ANALIZA SIGURNOSTI BANAKA PREMA JAVNO DOSTUPNIM PODACIMA

Matvej, Ena

VISOKO UČILIŠTE ALGEBRA

DIPLOMSKI RAD

ANALIZA SIGURNOSTI BANAKA PREMA JAVNO DOSTUPNIM PODACIMA

Ena Matvej

Zagreb, travanj 2020.

„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 koristila sam tuđe materijale navedene u popisu literature, ali nisam kopirala niti jedan njihov dio, osim citata za koje sam navela autora i izvor, te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spremna sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada“.

U Zagrebu, travanj 2020.

Predgovor

Iskreno zahvaljujem svom mentoru, Zlatanu Moriću, pred. na njegovom vemenu, podršci, razumijevanju i pomoći prilikom izrade ovog rada.

Zahvaljujem i svim profesorima Visokog Učilišta Algebra koji su sudjelovali u mojem obrazovanju na stečenom znanju i velikom strpljenju. Hvala svima na ukazanoj spremnosti pomoći u bilo koje doba dana, na brzim odgovorima te iznimnoj stručnosti. Također zahvaljujem svim djelatnicima, predavačima i asistentima što su učinili studiranje pozitivnim iskustvom.

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

Sažetak

Uz pretpostavku da nijedan sustav nije savršen, a pogotovo uzevši u obzir faktor ljudske pogreške, postoji velika vjerojatnost da zaposlenici banaka predstavljaju značajan potencijalni sigurnosni incident koji ne treba zanemariti.

U radu će biti analizirano koliko je informacija koje predstavljaju određen rizik za sustav moguće prikupiti o bankama preko interneta na javno dostupnim mjestima.

Ključne riječi: sigurnost banaka, prikupljanje podataka, povjerljivost podataka, OSINT, Maltego, Spiderfoot

Abstract

Assuming no system is perfect, especially given the factor of human error, there is a great possibility that bank employees represent vast potential security incident which must not be neglected.

In this thesis, it will be analyzed how many information, that present certain risk to banks, is possible to gather on the Internet.

Key words: bank security, reconnaissance, data confidentiality, OSINT, Maltego, Spiderfoot

Sadržaj

1. Uvod

Svatko od nas ima barem neke osobne podatke na internetu. Danas je to neminovno. Rijetko tko nema profil na nekoj od društvenih mreža ili drugoj platformi. Potencijalni problemi nastaju jer korisnici zaboravljaju koliko su informacije koje dijele, čak i one naizgled bezopasne, zapravo inkriminirajuće i iskoristive protiv njih ili protiv tvrtke za koju rade. Obična fotografija sa psom u šetnji gdje je u opisu napisano ime psa može predstavljati sigurnosni propust jer je često pitanje za oporavak zaporke ime kućnog ljubimca.

Banke imaju mnogo zaposlenika s različitim pravima pristupa. Velika je vjerojatnost da aktivnosti njihovih zaposlenika na internetu (društvene mreže, streaming kanali, blogovi) na neki način ugrožavaju njihove poslovne korisničke račune koje bi potencijalni napadači mogli iskoristiti za jednostavan ulazak u sustav banke. Također postoji mogućnost da djelatnici sami u slobodno vrijeme na internetu aktivno sudjeluju u zajednicama koje imaju veze s onime čime se na poslu bave. Na taj se način mogu izvući informacije o sustavu banke.

U radu ću prikupiti sve informacije do kojih je moguće legalno doći, koristeći automatizirane alate Maltego i Spiderfoot. Ručno ću pretraživati zaposlenike po društvenim mrežama LinkedInu, Facebooku i Twitteru te ću ručno pretraživati podatke o bankama pomoću tražilice Shodan. U online arhivi ću proći sve web stranice banaka kako bi pronašla neke starije informacije koje bi danas eventualno predstavljale sigurnosnu ugrozu. Opisivat ću na koji način su podaci prikupljeni te će u svakom trenu postupak moći biti ponovljiv.

2. OSINT

Open source intelligence ili OSINT je način prikupljanja podataka s javno dostupnih mjesta. To je pojam za bilo koju informaciju koja je prikupljena iz novina, članaka na internetu, knjiga, društvenih mreža, blogova i slično.

Prema NATO Open Source Intelligence Handbook V1.2 priručniku iz 2001. godine, postoje 4 kategorije podataka.

1. Podaci iz otvorenih izvora (*open source data*): neobrađeni podaci koji dolaze iz primarnih izvora kao što su meta podaci iz telefonskih poziva, satelitske snimke, ankete, podaci s radija i televizije. Takvi podaci imaju malu informativnu vrijednost.
2. Informacije iz otvorenih izvora (*open source information (*OSINF*)):* podaci koji su prošli kroz određena filtriranja i kategorizacije ovisno o potrebama za što su informacije potrebne. Primjeri OSINF-a su knjige, članci, disertacije na određenu temu. Razlika između OSINF-a od ostalih tipova javno dostupnih informacija je da bi ih bilo moguće prikupiti, potrebno ih je platiti, imati dozvolu ili treba naručiti informacije koje se žele prikupiti.
3. OSINT: to su informacije koje imaju informativnu vrijednost. Takve su informacije odmah spremne jer su prošle kroz filtriranje.
4. Potvrđene informacije (OSINT-V): takve informacije su pouzdanije i preciznije jer su potvrđene i iz drugih izvora koji nisu samo OSINT. Primjer OSINT-V informacija su televizijske vijesti kombinirane s informacijama dobivanim iz satelita.

Tu je moguće vidjeti da prva i druga kategorija spadaju u glavne (primarne i sekundarne) izvore podataka, a OSINT ih kombinira kako bi postigao željeni rezultat.

OSINT-om se najviše služe vlade, policijske službe, sigurnosne agencije, poslovne organizacije, kriminalci i hakeri te korisnici koji žele privatnost. Korištenje OSINT-a je vrlo jeftino, uglavnom zahtjeva samo internetsku konekciju, nizak je rizik da meta sazna da ju se istražuje, a za prikupljanje podataka ne treba ured te je moguće pretraživati s bilo koje točke na zemlji. Također, takvo prikupljanje podataka ne krši autorska prava jer je sve javno objavljeno.

Iako je OSINT odličan za prikupljanje informacija o meti, kao i ostale metode, ima svoje nedostatke. Prikupljanje informacija preko OSINT-a će dati velike količine podataka. Iako postoje alati koji mogu filtrirati dobivene podatke, to i dalje mogu biti enormne količine podataka gdje se javlja problem razlučivanja što je bitno, a što nije pa bitne informacije mogu lako biti previđene. OSINT alati, također, ne razlikuju istinite od zavaravajućih podataka nego samo serviraju sve podatke do kojih dođu pa bi svi OSINT-ovi izvori trebali biti verificirani. Ta oba problema iziskuju ljudski trud kako bi se eliminirali ili ublažili. Ručno bi se trebali verificirati svi izvori kako bi se razlučile istinite informacije koje treba filtrirati od onih nebitnih.[1]

OSINT je dostupan svima, njime se služe vlade za prevencije napada, smanjenje ugroza, ali se njime služe i neetičke stranke. Tu se pojavljuje dilema oko etičnosti korištenja dostupnih informacija. Trebaju li se takve informacije tretirati kao javno dostupni materijal koji može biti slobodno citiran ili trebaju postojati neke restrikcije kod korištenja osobnih podataka? Autori Layton i Watters smatraju da bi podaci, iako su tehnički dostupni široj javnosti, svejedno trebali biti etički tretirani što znači i da se svi podaci uzeti s društvenih mreža i foruma moraju uzeti doslovno, bez vađenja iz konteksta.[2]

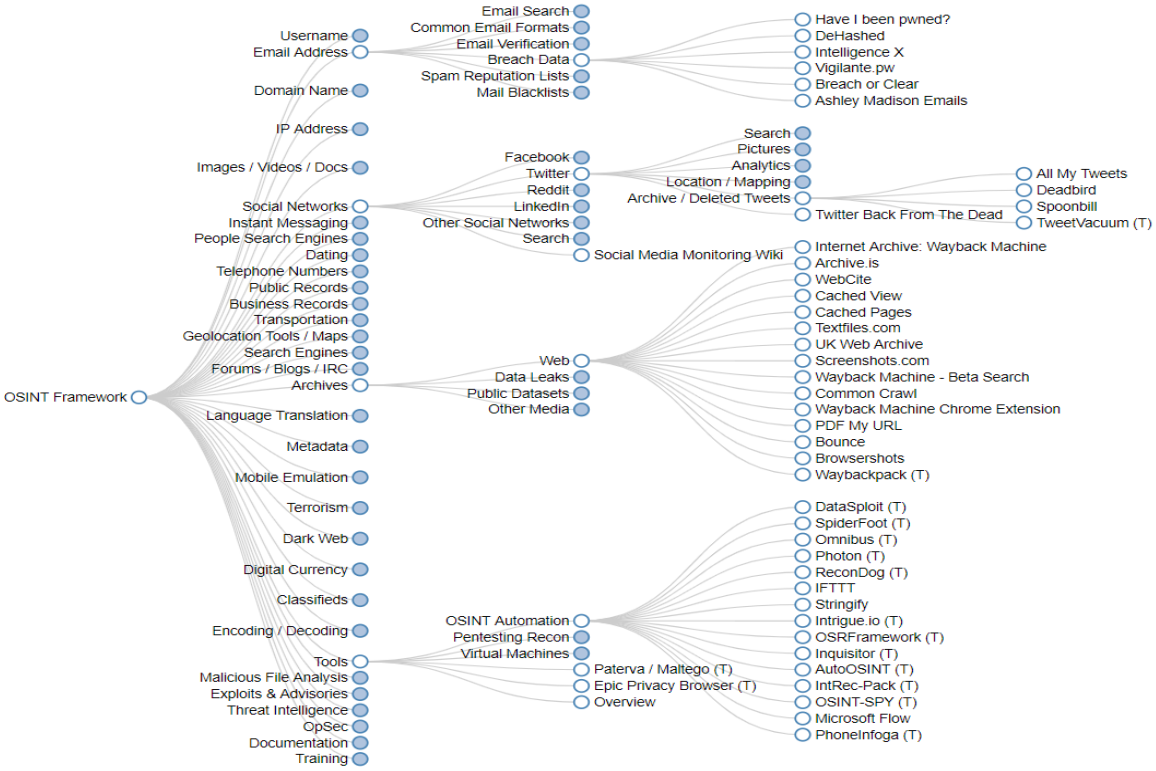
Nije ilegalno pročitati informaciju koja leži na javno dostupnom mjestu, ali nije etično ako je to nečija lozinka. Problem nastaje ako se te informacije iskoriste u neetične i ilegalne svrhe. To čini OSINT prilično moćnim alatom. Dakle, samo ako su neki podaci javno dostupni, ne znači nužno da mogu slobodno biti i korišteni u svrhe koje onaj tko ih je objavio ili kome pripadaju ne želi da budu korištene.[3]

2016. godine sastavljena je lista OSINT *framework* s alatima za prikupljanje podataka, od email adresa, korisničkih imena, do *exploita*. Na tom se popisu mogu pronaći mnogi alati koji olakšavaju cijeli proces prikupljanja podatak, a neki odo njih su korišteni i u ovome radu.

[1] Hassan, N. A.: Digital Forensics Basics. Berkley: Apress, 2019.

[2] Layton, R., Watters, P. A.: Automating Open Source Intelligence: Algorithms for OSINT, Amsterdam: Elsevier Science, 2015.

[3] Eysenbach, G., Till, J. E.: Ethical Issues In Qualitative Research On Internet Communities. BMJ (Clinical Research Ed.), 323(7321), (2001), 1103–1105.



Slika 2.1 OSINT *framework*[4]

Tehnike za prikupljanje podataka mogu se podijeliti na dvije vrste: aplikacijski priključci (API) i web pauci (engl. *web crawlers*). Aplikacijski priključci su servisi koji daju pristup ugrađenim funkcionalnostima online platforma. Ponekad je za pretragu potrebna autentikacija ili je usluga ograničena po određenom broju podataka. Ograničenja aplikacijskih priključaka mogu navesti korisnike okretanju web paucima. Web pauci su dijelovi softwarea koji kruže po predefiniranim web stranicama i prikupljaju njihov izvorni kod (engl. *source code*). Taj izvorni kod se onda raščlanjuje, a prikupljeni podaci se pohranjuju u baze.[5] Koriste se u slučajevima kada bi ručna pretraga trajala predugo i zahtijevala bi previše ljudskih resursa i trebalo bi prolaziti kompletnu web stranicu, prelazeći s jedne podstranice na drugu i vaditi sve podatke. Web pauzi automatiziraju takav proces.[6]

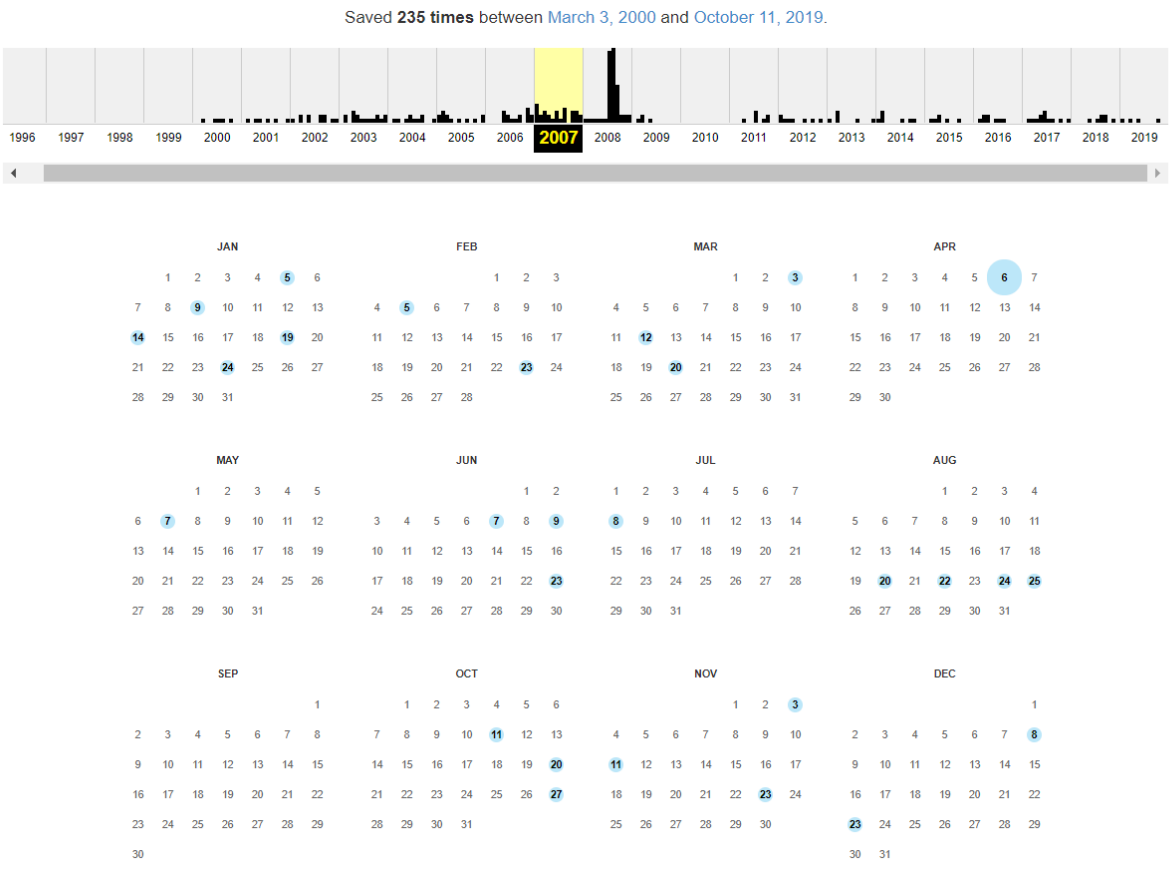
[4] https://osintframework.com/
[5] Layton, R., Watters, P. A.: Automating Open Source Intelligence: Algorithms for OSINT, Amsterdam: Elsevier Science, 2015.
[6] Akhgar, B, Bayerl, P. S., Sampson, F.: Open Source Intelligence Investigation: From Strategy to Implementation, Švicarska: Springer, 2016.

Alati Wayback Machine, Spiderfoot i Shodan koji se koriste u ovome radi spadaju u web pauke, a Maltego radi na principu aplikacijskih ključeva.

2.1. Archive.org

https://archive.org/ je online knjižnica u kojoj se mogu naći milijuni web stranica, knjiga, glazbe, filmova i sličnih sadržaja. Knjižnica pohranjuje web stranice te ih je moguće pregledavati u njihovim starijim izdanjima ukoliko su ikada bile spremljene u online arhivu. Pomoću alata *Wayback Machine* koji je integriran u archive.org, moguće je pregledavati stranice kako su davno prije izgledale jer arhiva sadrži *snapshote* koji su stari preko 20 godina. Kako se nekada nije pazilo na sigurnost od napadača preko interneta kao danas, postoji mogućnost da su banke objavljivale u prošlosti više informacija nego što objavljuju danas.

U online arhivi moguće je pronaći stari izgled web stranica banaka, novosti koje su tada bile aktualne, tadašnje tečajne liste te oglase za posao na koje ću se najviše fokusirati te kroz njih pokušati pronaći više informacija o bankovnim sustavima i kakve točno stručnjake banke traže.



Slika 2.2 Archive.org

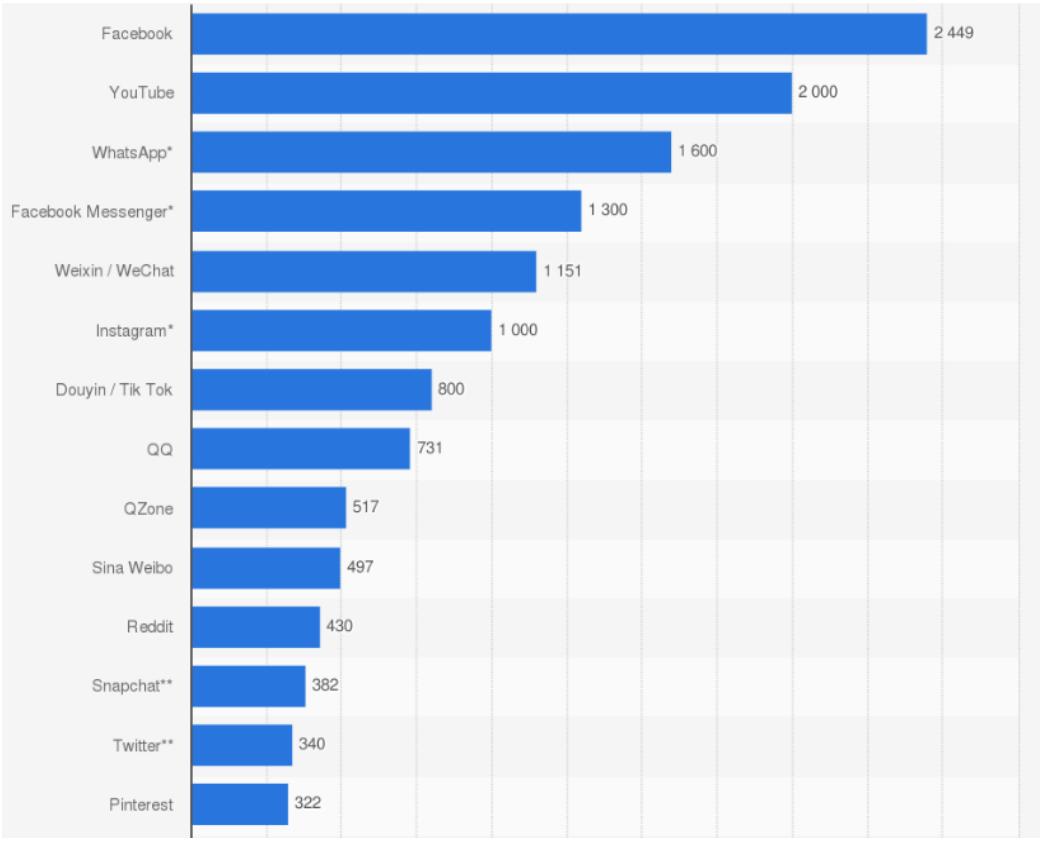
Način na koji su podaci prikupljeni kroz archive.org za ovaj rad je tako da je svaka banka pretražena u arhivi i zatim sam ručno posjetila većinu točaka (engl. *snapshots*) kako bi pronašla korisne informacije koje bi mogle predstavljati sigurnosni problem ili ako sam naišla na imena zaposlenika, na primjer na stranici za kontakt ili osobu kojoj se javiti za zaposlenje ili voditelja nekog odjela, popisala bih osobe za buduća pretraživanja i provlačenja kroz daljnje alate.

2.2. Društvene mreže

U ovom današnjem digitalnom dobu teško je sresti osobu koja je povezana s internetom, a nema račun na barem jednoj društvenoj platformi. Društvena platforma je širi pojam koji obuhvaća tipove platformi koji se razlikuju po svojoj funkciji. Društvene mreže služe za povezivanje s drugim ljudima i dijeljenje informacija i ideja. Najpoznatiji primjeri su Facebook i LinkedIn. Postoje platforme samo za dijeljenje fotografija (Instagram) ili samo za dijeljenje videa (YouTube). Blogovi (Wordpress), mikroblogovi (Twitter) i forumi, od kojih je danas najpoznatiji

Reddit su više tekstualno orijentirani. Također još razlikujemo i platforme za društvene oznake (engl. *social bookmarking*) poput Pinteresta.[7]

Najzastupljenija platforma je Facebook sa skoro dvije milijarde i petsto milijuna korisnika. Druga platforma po popularnosti je YouTube s dvije milijarde korisnika.



Slika 2.3 Najpopularnije društvene platforme u siječnju 2020.[8]

To otvara brojne mogućnosti za prikupljanje podataka zbog velike količine osobnih informacija koje korisnici na platformama dijele. Naprimjer, na Facebooku se mogu pronaći lokacije koje je pretraživana osoba posjetila, politička stajališta koja zastupa, gdje radi, tko su mu/joj kolege s posla, kojim se hobijima bavi i slično. Facebook se često koristi za prijavljivanje na druge stranice kako se ne bi morao otvarati novi korisnički račun. Ukoliko se netko domogne lozinke od Facebook računa, tad mu se ostvaruje pristup i na mnogo drugih stranica u ime žrtve.

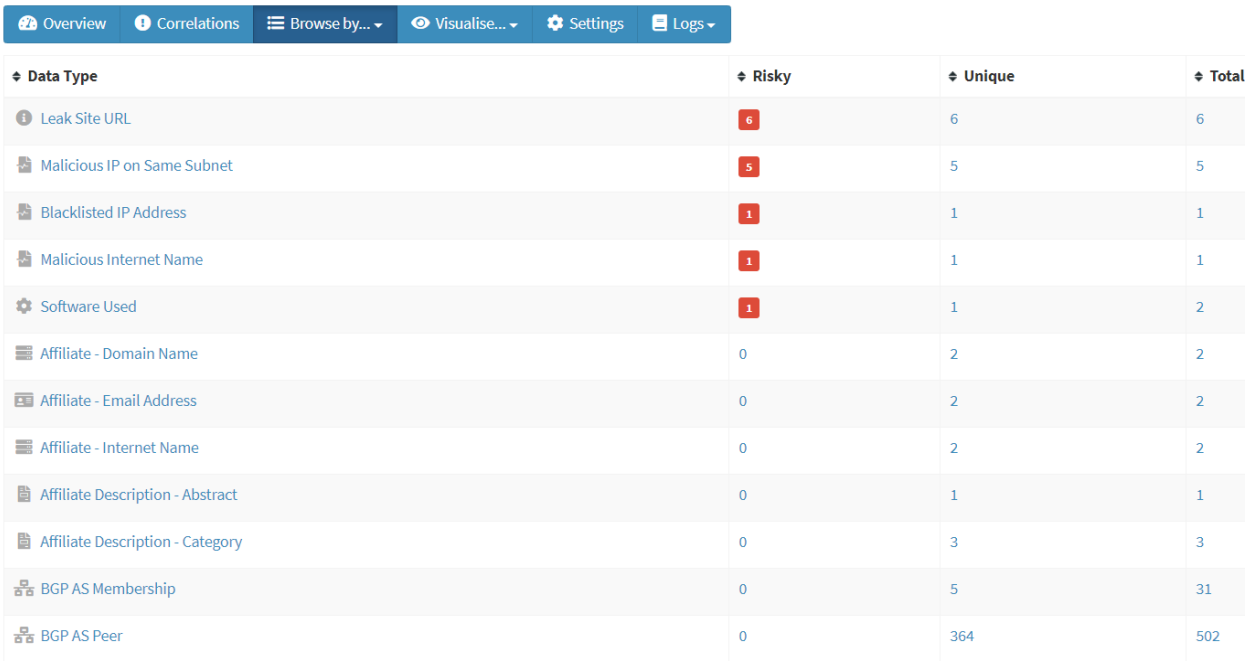
[7] Hassan, N. A., Hijazi, R.: Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence: Berkley: Apress, 2018.
[8] https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ preuzeto 8. ožujka 2020.

Pregledavajući web stranice banaka naišla sam na neka imena zaposlenika koje je vrijedno istražiti za bilo kakve dodatne informacije. Zaposlenike banaka sam tražila na mreži LinkedIn pa sam ih detaljnije istraživala preko Googla, Facebooka, Twittera i Maltega kako bih pronašla kakve postove objavljuju i kakav sadržaj dijele. Upravo su njihove objave upućivale na ono čime se na svom poslu bave i time dali uvid u sustav banke za koju rade. Također sam otvorila LinkedIn profil ciljano za svaku banku kako bi mi LinkedInov algoritam predložio „kolege“. Na taj način sam našla dosta zaposlenika koji se bave ciljano održavanjem sustava te sam ih mogla provlačiti kroz daljnje alate za automatizirano pretraživanje koji su navedeni i opisani niže.

2.3. Spiderfoot

Spiderfoot je jedan od automatskih alata koji spadaju pod OSINT. Otvaranjem besplatnog računa na Spiderfootu i pokretanjem jednostavnih pretraga unoseći web stranicu u Spiderfootovu tražilicu, alat je u dvadesetak minuta prikupio dovoljno interesantnih podataka koje je čak i sortirao po kritičnosti sigurnosnog rizika.

Spiderfoot inteligentno pretražuje sva dostupna mjesta i tražitelju informacija ih servira po vrsti podataka koje je pronašao. Unoseći web stranicu u tražilicu Spiderfoota, moguće je dobiti rezultate o IP adresi stranice, mail adresama povezanim s tom domenom, jesu li procurile lozinke od korisničkih računa povezanih s nađenim mail adresama, brojeve telefona, fizičke adrese, otvorene portove na web serveru, operativni sustav servera iza web stranice i mnoge druge informacije.

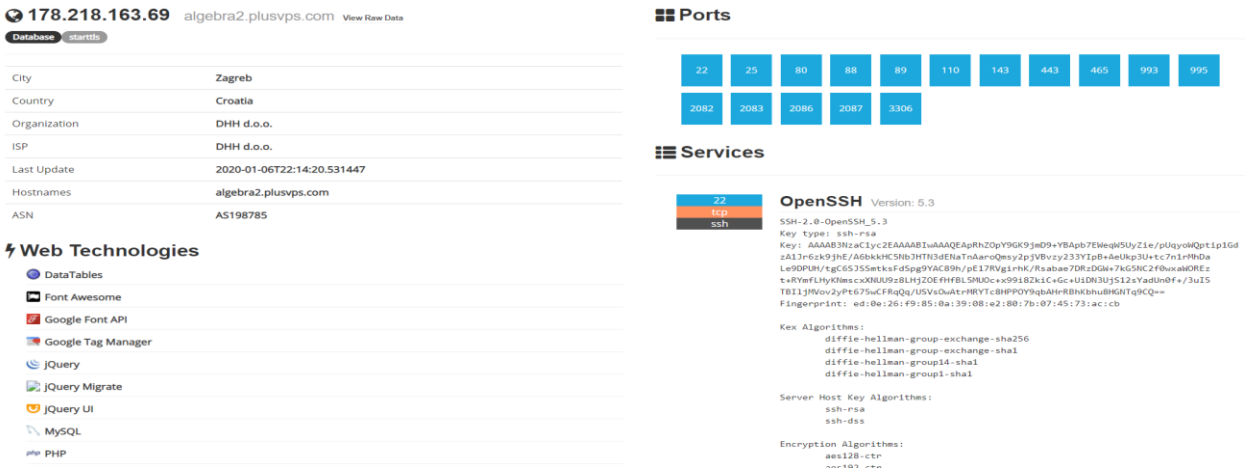


Data Type	Risky	Unique	Total
Leak Site URL	6	6	6
Malicious IP on Same Subnet	5	5	5
Blacklisted IP Address	1	1	1
Malicious Internet Name	1	1	1
Software Used	1	1	2
Affiliate - Domain Name	0	2	2
Affiliate - Email Address	0	2	2
Affiliate - Internet Name	0	2	2
Affiliate Description - Abstract	0	1	1
Affiliate Description - Category	0	3	3
BGP AS Membership	0	5	31
BGP AS Peer	0	364	502

Slika 2.4 Pronađeni podaci u Spiderfootu sortirani po tipu podatka

2.4. Shodan

Shodan je tražilica koja pretražuje baš poput Googlea, no za razliku od Googlea, Shodan pretražuje i neindeksirane elemente interneta.

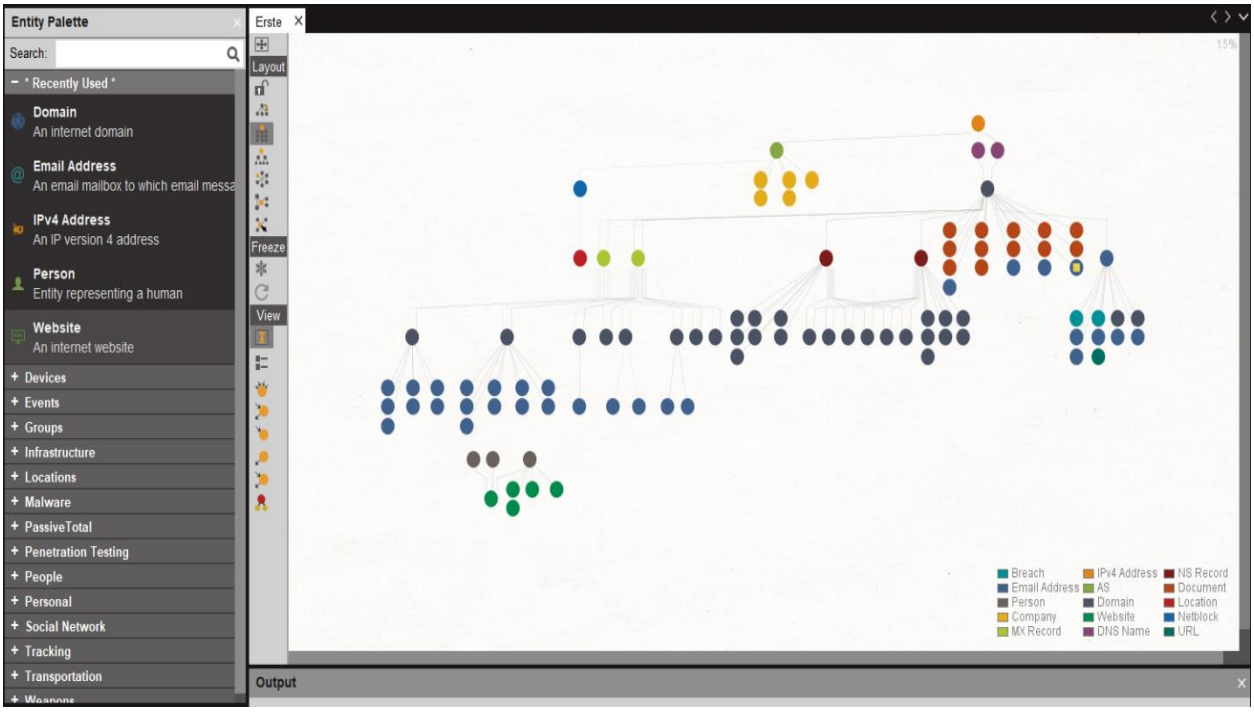


Slika 2.5 Rezultati pretrage u Shodanu

Unošenjem samo IP adrese u tražilicu, Shodan otkriva i imenuje web tehnologije korištene na stranici, lokaciju, otvorene portove i ostale ranjivosti koje pronađe.

2.5. Maltego

Maltego je još jedan OSINT automatizirani alat za pretragu kojemu se kao ulazni podatak može dati bilo koja vrijednost. Može se pretraživati po imenu i prezimenu, broju telefona, domeni, IP adresi, nazivu kompanije, ulici, tipu vozila, identifikacijskom broju i mnogim drugim vrstama podataka. Maltego zna razlikovati te podatke i može pametno pretraživati baze podataka da iskopa čim više informacija o traženim podacima. Sam alat se može i nadograditi sa što besplatnim, a što plaćenim nadogradnjama kako bi alat imao pristup dodatnim bazama podataka i mogao preciznije tražiti određene podatke. Zbog toga je neizostavan alat za penetracijske testere, ali i za sve koji žele bolje istražiti svoju metu.[9]



Slika 2.6 Maltego

[9] Chauhan S., Panda N. K.: Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques, Massachusetts: Syngress, 2015.

3. Banke

Odabrano je deset hrvatskih banaka o kojima ću izvući čim više podataka te pokušati pronaći informacije o njihovim sustavima koje bi potencijalni napadači iskoristili protiv njih.

3.1. Erste&Steiermärkische Bank

Erste banka ima 151 poslovnicu[10] diljem Hrvatske i 3.274 zaposlenika po financijskom izvješću[11] iz 2019. godine.

Pregledavajući oglase za posao, moguće je naići na informacije kakve stručnjake Erste banka traži. 20. lipnja 2006. godine u oglasu za posao navedeno je da se traži osoba za rad na „vrhunskim platformama (Windows, mainframe, Unisys i IBM)“.

Na LinkedInu je moguće pronaći dosta zaposlenika iz Erste banke, najviše iz područja ekonomije i financija. Iz područja informatike malo zaposlenika je imalo korisne informacije o tome što rade. Erste banka očito ima jedan odjel Unix, Network and Storage jer na LinkedInu postoji bivši zaposlenik koji je naveo da je bio voditelj upravo tog odjela.[12] Drugi zaposlenik to samo potvrđuje navodeći da je bio Linux, Unix i SAN storage administrator još dok je radio u Erste banci.[13]

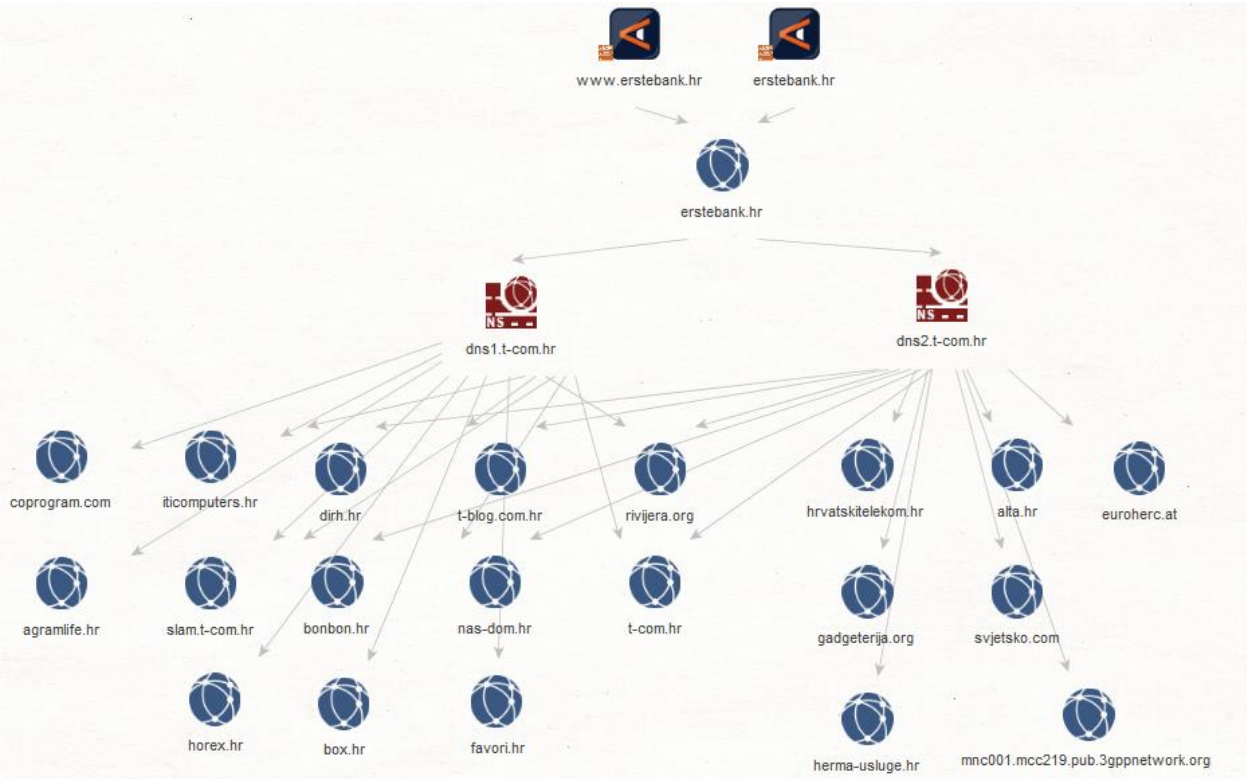
Koristeći Spiderfoot vidi se da se web stranica banke nalazi na adresi 213.150.2.79 te da je iza toga Apache server. Također izbacuje da se koristi aplikacija Adobe Illustrator CC 23.0 i to na Machintoshu i Adobe InDesign CC 13.0 na Windowsu.

Shodan je izvukao više različitih web tehnologija na njihovoj web stranici.

[10] https://www.erstebank.hr/hr/o-nama/grupacija
[11] https://www.erstebank.hr/hr/o-nama/financijska-izvjesca
[12] https://www.linkedin.com/in/ivanknezovic/
[13] https://www.linkedin.com/in/antonio-smoljo-41375310a

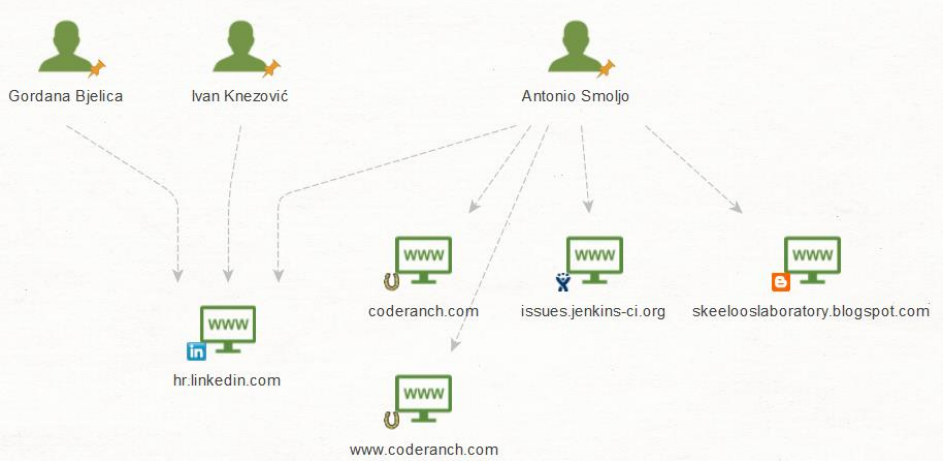
Slika 3.1 Web tehnologije Erste banke

Pomoću Maltega, može se dobiti neki uvid u strukturu web servera. Vidljivo je da se domena nalazi na dva dijeljena T-Comova *name* servera DNS1 i DNS2 na kojima se nalaze i druge domene.



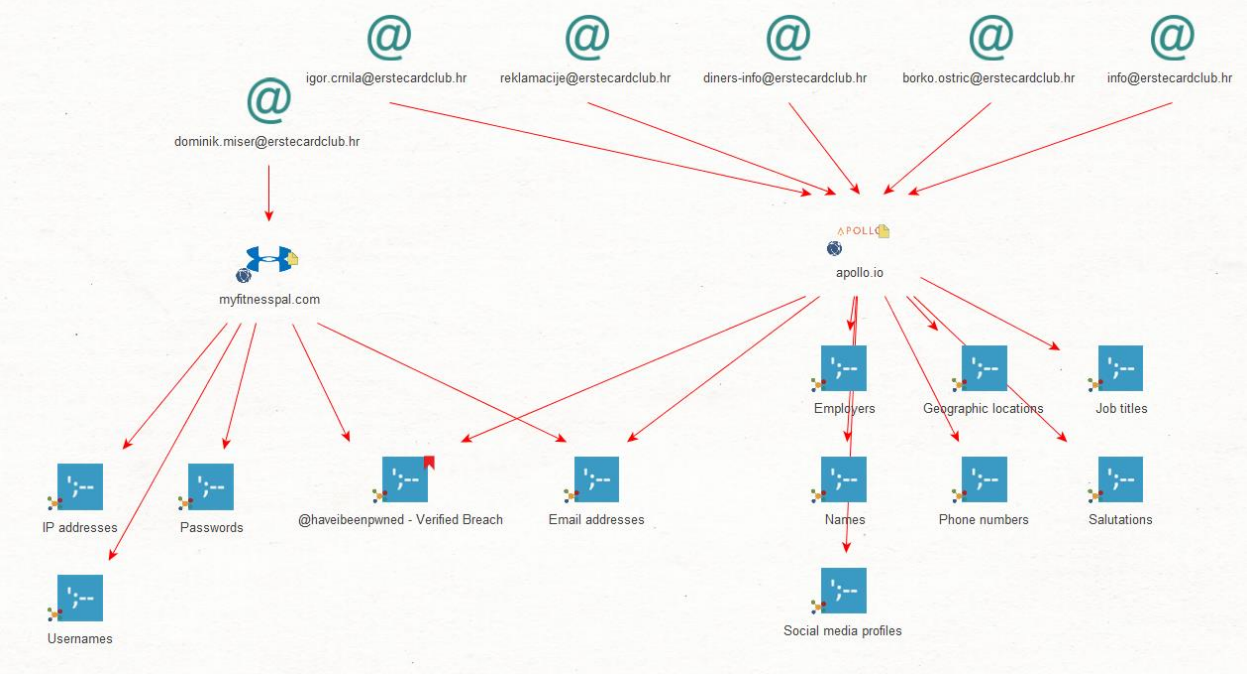
Slika 3.2 Domena erstebank.hr

Nakon pregledavanja koje je podatke sve moguće prikupiti o web stranici banke, pretražila sam i zaposlenike na čija sam imena dosad naišla. Dok pretraga najčešće odvede na društvene mreže, jednog je od bivših zaposlenika uspjela povezati s pitanjima na forumima gdje se informirao o WebSphere Application serveru.



Slika 3.3 Zaposlenici i rezultati pretrage

Također je kompromitirano nekoliko mail adresa zaposlenika.



Slika 3.4 Kompromitirane mail adrese zaposlenika Erste banke

3.2. Hrvatska poštanska banka

Po financijskom izvještaju iz 2018. godine Hrvatska poštanska banka ima 1.118 zaposlenih i 9 regionalnih centara, 48 poslovnica i ispostava te više od 1.000 poštanskih ureda raspoređenih na cijelom teritoriju Republike Hrvatske.[14]

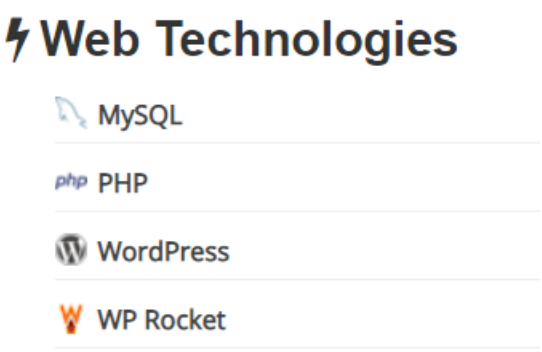
HPB je u oglasima za posao precizirao da traže iskusne osobe u radu s Linux/Unix operativnim sustavima i da je prednost „poznavanje Red Hat, HP-UX i Solaris operativnih sustava, enterprise diskovnih sustava Hitachi, IBM WebSphere, Tomcat, VMware, backup sustava Commvault".

Na društvenim mrežama ima malo zaposlenika i ni jedan zaposlenik iz IT-a nema navedeno čime se konkretno bavi, no jedan je zaposlenik[15] prešao iz Erste banke u HPB, a vidljivo je da je u Erste banci radio kao Linux, Unix i SAN *storage* administrator, tako da je zaposlen najvjerojatnije zbog tih znanja i vještina što bi značilo da ih primjenjuje i na novom poslu što se i podudara s profilom osoba kakve traže u oglasima za posao.

Web stranica banke nalazi se na adresi 52.232.62.160, a Spiderfoot je otkrio i da koristi Nginx server. Mnogo zaposlenika koristi nesigurne lozinke sačinjene samo od malih slova koje su procurile u baze podataka te su njihovi korisnički računi ugroženi. Spiderfoot je otkrio i da HPB koristi aplikaciju Acrobat Distiller 15.0 za Windowse.

[14] https://www.hpb.hr/wp-content/uploads/2019/03/HPB-Godi%C5%A1nje-izvje%C5%A1%C4%87e-2018.pdf
[15] https://www.linkedin.com/in/antonio-smoljo-41375310a/

Slika 3.5 Ugroženi računi i njihove lozinke

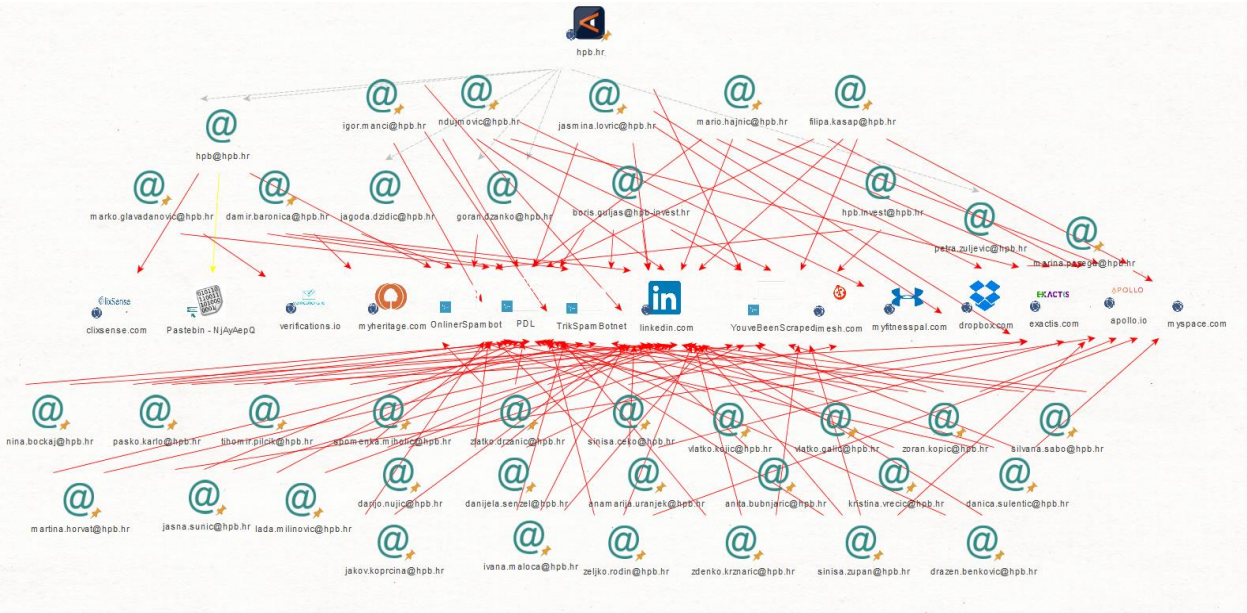


Slika 3.6 Web tehnologije HPB banke

Maltego je otkrio da se domena hpb.hr nalazi na 2 njihova web servera i na jednom dijeljenom T-Comovom serveru. Kako se i Erste, PBZ i Poba nalaze na T-Comovim serverima, a Spiderfoot je našao da se oni nalaze na Apache serveru, a HPB na Nginx serveru, sustavom eliminacije možemo zaključiti da su T-Com serveri Apache, a HPB web server je Nginx.

Maltego je izlistao sve mail adrese koje je uspio pronaći. Uspoređivanjem tih mail adresa s onima u arhivi mail adresa koje su procurile, Maltego je pronašao adrese koje su nesigurne jer su procurile lozinke, osobni podaci, telefonski brojevi i slične informacije. U tu pretragu su još dodane mail

adrese koje je pronašao Spiderfoot. Hrvatska poštanska banka ima daleko najviše kompromitiranih mail adresa zaposlenika od drugih banaka. To ukazuje na lošu educiranost zaposlenika koji poslovnu mail adresu koriste u privatne svrhe te da otvaraju sumnjive mailove i linkove. Od 63 mail adrese koje su automatizirani alati uspjeli pronaći, čak 39 mail adrese su kompromitirane.



Slika 3.7 Baze podataka u kojima se nalaze pronađene mail adrese

3.3. Privredna banka Zagreb

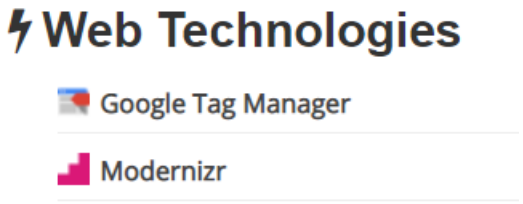
Prema podacima iz financijskog izvještaja iz 2019. godine, banka zapošljava 3.395 zaposlenika[16], ima oko 200 poslovnica.[17]

U oglasima za posao moguće je pronaći da banka traže „poznavanje UNIX ili Linux operacijskih sustava“ te „izvrsno poznavanje IBM AIX i/ili Linux operacijskih sustava“ kao i „iskustvo s aplikacijskim poslužiteljima (WAS, Tomcat, JBoss)“.

Pretražujući društvene mreže vidljivo je da nema mnogo IT zaposlenika otvorene profile ili barem ne navode svoj sektor. Jedan zaposlenik[18] ima navedene svoje specijalnosti na profilu, a to su Windows Vista, Windows XP i Windows 7. Moguće je zaključiti da PBZ koristi ta tri operativna sustava.

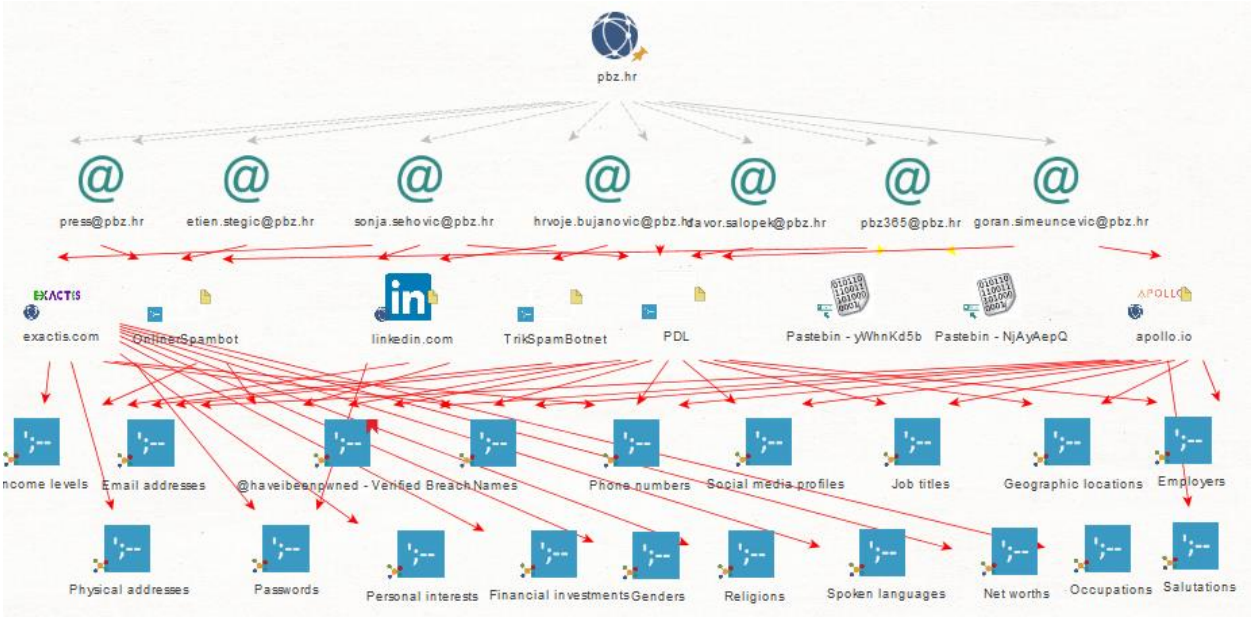
[16] https://www.pbz.hr/document/documents/PBZ/financijska-izvjesca/2019_godisnje/GI-2019_FINAL.pdf
[17] https://www.pbz.hr/gradjani/mreza.html
[18] https://www.linkedin.com/in/nikola-popadić-a92b9757/

Ako se PBZ provrti kroz Spiderfoot, vidljivo je da se web stranica nalazi na IP adresi 193.227.213.244 te da je poslužitelj Apache server.



Slika 3.8 Korištene web tehnologije dobivene Shodanom

Pomoću Maltega vidljivo je da PBZ koristi 2 Metronetova dijeljena servera i jedan T-Comov server te da ima 2 svoja web servera. Nekoliko mailova zaposlenika našlo se u bazama s adresama čija je sigurnost narušena curenjem lozinke i ostalih informacija.



Slika 3.9 Kompromitirani podaci zaposlenika Privredne banke Zagreb

3.4. Zagrebačka banka

Zagrebačka banka ima daleko najviše zaposlenika od svih promatranih banaka, čak 3.838, dok Grupa Zagrebačke banke ima 5.317 zaposlenika. U Republici Hrvatskoj ima 117 poslovnica.[19]

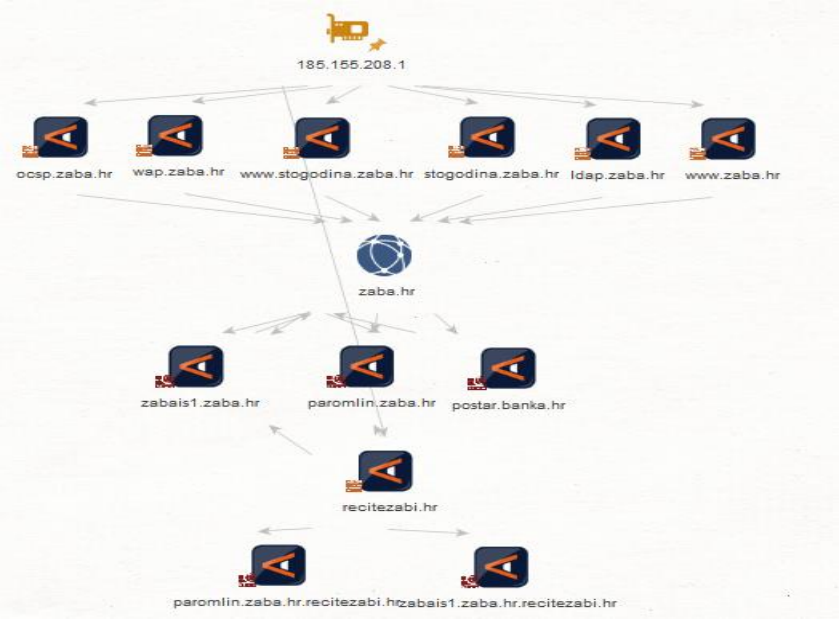
[19] https://www.zaba.hr/home/o-nama/investitori/financijski-izvjestaji

Iako u arhivi ima preko 200 *snapshota*, nema mnogo informacija na web stranici banke. *Snapshotane* su uglavnom naslovnice, a daljnje klikanje po stranici i pokušaji otvaranja stare stranice za karijeru u banci vode u prazno jer *snapshoti* ne postoje. No, u novim oglasima za posao je navedeno samo da traže sistemske inženjere za Windows i Unix operativne sustave.

Zaposlenici iz Zagrebačke banke su relativno aktivni na društvenim mrežama i čini se da redovito ažuriraju svoje profile. Na LinkedInu je moguće pronaći mnogo IT zaposlenika i skoro svaki od njih ima navedeno čime se bavi. Pregledavajući njihove profile, može se zaključiti da se dosta svakodnevnih procesa poslovanja Zagrebačke banke bazira na IBM-ovim tehnologijama[20]. Osim što imaju certificiranog stručnjaka za IBM tehnologije, mnogo ostalih zaposlenika[21] ima navedeno određeno poznavanje WebSphere Application Servera i AIX i Linux sustava općenito.

Spiderfoot je otkrio da je IP adresa stranice 185.155.208.1 te da se koriste neke aplikacije poput Adobe InDesign CS6 (Windows), Adobe InDesign CC 2015 (Macintosh) te Microsoft Word 2010.

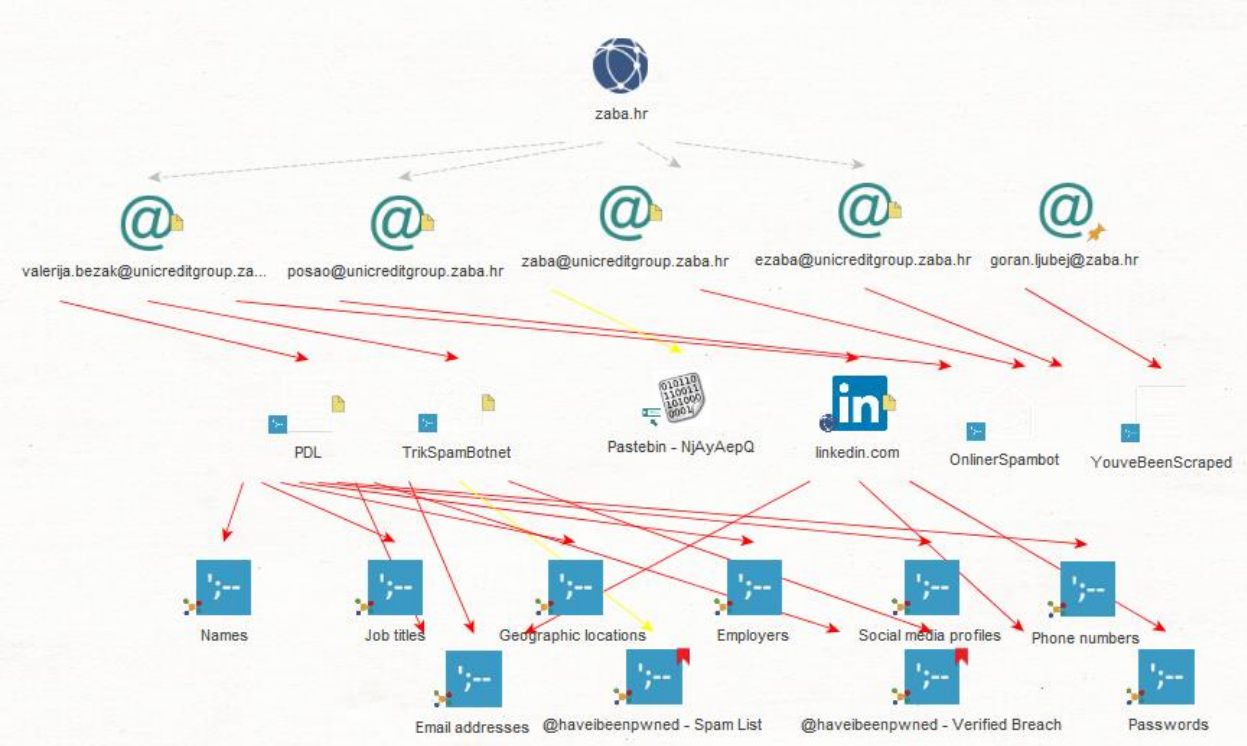
Koristeći Maltego moguće je vidjeti da Zagrebačka banka koristi vlastite web servere.



Slika 3.10 Mreža Zagrebačke banke

[20] https://www.linkedin.com/in/miroslav-kozomara-8017b8106/
[21] www.linkedin.com/in/hrvoje-ribičić-521840119/, www.linkedin.com/in/goranljubej/, www.linkedin.com/in/maša-žigo-7236493/

Zagrebačka banka, kao i ostale banke, ima poteškoća sa zaposlenicima koji koriste poslovnu mail adresu u različite privatne svrhe ili otvaraju sumnjive poveznice pa se tako našlo nekoliko mail adresa u bazama podataka s kompromitiranim lozinkama.



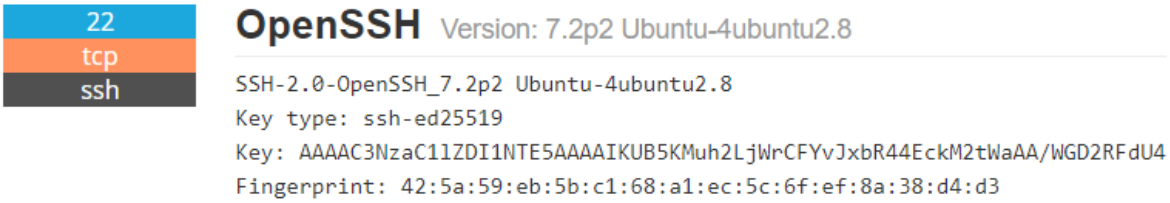
Slika 3.11 Procureni podaci o zaposlenicima Zagrebačke banke

3.5. Addiko banka

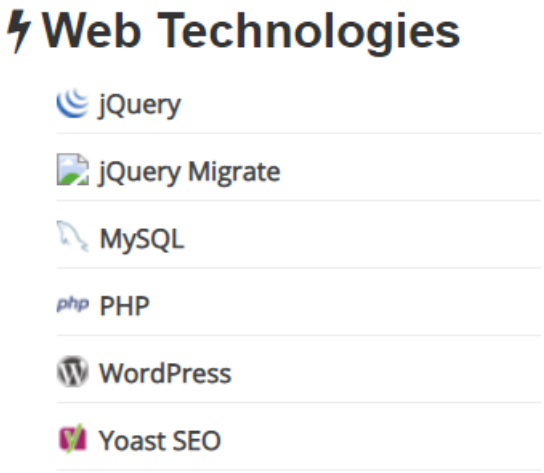
Addiko u Hrvatskoj ima 1.107 zaposlenika kroz 46 poslovnica[22]. U arhivi zapisi počinju od 18. srpnja 2016. godine što može značiti da *snapshoti* bivše Hypo Alpe-Adria-Banke nisu niti postojali ili je Addiko banka tražila brisanje nakon što je 11. srpnja 2016. preuzela Hypo banku. Danas postoji tek nešto više od 40 *snapshota*, no to su samo naslovnice te se ne može dobiti više podataka sa stranica.

Spiderfoot je otkrio da Addiko banka koristi Apache server za svoju web stranicu, koja se nalazi na IP adresi 52.59.150.186. Također je našao i da je otvoren port 22 što je potvrdio i Shodan.

[22] https://www.addiko.hr/static/uploads/Addiko-bank-hrv-2019_final_WEB-objava.pdf



Slika 3.12 Otvoren port 22



Slika 3.13 Web tehnologije koje Addiko banka koristi

Domena addiko.hr koristi dva dijeljena Iskonova servera te nemaju vlastite web servere. Kako je Spiderfoot vidio da web stranica vrti na Apache serveru, očito se to odnosilo na Iskonove servere. Maltego nije uspio pronaći mail adrese koje su procurile, osim jedne info mail adrese koja se našla u online *spambot* bazi.

3.6. Sberbank

Prema financijskom izvještaju vidljivo je da banka ima 489 zaposlenika i 31 poslovnicu.[23]

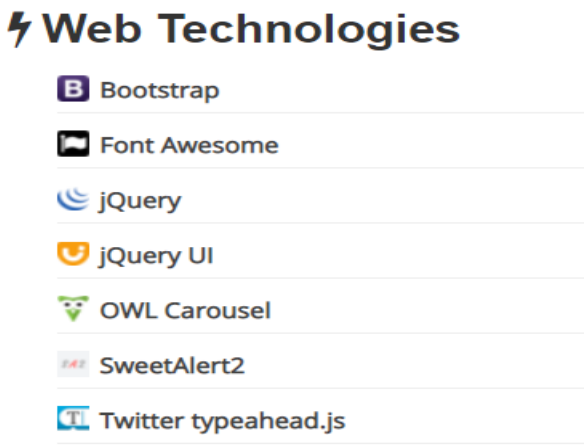
Iako u arhivi ima preko 300 *snapshota* koji postoje od 2013. godine, malo se korisnih informacija za potencijalne napadače može naći.

Sberbank također nema puno zaposlenika na LinkedInu tako da potencijalni napadači ne mogu tu dobiti bolji uvid u sustav, no zahvaljujući par profila može se pretpostaviti da se dosta radi na

[23] https://www.sberbank.hr/media/3825/sbe_annual_reports_final_2018-web-final.pdf

Windowsima i Microsoftovoj tehnologiji što je vidljivo iz profila gdje zaposlenik[24] piše o migraciji Active Directoryja i sastavljanju PowerShell skripta za automatiziranje raznih procesa. Također se spominje i da je Sberbank 2015. godine imao preko 500 korisničkih računa i više od 100 servera. Na drugom profilu[25] je vidljivo da Sberbank ima i certificirane stručnjake za Microsoftove tehnologije.

Web stranica banke nalazi se na IP adresi 213.191.158.70 te je negdje instaliran Adobe Photoshop CS6 na Macintoshu.

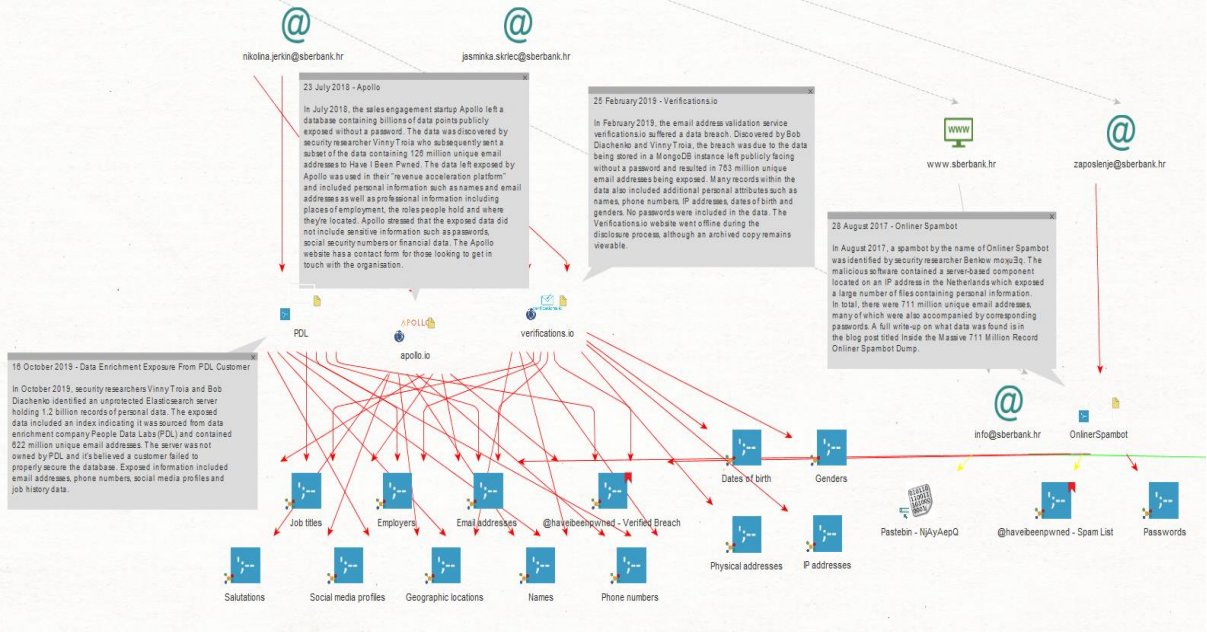


Slika 3.14 Sberbank web tehnologije

Sberbank koristi iste Iskonove dijeljene web servere na kojima su i web stranice Addiko banke jer se na tim serverima kroz obje pretrage dobiju nazad iste domene koje nisu vezane uz banke, poput stranice za vjenčanja ili ronilačkog kluba.

Maltego je pronašao nekoliko mail adresa koje su se našle u bazama podataka s mailovima čiji su osobni podaci procurili.

[24] https://www.linkedin.com/in/vremenar/
[25] https://www.linkedin.com/in/berislav/

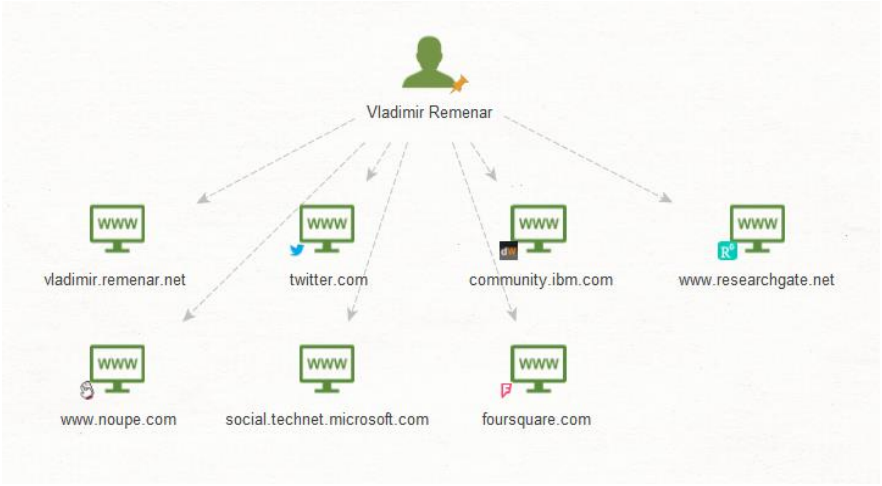


Slika 3.15 Procureni podaci zaposlenika

Zanimljivo je i što jedan od zaposlenika u IT odjelu Sberbanke vodi privatni blog o administriranju SQL-a i Windowsa. Može se pretpostaviti da je dosta znanja stekao na poslu i da se postovi koje objavljuje u blogu mogu primijeniti i na njegovom radnom mjestu.

Slika 3.16 Naslov bloga zaposlenika Sberbanke

Maltego je pronašao još jednog zaposlenika u IT odjelu koji ima svoju stranicu o sigurnosti i dijeli svoje iskustvo sa svojim čitateljima na društvenim mrežama.



Slika 3.17 Stranice na kojima zaposlenik dijeli savjete

Slika 3.18 Dio Twitter računa zaposlenika Sberbanke

3.7. Podravska banka

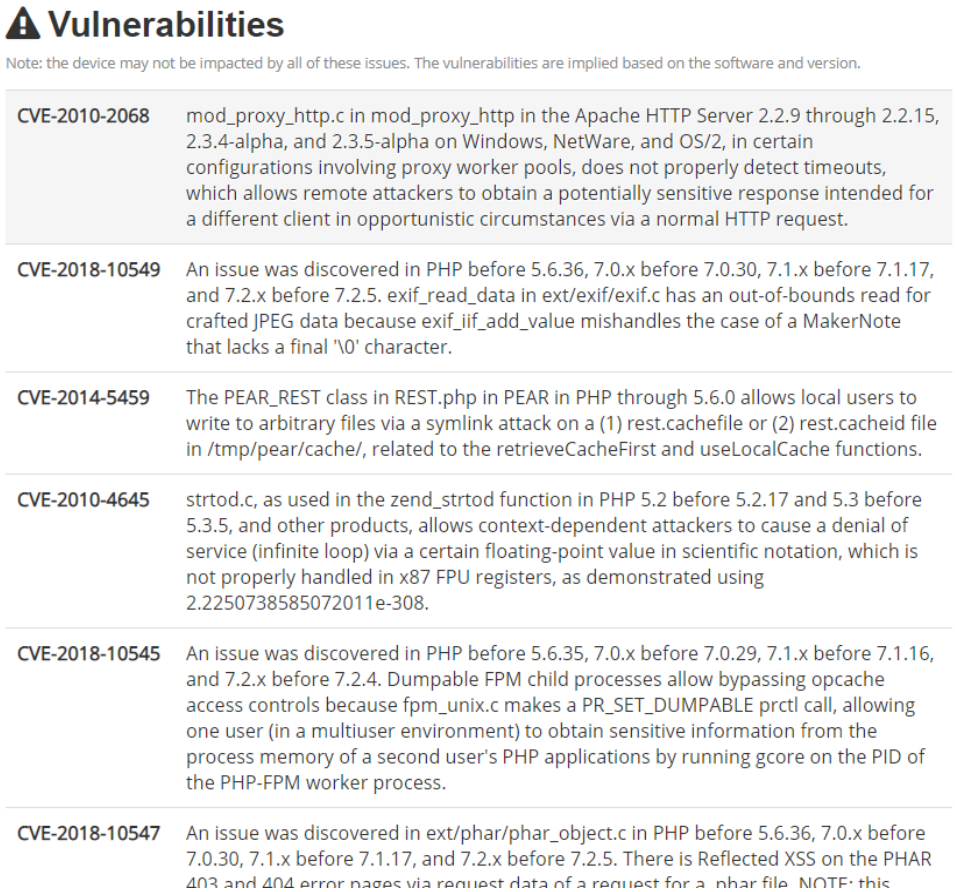
Podravska banka ima 22 poslovnice i ukupno 221 zaposlenu osobu.[26]

U arhivi nema previše korisnih informacija za potencijalne napadače. Na LinkedInu se nalazi malo zaposlenika, većina ih nema slike profila i nema podatke na svojim profilima. Osim što to izgleda neprofesionalno i sumnjivo, čini se i da nije problem stvoriti lažni korisnički račun i lažno se

[26] https://www.poba.hr/index.php?cat=odnosi_s_investitorima&art=127

predstavljati kao zaposlenik banke. Većina korisnika koji su navodni zaposlenici banke imaju između 0 i 5 konekcija.

Web stranica se nalazi na adresi 195.29.166.234 na Apache 2.2.15 serveru na CentOS-u. I Spiderfoot i Shodan upozoravaju na korištenje Flasha na web stranici banke koji se danas više ne koristi zbog svoje ranjivosti. Spiderfoot je otkrio dosta aplikacija i njihovih verzija s druge strane servera, na primjer Mario Brajnić koristi Word 2016, Iva Puk Word 2010, Kristina Vutuc-Pecikozic Word 2013 i vidljivo je da su instalirani Acrobat Distiller 5.0.5 i Adobe Photoshop 21.0 za Windowse.

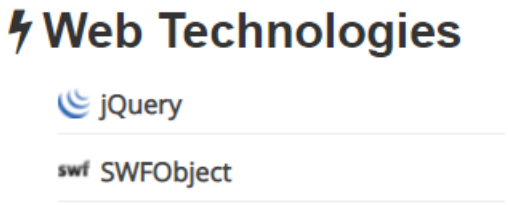


Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

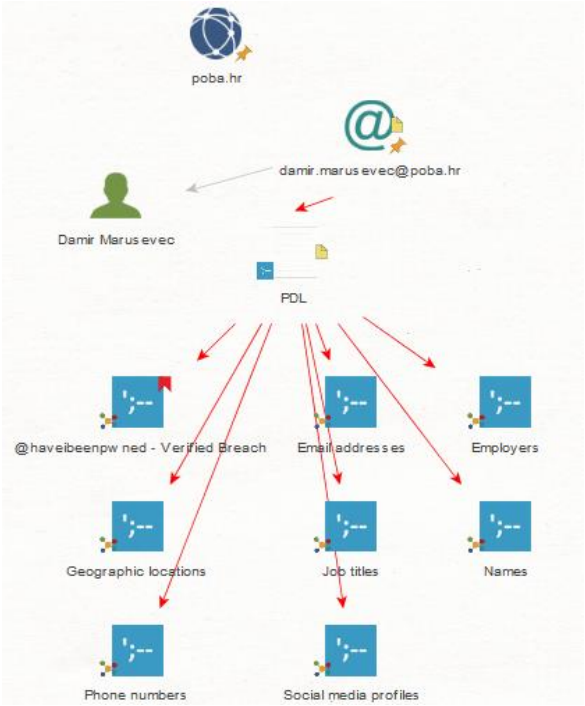
CVE-2010-2068	mod_proxy_http.c in mod_proxy_http in the Apache HTTP Server 2.2.9 through 2.2.15, 2.3.4-alpha, and 2.3.5-alpha on Windows, NetWare, and OS/2, in certain configurations involving proxy worker pools, does not properly detect timeouts, which allows remote attackers to obtain a potentially sensitive response intended for a different client in opportunistic circumstances via a normal HTTP request.
CVE-2018-10549	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final '\0' character.
CVE-2014-5459	The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.
CVE-2010-4645	strtod.c, as used in the zend_strtod function in PHP 5.2 before 5.2.17 and 5.3 before 5.3.5, and other products, allows context-dependent attackers to cause a denial of service (infinite loop) via a certain floating-point value in scientific notation, which is not properly handled in x87 FPU registers, as demonstrated using 2.2250738585072011e-308.
CVE-2018-10545	An issue was discovered in PHP before 5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before 7.2.4. Dumpable FPM child processes allow bypassing opcache access controls because fpm_unix.c makes a PR_SET_DUMPABLE prctl call, allowing one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications by running gcore on the PID of the PHP-FPM worker process.
CVE-2018-10547	An issue was discovered in ext/phar/phar_object.c in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. There is Reflected XSS on the PHAR 403 and 404 error pages via request data of a request for a .phar file. NOTE: this

Slika 3.19 Ranjivosti koje Shodan navodi na stranici Podravske banke



Slika 3.20 Web tehnologije na stranici Podravske banke

Podravska banka koristi T-Comove web servere, iste one na kojima se nalaze i Erste, HPB i PBZ na kojima se najvjerojatnije nalazi Apache. Maltego je uspio pronaći samo jednog zaposlenika u bazama podataka s procurenim osobnim podacima.



Slika 3.21 Osobni podaci zaposlenika

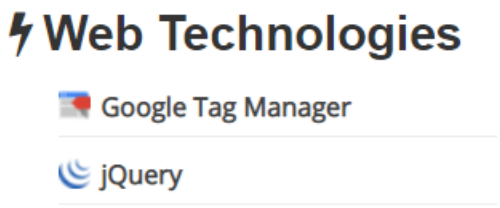
3.8. Raiffeisen bank

U Raiffeisen banci radi 2.121 zaposlenik te ima 66 poslovnica diljem Hrvatske.[27]

Pretražujući oglase za posao Raiffeisen ističe da „dodatnu prednost imaju kandidati koji poznaju Linux operativni sustav, OpenShift i osnovno poznavanje Microsoft serverskih tehnologija (Active Directory, DNS, DHCP, GPO)“[28].

Na LinkedInu ima dosta zaposlenika, neki od njih imaju položene IBM-ove certifikate[29] ili rade na WebSphere Application Serveru[30]. Kako u oglasu traže poznavanje Microsoft serverske tehnologije, logično je za pretpostaviti da imaju i zaposlenike koji su stručni u tome. Takve je zaposlenike isto moguće naći na LinkedInu[31]. Voditelj unutarnjeg Service Deska banke navodi odlično poznavanje Windowsa, ali ne spominje druge operativne sustave, dakle zaposlenici svoje svakodnevne aktivnosti najvjerojatnije obavljaju na Windows sustavima[32].

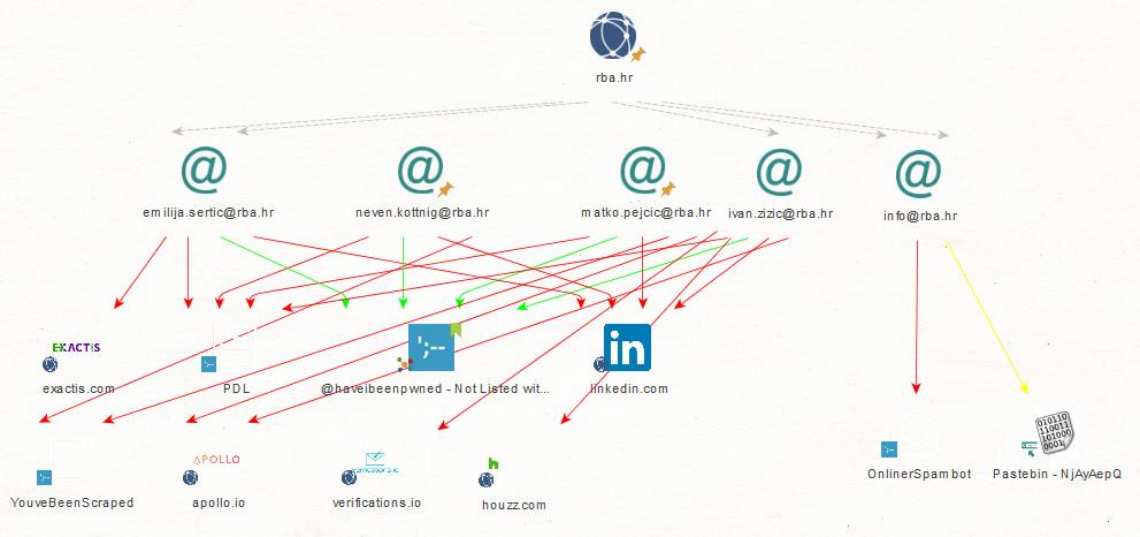
Spiderfoot je našao da je IP adresa stranice banke 193.23.182.195 te da se koriste neke aplikacije poput GPL Ghostscript 8.15, Adobe InDesign CS4 (6.0.6) i Acrobat Distiller 9.4.0 za Windows.



Slika 3.22 Web tehnologije korištene na stranici Raiffeisen banke

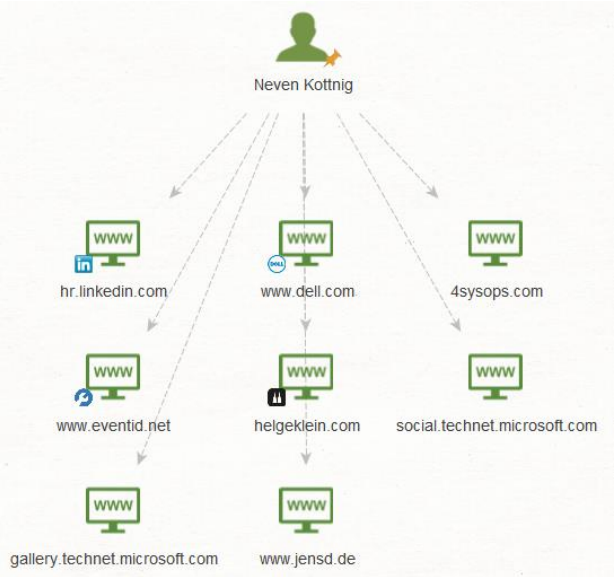
Maltego je otkrio da se domena rba.hr nalazi na njihovim vlastitim web serverima te da i kod njih postoji ugroženih mail adresa.

[27] https://www.rba.hr/o-nama/financijski-pokazatelji/2018
[28] https://www.rba.hr/pridruzite-nam-se
[29] https://www.linkedin.com/in/zzugec/
[30] https://www.linkedin.com/in/matko-pejčić-a5103b5/
[31] https://www.linkedin.com/in/neven-kottnig-9b03137b/
[32] https://www.linkedin.com/in/karlotopol/



Slika 3.23 Procureni podaci iz mail adresa zaposlenika

Jedna od tih ugroženih mail adresa pripada njihovom Microsoft sistem administratoru. Nakon detaljnije pretrage zaposlenika po imenu, Maltego je našao stranice gdje je zaposlenik bio aktivan. Na taj način je pronađeno nekoliko njegovih postova na forumima gdje se informira o printeru instaliranom na Windows 2008 R2 serveru.



Slika 3.24 Stranice na kojima je zaposlenik ostavio tragove

3.9. OTP banka

U Hrvatskoj ima 120 poslovnica OTP banke i zaposleno je preko 2.000 zaposlenika.[33]

Kako su oglasi za posao na web stranici OTP banke koncipirani tako da se klikne na naziv radnog mjesta što skida PDF s opisom posla i potrebnim vještinama, u arhivi nema spremljenih opisa. Mogu se pronaći samo nazivi radnih mjesta i lokacije. Vidljivo je da je OTP banka u 2008. godini tražila sistemskog inženjera u Zadru, no nema podataka o potrebnom znanju i profilu osobe kakvu traže. Aktualni oglasi za posao ne odaju mnogo informacija jer nisu ciljani za poslove u informatičkom sektoru. Navodi se samo da traže klasično poznavanje Microsoft Office paketa što ne govori puno. Za većinu oglasa, mjesto rada je u Zadru, tako je i za sistemskog inženjera kojeg su tražili 2008. godine što može upućivati na to da su i serveri u Zadru, ali to ponovno, ne govori mnogo potencijalnim napadačima.

Naziv radnog mjesta	Lokacija	Broj izvršitelja	Vrijedi	
			Od	Do
Referent	Zadar	1	19.2.2008.	26.2.2008.
Sistem inženjer/Viši sistem inženjer	Zadar	1	21.2.2008.	28.2.2008.
Projektant/Viši projektant	Zadar	2	21.2.2008.	28.2.2008.
Analitičar - pripravnik	Zadar	1	21.2.2008.	28.2.2008.

Slika 3.25 Radna mjesta s lokacijom u Zadru

Informatičari OTP banke ne odaju mnogo informacija na svojim profilima na LinkedInu pa se ni tu ne može mnogo izvući osim ponekog, ne pretjerano specifičnog spominjanja Microsoft servera i virtualizacije.[34]

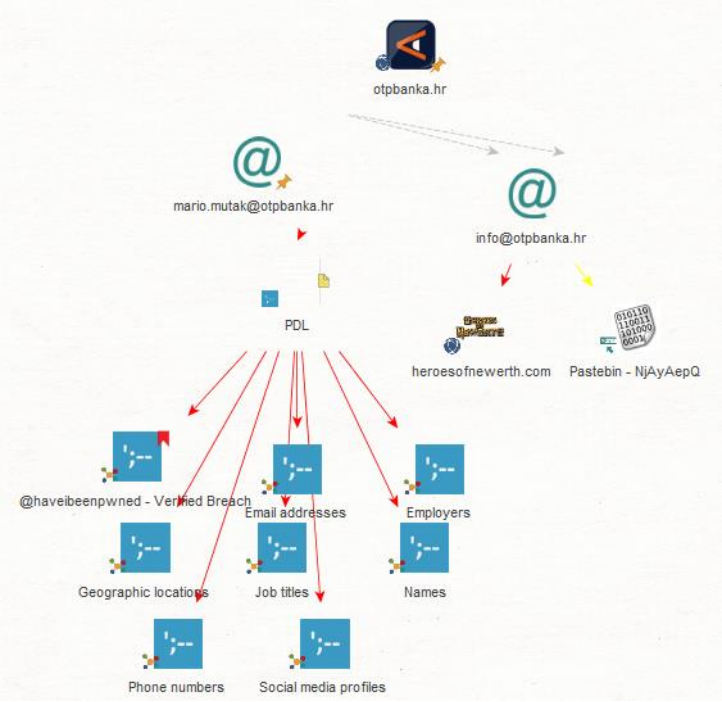
IP adresa stranice banke je 212.15.181.71, no nema mnogo podataka koji se mogu izvući kroz Spiderfoot ili Shodan. Vidljivo je da je negdje instaliran Adobe Photoshop CC 2018 za Macintosh.

Slika 3.26 Web tehnologije korištene na stranici OTP banke

[33] https://www.otpbanka.hr/hr/o-nama/otp-banka
[34] https://www.linkedin.com/in/mario-mutak-0226278/

O OTP banci ni Maltego nije uspio pronaći previše korisnih informacija osim mapiranja mreže. Izgleda da banka koristi svoje vlastite web servere za web stranicu.

Maltego je pronašao jednu mail adresu zaposlenika koja se našla u javim bazama podataka, osim info mail adrese banke.



Slika 3.27 Procurene mail adrese OTP banke

3.10. Croatia banka

Croatia banka ima najmanje poslovnica i zaposlenika od svih promatranih banaka. Banka zapošljava 175 osoba kroz 11 podružnica i 3 poslovnice.[35]

Iako ima preko 230 *snapshota* u arhivi, samo ih je 5 na stranici natječaja za posao i ni jedan nije u trenu kad je bilo otvorenih natječaja tako da na taj način nije moguće dobiti uvid u sistemsko stanje Croatia banke.

Na društvenim mrežama, zaposlenici nemaju dovoljno relevantnih podataka da bi se stvorila ikakva slika o sigurnosti banke.

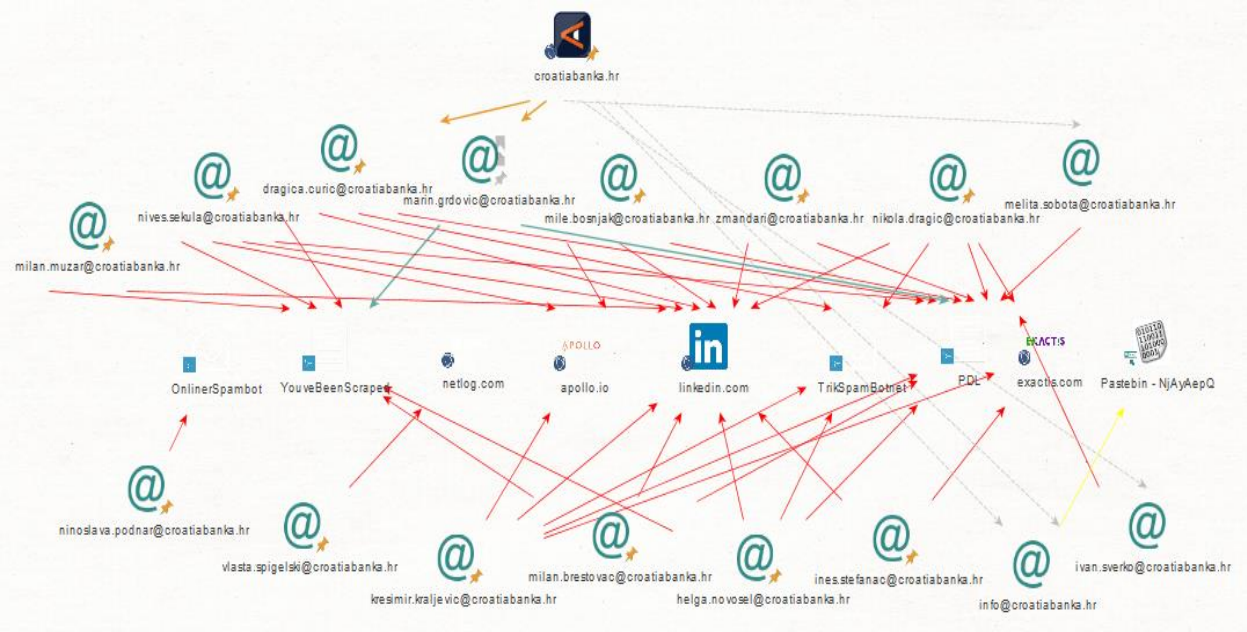
[35] https://www.croatiabanka.hr/media/147057/godisnje-izvjesce-za-2018-godinu.pdf

Spiderfoot je našao da je IP adresa web stranice 31.45.236.164 te da se neki od servera identificira kao Microsoft-HTTPAPI/2.0 što je i Shodan potvrdio. Također mnogo zaposlenika ima kompromitirane mail adrese te su im procurile lozinke.

Data Element
dragica.curic@croatiabanka.hr:zdravka [exploit.in]
helga.novosel@croatiabanka.hr:xxx [linkedin.com]
ines.stefanac@croatiabanka.hr:hajduk1 [exploit.in]
kresimir.kraljevic@croatiabanka.hr:crespo [exploit.in]
milan.brestovac@croatiabanka.hr:vurnaza [exploit.in]
milan.muzar@croatiabanka.hr:milan123 [exploit.in]
mile.bosnjak@croatiabanka.hr:xxx [linkedin.com]
mladen.ivancic@croatiabanka.hr:MLADEN [exploit.in]
mpast@croatiabanka.hr:xxx [linkedin.com]
nikola.dragic@croatiabanka.hr:kokokoko [exploit.in]

Slika 3.28 Kompromitirani računi zaposlenika Croatia banke

Croatia banka ima dosta kompromitiranih mail adresa zaposlenika. Maltego je usporedio sve mail adrese koje su dosad pronađene u Spiderfootu i koje je pronašao sam s onima u bazama kompromitiranih mail adresa i bilo je mnogo podudaranja. Od 34 mail adresa koje su uspoređivane, 16 ih je bilo u bazama.

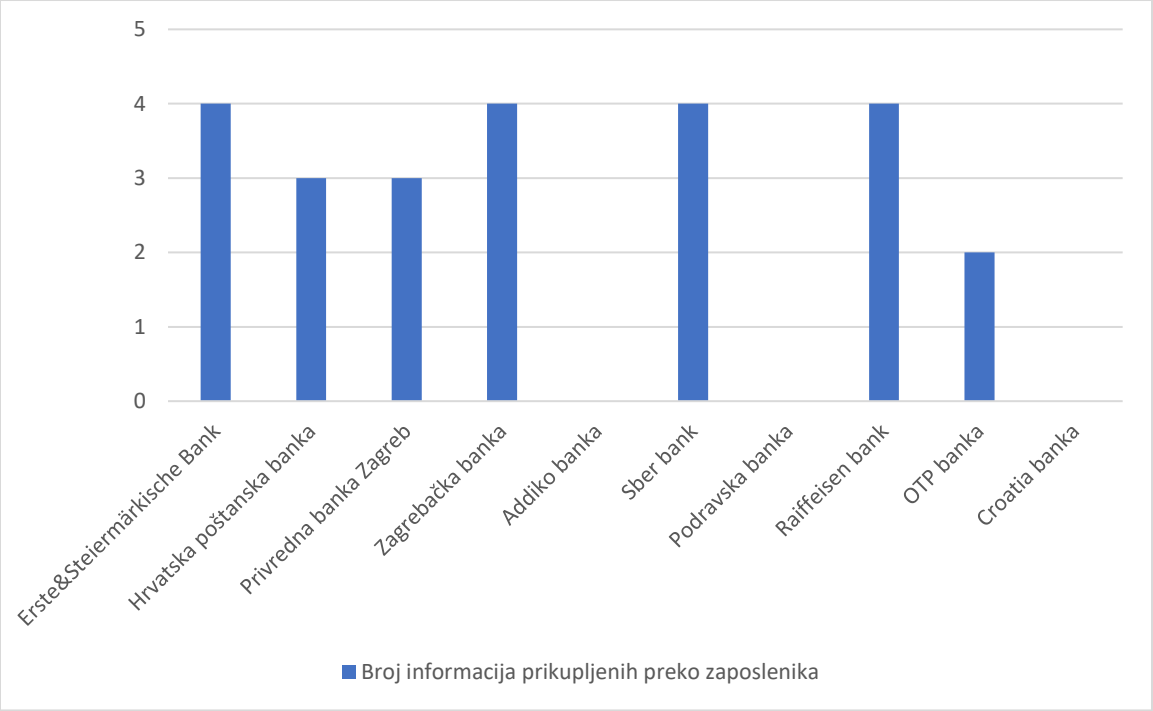


Slika 3.29 Baze u kojima se mogu naći zaposlenici Croatia banke

4. Usporedba banaka po sigurnosti

U ovome će poglavlju kroz grafove biti prikazana količina podataka pronađenih za pojedine banke. Grafovi su sastavljeni od svih podataka navedenih gore u radu, a svedeni su na brojeve koji prikazuju količinu prikupljenih podataka kako bi se vizualno lakše dočarali odnosi prikupljenih podataka između banaka. Korišteno je šest referentnih točaka, a to su redom:

- broj informacija koje su na bilo koji način prikupljene preko zaposlenika; kroz društvene mreže, blogove, forume ili bilo koji drugi način objavljene od strane zaposlenika
- broj informacija iz oglasa za posao; aktualni oglasi ili prijašnji oglasi koji više nisu aktivni, ali ih se može pronaći na službenim web stranicama ili u web arhivi
- informacije o web serverima
- broj pronađenih adresa elektroničke pošte koje su kompromitirane
- broj aplikacija koje su pronađene skenirajući web servere
- broj web tehnologija koje su otkrivene pregledavajući web servere



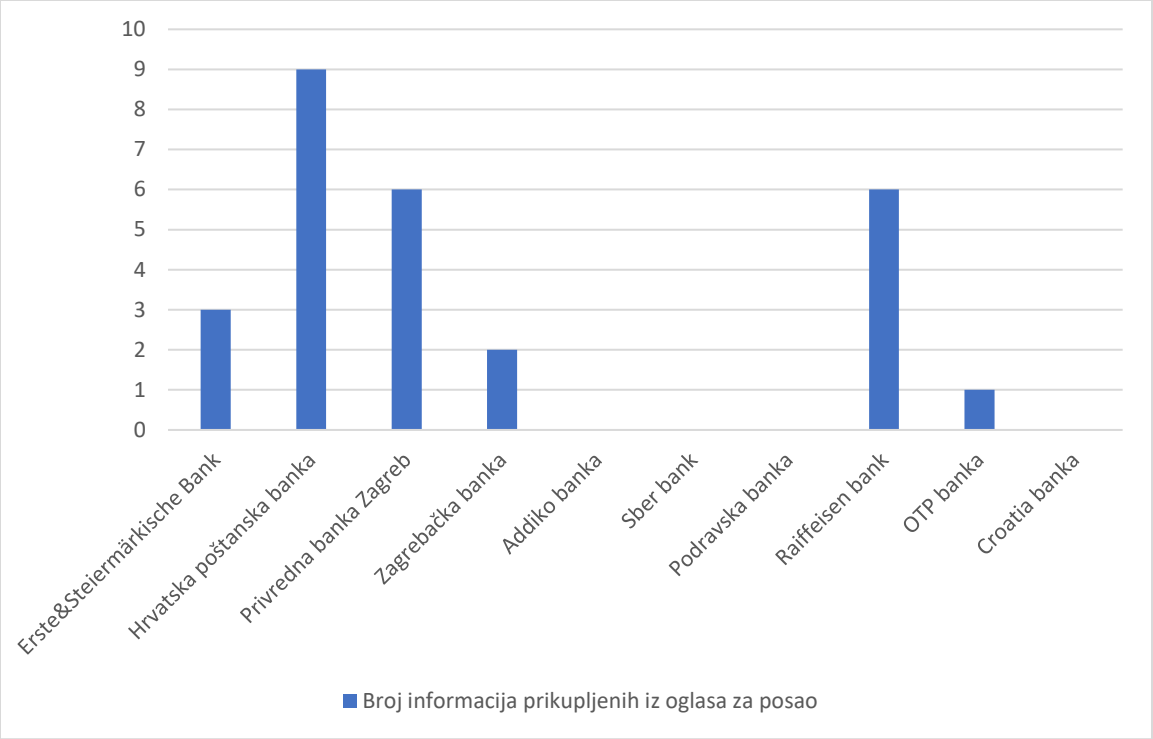
Slika 4.1 Broj informacija prikupljenih preko zaposlenika

Informacije koje zaposlenici objavljuju na internetu vezano uz svoj posao bi svako ozbiljno poduzeće trebalo zanimati, što zbog ugleda, a što zbog sigurnosti. Pogotovo ako je sigurnost jako važna za poslovanje poduzeća, a kod banaka je to jedan od najvažnijih faktora. Zaposlenici predstavljaju veliki sigurnosni rizik jer imaju uvid u unutarnji rad i sustav banke i time raspolažu s mnogo inkriminirajućih podataka.

Ako govorimo o zaposlenicima u informatičkom sektoru, što je zaposlenik veći stručnjak to su veće šanse da će se njegovo ime više spominjati na internetu. Takve osobe često drže predavanja o internetskoj sigurnosti, predavanja o tehnologijama ili o samim operativnim sustavima. To može upućivati da se upravo time i bavi na svom poslu. Tako da je i to neka vrsta ugrožavanja sigurnosti.

Noviji ili mlađi zaposlenici koji rade u manjim timovima i nemaju starijih kolega koji bi im mogli pomoći mogu pribjeći forumima gdje će se raspitivati o problemima s kojima se susreću na poslu i time dati uvid u sustav na kojem rade.

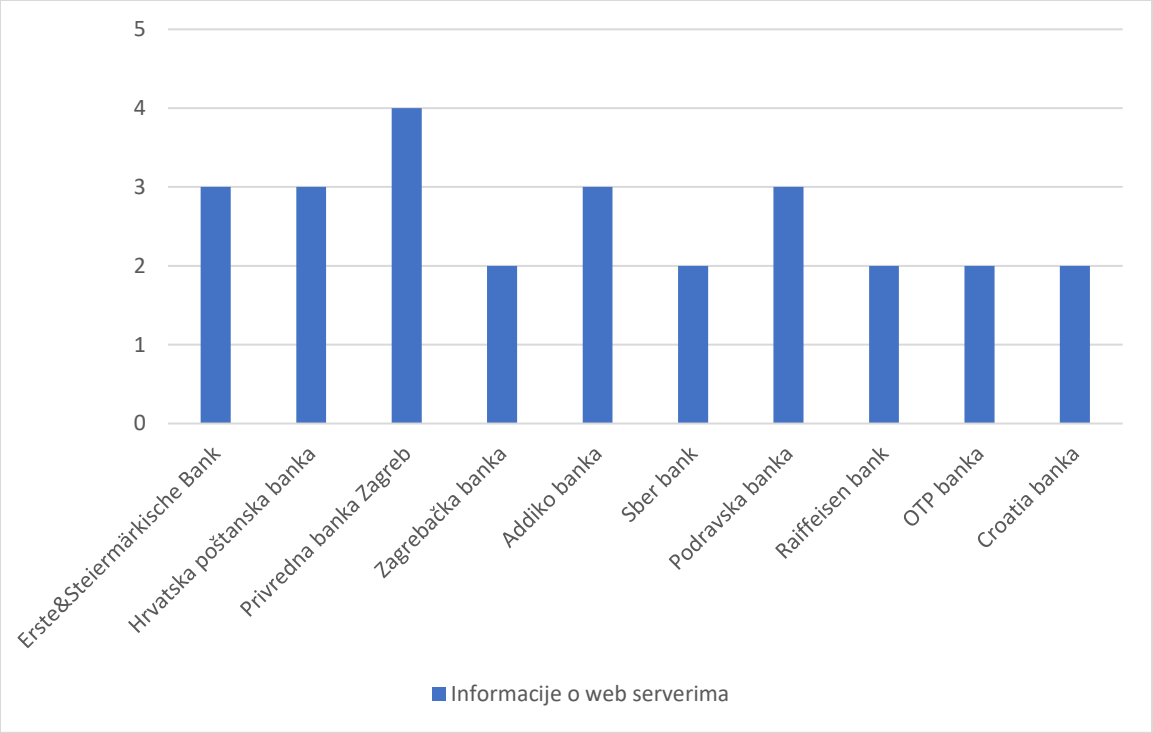
Zaposlenici, i iskusni i oni manje iskusni, često imaju online životopise u obliku LinkedIn profila gdje se mogu saznati informacije o njihovom poslu. Na mnogo načina ponašanje zaposlenika na internetu može odati neke podatke o sustavu, ali to ne znači da bi se svi trebali pritajiti i više nikad ništa ne objavljivati kako ne bi ugrozili banku za koju rade. Štoviše, veću sigurnost ulijeva vidjeti da neka banka ima zaposlene poznate stručnjake koji rade na sigurnosti, nego potpuno anonimne osobe koji imaju profile na društvenim mrežama popunjene samo sa svojim obrazovanjem i bez konkretnog iskustva. No, ukoliko dođe do situacije u kojoj zaposlenik treba pitati za savjet na forumu, to bi trebalo biti anonimno i na način na koji se ne može povezati s bankom za koju zaposlenik radi.



Slika 4.2 Broj informacija prikupljenih iz oglasa za posao

Za osobe koje traže posao uvijek je bolje da je čim više podataka navedeno u oglasu kako bi znali zadovoljavaju li tražene kriterije. Kandidati vole unaprijed dobiti sve informacije o radnom mjestu kako ne bi gubili svoje vrijeme hodajući po različitim poduzećima obavljajući intervjue. Za poduzeće je isto bolje staviti sve informacije u oglas da izbjegnu nekompetentne ljude koji se prijave jer je i njima neuspješni intervju gubitak dragocjenog vremena. S više informacija u oglasu mogu se javiti osobe koje imaju točno ona znanja koja su poduzeću potrebna, no to također može potencijalno i otkriti neke informacije o sustavu. Važno je naći ravnotežu u danim informacijama da otkriju dovoljno da oglas nije svestran, ali i da ne kompromitiraju cijeli sustav.

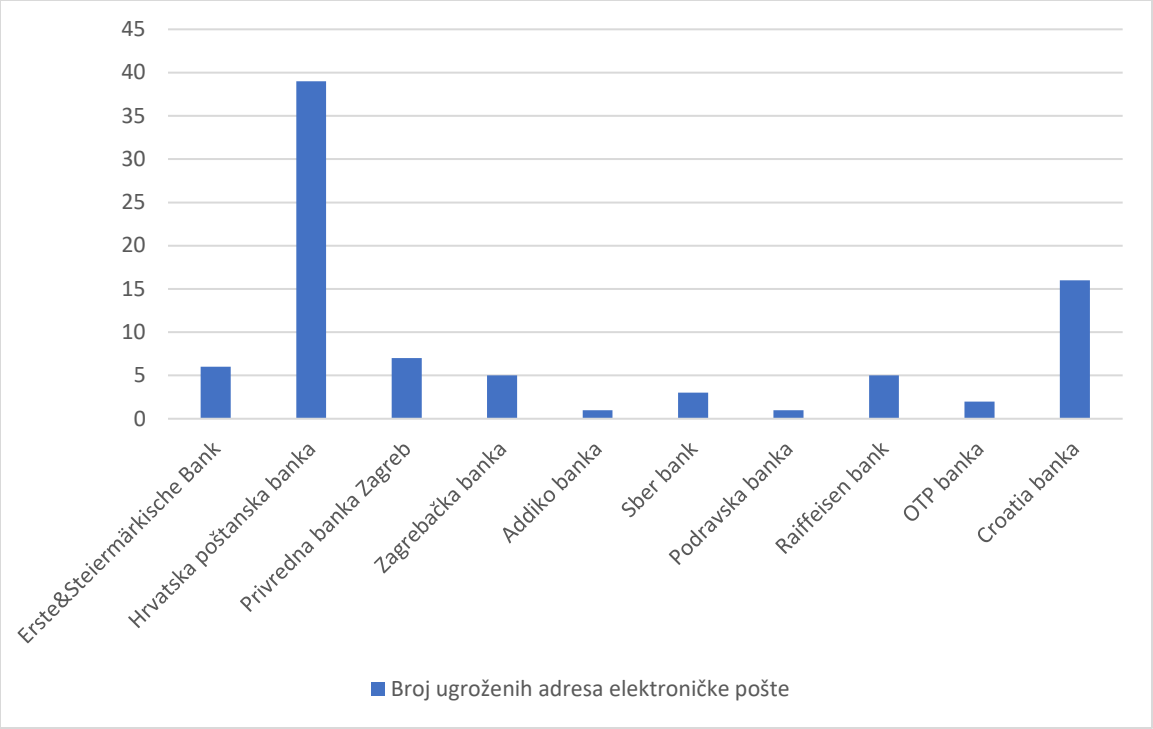
Takva bi se problematika mogla relativno smanjiti s online molbama u kojima banka, na primjer, traži Linux administratora pa zainteresirane osobe popunjavaju obrazac gdje sami navode sva svoja znanja i vještine bez da banka otkriva što njima konkretno treba. Ukoliko kandidat ima neka znanja i vještine potrebne banci, tada ih se zove na razgovor. Naravno da takva metoda iziskuje nešto više truda od kandidata jer mora sam sastaviti što sve zna raditi i kojim se alatima služiti, ali to može i banci biti pokazatelj zainteresiranosti za radno mjesto, a usput, možda i primijete vrhunskog kandidata koji ne odgovara baš tom radnom mjestu, ali je izvrstan u drugim stvarima pa ga svejedno zaposle u neki drugi tim.



Slika 4.3 Broj informacija o web serverima

Znati koji je operativni sustav s druge strane potencijalnom napadaču može puno značiti. Ukoliko zna koji je operativni sustav i njegova verzija, dalje nije teško pronaći *exploit* za taj određeni sustav. Stranice poput exploit-db.com imaju popis svih poznatih potvrđenih i nepotvrđenih ranjivosti za operativne sustave, aplikacije i razne alate. Naravno da ne daju svi *exploiti* direktan pristup sustavu, ali treba li se poduzeće poput banke uopće dovoditi u ikakav rizik? *Exploit* je zapravo način iskorištavanja bilo kakve postojeće ranjivosti i otvaranje vrata do ranjive aplikacije ili sustava što onda može napadaču omogućiti ubacivanje virusa za praćenje, kriptiranje podataka za otkupninu i slično.

Bilo kakvo odavanje informacija o sustavu može olakšati napade. O samome web serveru, sve nepotrebne informacije moguće je sakriti kod podešavanja servera. Samo neke od metoda koje se mogu primijeniti su micanje nepotrebnih HTTP *headera*, skrivanje osnovne *.php* datoteke, može se ugasiti potpis servera (engl. *ServerSignature*).



Slika 4.4 Broj ugroženih adresa elektroničke pošte zaposlenika

Trebam napomenuti da je u grafu broj mail adresa koje je moguće pronaći na internetu, a koje su se našle u bazama podataka ugroženih adresa jer su procurili neki podaci poput naziva radnog mjesta, adrese korisnika, osobnih podataka, lozinke i slično. Važno je napomenuti da nije testiran ukupan broj svih mail adresa zaposlenika pojedine banke nego samo mail adrese koje je bilo moguće pronaći na internetu tako da je realni broj zaposlenika u tim bazama ugroženih adresa zasigurno puno veći.

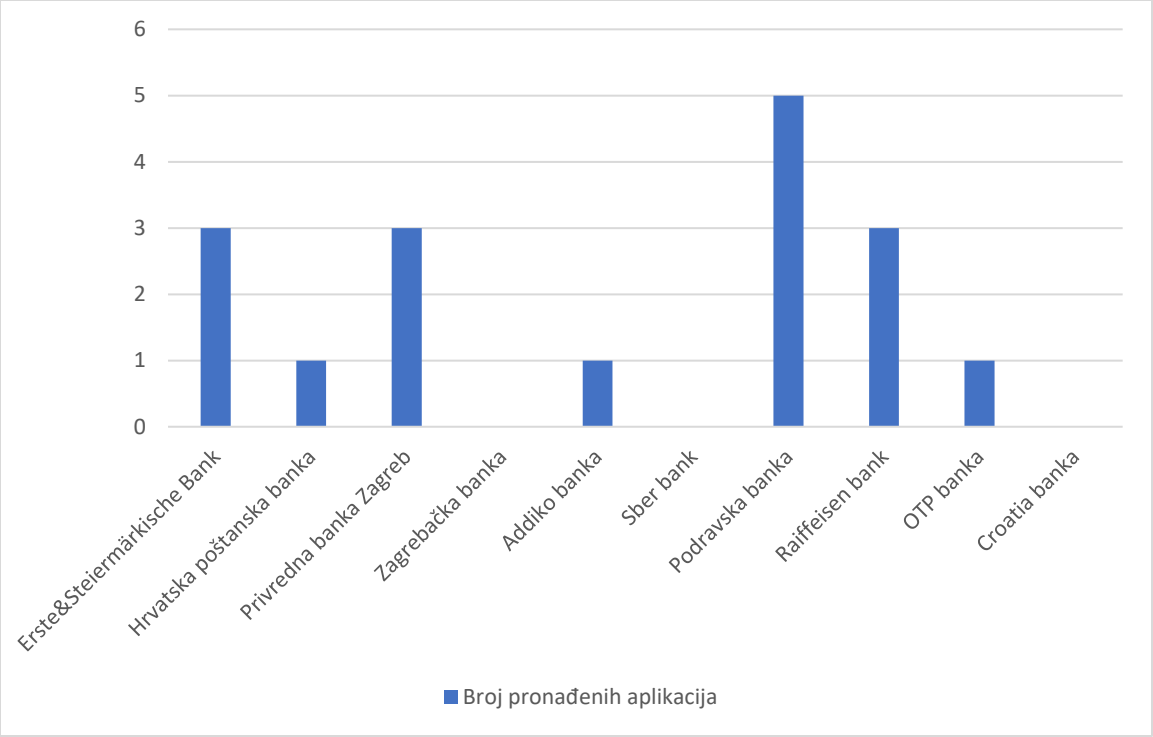
Za radna mjesta u poduzećima koja su u uredu i obavljaju se na računalima, normalno je da zaposlenici dobiju svoju adresu elektroničke pošte. Na taj način klijenti, ali i poduzeće mogu komunicirati sa svojim zaposlenikom. Banke nisu iznimka. Većina zaposlenika ima svoju mail adresu.

Često dolazi do problema s ljudima koji nisu navikli na korištenje više različitih mail adresa. Ukoliko su prije zaposlenja imali mail adresu otvorenu na nekim besplatnim davateljima mail usluge, takvi ljudi imaju tendenciju s vremenom napustiti svoju privatnu mail adresu i početi sve više upotrebljavati poslovnu čak i u privatne svrhe jer su poslovni pretinac dužni pregledavati, a nezgrapno im je redovito pregledavati oba pretinca.

Korištenje poslovne mail adrese u privatne svrhe uvelike ugrožava razinu sigurnosti. Zaposlenici koriste svoju poslovnu adresu za registraciju na razne stranice za koje je upitno na koji način pohranjuju *login* podatke. Te razne stranice mogu spremati mail adrese i lozinke te ih preprodavati dalje ili mogu biti napadnuti te im napadač može neovlašteno otuđiti povjerljive podatke bez da registrirane osobe išta znaju o tome. To predstavlja veliki problem jer osobe koje već koriste poslovnu email adresu u privatne svrhe, najvjerojatnije koriste i istu lozinku za sve. To bi potencijalnom napadaču dalo izravan pristup elektroničkoj pošti zaposlenika, a možda i cijelom korisničkom računu u banci, ukoliko pretpostavimo da je ista lozinka.

Također, zaposlenici mogu u svoje poslovne pretince dobivati razne *phishing* mailove i otvarajući poveznice iz takvih zlonamjernih mailova mogu navući razne viruse u sustav banke. Znajući da neka banka ima mnogo zaposlenika koji nisu dovoljno educirani o sigurnosti na internetu, logično je za pretpostaviti i da postoji određeni broj zaposlenika koji bi kliknuli na sumnjive mailove ukoliko bi im takvi bili poslani. To bi potencijalnim napadačima otvorilo vrata u sam sustav banke kad bi taj mail otvorili na računalu na svom radnom mjestu.

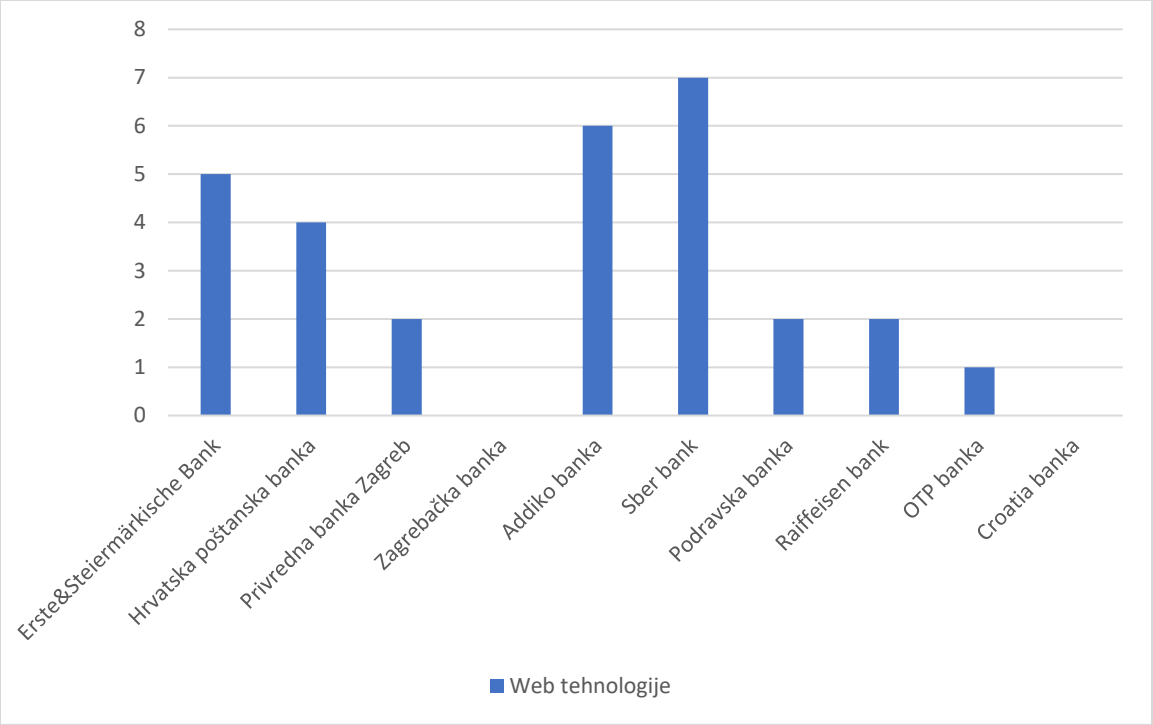
Edukacija zaposlenika je jako važan faktor koji se ne smije zanemariti. Banke moraju educirati svoje zaposlenike o sigurnom i odgovornom ponašanju na internetu i posljedicama korištenja poslovnih računa u privatne svrhe. Osim samih edukacija, može se uvesti *group policy* gdje se od zaposlenika traži da moraju promijeniti lozinku svakih mjesec dana. Važno bi bilo i zabraniti zapisivanje lozinka na papiriće i ostavljati ih igdje gdje bi ih netko mogao pronaći. Važno je naučiti zaposlenike da je banka sigurna koliko je siguran i njezin najnepouzdaniji zaposlenik.



Slika 4.5 Broj pronađenih aplikacija

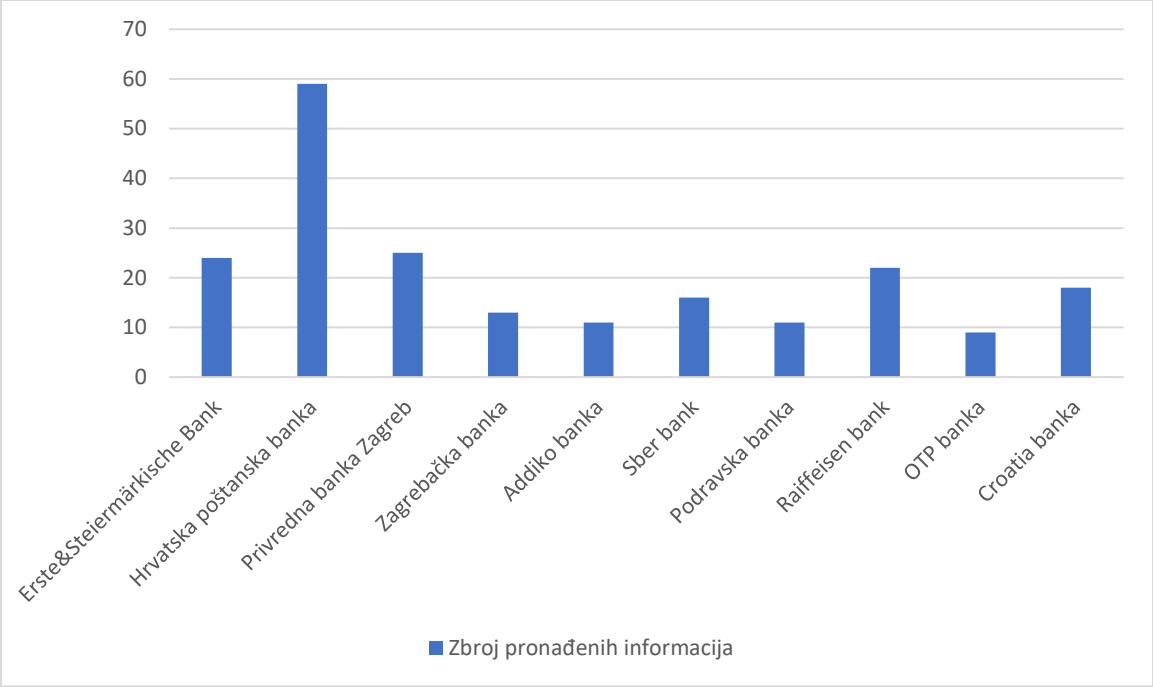
Web pauk Spiderfoot je pretražujući stranice banaka uspio pronaći aplikacije u kojima su rađeni dokumenti objavljeni na web stranicama. To može dati uvid u to koliko banke drže do ažuriranja i moderniziranja aplikacija koje koriste zaposlenici. Banka koja koristi verzije aplikacija starije od 5 godina za koje više ni Microsoft ne daje podršku ispada nepouzdanijom od banke koja redovito kupuje najnovije aplikacije.

Problem kod starih verzija aplikacija je ranjivost. Kako tehnologija redovito ide naprijed, tako se i svakim danom pronalaze nove ranjivosti za postojeće aplikacije te načini kako ih iskoristiti. S novim prolascima ranjivosti, proizvođači izdaju i zakrpe kako bi umanjili te ranjivosti. Ukoliko proizvođači izdaju novu verziju aplikacije, važno je prijeći čim ranije na nju jer će prije ili kasnije proizvođač prestati izdavati zakrpe za stariju verziju, a bankama je važno redovito zatvarati bilo kakav mogući prozor za potencijalne napadače.



Slika 4.6 Broj informacija o korištenim tehnologijama na web stranicama

Kao i kod aplikacija, važno je biti ažuran i redovito instalirati zakrpe odmah kako ih proizvođači izbace. Stare tehnologije poput Adobe Flasha koje su poznate po svojoj nesigurnosti treba napustiti, nepouzdane *pluginove* u WordPressu treba izbjegavati i uvijek treba paziti na to da se koriste najnovije tehnologije na tržištu, no naravno, ne toliko nove da još nisu provjerene i koje su još u razvoju te nisu stabilne.



Slika 4.7 Ukupne pronađene informacije

Posljednji grafički prikaz prikazuje ukupan zbroj svih pronađenih podataka o bankama. Brojevi u tom grafu su dobiveni zbrajanjem količine podataka iz svih prijašnjih grafova. Moguće je vidjeti kako se najnesigurnija banka čini Hrvatska poštanska banka, dok je najmanje podataka pronađeno za OTP banku.

Zaključak

Teško je precizno odrediti što je sigurno, a što nije. O bankama poput Erste&Steiermärkische Bank, Hrvatske poštanske banke ili Privredne banke Zagreb ima dosta podataka. Sberbank ima čak i zaposlenike koji otvoreno vode blogove o sustavima te educiraju druge o problemima s kojima se susreću i sami na svom radnom mjestu. Znači li to da su te banke ugroženije od banke poput Croatia banke o kojoj nisam uspjela pronaći nikakve informacije o njihovom sustavu ili OTP banke o kojoj ima ukupno najmanje informacija?

Privatnost na internetu ne znači nužno i sigurnost, isto kao i objavljivanje potencijalno kompromitirajućih informacija ne znači da je sigurnost banke ugrožena i da su napadačima vrata sustava otvorena.

Treba uzeti u obzir da sam koristila samo legalne načine prikupljanja podataka. Potencijalni napadači ne bi prezali ni pred čim da uđu u sustav te nije isključeno da bi usprkos nedostatku informacija o sustavu Croatia banke svejedno došli do cilja. Jednako tako iako neka banka ima servirane podatke na internetu, IT zaposlenici mogu biti veliki stručnjaci koji bi uspješno spriječili neki proboj.

Najvažniji faktor je upravo onaj koji je i najrizičniji, a to su zaposlenici. Najsigurniji sustavi su oni s najviše informatički obrazovanim zaposlenicima i čim manje slabih karika. Ljudi su ti koji i održavaju sustave i brinu za njihovu sigurnost, ali su i ti koji potencijalno ostavljaju nečuvane ulaze za napadače. No treba i napadače gledati također samo kao ljude te znati da i za najbolje čuvan sustav postoji netko pametniji tko može provaliti u njega. Dakle, kao što je i Benjamin Franklin rekao, ništa na svijetu nije sigurno osim smrti i poreza pa čak ni banke.

Popis slika

Literatura

[1] *Nato Open Source Intelligence Handbook,* V1.2, 2001.

[2] HASSAN, N. A. *Digital Forensics Basics*. Berkley: Apress, 2019.

[3] LAYTON, R., WATTERS, P. A. *Automating Open Source Intelligence: Algorithms for OSINT,* Amsterdam*:* Elsevier Science, 2015.

[4] EYSENBACH, G., TILL, J. E. Ethical Issues In Qualitative Research On Internet Communities. *BMJ (Clinical Research Ed.),* 323(7321), (2001), 1103–1105.

[5] AKHGAR, B, BAYERL, P. S., SAMPSON, F. *Open Source Intelligence Investigation: From Strategy to Implementation,* Švicarska: Springer, 2016.

[6] HASSAN, N. A., HIJAZI, R. *Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence:* Berkley: Apress, 2018.

[7] https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ preuzeto 8. ožujka 2020.

[8] CHAUHAN S., PANDA N. K. *Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques*, Massachusetts: Syngress, 2015.