Aspekti kibernetičke sigurnosti malih i srednjih poduzeća

Dražić, Ante

Sveučilište Jurja Dobrile u Puli

Fakultet ekonomije i turizma

„Dr. Mijo Mirković“

Ante Dražić

ASPEKTI KIBERNETIČKE SIGURNOSTI MALIH I SREDNJIH PODUZEĆA

Završni rad

Pula, 2021.

Sveučilište Jurja Dobrile u Puli

Fakultet ekonomije i turizma

„Dr. Mijo Mirković“

ASPEKTI KIBERNETIČKE SIGURNOSTI MALIH I SREDNJIH PODUZEĆA

Završni rad

Ante Dražić

JMBAG: 0303079449, redovan student

Studijski smjer: Informatički menadžment

Kolegij: Ekonomska informatika

Mentor: prof. dr. sc. Vanja Bevanda

Pula, rujan 2021.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisan Ante Dražić, kandidat za prvostupnika poslovne ekonomije, smjera Informatički menadžment ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

Ante Dražić

U Puli, 20. rujna 2021.

IZJAVA O KORIŠTENJU AUTORSKOG DJELA

Ja, Ante Dražić dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom „Aspekti kibernetičke sigurnosti malih i srednjih poduzeća“ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

Student

Ante Dražić

U Puli, 20. rujna 2021.

Sadržaj

1. Uvod

Razvojem poluvodiča te izumom tranzistora polovinom prošlog stoljeća započinje doba koje nazivamo informacijsko doba. Ono je okarakterizirano kao prekretnica u povijesti čovječanstva. Pojavljuju se uređaji koji omogućuju da probleme riješimo brže, lakše i efikasnije. Povezivanjem odnosno umrežavanjem uređaja povećava se i njihova korisnost jer dobivaju mogućnost međusobne razmjene informacija te kolektivnog rješavanja problema. U vojnim i akademskim krugovima nastaju prve mreže. Mreže se postepeno šire na kućanstva i poduzeća, a internetski se promet udvostručuje svakih 18 mjeseci[1].

Poduzeća u kontekstu suvremenog poslovanja postaju sve više ovisna o informatičkoj infrastrukturi, a time se povećava i potreba za zaštitom iste. Mala i srednja poduzeća u današnje vrijeme konstantno bilježe porast slučajeva kibernetičkih napada. Ovakve vrste poduzeća su privlačne potencijalnim napadačima zbog niže sofisticiranosti informacijskih sustava i manjeg broja obučenog radnog kadra koji je spreman odgovoriti na kibernetičke napade za razliku od velikih poduzeća.

Poznavanje kibernetičke sigurnosti je stoga jako važno kako bismo prepoznali moguće kibernetičke prijetnje, zaštitili poslovne informatičke sustave od potencijalnih proboja te utvrdili korake za oporavak u slučaju kibernetičkih napada.

Rad se sastoji od deset poglavlja. U sedmom se poglavlju nalazi praktični dio rada u kojem se iz perspektive napadača razmatra način krivotvorenja identiteta pošiljatelja i pozivatelja u svrhu izvođenja smishing i vishing napada na telekomunikacijsku infrastrukturu poduzeća te način napada na sažetak lozinke koji se koristi za prijavu na operacijski sustav Microsoft Windows 10. Napadač bi uporabom navedenih tehnika mogao ostvariti pristup poslovnim informacijama kojima mu inače ne bi bilo dozvoljeno pristupiti.

[1] Edholm's law, https://en.wikipedia.org/wiki/Edholm%27s_law, pristupljeno 13. lipnja 2021.

2. Kibernetička sigurnost

Glavni fokus informacijske sigurnosti prema ISO/IEC 27000:2018 normi stavlja se na osiguranje informacija, a to je čin održavanja povjerljivosti, cjelovitosti i raspoloživosti informacija koji osigurava da se informacija na bilo koji način ne ugrozi kad se pojave kritični problemi. Zaštita informacija obavlja se upravljanjem sigurnosnim rizicima.

Proces upravljanja rizicima sastoji se od (Wikipedia 2021):

- identifikacije informacije, povezane imovine, prijetnji i ranjivosti,
- evaluacije rizika,
- odlučivanja kako riješiti ili tretirati rizike, tj. izbjeći ih, ublažiti, podijeliti ili prihvatiti,
- odabira ili osmišljavanja odgovarajućih sigurnosnih kontrola te implementacije istih gdje je mitigacija potrebna te
- praćenja aktivnosti, donošenja potrebnih prilagodbi za rješavanje svih problema, izmjena i sagledavanja mogućnosti poboljšanja.

Povjerljivost predstavlja zaštitu informacije od neautoriziranih pojedinaca, subjekata ili procesa. Ona može biti narušena primjerice kad osoba upiše broj svoje kreditne kartice na web stranicama internetske trgovine, a zlonamjerna ekstenzija instalirana u web pregledniku ga „uhvati“ i pošalje na C2 (eng. Comand and Control) poslužitelj napadaču.

Cjelovitost predstavlja zaštitu informacije od neovlaštene izmjene bilo slučajne ili namjerne. Ona može biti narušena primjerice kad na računalu pokrenemo zlonamjerni softver koji briše ili mijenja korisničke datoteke.

Raspoloživost predstavlja svojstvo sustava da informacija bude dostupna uvijek kad je to potrebno. Ona može biti smanjena primjerice pod utjecajem DDoS (eng. Distributed Denial of Service) napada koji smanjuju dostupnost ili onemogućavaju normalno funkcioniranje usluge.

3. Nacionalni CERT

Nacionalni CERT (eng. Computer Emergency Response Team) je posebno tijelo zaduženo za zaštitu računalne sigurnosti javnih informacijskih sustava unutar hrvatske internetske domene ili hrvatskog IP adresnog prostora, osim za tijela državne uprave za koja je zadužen Zavod za sigurnost informacijskih sustava (ZSIS). Osnovan je 30. listopada 2007. godine prema Zakonu o informacijskoj sigurnosti i djeluje unutar Hrvatske akademske i istraživačke mreže CARNET.

Nacionalni CERT u okviru svog djelovanja provodi proaktivne i reaktivne mjere. Proaktivnim mjerama djeluje prije incidenata, a reaktivnim mjerama djeluje na incidente koji mogu ugroziti računalnu sigurnost javnih informacijskih sustava u Republici Hrvatskoj[2].

Proaktivne mjere se javno objavljuju i podrazumijevaju[2,3]:

- praćenje stanja na području računalne sigurnosti i objavljivanje sigurnosnih preporuka u svrhu priprema za moguće štete,
- kontinuirano praćenje područja računalno-sigurnosnih tehnologija te diseminiranje novih saznanja,
- prikupljanje, agregaciju i diseminaciju relevantnih informacija iz područja računalne sigurnosti u vidu dokumenata, preporuka i uputa,
- educiranje najšire javnosti putem promidžbenih akcija, a u svrhu unaprjeđivanja svijesti o značaju računalne sigurnosti,
- edukaciju i obuku o računalnoj sigurnosti provođenjem edukativnih akcija,
- provjeru ranjivosti i izdavanje certifikata za ustanove članice CARNET-a te
- sigurnosna testiranja CARNET-ovih usluga i servisa te aplikacija koje pristupaju sustavu eMatica.

[2] Nacionalni CERT, https://hr.wikipedia.org/wiki/Nacionalni_CERT, pristupljeno 12. kolovoza 2021.
[3] Nacionalni CERT, https://gov.hr/hr/nacionalni-cert/1230, pristupljeno 12. kolovoza 2021.

Reaktivne mjere podrazumijevaju[4,5]:

- sigurnosna upozorenja koja se izrađuju i distribuiraju na osnovu prikupljenih saznanja, javno ili ciljano,
- koordinaciju rješavanja značajnijih incidenata u koje je uključena barem jedna strana iz Republike Hrvatske, a u čije rješavanje je, radi opsega i značaja, uključeno više CERT-ova ili drugih relevantnih tijela te
- postupanje s računalno-sigurnosnim incidentima.

4. Resursi informacijskog sustava

Da bismo utvrdili što trebamo štititi važno je utvrditi koja imovina ima vrijednost i za koga. Resursi informacijskog sustava uključuju hardverske komponente, softverske komponente i informacijsku imovinu.

U softverske komponente možemo ubrojiti: aplikacijski softver, sistemski softver, softver za upravljanje bazama podataka, softverske razvojne alate, uslužne programe te ostali softver[6].

U hardverske komponente možemo ubrojiti: računala i računalnu opremu (stacionarna i prijenosna osobna računala, poslužitelje, monitore, tipkovnice, pisače i slično), komunikacijsku opremu (usmjernike, preklopnike, vatrozide i slično), medije za pohranu podataka (magnetne diskove, magnetne trake, optičke diskove i slično) te ostalu tehničku opremu koja podržava rad informacijskog sustava (uređaje za neprekidno napajanje električnom strujom, klimatizacijske uređaje i slično)[6].

U informacijsku imovinu možemo ubrojiti: podatke u bazama podataka, datoteke s podacima, programski kod, sistemsku i aplikacijsku dokumentaciju, korisničke priručnike, planove, interne akte i slično[6].

[4] Nacionalni CERT, https://hr.wikipedia.org/wiki/Nacionalni_CERT, pristupljeno 12. kolovoza 2021.
[5] Nacionalni CERT, https://gov.hr/hr/nacionalni-cert/1230, pristupljeno 12. kolovoza 2021.
[6] NN 37/2010 (26.3.2010.), Odluka o primjerenom upravljanju informacijskim sustavom, https://narodne-novine.nn.hr/clanci/sluzbeni/full/2010_03_37_958.html, pristupljeno 12. kolovoza 2021.

5. Ranjivosti

Ranjivosti (eng. vulnerabilities) su propusti koje napadač može iskoristiti da dobije neovlašten pristup sustavu. Da bi iskoristio ranjivost, nakon otkrića iste napadač mora osmisliti metodu iskorištavanja (eng. exploit).

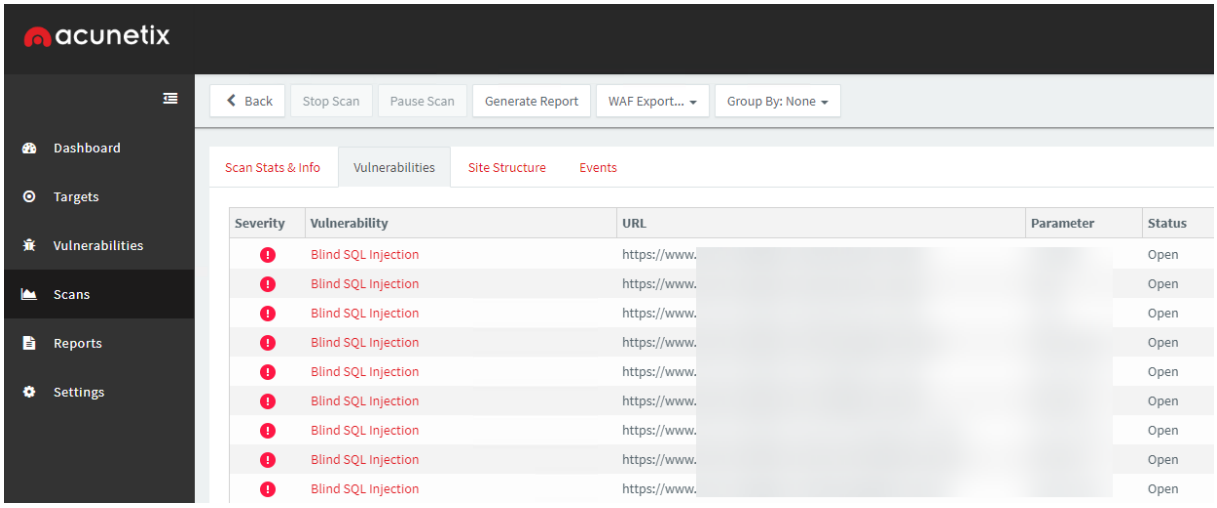
Prema ISO/IEC 27005:2018 normi ranjivosti mogu biti vezane za:

- hardver: osjetljivost na vlagu ili prašinu, osjetljivost na nezaštićeno skladištenje, dotrajalost koja uzrokuje kvar i pregrijavanje,
- softver: nedovoljno testiranje, nesigurno kodiranje, nedostatak revizije i greška dizajna,
- mrežu: nezaštićeni komunikacijski vodovi (primjerice nekorištenje kriptografije) i nesigurna mrežna arhitektura,
- osoblje: neadekvatan proces zapošljavanja, nedovoljna svijest o sigurnosti i insajderske prijetnje,
- lokaciju: područje izloženo prirodnim katastrofama (primjerice poplava ili potres) i prekid napajanja te
- organizaciju: nedostatak redovitih revizija, nedostatak planova kontinuiteta i nedostatak sigurnosti.

Organizacija MITRE Corporation[7] održava repozitorij javno objavljenih ranjivosti naziva Common Vulnerabilities and Exposures (CVE)[8]. Repozitorij je prvi puta javno objavljen u rujnu 1999. godine te je sadržavao podatke o ranjivostima samo nekolicine manjih organizacija[9]. Do danas se ta brojka drastično povećala te se jako teško može pronaći neka veća organizacija koja ne sudjeluje u njemu. U repozitoriju se objavljuju ranjivosti po Common Vulnerability Scoring System (CVSS) ocjeni koja označava ozbiljnost ranjivosti. Svaka ranjivost ujedno sadržava i pripadajuću CVE oznaku koja služi kao jedinstveni identifikator ranjivosti u repozitoriju.

[7] The MITRE Corporation, https://www.mitre.org/, pristupljeno 14. kolovoza 2021.
[8] CVE, https://cve.mitre.org/, pristupljeno 14. kolovoza 2021.
[9] History, https://cve.mitre.org/about/history.html, pristupljeno 14. kolovoza 2021.

Postoje različita mišljenja stručnjaka o tome treba li detalje o ranjivostima javno objavljivati. Neki od stručnjaka smatraju da je najispravnija odluka odmah po otkrivanju javno objaviti detalje o ranjivosti zato što se takvim pristupom administratorima sustava nameće da brže zakrpaju svoje sustave. Administratori bi također mogli iskoristiti objavljene detalje za testiranje svojih sustava i utvrđivanje ranjivosti. Drugi smatraju da takav način javnog objavljivanja nije pametan zbog toga što zlonamjerni akteri mogu iskoristiti situaciju, stoga oni predlažu da se detalji o ranjivosti otkriju samo proizvođačima dok se ne izradi zakrpa. Također, etički je najprihvatljivije prvo obavijestiti proizvođača i dati mu vremena da izradi zakrpu jer u nekim situacijama sama istraga, izrada zakrpe i testiranje mogu oduzeti dosta vremena.



Slika 1. Alat za skeniranje ranjivosti web aplikacija Acunetix WVS (izvor: https://www.principlelogic.com/wp-content/uploads/2019/08/SQL-injection.png)

Skeniranje softvera specijaliziranim alatima za otkrivanje ranjivosti može nam uvelike pomoći pri otkrivanju najčešćih oblika ranjivosti. Na slici 1. možemo vidjeti snimku zaslona jednog takvog alata koji prikazuje pronađene ranjivosti u web aplikaciji. Alat prikazuje pojedinosti o otkrivenoj ranjivosti i ostale parametre koji pomažu korisniku da pronađe i zakrpa ranjivi kod.

6. Napadači

6. 1. Motivi i vrste napadača

Nekada u prošlosti računala su hakirali najčešće programeri početnici, željni dokazivanja odnosno demonstracije svojih vještina široj javnosti. Danas se situacija uvelike promijenila te iza većine napada stoje grupe organiziranog kriminala i zlonamjerne skupine koje se nazivaju naprednim ustrajnim prijetnjama (eng. Advanced Persistent Threat, APT). Također, zadnjih par godina istaknuti su i insajdeski napadi u samim organizacijama te haktivistički napadi pokrenuti zbog nezadovoljstva s politikama organizacija.

Grupe organiziranog kriminala su danas najprominentnija skupina napadača. Ciljaju pojedince i organizacije u raznim državama, bez obzira na njihovo financijsko stanje. Iz organizacija najčešće izvlače povjerljive podatke koje potom prodaju na anonimnim crnim tržištima (primjerice koristeći Tor protokol), a zauzvrat dobivaju elektronički novac ili kriptovalute. Svoje alate i tehnike napada brzo adaptiraju potrebama na tržištu. Znaju se služiti tehnikama ucjenjivanja kako bi žrtvu natjerali na plaćanje otkupnine, u protivnom oni objavljuju žrtvine povjerljive dokumente. Neki od učestalijih načina zarade za grupe organiziranog kriminala su: krađa povjerljivih podataka, usporavanje ili onesposobljavanje servisa DDoS napadima, e-mail spam, krađa bankovnih podataka (eng. bank fraud) i prijevara oglašivača (eng. click fraud). U stvarnom svijetu ih možemo zamisliti kao otmičare ili pljačkaše, razlika je u tome što je digitalno razbojništvo puno unosnije te pruža puno veću stopu sigurnosti.

Prema nekim procjenama napadač koji drugima iznajmi infrastrukturu preko koje se pokrene 800 tisuća DDoS napada godišnje može zaraditi do 26 tisuća dolara mjesečno. Slanjem neželjene pošte s 10 tisuća zaraženih uređaja napadač može zaraditi do 3,5 milijuna dolara godišnje. Krađom bankovnih podataka od 30 tisuća žrtava iz Europe napadač može zaraditi do 47 milijuna dolara tijekom 2,5 mjeseca. Prijevarom oglašivača s 140 tisuća zaraženih uređaja napadač može dnevno zaraditi do 900 tisuća dolara. (Putman, Abhishta i Nieuwenhuis 2018)

Napredne ustrajne prijetnje su napadači koji provode ciljane dugoročne kibernetičke napade na vlade različitih država, organizacije, aktiviste i opozicijske političare. Ovakvi napadači često su sponzorirani od strane država te posjeduju napredne alate i tehnike za proboj informacijskih sustava. U stvarnom svijetu ovakve napadače možemo zamisliti kao vojnike te je ovakve napade potrebno tretirati jednako ozbiljno kao i konvencionalne vojne napade.

APT napadi obično se odvijaju u nekoliko faza (Centar informacijske sigurnosti 2011):

1. Faza istraživanja u kojoj se pasivno sakupljaju informacije o žrtvi s ciljem određivanja najbolje metode napada.
2. Faza pripreme u kojoj se napadač priprema za napad. On razvija i ispituje prikladne alate i metode za ciljani napad na žrtvu. To može uključivati skeniranje mreže u cilju prepoznavanja slabosti i propusta, pisanje i pribavljanje zlonamjernog koda te izradu zlonamjernih poruka elektroničke pošte.
3. Faza napada u kojoj napadač pokreće napad i traži znakove uspješnog proboja ili neuspjeha. Napad se obično izvodi uz pomoć dokumenta-zamke koji se korisniku dostavlja kao privitak phishing poruke elektroničke pošte.
4. Faza dobivanja pristupa koja nastupa kad je napadač uspješno uspostavio vezu s računalnom mrežom organizacije. Tada on pokušava ustanoviti gdje se nalazi u mreži. Tada se kreće kroz mrežu u potrazi za podacima od interesa, a usput instalira dodatne servise i alate za udaljeno upravljanje (eng. Remote Administration tool, RAT).
5. Faza skupljanja podataka koja nastupa kad napadač identificira podatke od interesa, te ih pokušava skupiti na jedno računalo i izvući ih iz mreže.
6. Faza održavanja veze koja nastupa nakon što je napadač uspješno uspostavio vezu s mrežom u svrhu skupljanja podataka. Tada će on najčešće pokušati održati pristup mreži kroz dulje vremensko razdoblje u svrhu skupljanja što veće količine podataka.

Insajderski napadi su prijetnje organizacijama koje dolaze od samih ljudi unutar organizacije poput zaposlenika, bivših zaposlenika ili poslovnih suradnika, koji imaju unutarnje informacije o sigurnosnim praksama organizacije, podacima ili računalnim sustavima. Prijetnja može uključivati prijevaru, krađu povjerljivih ili komercijalno vrijednih informacija, krađu intelektualnog vlasništva ili sabotažu računalnih sustava. Insajderski napadi mogu dolaziti u tri kategorije: zlonamjerni insajderi koji iskorištavaju svoj pristup kako bi nanijeli štetu organizaciji, nemarni insajderi koji griješe i zanemaruju politike organizacije te infiltratori koji su vanjski akteri sa legitimnim pristupnim podacima bez autorizacije. (Wikipedia 2021)

Haktivizam je riječ koja dolazi od riječi hakiranje i aktivizam. Haktivist je osoba koja koja koristi svoja informatička znanja u svrhu iskazivanja vlastitog nezadovoljstva, za promicanje političke agende ili poticanje društvenih promjena. Ciljevi haktivizma često su povezani sa slobodom govora i ljudskim pravima. Haktivisti se obično udružuju u decentralizirane pokrete, često bez strukture i hijerarhije, koji nastoje ostvariti zajedničke ciljeve, primjerice „Anonymous“. (Wikipedia 2021)

6. 2. Primjer grupe organiziranog kriminala i napredne ustrajne prijetnje

Kao primjer grupe organiziranog kriminala možemo navesti Webstresser koji je bio najveći svjetski web servis preko kojeg su korisnici mogli unajmiti uslugu DDoS napada.

Svaki registrirani korisnik na usluzi Webstresser mogao je platiti naknadu od 15 eura te bi mu na raspolaganje bivala stavljena infrastruktura koja omogućuje DDoS napade na mrežne usluge po vlastitom izboru.

Servis kojim je upravljao hrvatski državljanin imao je preko 150 tisuća registriranih korisnika te je preko njega pokrenuto 4 milijuna DDoS napada do 24. travnja 2018. g. kad je ugašen koordiniranom međunarodnom policijskom akcijom naziva „Power Off“.

Servis je predstavljao najveću prijetnju mrežnim uslugama financijskih institucija, poslovnih organizacija i državnih institucija širom svijeta.

Nekada su napadači koji su izvršavali DDoS napade trebali biti dobro upućeni u načine funkcioniranja internetske tehnologije, no s pojavom ovakvih ilegalnih servisa to više nije slučaj. (Ministarstvo unutarnjih poslova Republike Hrvatske 2018)

Kao primjer napredne ustrajne prijetnje možemo navesti grupu Equation koju tvrtka Kaspersky Lab prvi put spominje u izvještaju[10] objavljenom 2015. g.

Ovaj je napadač razvio vrhunske špijunske alate koji ciljaju vojnu i telekomunikacijsku industriju, ambasade, vlade te razne institute u zemljama poput Irana, Kine, Pakistana, Rusije i preko 30 drugih. Špijunski alati se na uređaje mogu instalirati udaljeno pomoću tzv. zero-day ranjivosti za kojih u trenutku infekcije proizvođač softvera nije znao, niti je postojala zakrpa.

Nakon infekcije, alati mijenjaju firmware tvrdih diskova i stvaraju tajnu particiju na koju se spremaju prikupljeni podaci. Sama činjenica da su alati mijenjali firmware na tvrdim diskovima brojnih proizvođača ukazuje na sofisticiranost zlonamjernih programa. Zbog načina na koji se zlonamjerni alati instaliraju, formatiranje tvrdog diska i reinstalacija operacijskog sustava ne brišu skrivenu particiju.

Također, navodi se da je napadač imao crva (eng. computer worm) koji je bio u stanju preko USB memorije izvući podatke iz uređaja koji nisu bili spojeni na Internet. Uz to, maliciozni kod se na sličan način preko USB memorije mogao i učitati na uređaje kao u slučaju Stuxnet crva koji je ciljao nuklearna postrojenja u Iranu, a za kojeg postoje indicije da je bio vezan za ovog napadača.

[10] Equation Group: The Crown Creator of Cyber-Espionage, https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage, pristupljeno 15. kolovoza 2021.

7. Vektori napada

7. 1. Phishing, smishing i vishing

Phishing je tehnika napada kojom napadač koristeći elemente društvenog inženjeringa pokušava uvjeriti žrtvu da svoje osobne informacije ili pristupne podatke upiše u krivotvorenu internetsku stranicu ili da pokrene zlonamjerni softver.

Prema izvještaju[11] FBI Internet Crime Complaint Center (IC3), phishing, vishing, smishing i pharming su bile najučestalije vrste napada u 2020. godini s više od 241 tisuću zabilježenih slučajeva, više nego dvostruko od bilo koje druge metode napada.

Prilikom otvaranja poveznica u porukama elektroničke pošte, autentičnost određene web lokacije možemo provjeriti usporedbom domene koja se obično nalazi u adresnoj traci web preglednika sa domenom legitimne web lokacije.

Kako bi organizacija spriječila širenje krivotvorenih poruka elektroničke pošte sa svoje internetske domene, potrebno je da omogući SPF[12] (eng. Sender Policy Framework), DKIM[13] (eng. DomainKeys Identified Mail) i DMARC[14] (eng. Domain-based Message Authentication, Reporting and Conformance). SPF je DNS[15] (eng. Domain Name System) zapis kojim javno obznanjujemo koji su poslužitelji autorizirani za slanje elektroničke pošte s naše domene. DKIM poput SPF-a koristi DNS zapis, u ovom slučaju za pohranu javnog ključa i asimetričnom kriptografijom potpisuje poruku elektroničke pošte odnosno osigurava da poruka neće moći biti izmijenjena u transportu. DMARC se oslanja na prethodno spomenute protokole te DNS zapisom definira što će se dogoditi ako poruka elektroničke pošte ne prođe DKIM i/ili SPF provjeru, odnosno definira adresu na koju će biti poslani izvještaji o e-pošti koja je poslana, a nije prošla testove[16].

[11] 2020 Internet Crime Report, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf, pristupljeno 15. kolovoza 2021.
[12] Sender Policy Framework, https://en.wikipedia.org/wiki/Sender_Policy_Framework, pristupljeno 15. kolovoza 2021.
[13] DomainKeys Identified Mail, https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail, pristupljeno 15. kolovoza 2021.
[14] DMARC, https://en.wikipedia.org/wiki/DMARC, pristupljeno 15. kolovoza 2021.
[15] Domain Name System, https://en.wikipedia.org/wiki/Domain_Name_System, pristupljeno 15. kolovoza 2021.
[16] DKIM, SPF i DMARC, https://sistemac.srce.hr/node/69, pristupljeno 15. kolovoza 2021.

Slika 2. Primjer phishing poruke (izvor: https://csi.hr/wp-content/uploads/2021/04/PHISHING-SLIKA1.png)

Na slici 2. možemo vidjeti phishing poruku u kojoj se napadač predstavlja kao tvrtka Microsoft. Napadač pokušava uvjeriti žrtvu da posjeti zlonamjernu web lokaciju i upiše podatke za prijavu na svoj Microsoft korisnički račun. U poruci su također vidljivi elementi pokušaja uzrokovanja straha i tjeskobe, zato što se prijeti obustavljanjem korisničkog računa potencijalne žrtve u slučaju da žrtva ne otvori poveznicu.

Smishing (SMS phishing) i vishing (voice phishing) su oblici phishing napada koje napadači izvode koristeći uslugu javne telefonije. U današnje vrijeme široke dostupnosti VoIP (eng. Voice over IP) usluga, jako je važno da telefonski broj pozivatelja uzmemo s dozom opreza pošto vrlo lako može biti lažiran koristeći tehnike krivotvorenja ID-a pozivatelja (eng. Caller ID spoofing). Problem je postao toliko značajan da je od 30. lipnja 2021. na nivou Sjedinjenih Američkih Država obavezna implementacija autentifikacijskih protokola STIR/SHAKEN[17] koji pomažu sprječavaju lažiranja broja pozivatelja. Ovi protokoli su dizajnirani na način da ih je moguće postepeno implementirati i u drugim državama. Za sada osim Sjedinjenih Američkih država jedino Kanada radi na implementaciji ovih protokola[18].

[17] STIR/SHAKEN, https://en.wikipedia.org/wiki/STIR/SHAKEN, pristupljeno 15. kolovoza 2021.
[18] Frequently Asked Questions (FAQ), https://www.atis.org/wp-content/uploads/01_strat_init/dlt/docs/shaken-faq.pdf, pristupljeno 15. kolovoza 2021.

7. 2. Krivotvorenje identiteta pošiljatelja/pozivatelja

Za potrebe ovog završnog rada istražen je način na koji se može krivotvoriti identitet pošiljatelja i pozivatelja u svrhu izvođenja smishing i vishing napada. Osobito je bilo važno utvrditi koliko je proces izvodljiv iz perspektive napadača koji nema pozadinu u telekomunikacijskom sektoru i s kolikim stupnjem anonimnosti je moguće izvesti takav napad.

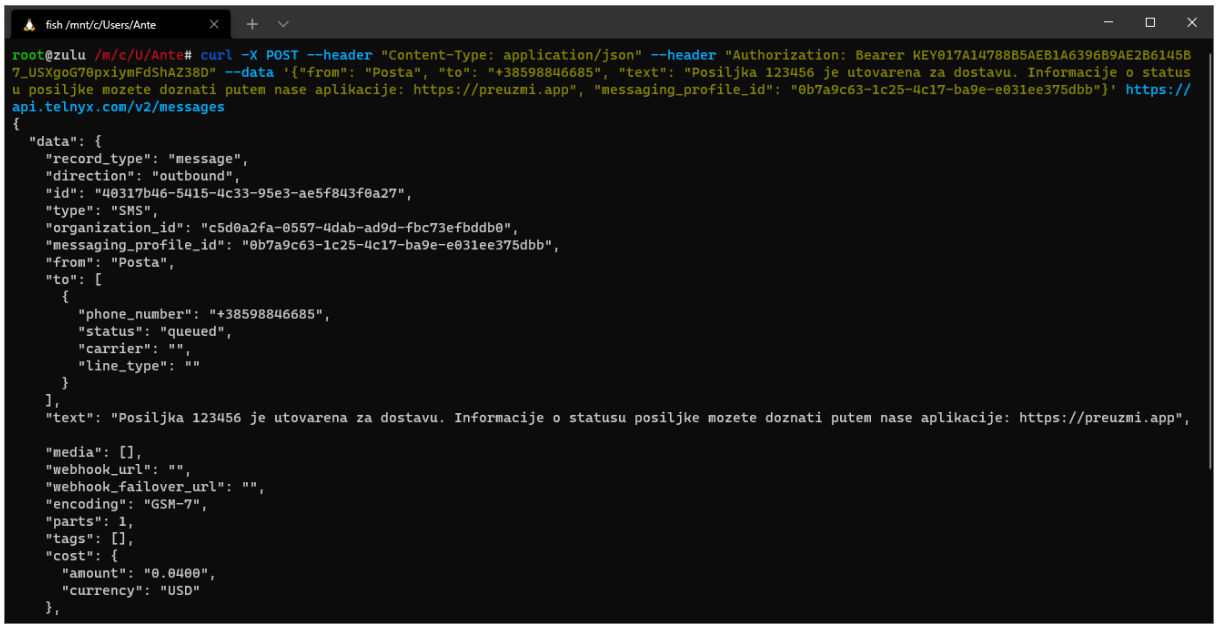
Testiranje je obavljeno koristeći dva servisa: cSpoof[19] koji se oglašava na forumima[20] često posjećivanima od strane hakera početnika te mu je glavna svrha slanje SMS poruka sa ID-om po želji i Telnyx[21] koji je legitiman servis orijentiran prvenstveno na poslovne korisnike bez vlastite telekomunikacijske infrastrukture.

Za korištenje servisa cSpoof nije bila potrebna nikakva verifikacija identiteta, dok je servis Telnyx zahtjevao osobnu iskaznicu odnosno dokaz o adresi prebivališta za korištenje usluga prema brojevima van Sjedinjenih Američkih Država.

Plaćanje za uslugu se na servisu cSpoof može obaviti jedino putem kriptovaluta Bitcoin i Litecoin, dok je za plaćanje usluge na servisu Telnyx bilo potrebno koristiti kreditnu karticu ili PayPal račun. Mogućnost plaćanja kriptovalutama za hakere predstavlja olakotnu okolnost jer im u slučaju pravilnog korištenja (primjerice kupnjom kriptovaluta na bankomatu sa gotovinom i korištenjem jednokratnih adresa) omogućuje veći stupanj anonimnosti od kreditnih kartica ili PayPal-a.

Način slanja SMS poruka relativno je jednostavan pošto oba servisa imaju API (eng. Application Programming Interface) na koji šaljemo zahtjev i sa kojeg primamo odgovor pomoću bilo kojeg alata koji podržava slanje HTTP/HTTPS zahtjeva i primanje odgovora. U ovom primjeru je korišten alat cURL[22] koji se pokreće iz naredbenog retka što je prikazano na slici 3.

[19] cSpoof, https://cspoof.com/, pristupljeno 16. kolovoza 2021.
[20] Primjerice https://hackforums.net/, https://nulled.to/ i dr.
[21] Telnyx. https://telnyx.com/, pristupljeno 16. kolovoza 2021.
[22] curl, https://curl.se/, pristupljeno 16. kolovoza 2021.



Slika 3. Slanje smishing poruke preko servisa Telnyx koristeći alat cURL (izvor: osobno istraživanje)

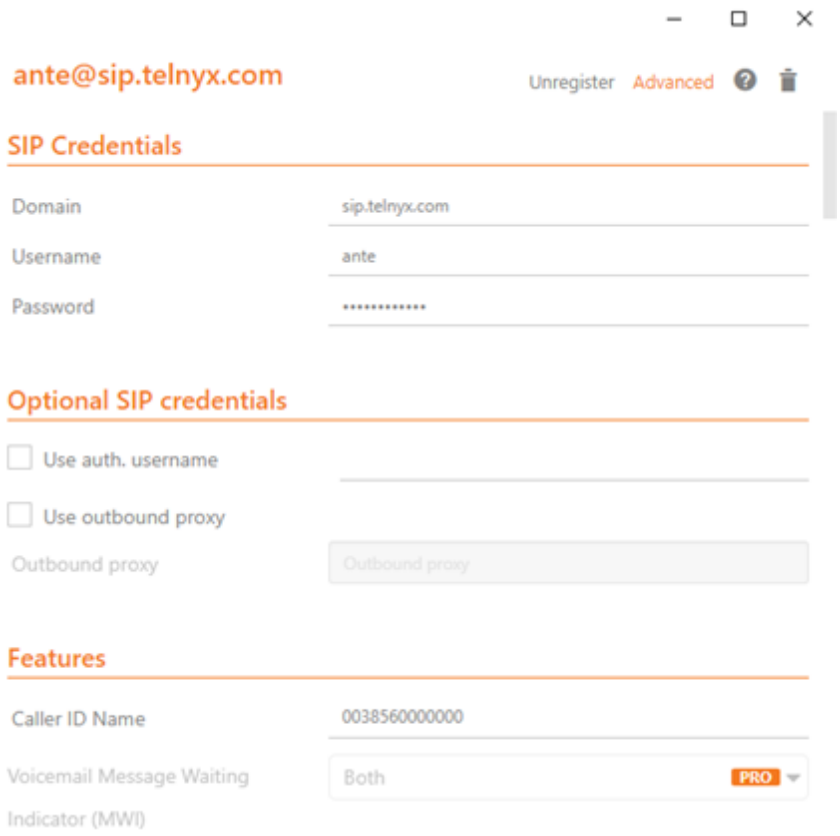
Servisi su uspješno dostavili SMS poruke koje su naplaćene 0.09 USD (cSpoof) i 0.04 USD (Telnyx) te je rezultat vidljiv na slici 4.

Slika 4. Dolazni SMS na mobilnom uređaju (izvor: osobno istraživanje)

Napadač SMS-om osim alfanumeričkog ID-a (max. 11 znakova) može koristiti i broj druge osobe. Primatelju poruke se u tom slučaju može, ako mu je broj memoriran u

imeniku, prikazati i memorirano ime vlasnika broja. U poruci koja je poslana u primjeru ID pošiljatelja je „Pošta“. Primatelja se obavještava o dospijeću paketa kojeg može pratiti ako preuzme aplikaciju sa priloženog linka. Aplikacija koja se preuzme preko poveznice može biti zlonamjerna.

Pozivanje je obavljeno preko servisa Telnyx koristeći besplatni Zoiper[23] softverski telefon. Upis neophodnih podataka u Zoiper prikazan je na slici 5.

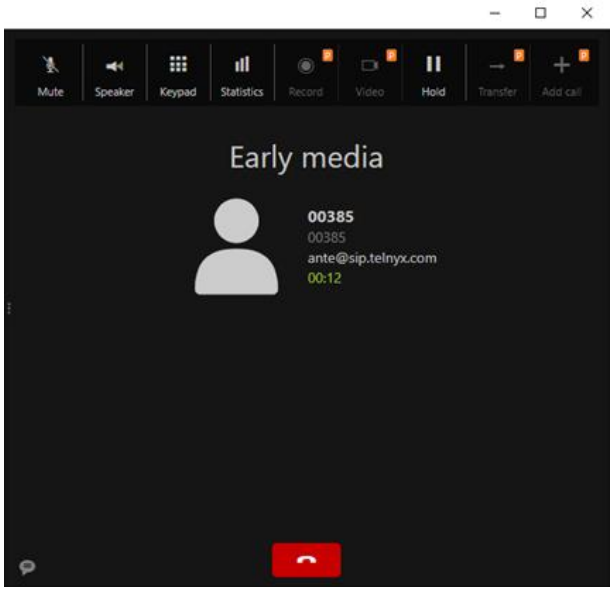


Slika 5. Spajanje na udaljeni SIP poslužitelj i definiranje broja pozivatelja (izvor: osobno istraživanje)

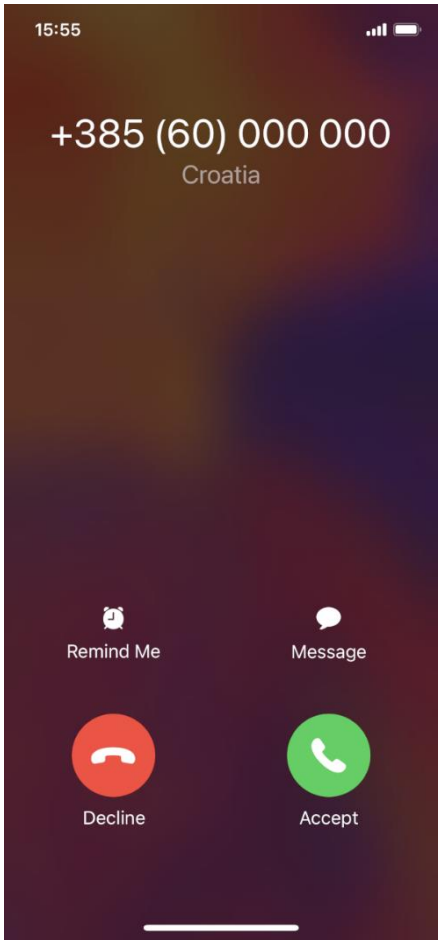
Pozivanje i dolazni poziv na mobilnom uređaju mogu se vidjeti na slikama 6. i 7.

Ovom tehnikom napadač može uputiti poziv i s brojeva prema kojima se obračunava posebna tarifa (eng. premium-rate numbers) te brzo prekinuti poziv prije nego što se primatelj poziva javi. Velika je šansa da će primatelj poziva primijetiti propušteni poziv te pozvati broj. Na taj način mu može biti naplaćena velika novčana naknada.

[23] Zoiper, https://www.zoiper.com/, pristupljeno 16. kolovoza 2021.



Slika 6. Pozivanje koristeći Zoiper softverski telefon (izvor: osobno istraživanje)



Slika 7. Dolazni poziv na mobilnom uređaju (izvor: osobno istraživanje)

7. 3. Napadi na lozinke

U današnje vrijeme uobičajena je praksa da se lozinke u bazu podataka pohranjuju nakon što su nad njima primijenjene kriptografske funkcije sažimanja (eng. hash functions). To su jednosmjerne funkcije koje omogućuju da se lozinke ne spremaju u bazu u svom izvornom obliku u kojem bi ih potencijalni napadač mogao lako iskoristiti za prijavu. Takve sažetke (eng. hash) prilično je lako generirati, no teško ih je „preokrenuti“ u izvorni oblik. Primjerice, pretpostavimo da se korisnik želi registrirati na sustav uporabom lozinke „stranica“ i da sustav koristi NTLM funkciju sažimanja. Riječ „stranica“ primjenom NTLM funkcije sažimanja postaje „ddc5ad8b655023fdb6f561cab0339f0d“ i takva se prilikom registracije korisnika na sustav zapisuje u bazu podataka.

```
izlaz = NTLM(ulaz);

„ddc5ad8b655023fdb6f561cab0339f0d“ = NTLM(„stranica“);
```

Prijava na sustav radi na istom principu. Korisnik unosi ulazni parametar (lozinku) i od nje se uporabom funkcije sažimanja (npr. NTLM) dobiva izlaz koji se uspoređuje sa rezultatom dobivenim iz baze podataka za spomenutog korisnika. Ako se izrazi podudaraju, program će omogućiti prijavu na sustav. Ako se izrazi ne podudaraju, prikazati će poruku o pogrešnoj lozinki. Ako napadač pokuša upotrijebiti lozinku koju je dobio iz baze podataka (u našem slučaju „ddc5ad8b655023fdb6f561cab0339f0d“) za prijavu, prijava neće uspjeti, jer se uporabom NTLM funkcije sažimanja na toj lozinki dobiva sažetak koja nije identičan sadržaju upisanom u bazu podataka.

```
izlaz = NTLM(ulaz);

„67c5241a8bfd578b9eebc160f9a1724d“ = NTLM(„ddc5ad8b655023fdb6f561cab0339f0d“);
```

Brute-force napadima napadač isprobava sve moguće kombinacije znakova u potrazi za lozinkom. Ovakvi napadi garantiraju pronalazak lozinke, no mogu biti dugotrajni u slučaju kompleksne lozinke. Napadač može znatno suziti opseg pretrage za lozinkom ako zna njen dio, veličinu ili ostala svojstva korištenjem maske (eng. mask attack). Od brute-force napada se možemo zaštititi uporabom velikih i kompleksnih lozinki (mala i velika slova, brojevi i posebni simboli).

Napad rječnikom funkcionira na sličan način kao i brute-force napad, razlika je u tome da napadač isprobava sve riječi iz rječnika dok ne dođe do lozinke. Ovakvi napadi mogu biti znatno brži od brute-force napada kod jednostavnih lozinki koje su uvrštene u rječnike. Uz spomenute napade postoje i napadi koji vrše kombinaciju više rječnika.

Zbog čestih proboja baza podataka popularnih internetskih servisa ne preporučuje se korištenje istih lozinki na više lokacija. Dobra preporuka je generiranje i spremanje lozinki unutar upravitelja lozinki, zato što je kompleksne lozinke prilično teško zapamtiti, a u slučaju izlaganja unutar nesigurnog okruženja (primjerice u tekstualnom dokumentu na radnoj površini) mogu biti kompromitirane.

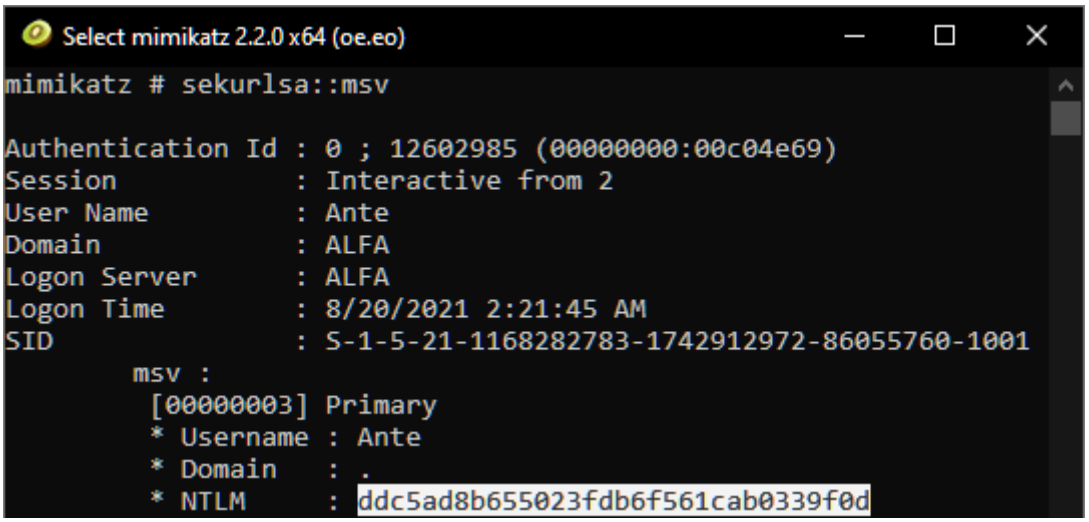
7. 3. 1. Primjer napada na lozinku (Microsoft Windows 10 sustav prijave)

U ovom je primjeru opisan način dobivanja lozinke iz njezinog sažetka (koji je prethodno dobiven uporabom NTLM funkcije sažimanja). Naime, operacijski sustav Microsoft Windows 10 primjenjuje ovu funkciju sažimanja na lozinkama koje se koriste za prijavu.

Postoje dva načina pomoću kojih možemo doći do sažetka: pregledom sadržaja SAM datoteke s tvrdog diska ili iz radne memorije (ako je korisnik već prijavljen na sustav).

U ovom primjeru opisan je način dobivanja sažetka iz radne memorije korištenjem alata mimikatz[24] i uporabe alata hashcat[25] da bi se od sažetka dobila lozinka. Nakon pokretanja alata, u naredbeni redak potrebno je unijeti naredbe „`privilege::debug`“ koja nam daje tzv. debug prava i „`sekurlsa::msv`“ koja nam prikazuje ime prijavljenog korisnika i njegov NTLM sažetak, što je vidljivo na slici 8.

[24] mimikatz, https://github.com/gentilkiwi/mimikatz, pristupljeno 16. kolovoza 2021.
[25] hashcat, https://github.com/hashcat/hashcat, pristupljeno 16. kolovoza 2021.

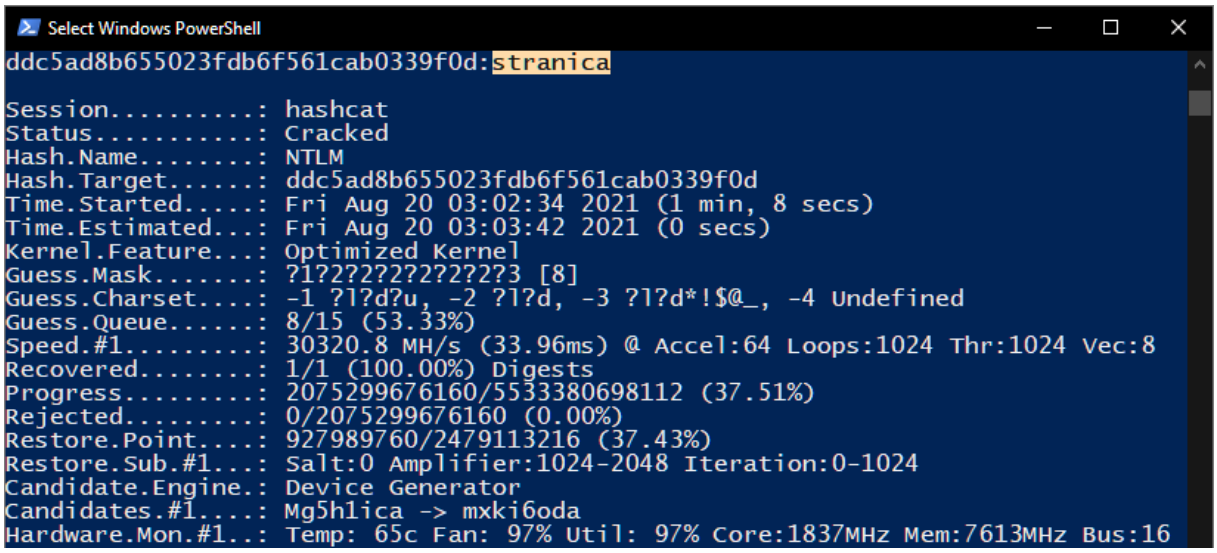


Slika 8. Prikaz prijavljenog korisnika i NTLM sažetka njegove lozinke (izvor: osobno istraživanje)

Potom dobiveni sažetak unosimo u alat hashcat s argumentima:

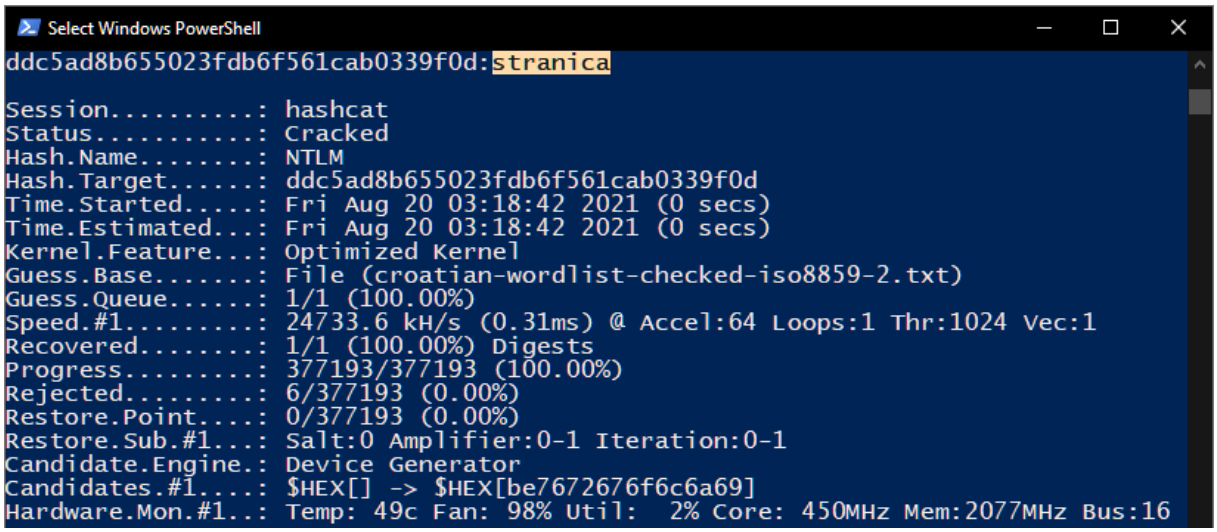
- vrsta napada (-a) — „-a 3“ za brute-force, „-a 0“ za napad rječnikom,
- funkcija sažimanja (-m) — „-m 1000“ za NTLM funkciju sažimanja,
- uporaba optimiziranog kernela (-O) — ograničava veličinu lozinke, no uvelike poboljšava performanse alata,
- profil opterećenja (-w) — u našem slučaju „-w 4“ što predstavlja najvišu potrošnju električne energije i najveće usporavanje normalnog rada na računalu, no istodobno i najveće moguće performanse alata,
- sažetak i
- rječnik (samo za primjer na slici 9.).

Na slici 9. možemo vidjeti detalje brute-force napada pokrenutog naredbom „`./hashcat.exe -a 3 -m 1000 -O -w 4 "ddc5ad8b655023fdb6f561cab0339f0d"`“. Alat je vratio rezultat u formatu „`sažetak:lozinka`“ na samom vrhu naredbenog retka. Na snimci zaslona su također vidljive i ostale informacije poput: odabrane funkcije sažimanja, sažetka, vremena početka, procijenjenog trajanja, vrste kernela, pretpostavljene maske, pretpostavljenog skupa znakova, brzine i drugog.



Slika 9. Brute-force napad (izvor: osobno istraživanje)

Na slici 10. možemo vidjeti detalje napada rječnikom pokrenutog naredbom „`./hashcat.exe -a 0 -m 1000 -O -w 4 "ddc5ad8b655023fdb6f561cab0339f0d" "croatian-wordlist-checked-iso8859-2.txt"`“.



Slika 10. Napad rječnikom (izvor: osobno istraživanje)

Za izvođenje napada je korišten hrvatski rječnik „`croatian-wordlist-checked-iso8859-2.txt`“[26] koji sadrži oko 377 tisuća riječi, a preuzet je sa poslužitelja Hrvatske udruge Linux korisnika. U oba slučaja napada alat nije poznavao nikakve karakteristike lozinke.

Napadi na lozinke izvršeni su uporabom grafičke kartice NVIDIA GeForce RTX 2060. Grafičke kartice su za razliku od klasičnih procesora pogodnije za izvođenje paralelnih operacija zbog toga što su izrađene na način da imaju više jezgri koje simultano mogu izvršavati aritmetičke operacije. Primjerice, navedena grafička kartica ima 1920 jezgri, dok moderni procesori imaju između 2 i 64.

Ovakvi napadi se osim uporabom vlastitog hardvera mogu izvoditi i koristeći unajmljeni hardver u oblaku. Napadači na takav način u samo par klikova mogu jednostavno doći do izuzetno jakog hardvera poput NVIDIA A100 grafičkih kartica s 6912 jezgri na servisu Google Cloud.

Zaključno, alat hashcat je iz NTLM sažetka brute-force napadom (-a 3) pri brzini ~30 milijardi sažetaka u sekundi pogodio lozinku od osam znakova za 68 sekundi, dok je uporabom napada rječnikom (-a 0) lozinku dobio iste sekunde (pošto se nalazila u hrvatskom rječniku).

[26] croatian-wordlist.txt.gz, http://ftp.linux.hr/spell/wordlist/croatian-wordlist.txt.gz, pristupljeno 16. kolovoza 2021.

7. 4. Drive-by preuzimanja

Drive-by preuzimanja su neželjena preuzimanja računalnog softvera sa interneta. Mogu se odnositi na: preuzimanje i pokretanje softvera koje je osoba odobrila bez da je znala za posljedice te preuzimanje i pokretanje softvera bez autorizacije (bilo kakvo skriveno preuzimanje zlonamjernog softvera) [27].

Da bi pokrenuli zlonamjerni softver na računalima žrtava napadači najčešće iskorištavaju ranjivosti u: Adobe Flash Player dodatku za web preglednik, Oracle Java dodatku za web preglednik, Microsoft Silverlight dodatku za web preglednik te Microsoft Internet Explorer web pregledniku (i njegovim ActiveX kontrolama).

Brojne su ranjivosti koje omogućuju napade ovakvog tipa u prošlosti bivale ugrađivane u komplete za iskorištavanje[28] (eng. exploit kits), koji bi utvrđivali ima li računalo koje se planira napasti ranjivi softver i ako ima iskorištavali ranjivost u tom softveru. U današnje vrijeme, dodatke za preglednike su uglavnom zamijenile sigurne HTML5 web aplikacije pa su ovakvi tipovi neželjenih preuzimanja u praksi vrlo rijetki. Ipak, usprkos uklonjenim nesigurnim dodacima i dobroj izolaciji modernih web preglednika, ponekad se znaju pojaviti tzv. RCE (Remote Code Execution) ranjivosti koje omogućavaju izvršavanje koda na računalu izvan samog preglednika.

Kompleti za iskorištavanje se pozivaju iz zlonamjernih oglasa (eng. malvertising) na web lokacijama. Obično su to stranice sa piratskim i drugim ilegalnim sadržajem koje ne mogu prodati svoj oglasni prostor legitimnim oglašivačima te se u potrazi za izvorom financiranja često odlučuju na očajničke mjere prodajući oglasni prostor hakerima. S druge strane, navedeni zlonamjerni oglasi se mogu „provući“ i na legitimne stranice zbog kompleksnosti cijelog oglašivačkog ekosistema. Naime, često se dešava da vlasnici web lokacija uopće ne znaju kome prodaju oglasni prostor zato što prodaju prepuštaju specijaliziranim servisima poput oglašivačkih mreža. Takvim načinom vlasnici web lokacija štede vrijeme, no vrlo malo mogu utjecati na kvalitetu oglasa koji će biti prikazani na njihovim web stranicama.

[27] Drive-by download, https://en.wikipedia.org/wiki/Drive-by_download, pristupljeno 20. kolovoza 2021.
[28] Drive-by downloads: Can you get malware just from visiting a website? https://blog.emsisoft.com/en/38301/drive-by-downloads-can-you-get-malware-just-from-visiting-a-website/, pristupljeno 20. kolovoza 2021.

8. Zlonamjerni softver

8. 1. Općenito o zlonamjernom softveru

Zlonamjerni softver (eng. malware, skraćeno od malicious software) je softver koji je dizajniran da našteti računalima ili računalnim mrežama. Postoji mnoštvo zlonamjernog softvera uključujući viruse, crve, trojance, ucjenjivački softver (eng. ransomware), špijunski softver (eng. spyware), oglašivački softver (eng. adware), zastrašivački softver (eng. scareware), ostali neželjeni softver itd. Programi se također klasificiraju u zlonamjerni softver ako potajno rade protiv interesa korisnika.

Internetski kriminal usko je povezan sa zlonamjernim softverom jer je on sredstvo putem kojega kriminalci (napadači) nanose financijsku i druge oblike štete običnim korisnicima i organizacijama.

Neka istraživanja pokazala su da ritam izdavanja zlonamjernog softvera premašuje ritam izdavanja legitimnog softvera. Napadači šire velike količine zlonamjernog softvera te računaju da će, zbog različitih razloga, uvijek uspjeti inficirati djelić uređaja koji na neki način dođe u doticaj sa zlonamjernim softverom. Danas postoji mnoštvo antimalware alata, sigurnosnih stijena (vatrozida) i ostalih alata za prevenciju infekcija zlonamjernim softverom te oporavak u slučaju postojeće infekcije. (Wikipedia 2021)

8. 2. Računalni virusi i crvi

Računalni virus je oblik zlonamjernog softvera koji se replicira na način da mijenja druge izvršne datoteke i ubacuje svoj kod u njih. U današnje vrijeme virusi su prava rijetkost i često ih se pogrešno miješa sa ostalim zlonamjernim softverom.

Tri glavne komponente virusa su[29]:

- vektor infekcije → način na koji se virus širi ili propagira,
- okidač → tzv. logička bomba koja virus pokreće reakcijom na neki događaj (npr. određeni datum, vrijeme, prisutnost drugog programa, popunjenost tvrdog diska ili otvaranje određene datoteke) te
- sadržaj → podaci koji čine štetu odnosno onaj dio virusa koji ga čini virusom.

[29] Computer virus, https://en.wikipedia.org/wiki/Computer_virus, pristupljeno 20. kolovoza 2021.

Računalni crv je oblik zlonamjernog softvera koji se replicira kako bi inficirao druge uređaje. Za razliku od računalnih virusa, crvi su često u potpunosti autonomni tj. ne zahtijevaju da ih čovjek pokrene nego se samostalno šire.

Jednom kad se neki uređaj inficira, on može proširiti infekciju unutar lokalne mreže zato što mrežni portovi unutar lokalne mreže obično nisu filtrirani i na takav način jako brzo inficirati veći broj ranjivih uređaja.

Drugi poznati načini repliciranja uključuju inficiranje USB memorije najčešće kroz „autorun.inf" datoteke te prečace s ekstenzijom „lnk". Jedan od poznatijih primjera računalnog crva je tzv. WannaCry, koji je ujedno i ransomware baziran na EternalBlue ranjivosti u SMB (Server Message Block) protokolu. Pretpostavlja se da je EternalBlue ranjivost uzrokovala preko milijardu dolara štete kroz WannaCry, NotPetya i BadRabbit ransomware.

8. 3. Zlonamjerni softver koji napada uređaje interneta stvari

Ovakav tip zlonamjernog softvera pretvara uređaje koji su spojeni na internet u oružje koje najčešće služi za pokretanje DDoS napada te prijevaru oglašivača.

Najčešće cilja loše zaštićene pametne uređaje kao što su kućanski aparati, IP kamere i kućni usmjerivači.

Najbolji primjer ovakvog zlonamjernog softvera je crv Mirai[30] koji je 2016. g. pokrenuo napad snage preko 1,1 Tbps usmjeren na poslužitelje tvrtke OVH. Mirai konstantno skenira IPv4[31] adresni prostor i traži ranjive uređaje sa otvorenim Telnet portom, potom metodom napada rječnikom isprobava listu ugrađenih kombinacija korisničkih imena i lozinki te naposlijetku inficira uređaj.

Najbolja zaštita od ovakvih napada je briga o uređajima koja uključuje redovitu provjeru nadogradnji softvera te postavljanje uređaja u privatni adresni prostor uz pomoć NAT (eng. Network Address Translation)[32], tako da ne budu direktno vidljivi s interneta.

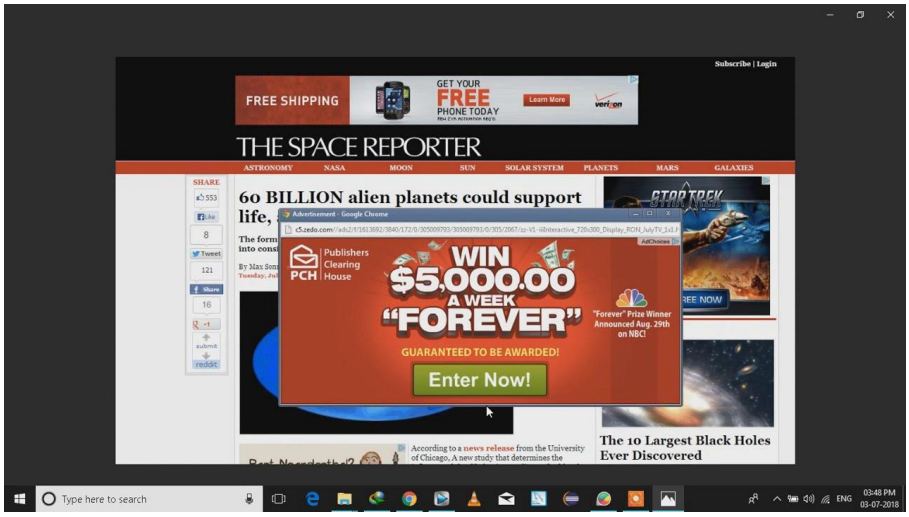
[30] Inside the infamous Mirai IoT Botnet: A Retrospective Analysis, https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/, pristupljeno 20. kolovoza 2021.
[31] IPv4, https://en.wikipedia.org/wiki/IPv4, pristupljeno 20. kolovoza 2021.
[32] Network address translation, https://en.wikipedia.org/wiki/Network_address_translation, pristupljeno 20. kolovoza 2021.

8. 4. Oglašivački softver

Oglašivački softver je softver koji prikazuje oglase na računalima korisnika te na takav način pribavlja novčanu korist za autore. Također se naziva PUA (eng. Potentially Unwanted Application) odnosno PUP (eng. Potentially Unwanted Program) te u suštini ne nanosi nikakvu štetu osim što zamara korisnika.

Softver ima dva tipa monetizacije: jedan tip je CPM (eng. Cost Per Mile) koji autora plaća po tisuću pregleda oglasa, dok je drugi CPC (eng. Cost Per Click) koji autora plaća kad korisnik klikne na oglas. Softver može prikazivati oglase na različite načine: putem slikovnih oglasa, punim zaslonom, unutar videa, unutar skočnih prozora te na druge načine. Neki autori softvera koriste oglašivački softver da bi zaradili na softveru kojeg inače izdaju besplatno, a neki nude i plaćenu verziju koja ne sadržava adware.

Funkcioniranje softvera može biti dizajnirano na takav način da analizira korisnikovu lokaciju i povijest pretraživanja pa mu prema tim parametrima daje relevantne oglase. Zbog toga, ovakvi alati često predstavljaju prijetnju po privatnost korisnika. Iako najbenigniji tip zlonamjernog softvera, u nekim slučajevima[33], zbog nebrige o sigurnosti prilikom razvoja softvera može otvoriti potencijalne ranjivosti. Na slici 11. možemo vidjeti primjer Zedo oglašivačkog softvera.



Slika 11. Primjer Zedo oglašivačkog softvera (izvor: https://i.ytimg.com/vi/mh-e6ZWxjYs/maxresdefault.jpg)

[33] Lenovo Superfish Adware Vulnerable to HTTPS Spoofing, https://us-cert.cisa.gov/ncas/alerts/TA15-051A, pristupljeno 21. kolovoza 2021.

8. 5. Ucjenjivački softver i zastrašivački softver

Ucjenjivački softver je tip zlonamjernog softvera koji prijeti da će objaviti žrtvine podatke ili onemogućiti pristup istima ako žrtva ne plati otkupninu[34]. Žrtva najčešće ima samo par dana za uplatu prije nego što se cijena otkupnine drastično poveća.

Iako postoje varijante ucjenjivačkog softvera koje zaključaju uređaj na način da ga specijalizirani alati i stručnjaci mogu lako otključati, postoje i teže varijante koje upotrebljavaju kriptografiju te šifriraju žrtvine podatke. U slučaju dobro implementirane kriptografije nemoguće je pribaviti privatni ključ koji je potreban za otključavanje podataka bez plaćanja otkupnine.

Ucjenjivački softver obično traži uplatu u digitalnim valutama koje je teško pratiti (primjerice Bitcoin, MoneyPak i PaySafeCard). Najčešće ih šire trojanci kao dodatan izvor zarade, no u prošlosti su se pojavljivali i primjeri koji su se samostalno širili, najpoznatiji je WannaCry.

Počevši od 2012. g. uporaba ucjenjivačkog softvera drastično se povećala. U prvih šest mjeseci 2018. g. zabilježeno[35] je preko 181 milijuna napada ucjenjivačkog softvera što bilježi porast od 229% u odnosu na isto razdoblje 2017. godine.

Zastrašivački softver je tip zlonamjernog softvera koji koristi tehnike društvenog inženjeringa da bi uzrokovao šok, tjeskobu ili privid opasnosti kod korisnika, odnosno da bi izmanipulirao žrtvu da kupi neželjeni softver[36].

Obično se predstavlja kao antivirusni program. Obavijesti o virusima su obično lažne, stoga softver ne uklanja stvarne viruse. Autori su svjesni mogućnosti koje pruža ovakav softver zbog neznanja i naivnosti ljudi.

Prema podacima FBI-a jedna skupina kriminalaca koja se bavila izradom zastrašivačkog softvera je uspjela steći novčanu korist od 71 milijun dolara. Zadnjih par godina najčešće se plasiraju zastrašivački skočni prozori u internetskim preglednicima u kojima napadači traže uplate u elektroničkom novcu.

---

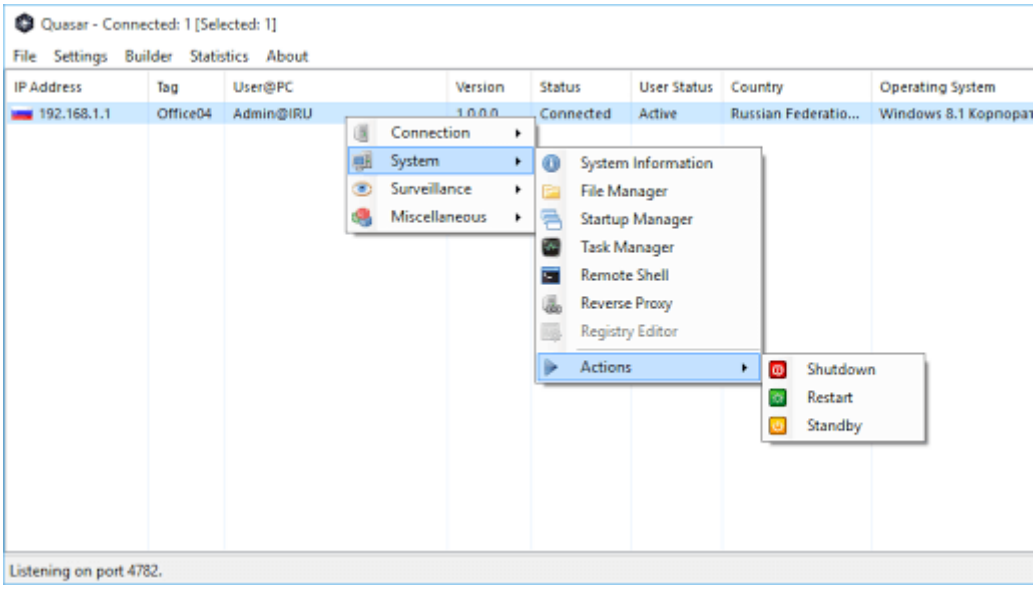
[34] Ransomware, https://en.wikipedia.org/wiki/Ransomware, pristupljeno 21. kolovoza 2021.
[35] Ransomware back in big way, 181.5 million attacks since January, https://www.helpnetsecurity.com/2018/07/11/2018-sonicwall-cyber-threat-report/, pristupljeno 21. kolovoza 2021.
[36] Scareware, https://en.wikipedia.org/wiki/Scareware, pristupljeno 21. kolovoza 2021.

8. 6. Alati za daljinsko upravljanje

Alat za daljinsko upravljanje je softver koji korisniku omogućuje udaljeni pristup nekom uređaju. Osoba sa takvim alatom može pratiti sadržaj na zaslonu, pristupiti datotečnom sustavu, gledati sliku sa web kamere, slušati zvuk sa mikrofona, isključivati i ponovno pokretati uređaj te raditi mnoge druge stvari koje bi mogla raditi da ima fizički pristup uređaju (primjer na slici 12.).

Postoje i legitimni oblici ovakvog softvera koji su primjerice upotrebljavani od strane roditelja kod nadzora svoje malodobne djece ili poslodavaca kod praćenja svojih zaposlenika unutar radnog vremena, stoga je teško blokirati uporabu ovakvog softvera. Ipak, zbog pretjerane uporabe u zlonamjerne svrhe, neke od mrežnih trgovina aplikacija traže od autora softvera da stalno prikazuje obavijest o praćenju uređaja[37].

Ovakvi alati su poprilično dostupni i mnogi su otvorenog koda odnosno moguće ih je besplatno preuzeti i modificirati prema vlastitim potrebama, stoga ne čudi činjenica da su često upotrebljavani kod hakera početnika. Također, vrijedi spomenuti da su u prošlosti bili korišteni i za praćenje aktivista koji su se borili protiv vlade[38].



Slika 12. Alat za daljinsko upravljanje Quasar RAT (izvor: https://pentesttools.net/wp-content/uploads/2017/12/QuasarRAT1.png)

[37] Google 'formally' bans stalkerware apps from the Play Store, https://www.zdnet.com/article/google-formally-bans-stalkerware-apps-from-the-play-store/, pristupljeno 22. kolovoza 2021.
[38] How the Boy Next Door Accidentally Built a Syrian Spy Tool, https://www.wired.com/2012/07/dark-comet-syrian-spy-tool/, pristupljeno 22. kolovoza 2021.

9. Načini zaštite

9. 1. Višestruka autentifikacija

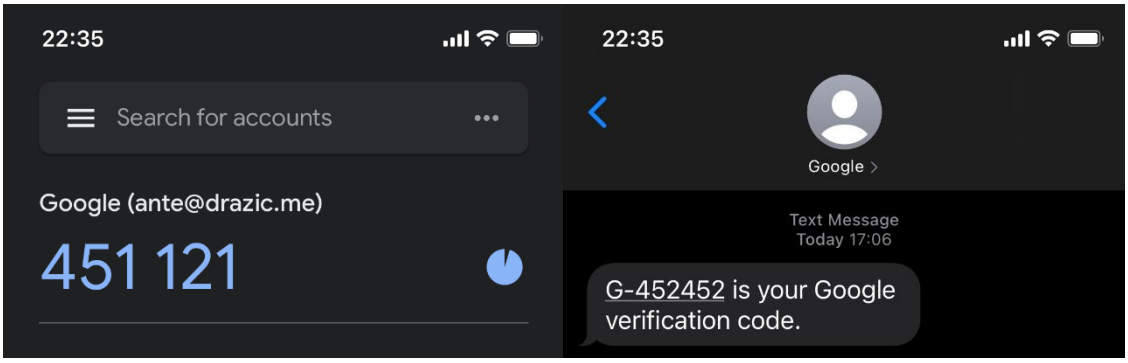
Zbog sklonosti korisnika da biraju loše lozinke te brojnih proboja podataka, broj web servisa koji upotrebljava višestruku autentifikaciju povećava se svakodnevno. Višestruka autentifikacija osigurava da će korisnik za pristup aplikaciji ili određenom dijelu aplikacije morati koristiti dva ili više dokaza (faktora). Ovakav koncept nije ništa novo i koristi se već godinama primjerice u bankarskom sektoru gdje se za prijavu na internetsko bankarstvo često upotrebljavao hardverski token.

U današnje vrijeme hardverske tokene su zamijenile mobilne aplikacije koje putem interneta dobivaju jednokratni kod koji korisnik upisuje u web aplikaciju internetskog bankarstva.

Razvoj web tehnologija je doveo do otvorenog standarda FIDO2[39] koji omogućuje uporabu hardverskih modula u web preglednicima prilikom prijave na web lokacije koje podržavaju takav način prijave.

Dokazi kojima korisnik potvrđuje da je on zaista onaj tko se predstavlja su:

- Nešto što korisnik zna - primjerice lozinka, PIN itd.
- Nešto što korisnik posjeduje - primjerice USB token, pametni telefon itd.
- Nešto što korisnik je - uporaba biometrije kao što je prepoznavanje lica, glasa, otiska prsta, rožnice itd.



Slika 13. Višestruka autentifikacija korištenjem aplikacije i korištenjem SMS-a (izvor: osobno istraživanje)

[39] FIDO2 Project, https://en.wikipedia.org/wiki/FIDO2_Project, pristupljeno 25. kolovoza 2021.

9. 2. Sigurnosno kopiranje podataka

Sigurnosna ili pričuvna kopija podataka izrađuje se u svrhu sprječavanja gubitka vrijednih podataka.

Kao što je ranije u radu spomenuto, postoji velik broj prijetnji koji potencijalno može ugroziti cjelovitost i dostupnost podataka. Uz spomenute prijetnje, često se dešava i da sami korisnici slučajno ugroze svoje podatke, a nisu rijetkost ni prirodne katastrofe poput vremenskih nepogoda.

U današnje vrijeme mediji za pohranu podataka postali su vrlo jeftini te je vrijedne podatke stoga poželjno redundantno spremati na više lokacija. Podaci se mogu spremati na: unutarnje (interne) diskove, vanjske (eksterne) diskove, USB memorije, NAS (eng. Network-Attached Storage), magnetske vrpce, CD, DVD i drugo.

Također, osim sigurnosne pohrane podataka na fizičke medije za pohranu podataka, danas je sve popularnije i korištenje oblaka. Postoje brojni servisi koji nude besplatne i naplatne opcije pohrane podataka ovisno o količini pohranjenih podataka, a neki[40] nude i neograničenu sigurnosnu pohranu podataka za samo 7 USD mjesečno.

Prilikom odabira rješenja za sigurnosnu pohranu podataka u obzir trebamo uzeti: jednostavnost korištenja, količinu prostora, cijenu, brzinu izrade sigurnosne kopije, sigurnost podataka te mogućnost brzog vraćanja i oporavka podataka[41].

[40] Cloud Backup: Easy, Secure Online Backup - Backblaze, https://www.backblaze.com/cloud-backup.html, pristupljeno 25. kolovoza 2021.
[41] Što je to backup (sigurnosna kopija)?, https://www.datasector.hr/hr/blog/sto-je-to-backup-sigurnosna-kopija/9, pristupljeno 25. kolovoza 2021.

9. 3. Antimalware i sandbox alati

Antimalware alati nam pomažu pri pronalasku i uklanjanju zlonamjernog softvera. U prošlosti su se ovakvi alati nazivali antivirusnim alatima, no pošto su virusi s vremenom postali rijetki i sama se terminologija promijenila. Danas je osim samih virusa u fokusu puno više prijetnji: crvi, oglašivački softver, ucjenjivački softver, alati za daljinsko upravljanje, zastrašivački softver i drugo.

Antimalware alati najčešće pronalaze prijetnje na temelju jedinstvenih potpisa kojih istraživači otkriju i stave u bazu podataka koju će alat kasnije koristiti. Ova metoda detekcije je dobra kod jednostavnih oblika zlonamjernog softvera, no kod složenijih oblika ona nije efikasna zbog toga što zlonamjerni softver može mutirati mijenjajući svoj potpis. Zbog toga se u današnje vrijeme sve češće upotrebljava heuristička detekcija koja je sposobna detektirati do sada nepoznate primjere zlonamjernog softvera, kao i prethodno spomenute mutirane varijante. Heuristička detekcija radi na principu promatranja API poziva koje zlonamjerni softver inače koristi te s obzirom na opseg korištenja takvih poziva zaključuje je li riječ o zlonamjernom softveru. Mana heurističke metode detekcije je da daje vrlo visok broj lažno pozitivnih detekcija.

Sandbox alati omogućuju pokretanje sumnjivih aplikacija u izoliranom okruženju s ciljem izbjegavanja infekcije zlonamjernim softverom ili narušavanja stabilnosti sustava.

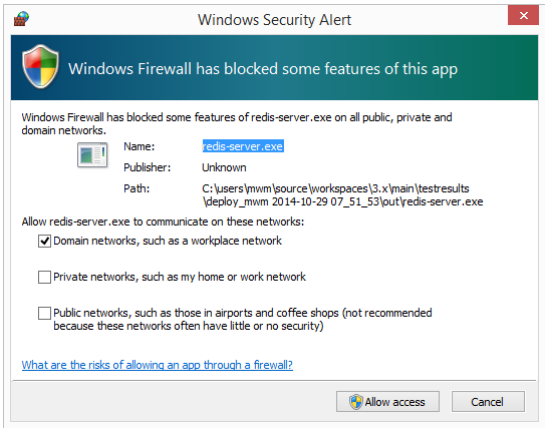
Sandbox je vrsta virtualnog okruženja u kojem se resursi svake aplikacije koja se unutra izvršava nadgledaju i ograničavaju. Procesima u takvom okruženju nije dopuštena izmjena sadržaja memorijskog prostora drugih procesa, niti pisanje po tvrdom disku. Ipak, zbog praktičnosti, mnogi sandbox alati dopuštaju zapisivanje pojedinih datoteka na tvrdi disk ukoliko ih korisnik odobri.

9. 4. Sigurnosna stijena ili vatrozid

Sigurnosna stijena ili vatrozid je softverski paket ili zasebni uređaj koji filtrira dolazni i odlazni mrežni promet prema unaprijed definiranim pravilima.

Glavne mogućnosti i zadaci vatrozida su[42]:

- prijava neovlaštenog pokušaja spajanja na računalo (od strane vanjskih mrežnih servisa),
- određivanje lokalnih mrežnih servisa kojima je dopuštena mrežna interakcija,
- sprječavanje detektiranja otvorenih mrežnih priključaka od strane udaljenih potencijalnih napadača (na način da odbacuje nezatraženi mrežni promet, tj. promet koji nije iniciran s korisničkog računala),
- nadziranje lokalnih mrežnih servisa,
- zaustavljanje neovlaštenog odlaznog prometa lokalnih mrežnih servisa te
- pružanje informacija o aplikaciji koja zahtjeva mrežnu komunikaciju.



Slika 14. Obavijest Windows Firewall-a o blokiranju mrežnog pristupa aplikaciji (izvor: https://i.stack.imgur.com/a45bg.png)

Slika 14. prikazuje upozorenje alata Windows Firewall koji se aktivirao zato što je aplikacija pokušala uspostaviti mrežnu komunikaciju. Alat ispituje korisnika želi li dozvoliti komunikaciju aplikacije prema mreži i to specifičnije prema kojoj vrsti mreže.

[42] Zaštita mreže - vatrozid, https://www.cis.hr/sigurnosni-alati/zastita-mreze-vatrozid.html, pristupljeno 26. kolovoza 2021.

9. 5. Sustavi za otkrivanje i sprječavanje upada

Sustav za otkrivanje upada (eng. Intrusion Detection System - IDS) je softverski paket ili zasebni uređaj koji promatra mrežne i sistemske aktivnosti i pokušava ustanoviti postoji li zlonamjerna aktivnost ili povreda politike sustava. Svaka takva aktivnost obično biva prijavljena administratoru kroz nadzornu ploču sustava.

Sustavi za otkrivanje upada se dijele na sustave za otkrivanje upada na lokalno računalo (eng. Host-based Intrusion Detection System - HIDS) i sustave za otkrivanje upada na mreži (eng. Network-based Intrusion Detection System - NIDS).

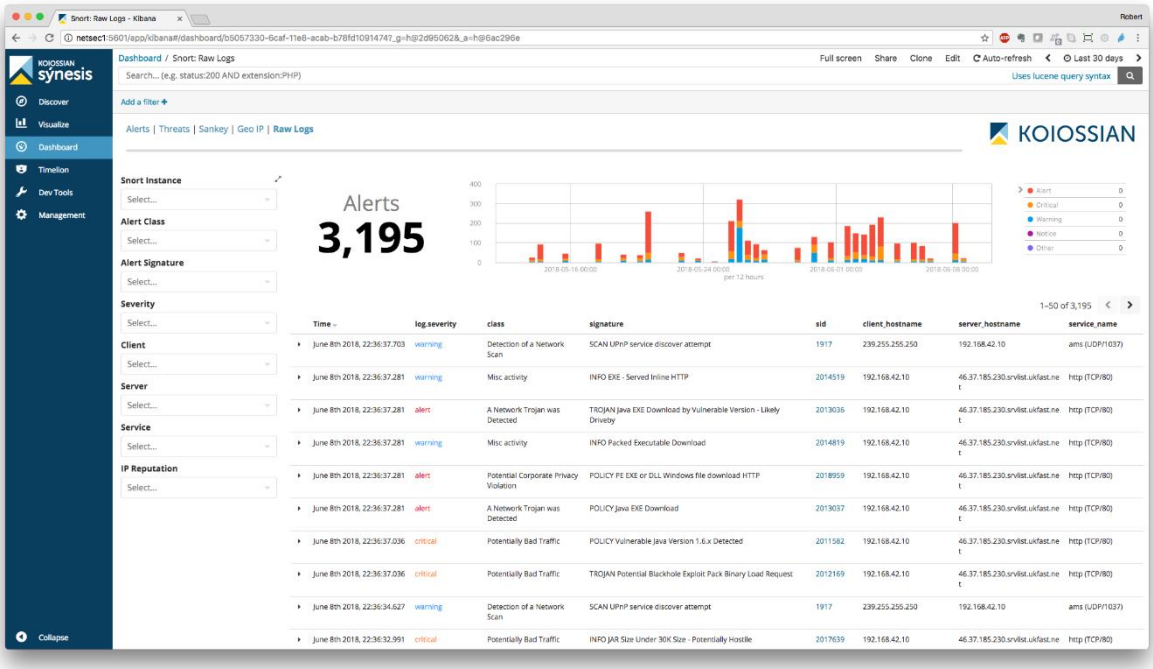
IDS-ovi mogu obavljati različite funkcije: praćenje korisnika i aktivnosti sustava, revizija konfiguracije sustava radi utvrđivanja ranjivosti i pogrešnih postavki, procjenjivanje cjelovitosti kritičnih sistemskih datoteka, prepoznavanje poznatih obrazaca napada u aktivnosti sustava, identifikacija abnormalne aktivnosti putem statističke analize, bilježenje tragova i utvrđivanje povrede politike ili odstupanja od normalne aktivnosti, ispravljanje grešaka u konfiguraciji sustava te instaliranje i upravljanje zamkama koje bilježe informacije o napadačima. (Pfleeger, Pfleeger i Margulies 2015):

Načini kojima napadač može izbjeći detekciju IDS-a[43]:

- Slanjem fragmentiranih paketa, izbjegavanjem učestalih obrazaca napada te korištenjem atipičnih mrežnih portova napadač može ostati „ispod radara“, zaobilazeći sposobnost sustava da otkrije potpis napada.
- Koordiniranim napadima niske propusnosti napadač može otežati korelaciju zabilježenih paketa.
- Lažiranjem mrežnih adresa napadač može prikriti izvor napada, najčešće iskorištavanjem loše zaštićenih ili pogrešno konfiguriranih proxy poslužitelja.

[43] What is an Intrusion Detection System?, https://www.barracuda.com/glossary/intrusion-detection-system, pristupljeno 26. kolovoza 2021.

Za razliku od IDS-ova, koji otkrivaju napade i prikazuju ih administratoru, postoje i sustavi za sprječavanje upada (eng. Intrusion Prevention System - IPS) kojima je cilj blokiranje samih napada. To su sustavi koji sadržavaju sve karakteristike IDS-ova, no uz to još imaju kapacitet odgovora na napade.



Slika 15. Nadzorna ploča IDS sustava (izvor: https://user-images.githubusercontent.com/10326954/41203874-8ae4ead0-6cdd-11e8-8962-b5c6b92d3067.png)

Slika 15. prikazuje alat Synesis koji se koristi za analizu IDS zapisa alata Snort. Nadzorna ploča alata prikazuje broj upozorenja, vrijeme incidenta, ozbiljnost prijetnje, klasu prijetnje, potpis, IP adresu klijenta i servera, vrstu servisa i slično.

9. 6. Uporaba blok-lanca u svrhu sprječavanja kartičnih prijevara

Blok-lanac ili blockchain je decentralizirana distribuirana baza podataka koja se sastoji od podatkovnih blokova povezanih u jednosmjerni lanac. Svaki novi blok poprima određena obilježja iz prethodnog i dodaje nove informacije.

Ovakav tip tehnologije doživio je svoj procvat od 2008. g. kad je nepoznati akter (ili više njih) imena Satoshi Nakamoto objavio bijelu knjigu (eng. white paper) naziva

Bitcoin: A Peer-to-Peer Electronic Cash System[44]. U tom radu autor iznosi mogućnost uporabe tzv. proof-of-work mehanizma zaštite mrežne cjelovitosti. Takav mehanizam kao dokaz koristi procesorsku brzinu uređaja koji sudjeluju u procesu rudarenja (eng. mining) kako bi spriječio izmjenu blokova od strane napadača. Rudari (eng. miners) u procesu rudarenja dobivaju šansu da osvoje nagradu koja im daje motivaciju da sudjeluju u zaštiti mreže trošeći svoje resurse. Šansa za dobivanje nagrade je proporcionalna brzini procesora da riješi kriptografsku zagonetku.

Napadač ima šansu da ugrozi mrežni konsenzus u slučaju da uspije prikupiti više od 50% procesorske brzine mreže, no takav napad na Bitcoin mrežu zahtjeva enormne resurse te je upitno bi li napadač mogao opravdati svoje ulaganje s obzirom da bi se napad mogao jako brzo prepoznati.

Uporaba blok-lanca i kriptovaluta može biti od izuzetne koristi trgovcima koji prodaju svoje proizvode putem interneta. Do pojave kriptovaluta, ustaljeni je način prihvaćanja plaćanja putem interneta bilo terećenje kreditnih kartica.

Naplaćivanje terećenjem kreditnih kartica ima brojnih nedostataka, primjerice:

- Moguća zloupotreba kreditnih kartica - u slučaju tzv. friendly fraud prijevare u kojoj vlasnik kartice od svoje banke zatraži povrat sredstava, trgovac je često prisiljen vratiti cjelokupan iznos i podmiriti naknadu posredniku koja može sezati do 15 USD[45] te utjecati na to da u budućnosti trgovac dobije nepovoljnije uvjete pri naplati zbog rizičnosti poslovanja.
- Mogući kibernetički napadi na infrastrukturu kartičnih posrednika koji mogu uzrokovati gubitak klijenta zbog nemogućnosti plaćanja usluge.

Kriptovalute rješavaju navedene probleme jer ne postoji centralizirano mjesto koje obrađuje transakcije i može postati nedostupno, niti postoji posrednik koji bi mogao osporiti transakciju i vratiti sredstva na račun platitelja.

[44] Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, pristupljeno 31. kolovoza 2021.
[45] Disputes and fraud, https://stripe.com/docs/disputes, pristupljeno 31. kolovoza 2021.

10. Zaključak

Konstantno povećanje uporabe mrežno povezanih uređaja u poslovanju, ali i kapaciteta računalnih mreža dovodi do stvaranja velike količine informacija unutar informacijskih sustava. U ekspanzijskoj stihiji informacijskih sustava, softverska, hardverska i informacijska imovina poduzeća su često ugrožene jer zaposlenici ne poznaju fundamentalna načela kibernetičke sigurnosti. Dodatne probleme stvara i natjecanje proizvođača hardvera i softvera da što prije izbace svoje proizvode na tržište, često bez ikakve revizije sigurnosti.

Ciljane, potpune i pravodobne informacije mogu predstavljati ogromnu vrijednost brojnim zlonamjernim akterima te zbog toga postoji motivacija da se na različite načine manipulira takvim informacijama. Zbog toga se organizacije svakodnevno suočavaju s prijetnjama koje tehnički evoluiraju, a na koje moraju koliko god je to moguće pokušati djelovati proaktivno (s ciljem prevencije sigurnosnog incidenta), a samo u slučaju nepredviđenih okolnosti reaktivno (nakon incidenta).

Praćenje objava o prijetnjama i ranjivostima na mrežnim stranicama CERT-ova, kao i instalacija sigurnosnog softvera te redovita nadogradnja aplikacija, operacijskog sustava i upravljačkih programa uvelike pridonose smanjivanju mogućnosti inficiranja uređaja zlonamjernim softverom. Vrlo je važno educirati zaposlenike o načinima kojima trebaju upravljati povjerljivim podacima kako klijenata, tako i samog poduzeća. Zaposlenici bi trebali otvarati samo internetske poveznice u čiju se autentičnost mogu uvjeriti, koristiti složenije lozinke gdje god je to moguće i uzimati sve informacije sa dozom opreza te evaluiraju njihovu vjerodostojnost polazeći od pretpostavke da su lažne.

Ograničeni budžeti predviđeni za kibernetičku zaštitu i zavaravanje da će prijetnje same od sebe zaobići organizaciju su obično glavni razlozi sve češćih proboja poslovnih podataka. Mala i srednja poduzeća bi, ukoliko se samostalno nisu u stanju nositi s kompliciranim kibernetičkim zadacima, trebala angažirati vanjske suradnike s ciljem djelovanja na takve zadatke.

Pred stručnjake se nameće mnoštvo izazova glede identifikacije raspoloživih resursa, ranjivosti i prijetnji te pravovremene procjene sigurnosnih rizika, a krajnji cilj toga je uspostava okvira u kojem su osigurane hardverske i softverske komponente, ali i povjerljivost, cjelovitost i dostupnost informacijske imovine.

Sažetak

Cilj ovog završnog rada je upoznavanje čitatelja s aspektima kibernetičke sigurnosti iz perspektive malih i srednjih poduzeća. Čitatelji će naučiti o tijelu koje je u Hrvatskoj zaduženo za promicanje mjera kibernetičke sigurnosti, resursima koje je potrebno štititi i ranjivostima koje mogu narušiti sigurnost i stabilnost poslovnog informacijskog sustava. Navedeni su motivi i vrste napadača, kao i pripadajući primjeri. Nadalje, opisani su vektori napada (phishing, smishing, vishing, napadi na lozinke i drive-by preuzimanja) preko kojih napadači obično izvode svoje napade. U praktičnom dijelu rada je prikazan način kojim napadači mogu izvesti smishing, vishing i napade na lozinke. Definiran je pojam zlonamjernog softvera, kao i najčešći oblici poput računalnih virusa, računalnih crva, zlonamjernog softvera koji napada uređaje interneta stvari, oglašivačkog softvera, ucjenjivačkog softvera, zastrašivačkog softvera i alata za daljinsko upravljanje. Spomenuti su načini pomoću kojih se poduzeća mogu zaštititi od napada i gubitka podataka, primjerice uporabom višestruke autentifikacije, redovitom izradom sigurnosnih kopija podataka, uporabom antimalware softvera, sigurnosne stijene (vatrozida) i sandbox softvera. Također, opisano je funkcioniranje sustava za otkrivanje i sprječavanje upada, kao i moguća primjena blok-lanca u svrhu sprječavanja kartičnih prijevara.

Summary

The goal of this undergraduate thesis is to familiarize the readers with the concepts of cybersecurity from the perspective of small and medium enterprises. The readers will learn about the body in charge of coordinating cybersecurity measures in Croatia, about the resources which need to be protected and the vulnerabilities which can disrupt the security and stability of the business information system. The motives and types of attackers are listed, as well as the accompanying examples. Furthermore, attack vectors (phishing, smishing, vishing, password attacks and drive-by downloads) through which attackers typically carry out their attacks are described. The practical part of the thesis shows how attackers can perform smishing, vishing and password attacks. The term malware is defined, as well as the most common forms such as computer viruses, computer worms, IoT malware, adware, ransomware, scareware and remote administration tools. Mention is made of ways in which businesses can protect themselves from attacks and data loss, for example by using multi-factor authentication, by making regular data backups, by using antimalware software, firewall and sandbox software. Also, the functioning of the intrusion detection and prevention system is described, as well as the possible application of a blockchain for the purpose of preventing card fraud.

Popis literature

Centar informacijske sigurnosti. 2011. *Advanced Persistent Threat napadi.* 19. prosinac. Pokušaj pristupa 8. kolovoz 2021. https://www.cis.hr/dokumenti/2988-advanced-persistent-threat-napadi.html.

Ministarstvo unutarnjih poslova Republike Hrvatske. 2018. *Ugašen najveći svjetski internetski servis za DDoS napade.* 25. travanj. Pokušaj pristupa 8. kolovoz 2021. https://mup.gov.hr/vijesti-8/ugasen-najveci-svjetski-internetski-servis-za-ddos-napade/276949.

Pfleeger, Charles P., Shari Lawrence Pfleeger, i Jonathan Margulies. 2015. *Security in Computing, 5th ed.* Prentice Hall.

Putman, C.G.J., Abhishta, i Lambert J.M. Nieuwenhuis. 2018. »Business Model of a Botnet.« 2.

Wikipedia. 2021. *Hacktivism.* srpanj. 16. Pokušaj pristupa 10. kolovoz 2021. https://en.wikipedia.org/wiki/Hacktivism.

—. 2021. *Information security.* 12. kolovoz. Pokušaj pristupa 17. kolovoz 2021. https://en.wikipedia.org/wiki/Information_security.

—. 2021. *Insider threat.* 15. srpanj. Pokušaj pristupa 10. kolovoz 2021. https://en.wikipedia.org/wiki/Insider_threat.

—. 2021. *Malware.* 18. kolovoz. Pokušaj pristupa 21. kolovoz 2021. https://en.wikipedia.org/wiki/Malware.

Popis slika