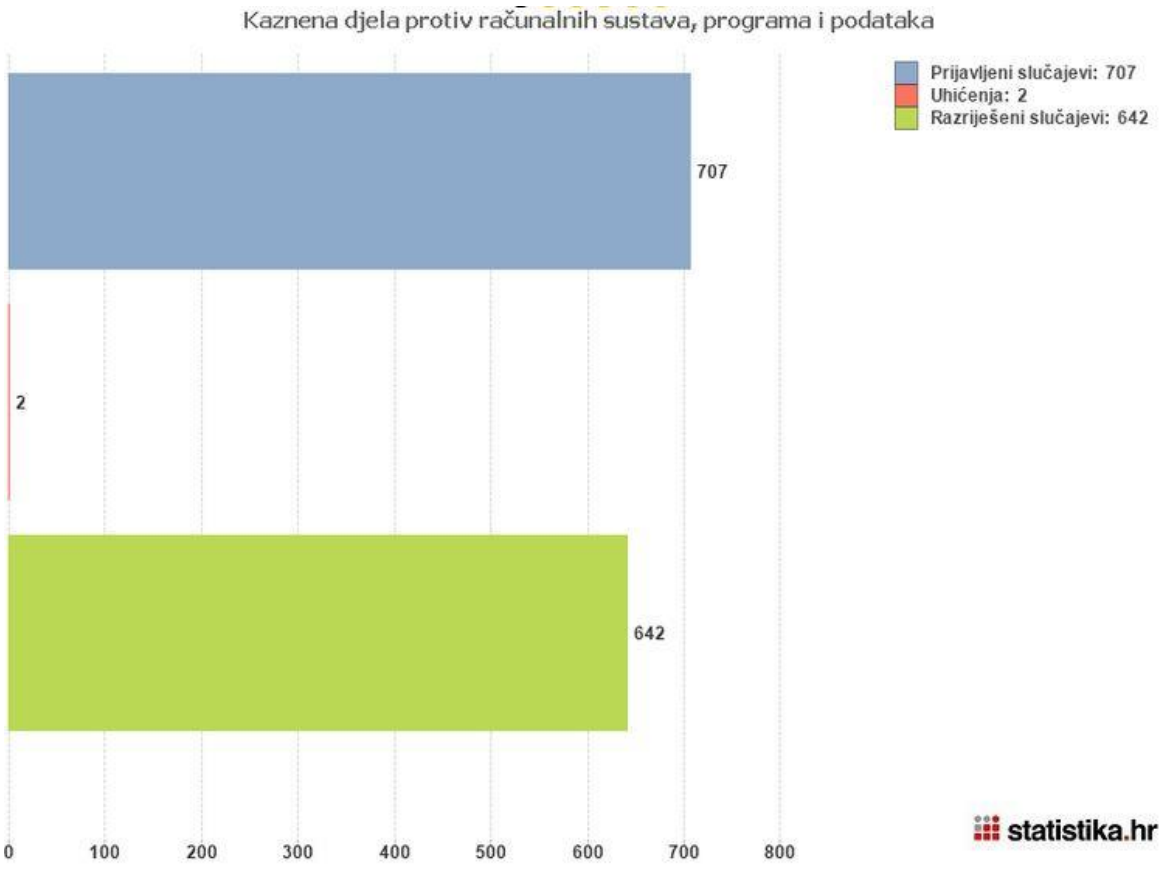
U sigurnosti je inteligencija bilo koja informacija koja može pridonijeti otkrivanju, suzbijanju, eliminaciji ili obrani od neke prijetnje. Upravo zbog toga je inteligencija vrlo važan dio sigurnosti, ako ne i najvažniji.

3. Računalni kriminalitet

Računalni kriminalitet je bilo koje kriminalno djelo izvedeno protiv nekog računalnog sustava ili uz pomoć računalnog sustava.

Porastom informatizacije društva raste i količina ovakvog kriminala. Svaka država mora moći definirati što je računalni kriminal i efektivno ga suzbiti i kazniti.

Graf prijavljenih i razriješenih slučajeva računalnog kriminala u 2013. godini prikazan je sljedećom slikom (Slika 3.1). Više od 90% slučajeva je razriješeno.



Slika 3.1 Graf prijavljenih i razriješenih slučajeva računalnog kriminala u 2013. godini (Statistika.hr, 2014)

3.1. Pravni aspekti informacijske sigurnosti

Postoji nekoliko dokumenata koji propisuju postupke i kazne vezane uz računalne sustave i njihovu sigurnost:

- Konvencija o kibernetičkom kriminalu (2001)
- Uredba o mjerama informacijske sigurnosti (2008)
- Zakon o informacijskoj sigurnosti (2007)
- Nacionalna strategija kibernetičke sigurnosti (2015)
- Kazneni zakon, glava dvadeset peta (2015)

Konvencija o kibernetičkom kriminalu je prva međunarodna konvencija o računalnom kriminalu. Bavi se krivotvorenjem, prijevarom, dječjom pornografijom i informacijskom sigurnošću. Republika Hrvatska je Konvenciju prihvatila 2002. godine.

Uredba o mjerama informacijske sigurnosti definira postupanje s klasificiranim podacima. Ova uredba je bitna za svaku korporaciju koja želi poslovati negdje gdje se rukuje s klasificiranim podacima, najčešće su to državni poslovi i poslovni nacionalne sigurnosti.

„Zakon o informacijskoj sigurnosti utvrđuje pojam informacijske sigurnosti, mjere i standarde informacijske sigurnosti, područja informacijske sigurnosti te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti.“ (Zakon o informacijskoj sigurnosti, 2007)

Nacionalna strategija kibernetičke sigurnosti definira načela, ciljeve, dionike i područje kibernetičke sigurnosti.

Kazneni zakon u svojoj dvadeset petoj glavi definira vrste računalnog kriminala te propisane kazne zatvora za svaku od njih.

3.2. Vrste računalnog kriminala

Vrste računalnog kriminala su nabrojane i opisane u Kaznenom zakonu, glavi dvadeset pet.

Prva vrsta računalnog kriminala je neovlašteni pristup nekom računalnom sustavu ili računalnim podacima. Neovlašteni pristup podrazumijeva pristupanje nekom računalnom sustavu za koje nemamo ovlasti.

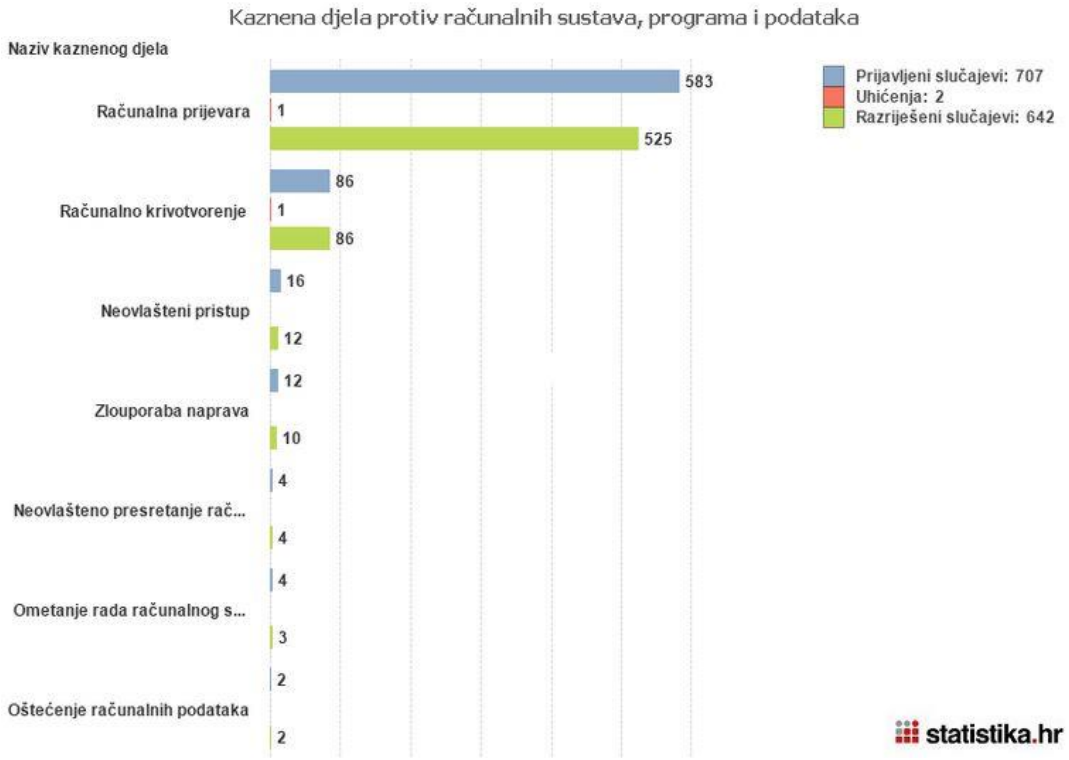
Druga vrsta računalnog kriminala je ometanje rada računalnog sustava. Ometanje rada je bilokakvo usporavanje ili onemogućavanje rada sustava.

Oštećenje računalnih podataka podrazumijeva neovlaštenu izmjenu, brisanje, uništavanje i onemogućavanje pristupa podacima. Uz oštećenje postoji i neovlašteno presretanje računalnih podataka, tj. snimanje podataka.

Računalno krivotvorenje i računalna prijevara su sljedeće dvije vrste računalnog kriminala. Krivotvorenje podrazumijeva izmjenu podataka koji imaju neku vrijednost ili izmjenu nekih drugih podataka kako bi ti podaci dobili vrijednost. Prijevara podrazumijeva izmjenu podataka na način kojim se nanosi šteta nekome drugom.

Posljednja vrsta je zlouporaba naprava. Zlouporaba naprava je izrada, prodaja ili posjedovanje specijalnih sustava koji omogućuju počinjenje gore navedenih kriminalnih djela. U zlouporabu naprava spada i posjedovanje i prodaja računalnih lozinki ili nekih drugih podataka potrebnih za pristup nekom računalnom sustavu.

Graf prijavljenih i razriješenih slučajeva po vrsti računalnog kriminala u 2013. godini prikazan je na sljedećoj slici (Slika 3.2). Vidljivo je da daleko najveći udio zauzima računalna prijevara i krivotvorenje.



Slika 3.2 Graf prijavljenih i razriješenih slučajeva po vrsti računalnog kriminala u 2013. godini (Statistika.hr, 2014)

3.3. Institucije za sprječavanje računalnog kriminala

U svakoj državi postoji nekoliko institucija za sprječavanje računalnog kriminala. Glavna institucija koju ima većina država je računalni tim za hitne intervencije (engl. *Computer*

Emergency Response Team, skraćeno CERT), a njegov djelokrug djelovanja propisan je u Zakonu o informacijskoj sigurnosti.

CERT je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj. (Zakon o informacijskoj sigurnosti, 2007) CERT je dio hrvatske akademske i istraživačke mreže (skraćeno CARNet) i zadužen je za sigurnosne incidente na javnim računalnim sustavima u Republici Hrvatskoj ili u drugim zemljama i organizacijama koje su povezane s Republikom Hrvatskom.

Zavod za sigurnost informacijskih sustava propisuje standarde sigurnosti informacijskih sustava, sigurnosne akreditacije informacijskih sustava, upravlja kripto materijalima koji se koriste u razmjeni klasificiranih podataka te odgovara na računalne ugroze sigurnosti informacijskih sustava.

Odjel za visokotehnološki kriminal Ministarstva unutarnjih poslova (skraćeno MUP), osnovan 2012. godine, služi suzbijanju kriminala u području računalnih tehnologija. Iako se bavi raznim vrstama računalnog kriminala, usmjeren je na suzbijanje kriminala u području intelektualnog vlasništva.

Posljednja institucija je Ured Vijeća za nacionalnu sigurnost (skraćeno UVNS) koje donosi mjere i standarde za razmjenu klasificiranih i neklasificiranih podataka između Republike Hrvatske i stranih zemalja i organizacija. Uz to, UVNS donosi i nekoliko pravilnika: Pravilnik o standardima sigurnosne provjere, Pravilnik o standardima fizičke sigurnosti, Pravilnik o standardima sigurnosti podataka, Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava te Pravilnik o standardima sigurnosti poslovne suradnje. UVNS je također zadužen za koordinaciju i upravljanje Nacionalnog CERT-a i Zavoda za sigurnost informacijskih sustava.

4. Računalne prijetnje korporacijama

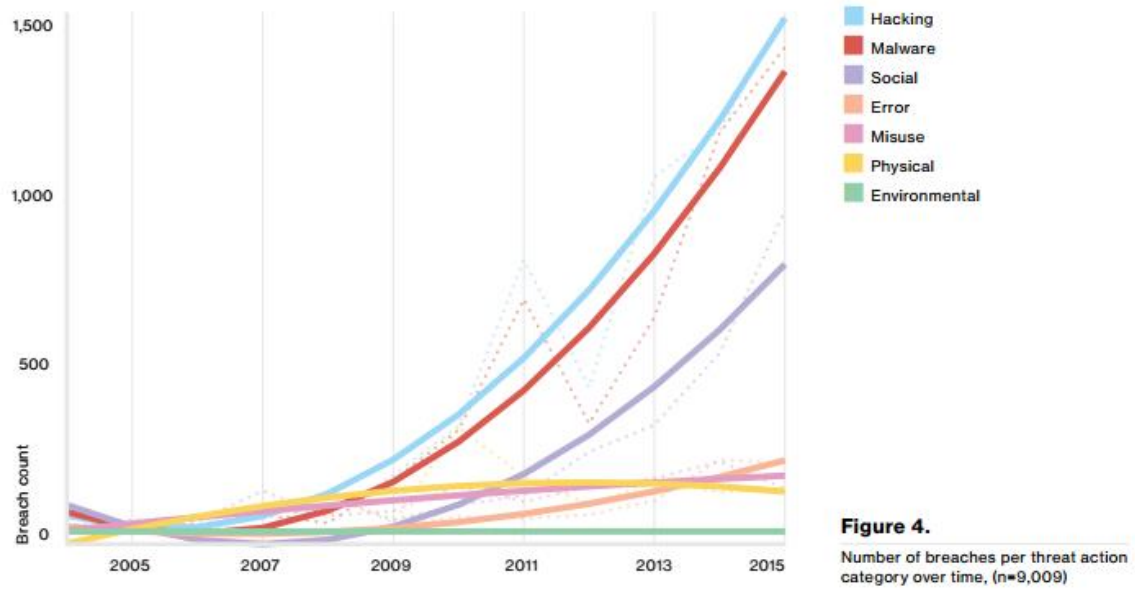
Današnje korporacije uvelike ovise o informacijskoj tehnologiji pa je informacijska sigurnost zbog toga postala jedna od najvažnijih vrsta korporativne sigurnosti.

Sve prijetnje korporacijama imaju jedan zajednički cilj: uništiti, ukrasti ili promijeniti podatke koji se nalaze u informacijskom sustavu korporacije.

4.1. Vrste prijetnji, njihov utjecaj i trendovi

Postoji nekoliko glavnih vrsti prijetnji u korporativnoj okolini. Svaka od njih donosi drugačije neželjene posljedice za korporaciju.

Graf kretanja prijetnji prikazan je na sljedećoj slici (Slika 4.1). Iz grafa se može iščitati da su hakiranje, zlonamjerni sadržaji i socijalni inženjering u velikom porastu od 2007. godine, dok ostale starije vrste prijetnji stagniraju.



Slika 4.1 Graf kretanja prijetnji (Verizon, 2016)

4.1.1. Napadi zlonamjernim sadržajima

Ovaj način napada podrazumijeva slanje zlonamjernog koda preko nekog kanala komunikacije korporacije, najčešće kanala elektroničke pošte.

Veliki dio ovih napada nije usmjeren na točno određenu korporaciju. Većina ovakvih napada ostvaruje se slanjem velike količine zaraženih privitaka u porukama elektroničke pošte na različite adrese, uz očekivanje da će barem dio tih privitaka biti otvoren od strane nekog zaposlenika u nekoj kompaniji. Obrana od ovakvih napada jednostavna je uz pomoć vatrozida (engl. *firewall*) elektroničke pošte, koji će većinu ovakvih poruka odbaciti.

Mali dio ovih napada je opasan. Taj dio sačinjavaju napadi koji su namijenjeni za točno određenu korporaciju. Napadač kod ovakvog napada istražuje razinu informacijske sigurnosti korporacije pa po tome oblikuje napad kako bi on imao što veću uspješnost. U slučaju elektroničke pošte to podrazumijeva oblikovanje zlonamjernog sadržaja kako bi prošao filtar vatrozida elektroničke pošte i završio u ulaznoj pošti nekog od zaposlenika. Na kraju je ostalo samo da poruka bude dovoljno uvjerljiva kako bi zaposlenik otvorio zaraženi privitak.

Štetne posljedice otvaranja zaraženog privitka mogu biti velike. Trenutno najpopularniji napad je onaj koji zahtijeva otkupninu (engl. *ransomware*). Nakon otvaranja datoteke koja sadrži *ransomware* podaci na računalu žrtve se kriptiraju te napadač zahtijeva određenu količinu novca u zamjenu za ključ koji će dekriptirati podatke. Posljedice ovakvog napada mogu biti još veće ukoliko taj *ransomware* kriptira podatke na računalu u slučaju kada postoji dijeljenje direktorija kojima žrtva ima pristup, time dolazi u opasnost velika količina korporativnih dokumenata.

Obrana od ciljanih napada zlonamjernim sadržajima može biti realizirana edukacijom korisnika i nabavkom specijaliziranih rješenja, što će svaki privitak ili skinutu datoteku automatski pokrenuti u sigurnoj okolini i analizirati njezino ponašanje.

4.1.2. Napad uskraćivanjem usluge

Napad uskraćivanjem usluge (engl. *Denial of Service*, skraćeno DOS) sastoji se od slanja velike količine prometa prema određenom uređaju korporacije, najčešće web serveru ili usmjerniku. Zbog velike količine prometa uređaj neće moći obrađivati legitimni promet pa će postati nedostupan za korištenje. Dok god napad traje uređaj neće biti u mogućnosti obrađivati legitimni promet.

Napadač će najprije zaraziti stotine ili tisuće uređaja koji imaju pristup Internetu, staviti ih zajedno u grupu (engl. *botnet*) te preuzeti kontrolu nad njima. Preko takvih uređaja napadač će generirati veliku količinu prometa koja je potrebna da izveze DOS napad. U ovom slučaju

se takav napad zove distribuirani napad uskraćivanjem usluge (engl. *Distributed Denial of Service*, skraćeno DDOS).

Posljedice za korporaciju nakon ovakvog napada su nemogućnost nastavka poslovanja. Ukoliko korporacija provodi web prodaju, a njihov web server je napadnut, oni neće moći prodati niti jedan proizvod dok god napad ne prestane ili se zaustavi.

Ukoliko je napadnut neki usmjernik (engl. *router*) koji služi za komunikaciju korporacije, korporacija neće moći komunicirati na kanalu koji je zahvaćen napadom. Napad na usmjernike opasan je za telekomunikacije kompanija koje ovise o otvorenosti komunikacijskih kanala.

4.1.3. Socijalni inženjering

Socijalni inženjering cilja na najslabiju točku informacijskog sustava, korisnike. Napadač će različitim taktikama i načinima uvjeravanja pokušati izvući informacije od zaposlenika ili uvjeriti zaposlenika da odradi neku radnju na svom računalu koja će napadaču omogućiti pristup.

U većini ovakvih napada napadač će se predstaviti kao legitimna korporacija ili stvarna osoba.

Primjer ovakvog napada je elektronička pošta koja izgleda kao da dolazi od legitimne korporacije, na primjer PayPal, te traži da korisnik upiše svoje podatke. Upisani podaci će se spremiti na napadačev sustav te će on nakon toga imati pristup PayPal računu korisnika.

U socijalni inženjering spada i telefonska prijevara (engl. *vishing*). Prilikom *vishinga* žrtva prima telefonski poziv ili elektroničku poruku gdje napadač govori da je žrtvin račun u banci ili neki drugi financijski dio u opasnosti zbog sumnjivih aktivnosti. Uz to, napadač traži žrtvu da nazove određeni telefonski broj i dâ informacije o svojoj kartici kako bi se utvrdio identitet vlasnika. Nakon što žrtva to napravi, napadač ima sve informacije o kartici žrtve pa te informacije može iskoristiti u zlonamjerne svrhe.

4.2. Odjeli informacijske sigurnosti u korporacijama

Većina malih i srednjih kompanija nema određene odjele za informacijsku sigurnost te većinu poslova oko sigurnosti odrađuju sistem administratori i informatička podrška.

Velike korporacije u velikoj većini slučajeva imaju određene timove za informacijsku sigurnost. Ti timovi se bave pronalaženjem i uklanjanjem računalnih prijetnji. Uz njih djeluju i odjel za fizičku sigurnosti te odjel za prijevare.

4.2.1. Uprava za sigurnost i njen ured

Uprava za sigurnost i njezin ured glavni je i najviši odjel za sigurnost u korporaciji. Predsjednik uprave za sigurnost (engl. *Chief Security Officer*, skraćeno CSO) nadgleda i upravlja svim aspektima sigurnosti u korporaciji. Članovi uprave za sigurnost nadležni su za različite dijelove sigurnosti; najčešće se dijele na fizičku sigurnost i informacijsku sigurnost.

Ured uprave za informacijsku sigurnost upravlja timovima za informacijsku sigurnost i odlučuje kako će se postupati prema određenoj prijetnji na temelju informacija dobivenih od centra za operativnu sigurnost.

4.2.2. Centar za operativnu sigurnost

Centar za operativnu sigurnost (engl. *Security Operations Center*, skraćeno SOC) nadležan je za sakupljanje sigurnosne inteligencije te prepoznavanje i uklanjanje prijetnji.

Glavni poslovi SOCa su analiza zlonamjernih sadržaja, praćenje sumnjivog prometa, praćenje pristupa kritičnim dijelovima informacijskog sustava, prevencija širenja zlonamjernog sadržaja te sprječavanje socijalnog inženjeringa.

5. Praktična analiza zlonamjernih sadržaja

5.1. Uvod

„Svrha analize zlonamjernog softvera je osigurati informacije koje su vam potrebne da biste odgovorili na upad u mreži. Vaši ciljevi bit će ustvrditi što se dogodilo i osigurati da ste pronašli sve zaražene strojeve i datoteke.“ (Sikorski et al., 2012)

Kako bi se korporacija kvalitetno obranila od prijetnji zlonamjernim sadržajima potrebno je unutar korporacije analizirati zlonamjerne sadržaje koji dolaze s različitih kanala komunikacije, kao što su elektronička pošta i internetska veza.

Analizu zlonamjernih sadržaja moguće je podijeliti na dinamičku analizu i statičku analizu.

Dinamička analiza podrazumijeva pokretanje zlonamjerne datoteke te praćenje njenog ponašanja na sustavu. Pod praćenjem se podrazumijeva pregled spajanja zlonamjerne datoteke na Internet te provjeru procesa koje zlonamjerna datoteka pokreće i što ti procesi rade.

Statička analiza ne podrazumijeva pokretanje zlonamjerne datoteke, već se ovdje pregledava njezin sadržaj. U naprednoj statičkoj analizi koristi se rastavljač (engl. *disassembler*), koji omogućuje pregled instrukcija pojedinog zlonamjernog programa.

Za statičku i dinamičku analizu korporacija može koristiti unutarnji laboratorij za analizu, već gotove alate, koji se mogu koristiti besplatno ili rješenja drugih tvrtki koje se bave analizom.

5.2. Alati za prikupljanje inteligencije

Korporacija mora pratiti stanje sigurnosti svog informacijskog sustava. Kako bi to bilo ostvareno, mora sakupljati informacije o sustavu pa ih analizirati.

Kvalitetna sigurnosna inteligencija ovisi o alatima koje korporacija koristi. Takvi alati postižu cijenu i do nekoliko stotina tisuća dolara, no njihova cijena ne garantira potpunu sigurnost. Garantira da će tim za informacijsku sigurnost dobiti pravovremene i točne informacije o stanju sigurnosti informacijskog sustava.

5.2.1. Splunk

Splunk je jedan od glavnih alata za prikupljanje informacija o stanju sustava. Može prikupljati različite informacije o različitim uređajima. Svaki uređaj koji generira logove može se pratiti putem Splunka.

Uz sakupljanje logova, glavni dio Splunka je njegovo analiziranje sirovih informacija. Omogućuje vizualizaciju informacija, uvrštavanje tih informacija u grafove. Dozvoljava i slanje dojava (engl. *alerts*) kada se dogodi neka određena promjena u sustavu.

Zbog ovih mogućnosti koristi se u informacijskoj sigurnosti. Tipična primjena Splunka u korporativnoj sigurnosti je praćenje kanala elektroničke pošte i mrežnog kanala.

Splunkom je moguće pratiti svu elektroničku poštu koja izlazi iz sustava ili ulazi u sustav korporacije. Nakon uspostavljanja praćenja, postavljaju se kriteriji koji će okinuti dojavu. Primjer takvog kriterija je postupanje ukoliko se pojavi elektronička pošta s domenom korporacije koja nije poslana s poslužitelja elektroničke pošte korporacije. To znači da se netko pretvara da je dio korporacije kako bi došao do nekih informacija ili ugrozio sustav. Nakon što je tim za informacijsku sigurnost primio dojavu o takvoj pošti, može reagirati i upozoriti zaposlenika koji je dobio tu poštu da se radi o pokušaju zlonamjerne radnje.

U financijskoj industriji Splunk se ponajviše koristi za praćenje prijava u baze podataka. Baze podataka u bankama ključan su dio poslovanja, jer se u njima nalaze informacije o klijentima banke, računima i karticama. Baza podataka poslat će *log* Splunku svaki put kada se netko prijavi ili pokuša prijaviti na bazu. Log će sadržavati podatke o korisničkom imenu korisnika, na koju se bazu pokušao prijaviti, s kojim pravima i u koje vrijeme. Svaki zaposlenik koji se želi spojiti na bazu mora dobiti odobrenje. Da bi dobio odobrenje mora imati opravdani poslovni razlog za spajanje. Nakon što dobije odobrenje ono se sprema na mjesto na koje Splunk ima pristup. Prilikom svake prijave Splunk će usporediti informacije koje je dobio od baze podataka i popis tko sve trenutno ima odobrenje. Ukoliko se spojio korisnik koji nema odobrenje generirat će se dojava timu za informacijsku sigurnost. Tim onda može dalje istražiti što se dogodilo.

Koliko je bitno sakupljati informacije toliko je bitno i ne pretjerati u količini informacija koje se analiziraju. Ako tim za informacijsku sigurnost dobiva veliku količinu informacija neće moći pravovremeno reagirati jer će obrada tih informacija uzeti previše vremena.

Splunk informacije moraju biti sažete i pravovremene, tek nakon detekcije mogućeg incidenta analizira se veća količina informacija koje okružuju taj incident.

5.2.2. IBM Qradar

IBM Qradar je *Security and Intelligence Event Management* (skraćeno SIEM) sustav. SIEM sustavi su rješenja koja prikupljaju sigurnosnu inteligenciju s različitih uređaja i analiziraju anomalije. Ukoliko detektiraju nekakvu anomaliju u radu sustava, obavještavaju sigurnosni tim te daju sve raspoložive informacije o tom događaju.

IBM Qradar je rješenje za velike korporacije koje imaju veliku količinu logova. Sakuplja logove različitih uređaja kao što su: mrežni uređaji, računala, poslužitelji, sigurnosne kamere i aplikacije. Qradar logove uspoređuje s osnovicom sustava (engl. *baseline*). Uspoređivanjem može detektirati sigurnosne anomalije, promjene u ponašanju uređaja i događaje koji mogu ugroziti sustav. Takve događaje analizira te ih predstavlja timu za informacijsku sigurnost u jednostavnom obliku s bitnim agregiranim informacijama.

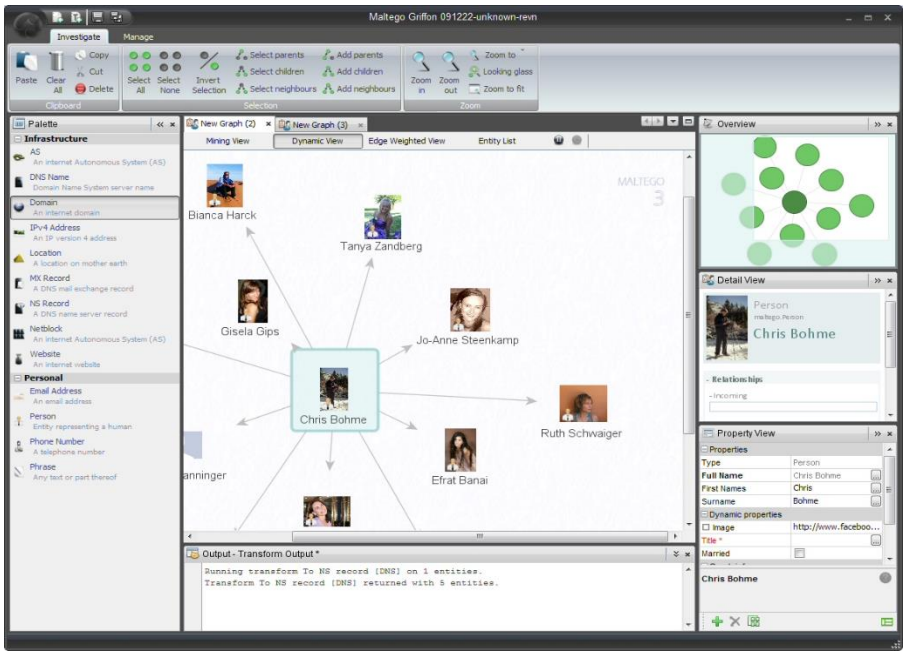
Qradar se koristi i za analizu razine sigurnosti uređaja. Analizira trenutno stanje sigurnosnih zakrpi na uređajima i daje uvid na što su određeni uređaj ili aplikacija ranjivi.

5.2.3. Maltego

Maltego je platforma koja omogućava korištenje inteligencije otvorenog tipa (engl. *Open Source Intelligence*, skraćeno OSINT).

OSINT se odnosi na sve neklasificirane informacije i uključuje sve što je slobodno dostupno na webu. OSINT je suprotan zatvorenoj vrsti obavještajnih podataka ili povjerljivih informacija. Uobičajeni OSINT izvori uključuju društvene mreže, forume, poslovne web stranice, blogove, videozapise i vijesti. (BrightPlanet, 2013)

Povezivanje osoba na Maltego platformi je prikazano na slici koja slijedi (Slika 5.1).



Slika 5.1 Povezivanje osoba (Wielenga, 2010)

Maltego omogućuje vizualizaciju odnosa različitih informacija. Može prikazati odnose između ljudi, socijalnih mreža, korporacija, organizacija, web stranica, *Domain Name System* (skraćeno DNS) imena, dokumenata i datoteka.

Maltego se u korporativne svrhe može primijeniti nakon analize zlonamjernog uzorka. Sve informacije kao što su domene i *Internet Protocol* (skraćeno IP) adrese je moguće preko Maltego platforme povezati s lokacijom i ljudima koji imaju veze s tom domenom. Daje mogućnost brzom napretku istrage o svrsi i razlogu napada.

Pošto se Maltego koristi i u obranu od zlonamjerne svrhe, korporacija može analizirati sebe i vidjeti koje su sve informacije o njima dostupne te ukoliko postoji nešto osjetljivo, a dio je javno dostupnih informacija, može zatražiti od onoga tko je objavio te informacije da ih ukloni ili pravnim postupkom tražiti uklanjanje tih informacija.

5.3. Laboratorij za analizu zlonamjernih sadržaja

Laboratorij za analizu zlonamjernih sadržaja omogućava timu za sigurnost pokretanje zlonamjernog softvera u sigurnom okruženju, kako bi razumjeli što čini i što je potrebno za zaštitu od prijetnje koju predstavlja određeni zlonamjerni program. Ako je dobro izveden, laboratorij može biti moćan alat za brzo razumijevanje i zaštitu od novih prijetnji ili nepoznatih aktera. (Liska, 2014)

Ukoliko se korporacija odluči za analizu u vlastitom laboratoriju, takav laboratorij je potrebno pripremiti za provođenje analiza. Bitno je da laboratorij bude odvojen od korporativnih računala i mreže, te da je pristup dozvoljen samo djelatnicima informacijske sigurnosti.

Postoji nekoliko elemenata takvog laboratorija.

5.3.1. Virtualna računala

Jezgra samog laboratorija su virtualna računala. Potrebno je pripremiti i instalirati nekoliko virtualnih računala s različitim operacijskim sustavima, kao što su Windows XP, Windows 7, Windows 8, Windows 10. Ukoliko korporacija koristi Apple računala potrebno je nabaviti nekoliko računala s Mac OS operacijskim sustavom kako bi se uzorci koji napadaju Apple računala mogli analizirati. Isto vrijedi i za Linux operacijski sustav.

Neki zlonamjerni programi različito se ponašaju na različitim operacijskim sustavima pa je zbog toga potrebno instalirati nekoliko verzija. Uz to, potrebno je pripremiti još jedno virtualno računalo koje će služiti za statičku analizu.

Kako bi se bilo moguće vratiti na prvobitno stanje bez zaraze, potrebno je primijeniti snimke početnog stanja. Zbog toga se nakon instalacije alata postavlja početna snimka (engl. *snapshot*) te se na taj *snapshot* vraća kada se analiza završi.

Kako se prilikom analiza ostala računala korporacije ne bi zarazila, potrebno je odvojiti mrežni segment na kojem se nalaze računala za analizu od korporativne mreže. Najpoželjnije je zakupiti posebnu vezu prema Internetu i samo ondje spojiti računala za analizu.

5.3.2. Alati za dinamičku analizu

Nakon instalacije virtualnih računala za dinamičku analizu potrebno je pripremiti nekoliko alata koji će se koristiti za analizu.

- Wireshark
- Process Monitor
- Regshot
- ApateDNS
- FakeNET

Uz ove alate potrebno je instalirati osnovne programe koji se koriste na računalu, kao što su Internet preglednici, alati za rad s dokumentima i alati za raspakiravanje. Razlog tomu je što

zlonamjerna datoteka ne mora doći u .exe formatu, može doći unutar dokumenta ili kao .jre datoteka pa je zbog toga potrebno instalirati alate koji će moći pokrenuti takvu datoteku.

5.3.3. Alati za statičku analizu

Na jednom računalu koje je određeno za statičku analizu korisno je imati nekoliko programa koji su dolje navedeni. Svi ovi alati moraju biti u mogućnosti analizirati kod bez pokretanja uzorka, no u svrhu sigurnosti najbolja praksa je pokretati te alate na virtualnom računalu.

- Strings
- PEstudio
- PEiD
- PEview
- UPX
- Resource Hacker

Kao i na računalima za dinamičku analizu korisno je instalirati osnovne programe.

5.4. Javno dostupni servisi za analizu

Postoje mnogobrojni alati za analizu zlonamjernih sadržaja dostupni putem Interneta. Neki su od njih dostupni besplatno, dok ih se većina plaća. Besplatni poznatiji alati su: VxStream Hybrid Analysis tvrtke Payload Security, VirusTotal tvrtke Google te Malwr koji je temeljen na Cuckoo Sandbox platformi. U većini slučajeva analize dostatno će biti koristiti javno dostupne alate, jer daju dovoljno informacija da bi se zaključilo o kakvom se zlonamjernom kodu radi te koje je mjere zaštite potrebno poduzeti. Jedini slučaj u kojem se nikako ne preporuča učitavanje na javno dostupne alate je onaj kada postoji sumnja da je zlonamjerni sadržaj namijenjen točno određenoj korporaciji pa može sadržavati podatke koji su osjetljivi za njezino poslovanje.

Svaki od navedenih besplatnih alata ima i svoju inačicu koja se plaća te omogućuje dodatne mogućnosti. VirusTotal u svojoj plaćenoj inačici nudi preuzimanje uzoraka koji su analizirani na platformi, dok Hybrid Analysis to sadrži u svojoj besplatnoj inačici.

U svrhu ovoga rada bit će korišteni VirusTotal i VxStream Hybrid Analysis. Malwr neće biti korišten, jer je u posljednje vrijeme nepouzdan te ne otkriva dovoljno informacija o uzorku.

5.4.1. VirusTotal

VirusTotal je platforma otvorena 2004. godine, a Google ju je kupio 2012. godine.

VirusTotal omogućuje analizu računalnih datoteka te Android aplikacija. Datoteku skenira nizom antivirusnih rješenja i daje povratnu informaciju za svaki antivirus, je li datoteka zlonamjerna i ako je pod kojim nazivom se vodi u tom antivirusu. Uz to, daje detaljne informacije o vrsti datoteke te njenom sadržaju.

Na ovoj platformi će se analizirati Locky. Locky je *ransomware* koji kriptira datoteke na unutarnjim i vanjskim diskovima pa traži određenu svotu novaca za dekriptiranje. Nakon uplate šalje ključ kojim se mogu dekriptirati datoteke.

Nakon učitavanja datoteke prvi prikaz sadrži: tip datoteke u obliku ikone, broj antivirusa koji su detektirali da je datoteka zlonamjerna, SHA-256 sažetak datoteke, ime i veličinu datoteke, datum i vrijeme posljednje analize datoteke te broj korisnika koji je ocijenio da je datoteka zlonamjerna (Slika 5.2).

Slika 5.2 Osnovne informacije o uzorku

Pomoću SHA-256 sažetka moguće je pretražiti je li uzorak bio učitan na neku drugu platformu za analizu.

Oznaka 55/65 govori da je uzorak poznat većini antivirusa pa u slučaju pokretanja uzorka postoji velika šansa da će antivirus na računalu zaustaviti pokretanje.

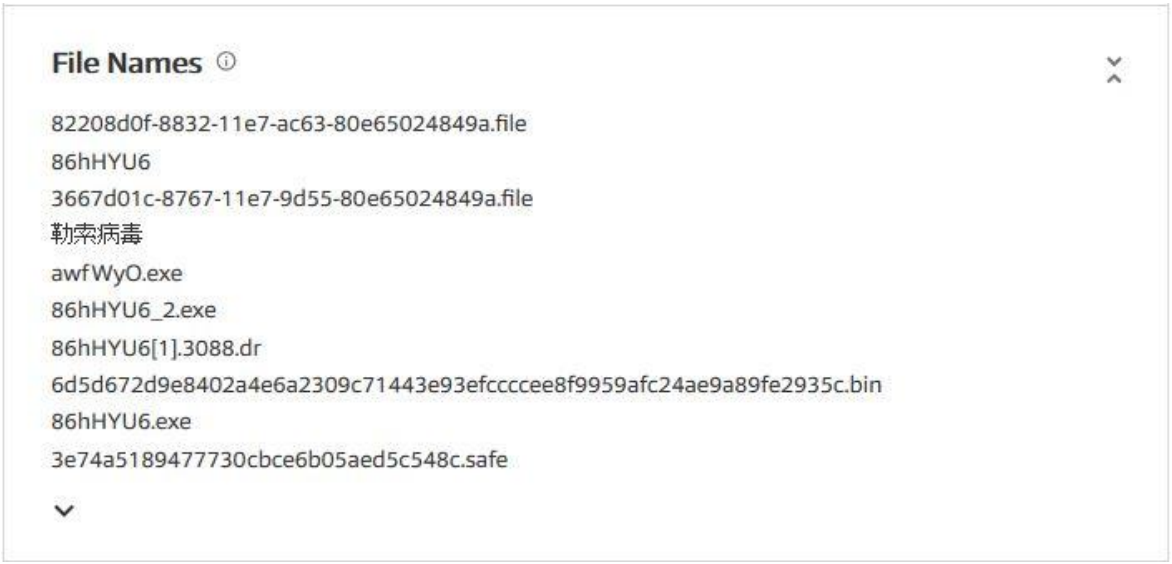
Sljedeća slika (Slika 5.3) prikazuje nekoliko antivirusa koji jesu ili nisu detektirali zlonamjernost uzorka. Vidljivo je da su TrendMicro i ViRobot uspješno detektirali uzorak kao Locky, dok su antivirusi Kingsoft i TotalDefense označili da je uzorak čist. To je saznanje vrlo korisno kako bi se ustvrdilo je li trenutni antivirusni sustav korporacije u mogućnosti obraniti korporaciju od ove prijetnje.

Tencent	Win32.Trojan.Locky.Qqte	TrendMicro	Ransom_LOCKY.TH818
TrendMicro-HouseCall	Ransom_LOCKY.TH818	VBA32	Trojan.Filecoder
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.Z.Locky.620544.B
Webroot	W32.Trojan.Gen	Yandex	Trojan.Filecoder!SStcrdHAtqM
ZoneAlarm	Trojan-Ransom.Win32.Cryptor.kw	CMC	Clean
Jiangmin	Clean	Kingsoft	Clean
nProtect	Clean	SUPERAntiSpyware	Clean
TheHacker	Clean	TotalDefense	Clean
WhiteArmor	Clean	Zillya	Clean

Slika 5.3 Popis antivirusa i razina detekcije

Pod karticom detalji nalaze se mnogobrojne informacije o datoteci. Najzanimljiviji dio za osnovnu analizu su imena pod kojima se taj uzorak pojavio (Slika 5.4). Sva imena datoteka imaju nešto zajedničko, a to je da imaju isti SHA-256 sažetak.

Zanimljivo je da ovaj uzorak ima različite ekstenzije kao .safe i .dr., no oni su i dalje .exe tip datoteke. Može se zaključiti da je u slučaju .safe ekstenzije napadač pokušao sakriti stvarnu ekstenziju datoteke te ju zamijenio s ekstenzijom koja ne izgleda zlonamjerno.

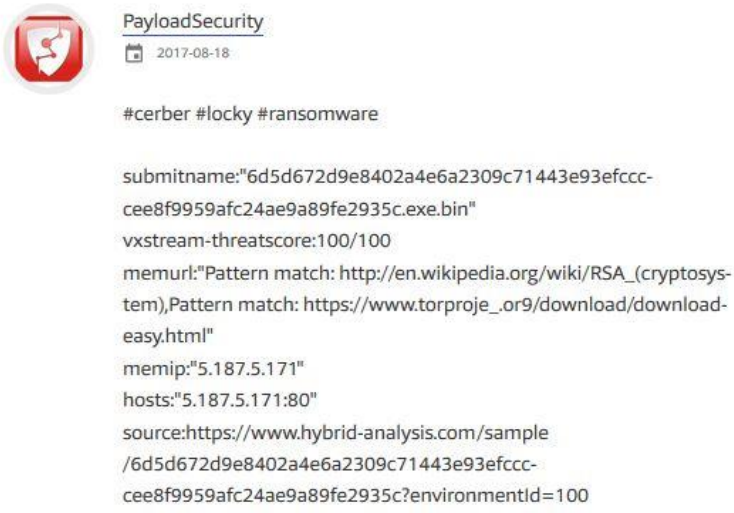


Slika 5.4 Imena uzorka

VirusTotal pod detaljima prikazuje i vrijeme kompiliranja, no ono je u velikoj većini slučajeva netočno jer je moguće izmijeniti vrijeme kompiliranja pri pisanju koda. Vrijeme kompiliranja ovog uzorka je 02.03.2013., no ono je zasigurno netočno jer se ovaj uzorak prvi put pojavio 2010. godine.

Posljednja kartica prikazuje komentare korisnika. Većina komentara sastoji se od naziva zlonamjernog koda te pomaže pri osnovnoj analizi ukoliko nije moguće zaključiti o kojoj se

vrsti radi. Ukoliko je uzorak učitan na Hybrid Analysis pojavit će se komentar PayloadSecurity koji će imati vrstu zlonamjernog koda te još dodatnih informacija, kao i poveznicu na Hybrid Analysis platformu gdje je taj isti uzorak analiziran. Slika prikazuje takav komentar (Slika 5.5)



Slika 5.5 PayloadSecurity komentar

Zaključno, VirusTotal je vrlo pouzdan i brz alat za osnovnu analizu datoteka te brzo utvrđivanje je li datoteka zlonamjerna. Koristan je pri određivanju efektivnosti antivirusa korporacije, te za brzu analizu gdje je jedino potrebna informacija je li uzorak zlonamjeran ili ne. Ukoliko je potrebno odraditi dublju analizu datoteke, prelazi se na Hybrid Analysis te ručnu dinamičku i statičku analizu.

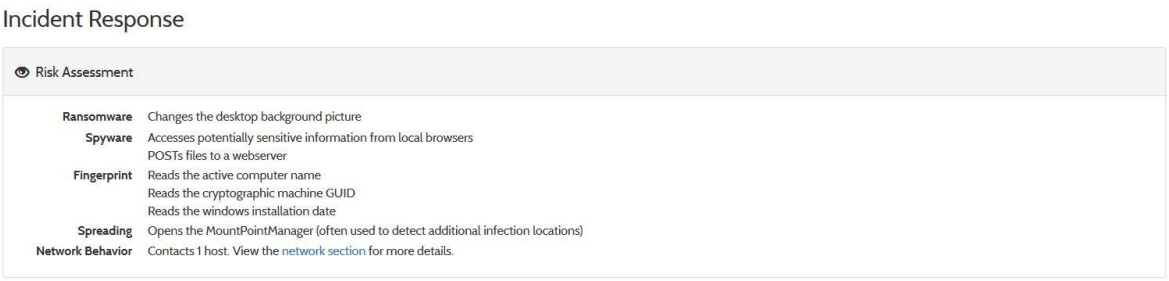
5.4.2. Hybrid Analysis

Hybrid Analysis je platforma koja odrađuje dinamičku i statičku analizu datoteke. Dok VirusTotal samo provjerava detektiraju li antivirusi zlonamjernu datoteku, Hybrid Analysis pokreće datoteku u virtualnom računalu i prati njeno ponašanje. Uz to koristi skripte za pokretanje datoteke koje simuliraju ljudsko ponašanje, kako zlonamjerna datoteka ne bi mogla prepoznati da se pokreće u automatiziranoj virtualnoj okolini.

Hybrid Analysis dozvoljava učitavanje velike količine različitih vrsta datoteka te može skenirati datoteke koje se nalaze na nekoj poveznici.

Na Hybrid Analysis platformi će biti analiziran Locky uzorak koji je bio analiziran i na VirusTotal platformi.

Na sljedećoj slici (Slika 5.6) prikazana je ocjena rizika koja je početni dio platforme i ima ključne informacije o tome što je platforma otkrila iz analizirane datoteke. Ovaj uzorak mijenja pozadinu radne površine pa je odmah moguće zaključiti da se radi o *ransomwareu*. Razlog promjene pozadine je obavijest korisniku da su sve datoteke na njegovom računalu kriptirane te način plaćanja kako bi dobio ključ za dekriptiranje. Na slici je također prikazano da datoteka pri pokretanju kontaktira jednu adresu na Internetu.



Slika 5.6 Ocjena rizika

Drugi, najzanimljiviji, dio su slike ekrana (Slika 5.7) koje je platforma snimila prije i poslije pokretanja koda. To je vrlo korisno jer je moguće vidjeti ostavlja li zlonamjerni kod neke vizualne tragove nakon pokretanja.

Slika 5.7 Slike ekrana

Posljednji dio je mrežni dio koji govori što je uzorak kontaktirao. U ovom slučaju je kontaktirao jednu adresu.

Zlonamjerne datoteke imaju dvije vrste adresa koje kontaktiraju. Jedna je *payload* adresa s koje će preuzeti zlonamjerni kod i pokrenuti ga. Koristi HTTP naredbu GET za preuzimanje. Payload adrese se dosta često koriste, jer omogućuju da osnovna datoteka nema zlonamjerne

znakove nego će njena osnovna zadaća biti isključivo preuzeti zlonamjerni kod i pokrenuti ga, na taj način osnovna datoteka može izbjeći detekciju.

Druga vrsta domene je *command & control* (skraćeno C&C) domena. Na tu domenu zlonamjerni kod šalje informacije koje je prikupio s računala te u nekim slučajevima omogućuje kontrolu nad računalom. Može se prepoznati ukoliko koristi *HyperText Transfer Protocol* (skraćeno HTTP) naredbu POST na neku adresu.

U ovom je slučaju moguće vidjeti da se događa POST na IP adresu 5.187.5[.]17/imageload.cgi. Slika (Slika 5.8) prikazuje HTTP POST zahtjev.

Endpoint	Request	URL
5.187.5.171:80	POST	/imageload.cgi

Slika 5.8 HTTP POST zahtjev

U nekim slučajevima Hybrid Analysis nije u mogućnosti detektirati sve domene koje zlonamjerni kod kontaktira. Njih je moguće otkriti pri dinamičkoj analizi alatom WireShark.

5.5. Analiza zlonamjernih sadržaja gotovim rješenjima

Analiza uzoraka gotovim rješenjima je brz i pouzdan način otkrivanja je li uzorak zlonamjeran. U većini rješenja postoje tri vrste platformi za analizu.

Platforma elektroničke pošte koja presreće svaku poruku poslanu s adrese izvan korporativne mreže te analizira njenu strukturu i privitke u potrazi za zlonamjernim datotekama ili poveznicama.

Platforma mrežnog prometa presreće preuzimanje svake datoteke te ju prije dopuštanja preuzimanja analizira.

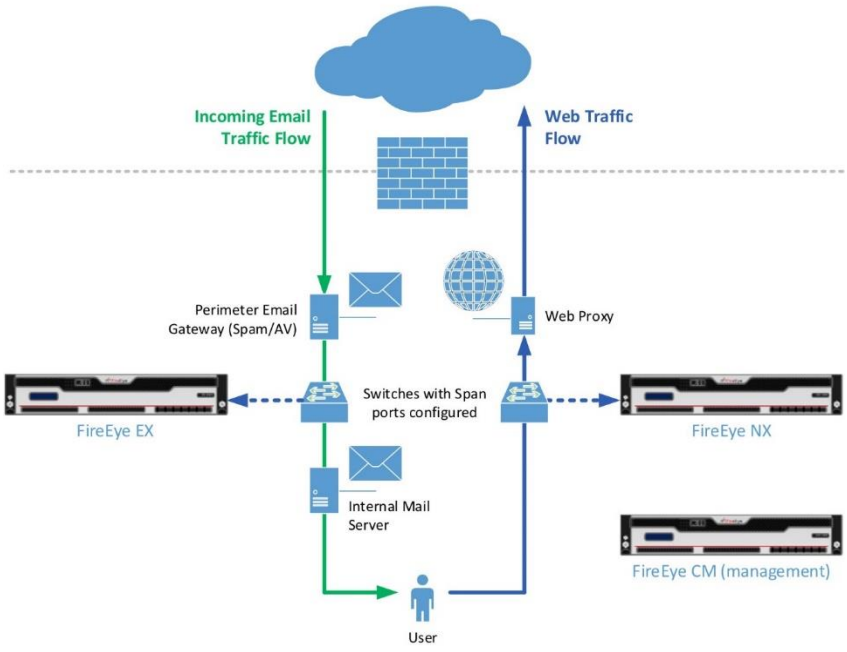
Platforma analize služi za analizu uzoraka koje tim za informacijsku sigurnost odabere, vrlo su slične Hybrid Analysis platformi.

5.5.1. FireEye

FireEye je kompanija osnovana 2004 i trenutno je jedna od najpoznatijih u svijetu informacijske sigurnosti. Nudi različita rješenja, kao što su platforma za analizu elektroničke pošte, platforma za analizu prometa, agenti za računala te penetracijska testiranja.

FireEye EX uređaj služi za analizu elektroničke pošte. Postavlja se između vanjskog poslužitelja elektroničke pošte i unutarnjeg poslužitelja elektroničke pošte. Svaka poruka koja dolazi s vanjske adrese te je uspješno prošla filtar poslužitelja elektroničke pošte analizira se u virtualnoj okolini ovog uređaja. Ukoliko pošta nije zlonamjerna prosljeđuje se na poslužitelj te onda primatelju. Ukoliko je pošta zlonamjerna uređaj stavlja poštu u karantenu i obavještava djelatnike za informacijsku sigurnost, uz to daje detaljne informacije o strukturi, vrsti, načinu zaraze zlonamjernog koda.

FireEye NX uređaj služi za analizu mrežnog prometa. Postavlja se nakon *Web Proxya* te analizira web promet. Sav promet i preuzete datoteke analiziraju se prije dopuštanja preuzimanja od krajnjeg korisnika. Ukoliko je datoteka zlonamjerna, kao i kod EX uređaja, stavlja se u karantenu te uređaj obavještava djelatnike za informacijsku sigurnost. Kao i EX daje detaljne informacije o strukturi zlonamjernog koda. Slika (Slika 5.9) prikazuje način spajanja EX i NX uređaja u korporativnu mrežu.



Slika 5.9 Način spajanja EX i NX uređaja u korporativnu mrežu (Al Damati, 2015)

5.5.2. ReversingLabs

ReversingLabs je kompanija za informacijsku sigurnost sa sjedištem u Hrvatskoj. Kao i FireEye ima različita rješenja za informacijsku sigurnost.

Glavni dio je TitaniumCore platforma koja služi za analizu zlonamjernih sadržaja. Analizira datoteke u virtualnoj okolini statičkom analizom te može analizirati milijune datoteka dnevno.

A1000 je uređaj koji služi za analizu zlonamjernih sadržaja u centru za operativnu sigurnost. Koristi TitaniumCore za analizu. Može raditi s velikim spektrom datoteka te koristi reputaciju kako bi i prije analize ukazao za neke datoteke jesu li zlonamjerne.

Na sljedećoj je slici (Slika 5.10) prikazan popis analiziranih datoteka i kratke informacije o njima.

Slika 5.10 Popis analiziranih datoteka i kratke informacije (ReversingLabs)

N1000 je uređaj koji spaja platformu za analizu elektroničke pošte i platformu za analizu mrežnog prometa. Također koristi TitaniumCore.

5.5.3. DefenseCode

DefenseCode je hrvatska tvrtka koja se bavi računalnom sigurnošću. Nudi dva proizvoda korporacijama kako bi povećale razinu informacijske sigurnosti.

Prvi je ThunderScan koji služi analizi izvornog koda (engl. source code) te daje uvid u sve ranjivosti u tom kodu. Podržava C#, Java, PHP, ASP, VB.Net, Visual Basic, VBScript, Javascript, Android Java, IOS Objective C, PL/SQL. Izrazito je koristan za korporacije koje izdaju svoja programska rješenja, jer većinom takva rješenja imaju veliki broj ranjivosti.

Drugi je WebScanner, koji je automatizirana platforma za penetracijsko testiranje web stranica. 'Napada' web stranicu različitim tehnikama kako bi pronašao ranjivosti, nakon

pronalaska daje izvješće o vrstama ranjivosti. Korporacije ovim alatom mogu testirati ranjivosti svojih web stranica.

5.6. Dinamička analiza

Dinamička analiza podrazumijeva pokretanje zlonamjernog koda te promatranje što je napravio i kako se ponaša. Najčešće se odrađuje u virtualnim računalima jer su ona jednostavna za vratiti u stanje prije zaraze. U nekim slučajevima zlonamjerni kod će prepoznati da radi u virtualnoj okolini pa se neće pokrenuti, u tim slučajevima potrebno je imati dedicirana fizička računala na kojima će se provoditi analiza.

5.6.1. Mrežni promet

Za hvatanje mrežnog prometa unutar virtualnog računala se koristi Wireshark. Prije pokretanja potencijalno zlonamjerne datoteke potrebno je pokrenuti Wireshark i pokrenuti hvatanje paketa na mrežnom sučelju koje je spojeno na Internet.

U statičkoj analizi ovog uzorka bilo je vidljivo da će uzorak pokušati ostvariti komunikaciju, pri dinamičkoj analizi je moguće provjeriti je li to istina.

Nakon uspješnog pokretanja uzorka u Wireshark vidi se da postoji velika količina *Simple Mail Transfer Protocol* (skraćeno SMTP) prometa. Ovo je prvi indikator da je zlonamjeran, jer Windows operativni sustav bez instaliranog SMTP agenta neće slati i primati SMTP promet. Na slici koja slijedi (Slika 5.11) je prikazan SMTP promet.

2490	138.658712	173.194.222.27	192.168.1.26	SMTP	106	S: 220 mx.google.com ESMTP h5si2707901lfg.210 - gsmtp
2491	138.658929	192.168.1.26	173.194.222.27	SMTP	76	C: EHLO mozilla.org.xpi
2492	138.659224	192.168.1.26	173.194.222.27	SMTP	72	C: EHLO mozilla.org
2497	138.714569	173.194.222.27	192.168.1.26	SMTP	225	S: 250 mx.google.com at your service, [188.129.106.148]
2498	138.715110	192.168.1.26	173.194.222.27	SMTP	88	C: MAIL FROM:<reporter@mozilla.org>
2499	138.715614	173.194.222.27	192.168.1.26	SMTP	225	S: 250 mx.google.com at your service, [188.129.106.148]
2500	138.716016	192.168.1.26	173.194.222.27	SMTP	87	C: MAIL FROM:<noreply@mozilla.org>
2501	138.716525	173.194.222.27	192.168.1.26	SMTP	225	S: 250 mx.google.com at your service, [188.129.106.148]
2502	138.717056	192.168.1.26	173.194.222.27	SMTP	95	C: MAIL FROM:<screenshots@mozilla.org.xpi>
2503	138.768855	173.194.222.27	192.168.1.26	SMTP	96	S: 250 2.1.0 OK a204si2559811lfa.58 - gsmtp
2504	138.768856	173.194.222.27	192.168.1.26	SMTP	95	S: 250 2.1.0 OK q28si27661351fd.30 - gsmtp
2505	138.769158	192.168.1.26	173.194.222.27	SMTP	87	C: RCPT TO:<inspector@mozilla.org>
2506	138.769583	192.168.1.26	173.194.222.27	SMTP	86	C: RCPT TO:<reporter@mozilla.org>

Slika 5.11 SMTP promet

Odabirom linije broj 2506 moguće je desnim klikom odabrati *Follow TCP Stream* kako bi se ispitala cijela komunikacija uz koju je taj paket vezan.

Sljedeća slika (Slika 5.12) prikazuje *Transmission Control Protocol* (skraćeno TCP) strujanje paketa. Vidljivo je da je uzorak pokušao poslati elektroničku poštu na adresu

reporter@mozilla.org, ali s lažirane adrese noreply@mozilla.org. Uz to poruka ima predmet Status, koji je jedan od predmeta koji MyDoom koristi za elektroničku poštu kojom se širi te je bila napisana pri provjeri nizova znakova u statičkoj analizi.

```
MAIL FROM:<noreply@mozilla.org>
250 2.1.0 OK q28si2766135lfd.30 - gsmtp
RCPT TO:<reporter@mozilla.org>
250 2.1.5 OK q28si2766135lfd.30 - gsmtp
DATA
354  Go ahead q28si2766135lfd.30 - gsmtp
From: "The Post Office" <noreply@mozilla.org>
To: reporter@mozilla.org
Subject: Status
Date: Fri, 25 Aug 2017 14:52:18 +0200
MIME-Version: 1.0
Content-Type: multipart/mixed;
          boundary="----=_NextPart_000_0008_EFC3B432.51C3E02D"
```

Slika 5.12 TCP strujanje paketa

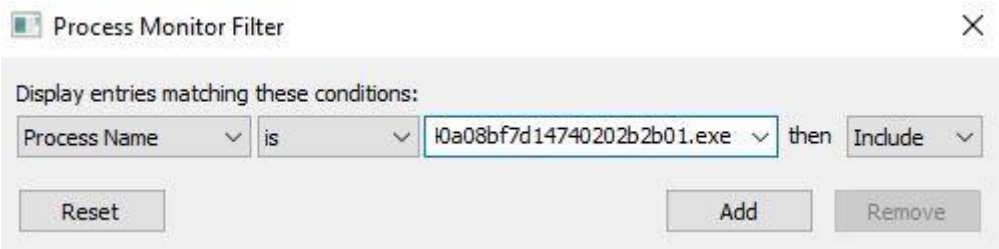
5.6.2. Praćenje procesa

Prilikom pokretanja uzorka moguće je pratiti što taj uzorak radi te koje funkcije poziva.

U statičkoj analizi zaključak je bio da će uzorak pokušati otvoriti ili napraviti novu datoteku i izmijeniti ključeve Windows registra.

Alat za praćenje procesa je Process Monitor (skraćeno ProcMon) koji je dio System Internals alata.

Nakon pokretanja uzorka potrebno je u ProcMonu napraviti filtar kako bi bilo lakše pratiti što uzorak radi. Na kartici Filter treba odabrati Filter… te u sljedećem prozoru postavke moraju izgledati kao na slici, uz iznimku da ime procesa mora biti isto kao ime uzorka. Na slici (Slika 5.13) prikazane su postavke filtara.



Slika 5.13 Postavke filtara

Na kraju je potrebno odabrati Add i OK. Sada će se u glavnom prozoru prikazivati samo događaji koje je pokrenuo uzorak.

Postoji velika količina operacija s Windows Registrom, vidljivo je da uzorak izmjenjuje ključeve po Registru, primjer je na slici (Slika 5.14).

Slika 5.14 Izmjene u registru

MyDoom traži potencijalne adrese elektroničke pošte u različitim tekstualnim datotekama pa je upravo zbog toga u ProcMon moguće vidjeti da otvara jednu od .txt datoteka. Na slici (Slika 5.15) prikazan je proces otvaranja .txt datoteke.

Slika 5.16 Proces otvaranja .txt datoteke

Na slici koja slijedi (Slika 5.17) vidljiv je i SMTP promet koji uzorak pokušava ostvariti kako bi svoju kopiju poslao na što više nađenih adresa u tekstualnim datotekama.

Slika 5.17 SMTP promet

5.7. Statička analiza

Statička analiza se koristi ukoliko dinamička ne pokaže dovoljno informacija ili je potrebno znati točno kako zlonamjerni kod radi. Jednostavna statička analiza podrazumijeva nekoliko koraka koji su opisani u ovom radu. Napredna statička analiza zahtijeva rastavljanje zlonamjernog koda (engl. *disassembly*) te ona neće biti opisana u ovom radu.

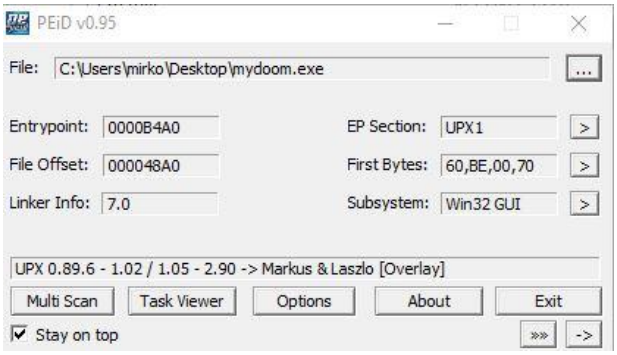
Primjer statičke analize će biti prikazan na uzorku MyDoom crva.

5.7.1. Otpakiranje datoteke

Većina autora zlonamjernog koda sakriva originalni kod kako ne bi mogao biti analiziran. Prikriveni kod (engl. *Obufuscated Code*) ima svoju potkategoriju naziva zapakirani kod (engl. *packed Code*) pa je takav kod moguće pročitati nakon otpakiranja.

Vrstu pakiranja moguće je provjeriti programom PEiD. Nakon učitavanja potencijalno zapakirane datoteke dobit ćemo informaciju o kojem se programu za pakiranje (engl. *packer*) radi.

Slika (Slika 5.18) prikazuje sučelje PEiD programa s već učitanim uzorkom. PEiD je uspješno detektirao da se radi o UPX Packer-u.



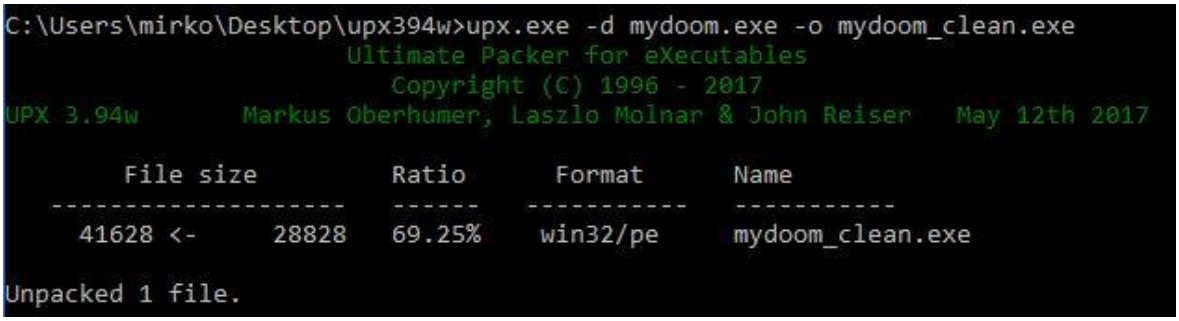
Slika 5.18 Sučelje PEiD programa

UPX je jedan od najpoznatijih *Packera* te ga je vrlo lako otpakirati linijskim alatom UPX.

Ova naredba će otpakirati mydoom.exe datoteku i spremiti otpakiranu datoteku u isti direktorij pod nazivom mydoom_clean.exe:

```
upx -d mydoom.exe -o mydoom_clean.exe.
```

Na sljedećoj slici (Slika 5.19) je vidljivo da je UPX uspješno otpakirao datoteku pa je sada moguće nastaviti analizu.



Slika 5.19 Ispis nakon otpakiranja

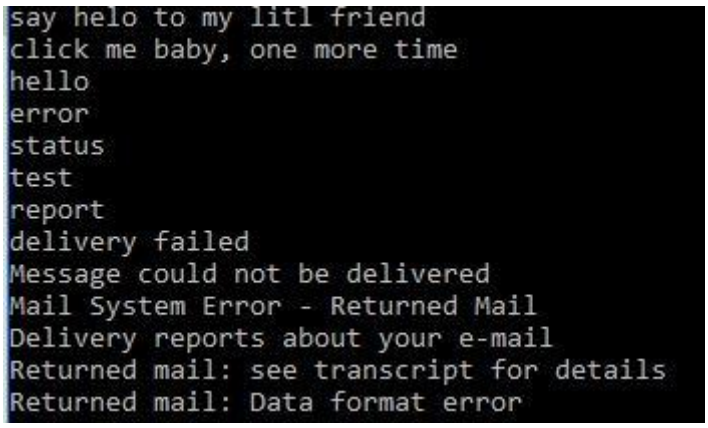
5.7.2. Nizovi znakova

Jedan od bitnih dijelova nakon otpakiranja datoteke je provjera koje smislene nizove znakova datoteka ima unutar koda. Ti znakovi mogu puno otkriti o tome što zlonamjerni kod radi te dati bitne informacije o vrsti zlonamjernog koda.

Nizove znakova iz .exe datoteke je moguće izvući linijskim alatom Strings. Naredba glasi:

```
strings64.exe mydoom.exe.
```

Na slici (Slika 5.20) je prikazan jedan zanimljiv dio rezultata Strings naredbe nad uzorkom. Većina navedenih rečenica bile su predmet ili tijelo elektroničkih poruka u kojima se širio najpoznatiji crv naziva MyDoom.



Slika 5.20 Ispis strings naredbe

Postoji velika količina nizova koje je moguće pročitati u ovom uzorku. Većina su ih domene na koje se crv širio.

5.7.3. Povezane funkcije

Postoje tri načina povezivanja funkcija s programom. Jedan od njih je statičko povezivanje, gdje se sav kod iz knjižnice (engl. *library*) prebacuje u program. Drugi način je dinamičko povezivanje, gdje se sav potreban kod iz *librarya* učitava pri pokretanju programa. Posljednji način je povezivanje pri pokretanju, gdje se kod iz *librarya* poziva tek kad ga funkcija u nekom programu zahtijeva. Posljednji način je najpoznatiji u izradi zlonamjernog koda, jer je nemoguće analizirati kod bez njegovog pokretanja.

PEstudio omogućuje provjeru dinamički povezanog koda. Uzorak učitava 5 *librarya*: kernel32.dll, advapi32.dll, msvcrt.dll, user32.dll te ws2_32.dll.

Slika (Slika 5.21) prikazuje učitane *librarye*.

Library (5)	Blacklisted (1)	Type	Symbols (106)
ws2_32.dll	x	Implicit	18
kernel32.dll	-	Implicit	54
advapi32.dll	-	Implicit	6
msvcrt.dll	-	Implicit	21
user32.dll	-	Implicit	7

Slika 5.21 Učitani *libraryi*

Ukoliko uzorak učitava advapi32.dll to ujedno znači da radi promjene u Windows Registru (engl. *Windows Registry*) pa je pri dinamičkoj analizi potrebno provjeriti koje je ključeve izmijenio. Ovaj uzorak koristi advapi32.dll te učitava RegCreateKeyEx, koji je zadužen za stvaranje nekog ključa u registru i RegSetValueEx, koji je zadužen za promjenu nekog ključa. Time je poznato da će ovaj uzorak stvoriti i modificirati ključeve u registru.

Uzorak koristi ws2_32.dll, što znači da će pokušati ostvariti komunikaciju s nekom adresom ili domenom. Poziva funkcije accept i bind, što mu omogućuje slušanje na određenom port-u. Funkcije connect i send omogućuju spajanje i slanje podataka na udaljenu adresu; često se koristi za spajanje na C&C adrese. Inet_addr funkcija pretvara IP adresu u format koji je čitljiv ostalim funkcijama. Gethostbyvalue i Gethostvalue funkcije omogućuju uzorku DNS pretragu.

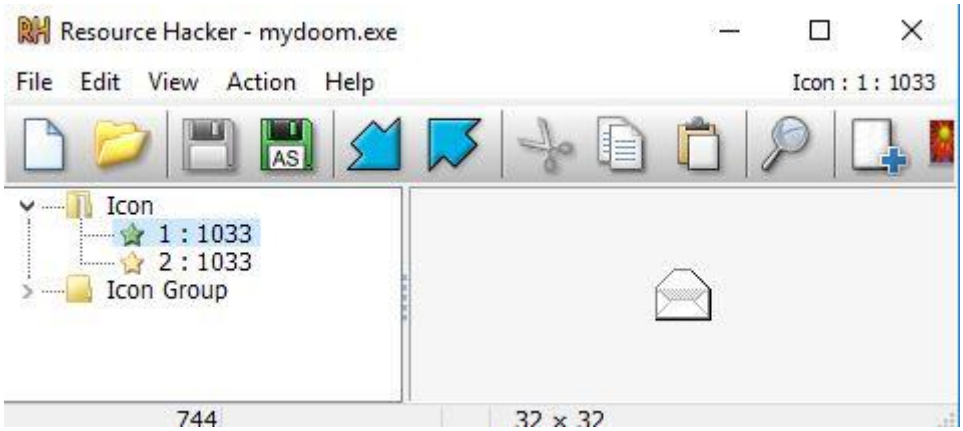
Posljednje što uzorak koristi, a relevantno je u analizi, jest kernel32.dll. Funkcija CreateFile stvara novu ili otvara postojeću datoteku. CreateFileMapping omogućava pristup nekoj datoteci preko memorijske adrese. FindFirstFile i FindNextFile omogućuju pretragu datotečnog sustava. GetWindowsDirectory vraća lokaciju instalacije Windows operativnog sustava. Moguće je zaključiti da će uzorak pokušati napraviti nekakvu datoteku u Windows direktoriju.

Funkcije daju dosta informacija o tome što će neki zlonamjerni kod pokušati napraviti. Teško je analizirati sve funkcije koje neki program učitava, no gore navedene funkcije neke su od najvažnijih u analizi zlonamjerne datoteke.

5.7.4. Resursi programa

Neki programi koriste vizualne resurse operativnog sustava te ih je moguće provjeriti alatom Resource Hacker. Resursi se nalaze u .rscr dijelu programa.

Nakon učitavanja uzorka u program vidljivo je da on koristi ikonu elektroničke pošte kao ikonu programa. Razlog ovoga je zavaravanje korisnika drugačijim izgledom. Slika (Slika 5.22) prikazuje ispis Resource Hacker alata.



Slika 5.22 Ispis Resource Hacker alata

6. Obrana od prijetnji

Postoji nekoliko poznatih vrsta obrana od prijetnji. Sigurnosna svijest spada u obranu koja se odnosi na rad ljudi, dok vatrozidi spadaju u fizičku informacijsku obranu. Penetracijsko testiranje i crveni timovi su dvije vrste testova koje korporacija može provesti kako bi ustvrdila razinu sigurnosti svog informacijskog sustava.

6.1. Sigurnosna svijest

Najslabija karika u informacijskoj sigurnosti je čovjek. Upravo zato organizacije pokušavaju podići sigurnosnu svijest svojih zaposlenika. Svaki zaposlenik korporacije trebao bi proći određeni sigurnosni trening. Na sigurnosnom treningu zaposlenike se uči o osnovnim pojmovima informacijske sigurnosti kao što je hakiranje, socijalni inženjering i zlonamjerne datoteke, kako bi zaposlenik prepoznao ukoliko dođe u kontakt s takvim napadima i o tome obavijestio nadležne osobe. Također se uči o tome kako se rukuje s povjerljivim informacijama.

Visoka sigurnosna svijest uvelike pomaže sigurnosti korporacije jer smanjuje mogućnost eskaliranja napada.

6.2. Vatrozid elektroničke pošte

Vatrozid elektroničke pošte je prva i glavna obrana ovog komunikacijskog kanala. On može filtrirati potencijalno zlonamjerne poruke i privitke.

Omogućuje postavljanje crne liste (engl. *blacklist*), koja sadrži popis već prije poznatih zlonamjernih domena elektroničke pošte te ne dozvoljava primanje poruka s tih domena.

Blokira slanje i primanje poruka koje imaju privitak koji nije poslovno opravdan i može biti zlonamjeran. Primjer takvih privitaka su: izvršne datoteke, Java datoteke, konfiguracijske datoteke i Javascript datoteke.

Omogućuje pregled svih primljenih i poslanih poruka, kako bi one bile dostupne u slučaju potrebe u istrazi.

Svaki vatrozid elektroničke pošte treba konfigurirati prema potrebama korporacije koja ga koristi, kako bi što efikasnije blokirao neželjenu i zlonamjernu poštu.

6.3. Vatrozid pristupa Internetu

Uz kanal elektroničke pošte, kanal pristupa Internetu drugi je najpodložniji iskorištavanju ili napadima.

Velika količina stranica na Internetu je zlonamjerna. Većina zlonamjernih sadržaja mora imati pristup nekoj adresi na Internetu da bi ispunili svoju svrhu. Iz ovoga se može zaključiti da dobra konfiguracija vatrozida na mrežnom kanalu povećava sigurnost korporacije.

Vatrozid se može konfigurirati na dva načina.

Prvi je način zabraniti sav promet te onda naknadno propuštati samo legitiman. Ovaj način je izrazito siguran, ali zahtijeva puno promjena i konfiguracije kako bi efektivno radio i dozvoljavao legitimni promet.

Drugi način je dopustiti sav promet, osim onoga za koji je sigurno da može biti zlonamjeran. Ovaj način nije toliko siguran kao prvi, ali zahtijeva manje konfiguracije i promjena.

Vatrozid može filtrirati domene i IP adrese po reputaciji. Većina komercijalnih rješenja spaja se na neki oblak (engl. *cloud*) sigurnosne inteligencije, gdje postoji popis domena i IP adresa koje su korištene ili se koriste u zlonamjerne svrhe. Vatrozid prikuplja zapise s tog popisa te blokira navedene domene i IP adrese.

6.4. Antivirusna rješenja

Antivirusna rješenja su posljednja razina zaštite. Nikako nisu stopostotna garancija da se neka zlonamjerna datoteka neće aktivirati na računalu. Rade na principu potpisa (engl. *signature*) te uspoređuju datoteke s bazom već detektiranih zlonamjernih datoteka u oblaku.

Antivirusna zaštita mora biti instalirana na sva računala i poslužitelje korporacije, jer je dovoljno jedno računalo koje nema antivirusnu zaštitu da napadač dobije pristup sustavu i ugrozi ga.

6.5. Penetracijsko testiranje

„Penetracijsko testiranje je tehnika procjene sigurnosti računalnog sustava ili mreže koja se temelji na oponašanju stvarnog napada. Prilikom testiranja, ovlašteni ispitivač provjerava metu izvodeći različite vrste napada jednakim tehnikama koje bi koristio i da je stvarni

napadač. Cilj mu je uočiti bilo kakvu ranjivost koju je moguće iskoristit za ostvarenje neovlaštenog pristupa.“ (CARNet, 2008)

Postoje dvije vrste penetracijskog testiranja: vanjski i unutarnji.

Vanjski test podrazumijeva da se ispitivač nalazi izvan korporativne mreže te pokušava dobiti pristup i ugroziti sustav. Sličan pristup bi imao i stvarni napadač koji nije dio korporacije.

Unutarnji test podrazumijeva da se ispitivač nalazi unutar korporativne mreže te pokušava dobiti pristup nedozvoljenim resursima i ugroziti sustav. Ova vrsta simulira napad od strane zaposlenika koji pokušava ugroziti sustav iz razloga kao što je smanjenje plaće ili otkaz.

Penetracijski test nije mjerilo potpune sigurnosti, jer u većini slučajeva napadač napada točno određeni uređaj te u nekim slučajevima ima ograničeni krug djelovanja. Pravi penetracijski test uključuje Crvene Timove (engl. *Red Teams*).

6.6. Crveni timovi

Crveni timovi i plavi timovi (engl. *Blue Teams*) proizlaze iz vojnog žargona gdje su crveni timovi fiktivni napadači, a plavi timovi obrana.

Crveni timovi su novitet u informacijskoj sigurnosti. Predstavljaju vrstu penetracijskog testiranja, ali na daleko većoj razini, te postoje specijalizirane tvrtke koje se bave ovom vrstom testa.

Razlika između crvenih timova i stvarnog napadača je da će crveni timovi, nakon sakupljanja informacija o ranjivosti informacijskoj sustava i zaposlenika, predati saznanja korporaciji. Stvarni napadač će te ranjivosti iskoristiti za zlonamjerne svrhe.

Crveni tim ima zadatak pronaći ranjivosti korporacije u određenom vremenu, najčešće ovakav test traje tjednima ili mjesecima. Crveni tim ima pravo koristiti sve postojeće alate i metode kako bi otkrio ranjivosti. Može koristiti stvarne alate koje napadači koriste, provoditi napade socijalnim inženjeringom, kopati po 'smeću' korporacije kako bi otkrio informacije, pokušati se infiltrirati u organizaciju kao zaposlenik i ostale metode.

Ovakav test će stvarno otkriti ranjivosti korporacije i njenih zaposlenika jer koristi sve metode koje bi stvarni napadač koristio.

Zaključak

Sigurnosna inteligencija je bitan dio informacijske sigurnosti korporacije. Zahtijeva kvalitetno sakupljanje informacija te temeljitu i brzu analizu.

Pregledom hrvatskih zakona vidljivo je da Republika Hrvatska ima postavljene okvire za računalni kriminalitet i propisane kazne. Korporativno gledajući, zakoni štite korporaciju od napadača te osiguravaju primjerene kazne ukoliko napadač bude uhvaćen.

Računalni kriminal u korporativnom okruženju manifestira se na različite načine. Prepoznavanjem vrsti kriminala te uspostavom odjela koji će se boriti protiv prijetnji prvi je korak ka sigurnijoj organizaciji i boljoj informacijskoj sigurnosti.

Analiziranjem zlonamjernih sadržaja koji su korišteni u pokušajima napada na korporaciju moguće je uspostaviti kvalitetnije sigurnosne kontrole. Analiza ima određene korake i alate, koji su opisani u ovom radu. Najvažnije je iz analize dobiti što više informacija o napadu i njegovim metodama. Korisno je voditi bazu podataka o svim analiziranim uzorcima.

Porastom računalnih prijetnji korporaciji raste i broj načina obrane. Bitno je educirati korisnike o sigurnosti te kako prepoznati napad, jer su oni prva crta obrane i najčešće oni koji su prva meta napada kako bi se dobio daljnji pristup u sustav. Preporuka je korisnike u korporaciji educirati jednom godišnje, jer se stanje tehnologije i vrste napada često mijenjaju. Domišljatost napadača je sve veće pa je zbog toga uvedeno testiranje crvenim timovima, koje je najkvalitetniji i najbolji način testiranja stvarne razine sigurnosti korporacije.

Popis kratica

ISECOM	Institute for Security and Open Methodologies	
CERT	Computer Emergency Response Team	računalni tim za hitne intervencije
CARNet	Croatian Academic and Research Network	Hrvatska akademska i istraživačka mreža
MUP		Ministarstvo unutarnjih poslova
UVNS		Ured vijeća za nacionalnu sigurnost
DOS	Denial Of Service	uskraćivanje usluge
DDOS	Destributed Denial Of Service	distribuirano uskraćivanje usluge
CSO	Chief Security Officer	glavni tajnik sigurnosti
SOC	Security Operations Center	centar za operativnu sigurnost
SIEM	Security Information and Event Management	sigurnosne informacije i upravljanje događajima
OSINT	Open Source Intelligence	inteligencija otvorenog tipa
DNS	Domain Name System	
IP	Internet Protocol	
C&C	Command and Control	naređuj i upravljaj
HTTP	HyperText Transfer Protocol	
SMTP	Simple Mail Transfer Protocol	
TCP	Transmission Control Protocol	
	ProcMon Process Monitor	

Popis slika

Literatura

[1] LISKA, A . *Building an Intelligence-Led Security Program*. Syngress, 2014.

[2] CRUMP, J . *Corporate Security Intelligence and Strategic Decision Making*. CRC Press, 2015.

[3] SIKORSKI, M . *Practical Malware Analysis*. No Starch Press, 2012.

[4] DEWDNEY, A.K. Computer Recreations: Of Worms, Viruses and Core War, *Scientific American*, (1989), 110.

[5] BILANDŽIĆ, M., LUCIĆ, D. A Predicting Business Opportunities and/or Threats – Business Intelligence in the Service of Corporate Security. *Collegium antropologicum, Vol.38 Supplement 1*, Zagreb, (2014), 25-33.

[6] Zakon o informacijskoj sigurnosti (2007), https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti, srpanj. 2017.

[7] Metodologija penetracijskoj testiranja (2008), http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-02-219.pdf, kolovoz. 2017.

[8] Analiza računalnog kriminaliteta za 2013 (2014), http://www.statistika.hr/index.php/46-racunalni-kriminal-u-hrvatskoj-u-2013, kolovoz. 2017.

[9] Verizon Dana Breach Investigations Report 2016 (2016), http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf, kolovoz. 2017.

[10] WIELENGA G . Interview: Intelligence Gathering Software on the NetBeans Platform (2010), https://dzone.com/articles/intelligence-gathering, kolovoz. 2017.

[11] AL DAMATI, R . Deployment Architectures for FireEye NX and EX (2015), https://community.fireeye.com/docs/DOC-6192, kolovoz. 2017.

[12] A1000 Malware Analysis Platform, https://www.reversinglabs.com/products/malware-analysis-appliance.html, kolovoz. 2017.

[13] What is OSINT and how can your organization use it? (2013), https://brightplanet.com/2013/04/what-is-osint-and-how-can-your-organization-use-it/, kolovoz. 2017.