UTVRĐIVANJE SIGURNOSNIH RANJIVOSTI NA UREĐAJIMA POVEZANIMA NA INTERNET U ZEMLJAMA EU KORIŠTENJEM ALATA SHODAN.IO

Lovrić, Ema

VISOKO UČILIŠTE ALGEBRA

ZAVRŠNI RAD

UTVRĐIVANJE SIGURNOSNIH RANJIVOSTI NA UREĐAJIMA POVEZANIMA NA INTERNET U ZEMLJAMA EU KORIŠTENJEM ALATA SHODAN.IO

Ema Lovrić

Zagreb, veljača 2023.

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

U Zagrebu, 28.2.2023..

Predgovor

Zahvaljujem svom mentoru, profesoru Zlatanu Moriću na uloženom vremenu i trudu prilikom izrade završnog rada.

Zahvaljujem i svim profesorima Visokog učilišta Algebra koji su svojim znanjima i vještinama doprinijeli mojem obrazovanju.

A Gradišćanska 24, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

Temeljem članka 8. Pravilnika o završnom radu i završnom ispitu na preddiplomskom studiju Visokog učilišta Algebra sačinjena je ova

Potvrda o dodjeli završnog rada

kojom se potvrđuje da studentica Ema Lovrić, JMBAG 0321012370, OIB 63788860133 u šk. godini 2021./2022., studij: Primjenjeno računarstvo - Preddiplomski studij, smjer: Sistemsko inženjerstvo, od strane povjerenstva za provedbu završnog ispita, dana 15.02.2022. godine, ima odobrenu izradu završnog rada

s temom: **Utvrđivanje sigurnosnih ranjivosti na uređajima povezanima na Internet u zemljama EU korištenjem alata shodan.io**

i sažetkom rada: Ovim radom želi se prikazati broj ranjivih, odnosno izloženih uređaja povezanih na Internet unutar EU. Radom se želi pružiti uvid u to koliko pojedine države unutar EU ulažu u sigurnost

svojih sustava te istaknuti važnost održavanja određene razine sigurnosti. Ishod

završnog rada bi trebao potaknuti korisnike da budu svjesni ranjivosti svojih uređaja i njihova okruženja te da teže održavanju visoke razine sigurnosti istih.

Mentor je: Zlatan Morić.

Odobrenjem završnog rada studentici je omogućen upis kolegija "Izrada završnog projekta/Praksa" te je sukladno članku 8. Pravilnika o završnom radu i završnom ispitu dužan najkasnije do početka nastave ljetnog semestra u sljedećoj školskoj godini, uspješno obraniti završni rad uspješnim polaganjem završnog ispita.

U protivnom studentica može zatražiti novog mentora/icu i temu te ponovo upisati kolegij "Izrada završnog projekta/Praksa" budući da rad koji nije predan i obranjen na završnom ispitu u roku određenom Pravilnikom završnom radu i završnom ispitu prestaje vrijediti. Izrada novog završnog rada se izvodi sukladno rokovima određenima za školsku godinu u kojoj je studentici određen novi mentor/ica i dodijeljen novi završni rad.

Potpis studentice: Potpis mentora: Potpis predsjednika povjerenstva:

Sažetak

Razvojem tehnologija i rastom broja uređaja povezanih na Internet, smanjuje se računalna sigurnost te je sve veći izazov osigurati sustave i zaštiti osobne podatke. OSINT inteligencijom prikupljaju se podaci sa svih javno dostupnih izvora podataka što čini velike količine podataka dostupne svima, kako sigurnosnim stručnjacima, tako i napadačima. Koristeći OSINT alat Shodan u radu su prikazane ranjivosti pojedinih protokola, uređaja i servisa u državama Europske Unije te je odrađena komparacija dobivenih rezultata kako bi se prikazalo koliko pojedine države ulažu u računalnu sigurnost. Cilj rada je podići svijest o sigurnosnim propustima kako bi ih korisnici sustava mogli detektirati i zakrpati.

Ključne riječi: OSINT, ranjivost, otvoreni izvori podataka, prikupljanje informacija, Shodan

Abstract

With the development of technologies and the growth of numbers of devices connected to the Internet, cyber security is decreasing, and it has become a real challenge to cesure systems and to protect personal data. OSINT intelligence collects data from all publicly available and open-source databases, which makes enormous amounts of data available to everyone, including cyber security experts and attackers. Using the OSINT tool Shodan, this paper shows the vulnerabilities of certain protocols, devices and services in the European Union countries. Except the analysis, the paper covers comparison of the obtained results to show how much certain countries invest in cyber security. The goal of this paper is to increase the awareness about cyber security flaws so that the users can detect them and protect them.

Key words: OSINT, vulnerability, open-source data, collecting informations, Shodan

Sadržaj

1. Uvod

Jedan od najvećih izazova današnjeg vremena, koje prati ubrzani razvoj tehnologije, je zaštiti privatne informacije te se osigurati od krađe podataka. Svakodnevnim korištenjem interneta u bilo koje svrhe, korisnici ostavljaju tragove u obliku privatnih podataka. Količina osobnih podataka na internetu je enormna i za sobom povlači određene sigurnosne prijetnje. Prilikom pristupanja pojedinim Internet stranicama i korištenjem društvenih mreža, blogova i foruma, podaci na internetu ostaju zapamćeni i povezuju se s pojedinim osobama, organizacijama i uređajima. Sukladno tome, bilo tko može pronaći velik broj informacija o svakom pojedincu ili organizaciji koristeći posebnu vrstu inteligencije – OSINT (engl. *Open Source Intelligence*). OSINT je vrsta inteligencije koja prikuplja informacije iz javno dostupnih izvora podataka. Rastom broja korisnika na internetu i količinom dostupnih informacija, razvio se broj alata koji automatizmom prikupljaju informacije iz raznih izvora te rade poveznice između pojedinih entiteta. Jedan od OSINT alata je Shodan koji pretraživanjem uređaja na internetu skenira IP adrese uređaje i sve dostupne podatke za njih. Kroz ovaj rad predstavljen je koncept OSINT-a te je prikazana izloženost informacija, odnosno ranjivost pojedinih protokola, vrsta uređaja i servisa u zemljama Europske Unije. Analizom podataka odrađena je komparacija dobivenih rezultata te su predložene sigurnosne preporuke za pojedine ranjivosti. Cilj rada je istaknuti koliko pojedine države ulažu u sigurnost uređaja izloženih na Internet te skrenuti pažnju na eventualne nedostatke.

2. Testiranja temeljena na otvorenim izvorima podataka OSINT

OSINT je vrsta inteligencije koja se bavi prikupljanjem informacija i podataka iz besplatnih i javno dostupnih izvora podataka. Pojam OSINT-a pojavio se osamdesetih godina i tada se odnosio na konvencionalne načine prikupljanja informacija kao što su novine, televizija, radio ili poslovna izvješća.

Informacije se prikupljaju sa javno dostupnih izvora podataka i iz izvora otvorenog koda, kao što su blogovi, forumi ili društvene mreže. Razvojem društvenih mreža i njihovom popularizacijom, počela se razvijati vrsta inteligencije posebno orijentirana na društvene mreže – SOCINT.

Razvojem Interneta i njegovih mogućnosti, razvijali su se i način prikupljanja podataka. Najčešće se informacije prikupljaju koristeći tražilice, kao što su Google, Bing, Yahoo i drugi. Osim klasičnog pretraživanja, informacije se prikupljaju i putem *deep weba* i *dark weba*.

Deep web predstavlja svaku stranicu koja nije indeksirana na web pretraživačima, odnosno svaku web stranicu na koju se potrebno prijaviti korisničkim podacima. *Dark web* omogućuje sigurno pretraživanje i podrazumijeva svaku stranicu za čiji je pristup potreban tor.

Svaka informacija prikupljena putem OSINT je postavljena na Internet od strane pojedinca ili organizacije. OSINT sadrži nekoliko koraka koji se ciklički ponavljaju. Prvi korak je planiranje, odnosno upoznavanje mete te kako doći do nje i zašto. Nakon toga slijedi najbitniji proces u kojemu se prikupljaju informacije o meti te se ti podaci procesiraju i interpretiraju te se na kraju analiziraju.

Pri procesu planiranja i pripremanja, u obzir se uzima da je svaki pristup Internetu i web stanicama vidljiv te trajno zabilježen. Mete o kojima se nastoje prikupiti informacije, mogu biti svjesne radnji te mogu utjecati na sadržaj koji se servira, što potencijalno dovodi do serviranja lažnih informacija ili uskraćivanja usluge. Obzirom da se za OSINT koriste lažni korisnički računi, nerijetko dolazi do brisanja istih. Zbog toga se u procesu planiranja kreira *Sock Puppet* – lažni online identitet.

Korištenje *sock puppeta* nužan je uvjet jer se nastoji izbjeći povezivanje OSINT-a sa stvarnim osobama kako bi ih se zaštitilo. Pri stvaranju identiteta nastoji se ne privlačiti pozornost, odnosno uklopiti se u sadržaj web stranice s koje se prikupljaju podaci. Legitimnost korisničkih računa održava se

U procesu planiranja treba obratiti pozornost na korištenje izoliranog sustava koji će biti odvojen od stvarne mreže i stvarnih podataka da bi se izbjegla kompromitacija internog sustava. Virtualiziranim uređajem izbjeći će se potencijalna zaraza malicioznim programima. Obzirom da se radi o prikupljanju velikih količina podataka, sustav će lako prepoznati velike količine mrežnog prometa prema samo jednom odredištu, odnosno prema samo jednoj IP adresi. Da bi se izbjegla navedena problematika, promet se rasprostranjuje na tisuće IP adresa koje će oponašati veću posjećenost web stranice.

U procesu prikupljanja podataka, dozvoljeno je samo njihovo praćenje i prikupljanje, što znači da svako sudjelovanje u njihovoj izmjeni ili bilo kakav utjecaj na njih nije dozvoljen. Svi podaci moraju imati svoje podrijetlo, odnosno mora biti vidljivo i poznato kako i kada se došlo do njih. U te svrhe se koriste pojedini alati koji automatski prate i označavaju podatke. Navedeni podaci su *hashirani* i pohranjeni u sigurne i zaštićene baze podataka, čime se u svakom trenu može dokazati postojanost i integritet. Da bi se povećala efikasnost OSINT-a, kreirani su botovi koji prikupljaju podatke. Time je omogućeno prikupljanje puno većih količina podataka i brže procesuiranje istih. Korištenjem botova broj posjećenih web stranica značajno raste, kao i promet koji se generira. Zbog toga raste potreba za većim brojem IP adresa. Prilikom prikupljanja podataka, obraća se pozornost na izbjegavanje stvaranja uzoraka ponašanja, kako bi se izbjeglo prepoznavanje OSINT-a.

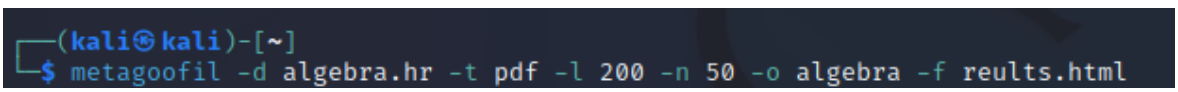
Osim Shodan alat koji je korišten u ovom projektu, postoji niz drugih alata koji se koriste za prikupljanje informacija iz javno dostupnih izvora podataka te su korišteni od strane stručnjaka za penetracijsko testiranje, ali i samih napadača. Neki od poznatijih i najčešće korištenih alata su Maltego, TheHarvester, SpiderFoot, Google Dorks i Metagoofil.

Maltego [16] je OSINT alat za prikupljanje podataka iz javno dostupnih izvora podataka. Prednost Maltego alata je što za svaki ulazni podatak, kao što je e-mail adresa, ime, IP adresa, organizacija ili Internet stranica pretražuje razne baze podataka kako bi prikupio što više podataka o danoj informaciji. S navedenim prikupljenima informacijama, alat obrađuje podatke i kreira poveznice između velikog broja prikupljenih podataka te navedene poveznice vizualno prikazuje. Sve kompleksne poveznice pojedinih entiteta prikazane su na

jednostavan način što korisnicima uvelike olakšava razumijevanje pretraženih informacija. Maltego alat jedan je od najčešće korištenih alata za penetracijsko testiranje u fazi izviđanja gdje penetracijski testeri nastoje prikupiti što je više moguće informacija o sustavu koji namjeravaju napasti.

SpiderFoot je još jedan od OSINT alata koji nudi automatsko prikupljanje informacija sa različitih izvora podataka. Ovaj alat otvorenog koda koristi više od 100 javno dostupnih izvora pomoću kojeg prikuplja informacije i povezuje ih na jednom mjestu. Prednost ovog alata je vrlo dobra pružena dokumentacija koja ne samo da korisnicima omogućuje jednostavnu instalaciju alata i pokretanje alata, nego im omogućuje razumijevanje samog alata, njegovih procesa i svojstava te je dostupan na svim operacijskim sustavima. SpiderFoot alat, kao i drugi OSINT alati, prikuplja i procesuira podatke o domeni, IP adresama, DNS zapisima, mreži, servisima i mnogim drugim informacijama. Prilikom penetracijskog testiranja, SpiderFoot uvelike olakšava prikupljanje informacija i njihovu analizu.

Metagoofil [24] je OSINT alat za prikupljanje informacija koji prikuplja meta podatke iz javno dostupnih dokumenata, kao što su PDF, DOC, XLS i PPT dokumenti. Metagoofil je alat otvorenog koda koji je besplatan. Za prikupljanje javno dostupnih informacija, Metagoofil prvo pretražuje dostupne dokumente kroz Google, zatim ih lokalno pohranjuje te pomoću alata Hachoir i PdfMiner izvlači meta podatke iz tih dokumenata. Kao i ostali alati, Metagoofil prikuplja pojedine informacije o zadanom entitetu te ih povezuje s određenim korisničkim imenima, verzijama softvera, servisima i uređajima. Instalacija alata i njegovo korištenje je vrlo jednostavno te je za potrebe prezentacije, alat instaliran na Kali Linux virtualnoj mašini. Pokretanjem metagoofil naredbe navode se parametri pretraživanja, odnosno navodi se domena koja se pretražuje, vrste datoteka povezane s tom domenom te količina informacija koja se želi pregledati i preuzeti. Slika 2.1 prikazuje naredbu kojom se pretražuju pdf datoteke o domeni algebra.hr. Parametri koji su dodatno specificirani su maksimalan broj rezultata koji će se pretraživati (-l 200) i broj datoteka koji će se preuzeti (-n 50) te će preuzete datoteke biti pohranjene u direktorij algebra i rezultati će biti spremljeni u html file results.html.



Slika 2.1 Metagoofil naredba

3. Pregled istraživanja u području testiranja baziranog na otvorenim izvorima podataka

2017. godine napravljeno je istraživanje „Vulnerability Scanning of IoT Devices in Jordan Using Shodan“[7]. Sukladno širenju popularnosti Interneta Stvari i IoT (engl. *Internet of Things*) uređaja, korisnici nisu svjesni ili zanemaruju činjenicu da su to uređaji koji su izloženi Internetu i sukladno tome da su sve njihove informacije javno dostupne. Kroz rad se nastoji podići svjesnost o ranjivosti IoT uređaja i potencijalnom gubitku privatnosti i sigurnosti te potaknuti stanovnike Jordana na brigu o istome. Istraživanjem je zaključeno da napadi na IoT uređaje imaju dva potencijalna ishoda -

Rad objedinjuje istraživanje ranjivosti IoT uređaja uz statističku analizu u svibnju 2017. godine. Istraživanjem je otkriveno 40849 IoT uređaja od kojih 9,2% ima omogućen UPnP (engl. *Universal Plug and Play*). Omogućavanjem UPnP-a uređaj automatski propušta portove i postaje vidljiv drugim uređajima u mreži, kao i IoT malicioznih softvera. Analizom nekih od najučestalijih servisa na Internetu pronađeno je da od svih uređaja koji imaju omogućen HTTP, 62% od njih ima uspješne HTTP konekcije. 41% uređaja koji koriste SMB protokol ima onemogućenu autentikaciju i 26% njih ima mogućnost anonimnog prijavljivanja, što dovodi do potencijale kompromitacije dijeljenih podataka. U radu je navedeno da je korištenje Telneta, koji ne kriptira podatke, dva puta popularnije, odnosno učestalije od SSH-a, čije je korištenje sigurno. Analizom ostalih servisa, zaključeno je da je samo 8% FTP konekcija uspješno te da je za 35% RDP uređaja kreirana snimka zaslona. Pretraživanjem uređaja u Jordanu, pronađeno je 16 uređaja izloženih Ticketbleed ranjivosti te 41 uređaj izložen Heartbleed ranjivosti.

Kao rezultat odrađene analize, autori predlažu praćenje preporuka stručnjaka, što podrazumijeva izbjegavanje ranjivih servisa i onemogućavanje nekorištenih servisa. Korisnicima se savjetuje ažuriranje uređaja i njihovih servisa te primjereno podešavanje uređaja i autentikacije.

Istraživanjem *„Vulnerability Analysis of Internet Devices from Indonesia Based on Exposure Data in Shodan“* [3] prikupljane su informacije za sve ASN-ove (engl. *Autonomous System Number*) u Indoneziji koristeći alat Shodan. Cilj rada bio je skrenuti pozornost organizacijama koje upravljaju ASN-ovima na izloženost uređaja povezanih na

Internet u Indoneziji te osvijestiti o ranjivostima koje ti uređaji imaju. Obzirom da u Indoneziji postoji velik broj IP adresa, kategoriziranih u 1699 ASN-ova, u radu su posebnom metodom grupiranja, IP adrese, odnosno AS-ovi podijeljeni u četiri kategorije ovisno o razini izloženosti. Za najveći broj AS-a, njih 1075 ne postoje nikakve informacije na Shodanu. U kategoriji niske razine izloženosti smješteno je 614 AS-a, a kategoriji srednje razine izloženosti pripada 9 AS-a. Samo jedan AS se nalazi u kategoriji visoke razine izloženosti.

U istraživanju rada skenirani su svi ASN-ovi koristeći bash skriptu koja automatski skenira sve subnete za svaki ASN. Za 624 ASN-a o kojima postoje informacije na Shodanu, odrađeno je 289 715 upita te su skeniranjem pronađeni i analizirani podaci o portovima, servisima, domenama, IP adresama i operacijskim sustavima. Od pronađenih skoro 12 tisuća jedinstvenih portova, 13,95% pronađenih informacija odnosi se na HTTP protokol, port 80. Prikupljene informacije o operacijskim sustavima prikazuju da 35,87% uređaja koristi Linux 3.x, nakon čega slijedi Windows Server 2012 R2 Standard sa znatno manjih 9,45%. Daljnjom analizom je pronađeno 98 152 informacija o servisima koje su pretežno raspoređene po sljedećim servisima: MikroTik bandwidth-test server (33,37%), apache httpd(16,54%) i OpenSSH (7,78%). Za upite o domenama istaknuti su rezultati dvije top-level domene – od ukupnih 3350, njih 1881 su jedinstvene .id domene i 1242 .com domene. Istraživanje je zaključeno pronalaskom 145 543 jedinstvenih IP adresa i 790 jedinstvenih organizacija.

4. Pregled alata i područja primjene u OSINT

Shodan.io je pretraživač (engl. *search engine*) koji u pozadini koristi bazu podataka svih javno dostupnih IP adresa te prikuplja podatke o svim uređajima povezanim na Internet. Uz pretragu baze podataka uređaja povezanih na Internet, Shodan nudi nekoliko dodatnih alata koji sudjeluju u kvalitetnijoj obradi podataka.

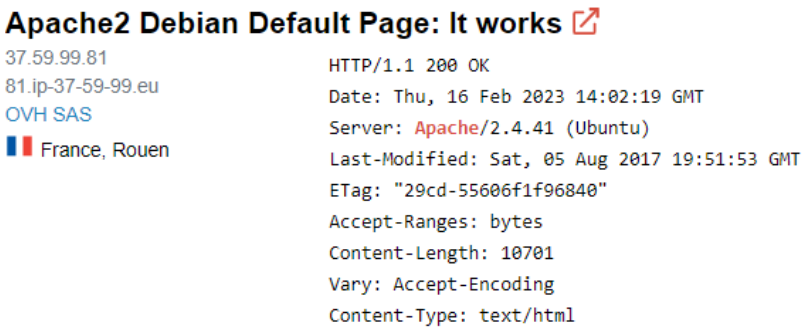
4.1. Shodan Search Query

Shodan je alat [1] koji omogućuje korisnicima da pretražuju Internet stvari, odnosno mrežu stvorenu od uređaja spojenih na Internet. Prilikom izvršavanja Shodan search querya primarno se dohvaća samo natpis (engl. *banner)*, odnosno ne pretražuju se meta podaci.

Dohvaćanje natpisa (engl. *Banner grabbing)* je metoda koja se koristi za dobivanje informacija o uređaju, odnosno informacije o servisima, vrsti i verziji softvera i operacijskom sustavu, na način da pretražuje uređaje povezane na Internet i skenira otvorne portove kao što su HTTP (80), FTP (21) i SMB(445).

Banner grabbing koristi alate za uspostavu konekcije s uređajem, kao što su telnet, nmap, wget i curl. Kada se uspostavi konekcija s uređajem, uređaju se pošalje bilo kakva vrsta zahtjeva (engl. *request*), na što udaljeni uređaj odgovara s *banner* porukom.

Iz *banner* poruke mogu se saznati i ranjivosti uređaja.



Slika 4.1 Banner poruka

Za primjer je izvršen *search query* „Apache“ koji dohvaća rezultate o korisnicima Apache servera. U gore navedenom primjeru vidljiva je *banner* poruka iz koje se mogu iščitati informacije o operacijskom sustavu i zadnjim izmjena na web stranici.

4.2. Shodan Filters

Za pregled meta podataka uređaja i servisa nije dovoljan search query, nego se za to koriste određeni Shodan filteri [1] koji pružaju specifičnije rezultate pretraga. U ovom dijelu rada prikazat će se sintaksa i pravila korištenja filtera.

Svi filteri pišu se u obliku *„ime filtera“ : „vrijednost*“.

Dolje navedena tablica prikazuje neke od najčešćih filtera, koji se kasnije zajedno kombiniraju kako bi se izvodila kompleksnija pretraživanja.

Tablica 4.1 Primjer Shodan filtera

Filter Name	**Description**	**example**
country	2-letter country code	country:HR
city	Name of the city	city:Zagreb
os	Operating system	os:windows
org	Organization assigned the netblock	org:google
port	Port number for the service	port:80

Ukoliko se radi o vrijednostima koje se sastoje od dvije ili više riječi, tada se te riječi stavljaju u navodnike:

City:“Novi Vinodolski“

Svaki filter koji prije imena filtera ima oznaku – označava da se navedena vrijednost zanemaruje, odnosno da ju želimo isključiti iz pretrage. Primjerice, filter svih IoT uređaja u Hrvatskoj, osim u Zagrebu:

Country:HR -City:Zagreb

Kao što je ranije navedeno, filteri se mogu međusobno kombinirati. Primjerice, ako se radi pretraga uređaja/servisa u Hrvatskoj, koji rade na HTTP ili HTTPS protokolima, u filter će se dodati portovi 80 i 443.

Country:HR port:80,443

4.3. Shodan Exploit

Shodan Exploit je alat [1] koji prikuplja ranjivosti i *exploite* iz drugih baza podataka, kao što su CVE, Exploit DB i Metasploit. Za Shodan Exploit kreirani su posebni filteri: *author, description, platform* i *type*, ili se može pretraživati po ključnim riječima.

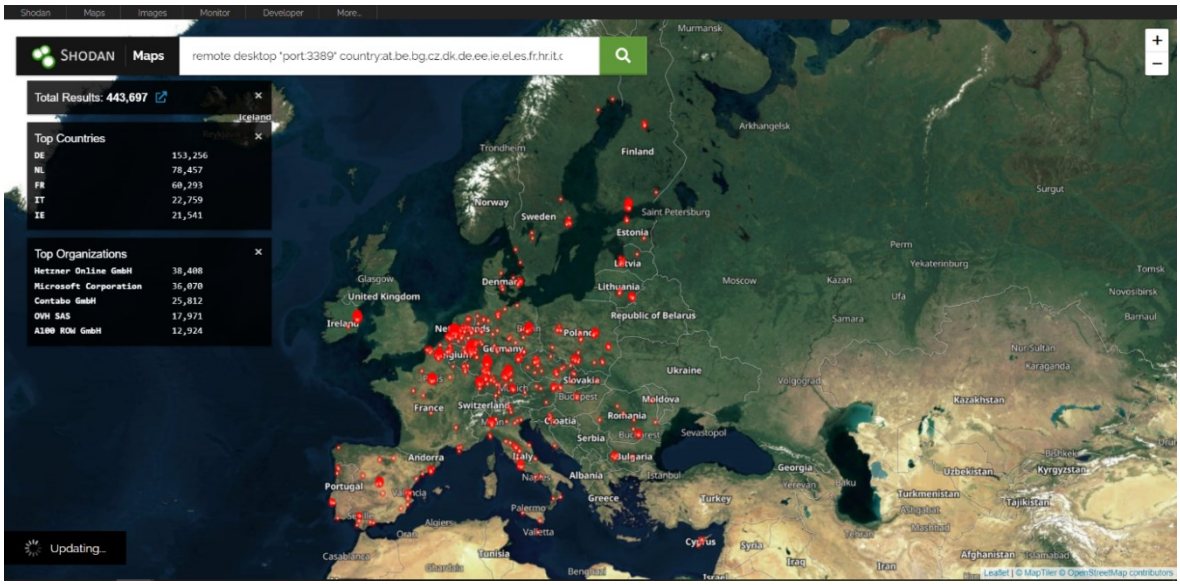
Sljedeća slika prikazuje pretragu Memcached UDP ranjivosti, koja preusmjerava na službenu Exploit DB stranicu.

Slika 4.2: Shodan Exploit - Memcached UDP ranjivost

Ovim alatom omogućeno je pretraživanje velikog broja ranjivosti/exploita na jednom mjestu.

4.4. Shodan Maps i Shodan Images

Za svaku izvršenu pretragu, odnosno za svaki dobiveni rezultat, Shodan nudi mogućnost vizualnog prikaza na zemljovidu kroz alat Shodan Maps [1]. Sljedeća slika prikazuje otvorene RDP (engl. *Remote Desktop Protocol*) portove za zemlje EU.



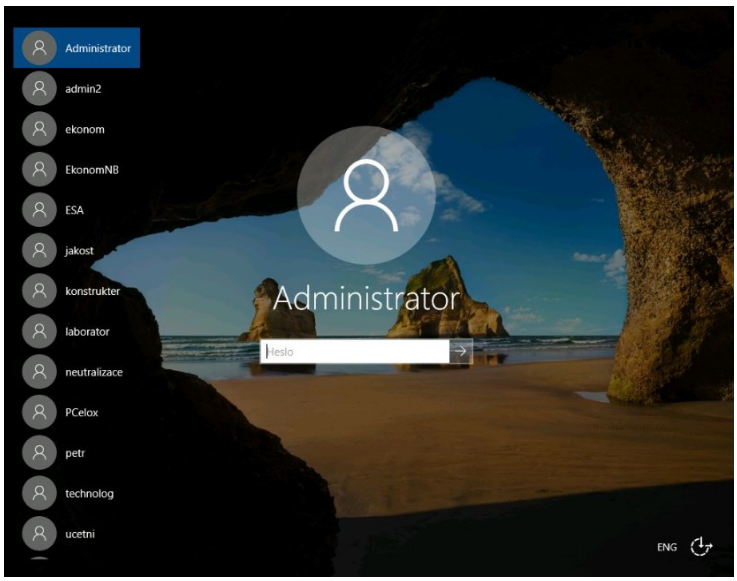
Slika 4.3 Satelitski prikaz pretrage Remote Desktop portova

Shodan Maps [1] alat nudi nekoliko mogućnosti prikaza dobivenih rezultata: Satellite, Streets i Pirate. Za izradu ovog rada nije dobivena licenca koja omogućuje prikaz navedenih stilova, nego je omogućen samo Satellite stil te je on i demonstriran.

Shodan Images alat uz rezultate pretraga, nudi i odgovarajuće snimke zaslona. Za Shodan Images koristi se zasebni filter:

Has_screenshot:true

Nastavno na prethodnu pretragu otvorenih Remote Desktop portova za zemlje EU, pronađena je sljedeća snimka zaslona.



Slika 4.4: Shodan Images za otvorene Remote Desktop portove

5. Analiza sigurnosnih ranjivosti protokola i uređaja u EU državama

Kroz sljedeće poglavlje će se korištenjem Shodan alata odraditi analiza najčešće korištenih i općepoznatih protokola, uređaja i ranjivih servisa u državama Europske Unije. Za svaku kategoriju odrađena je komparacija u odnosu na države te su predloženi preventivni načini zaštite od napada.

5.1. FTP, RDP, SMB, Telnet, SSL

U ovom dijelu rada odrađena je analiza jednih od najčešće korištenih protokola – FTP, RDP, SMB, Telnet i SSL. Neki od navedenih protokola uopće ne koriste enkripciju te se njihovo korištenje ne savjetuje, dok su drugi protokoli ranjivi samo po nekim parametrima te se ispravnom konfiguracijom može zaštiti cijeli sustav.

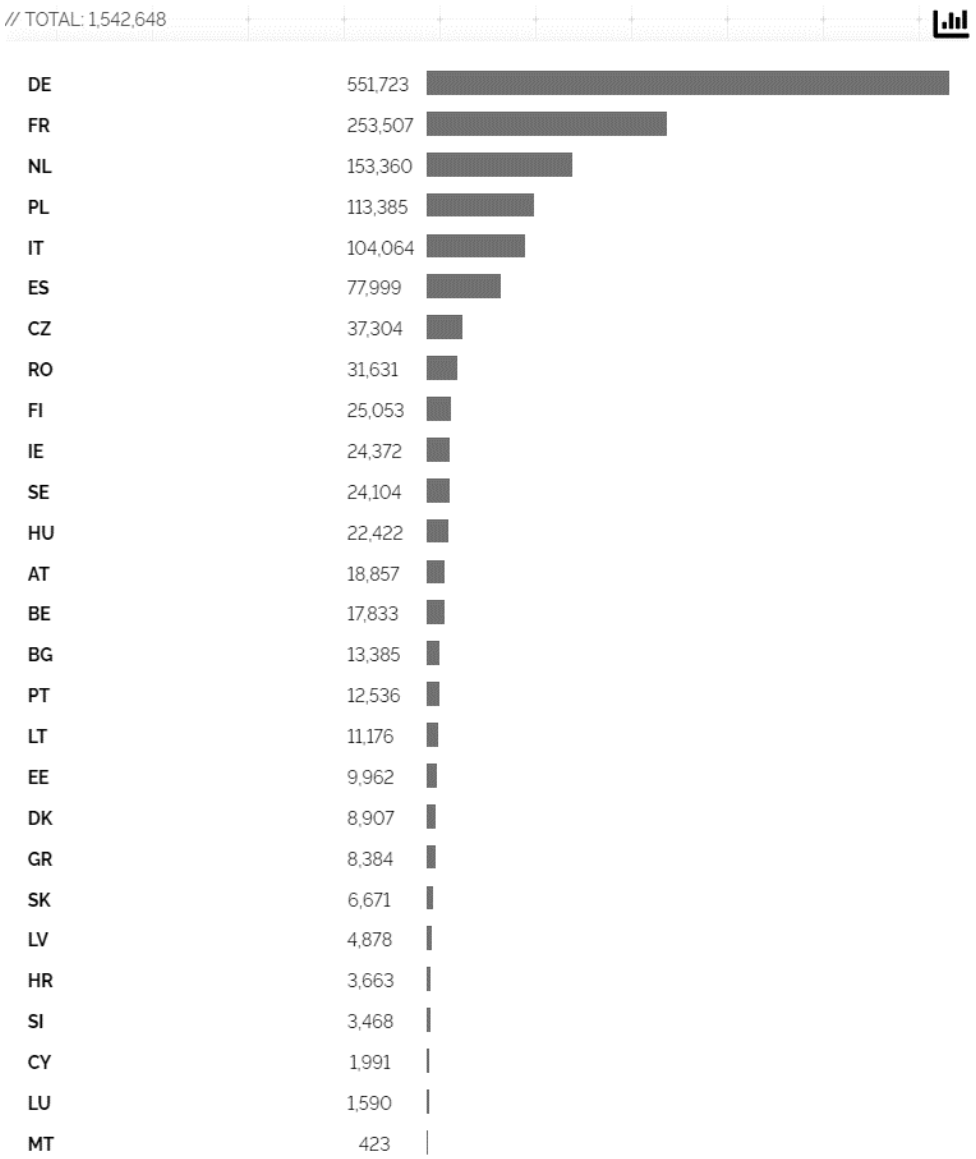
5.1.1. Analiza ranjivosti protokola

FTP (engl. *File Transfer Protocol*) je protokol [17] aplikacijskog sloja OSI modela za prijenos datoteka između uređaja mrežnim putem, koristeći TCP/IP konekcije. Protokol radi na portu 21. Kod prijenosa podataka FTP-om, svi podaci se prenose u nešifriranom tekstu (engl. *clear text*), odnosno podaci nisu kriptirani, a to uključuje i korisničke podatke za prijavu, kao i same datoteke koje se prenose. Korištenjem FTP-a promet se lako može presresti i podaci mogu biti dostupni napadaču.

Kroz Shodan je napravljena analiza uređaja u zemljama EU koji imaju otvoren port 21:

port:21 country:at,be,bg,hr,cy,cz,dk,ee,fi,fr,de,gr,hu,ie,it,lv,lt,lu,mt,nl,pl,pt,ro,sk,si,es,se

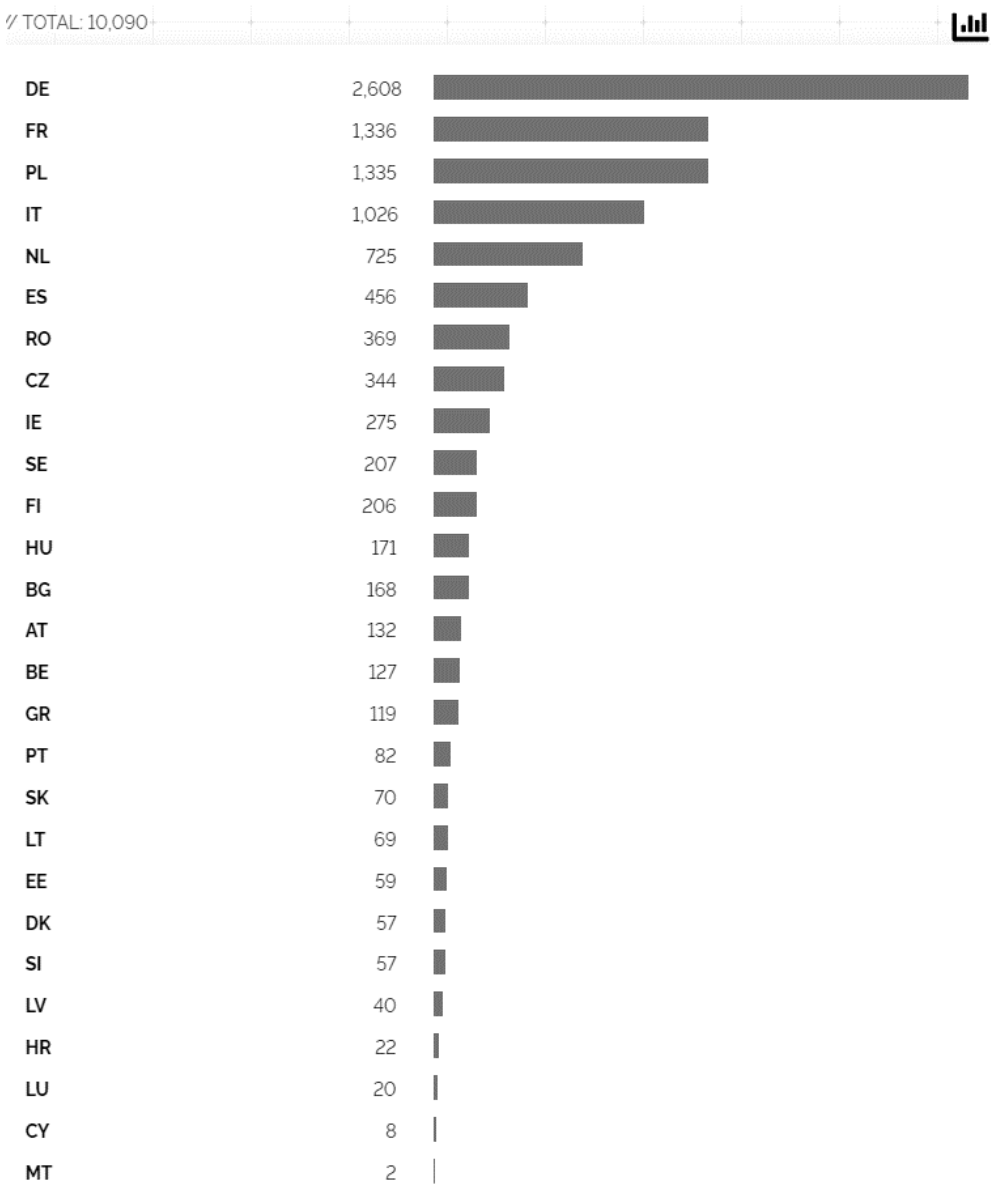
Ukupni broj rezultata za navedenu pretragu iznosi 1 542 546. Sljedeća slika prikazuje poredak rezultata po državama EU.



Slika 5.1 Otvoreni FTP portovi

Pojedini FTP serveri nude mogućnost anonimnih prijava, što iz sigurnosnih aspekata značajno ugrožava povjerljivost podataka. Od navedenih 1 542 648 otvorenih FTP portova analizirano je koliko ih ima mogućnost anonimnog pristupa. [10]

"220" "230 Login successful." port:21 port:21
country:at,be,bg,hr,cy,cz,dk,ee,fi,fr,de,gr,hu,ie,it,lv,lt,lu,mt,nl,pl,pt,ro,sk,si,es,se



Slika 5.2: Otvoreni FTP portovi - mogućnost anonimnog pristupa

RDP (engl. *Remote Desktop Protocol*) je Microsoftov mrežni protokol koji omogućuje korisnicima spajanje na udaljena računala. RDP funkcionira na način da se klijent unosom korisničkih podataka (korisničko ime/IP adresa i lozinka) spoji na udaljeno računalo. RDP radi na TCP i UDP portu 3389.

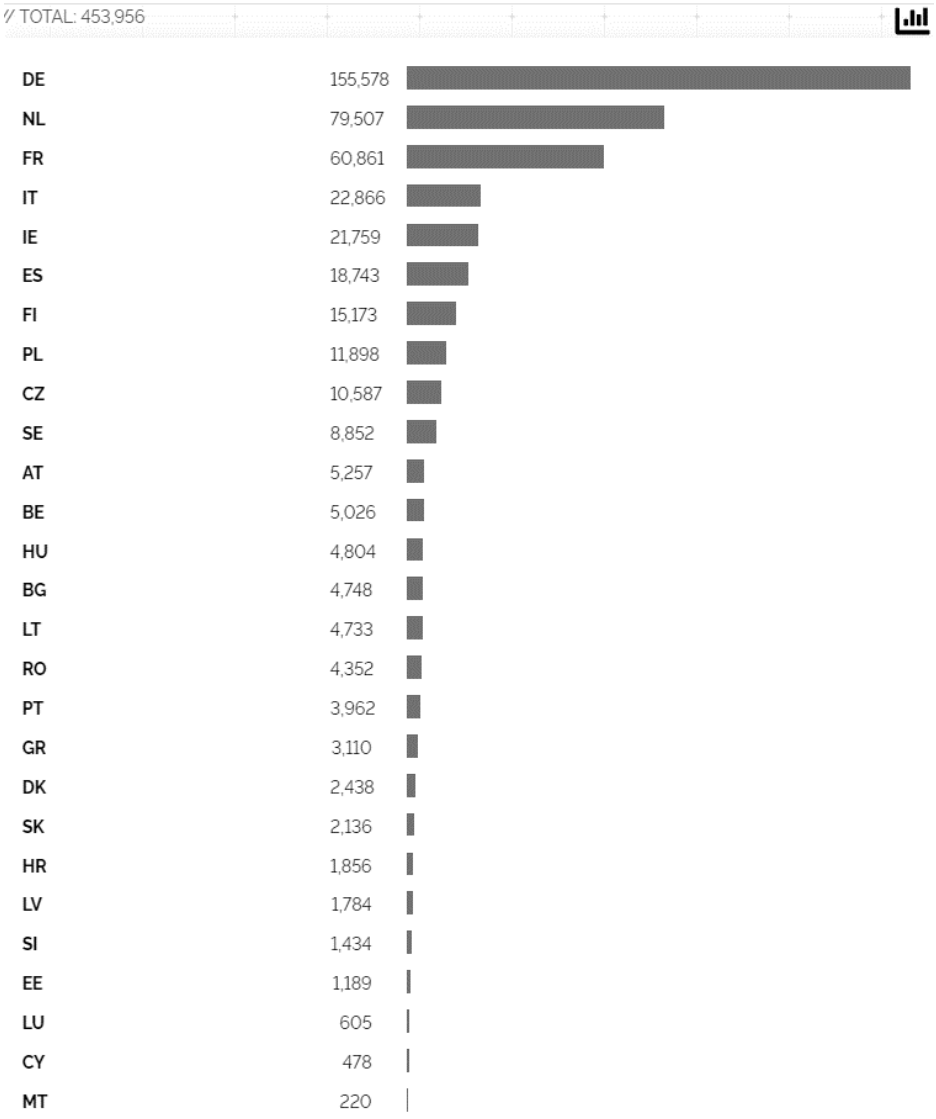
Ukoliko napadač zna IP adresu udaljenog računala, *BruteForce* napadom, kojim se isprobavaju razne kombinacije lozinki u nadi da će napadač pogoditi ispravnu lozinku, moguće je odgonetnuti ju i spojiti se na udaljeno računalo.

Kroz Shodan je napravljena pretraga otvorenih RDP portova (3389) u zemljama EU, koristeći sljedeći upit.

remote desktop "port:3389"

country:at,be,bg,hr,cy,cz,dk,ee,fi,fr,de,gr,hu,ie,it,lv,lt,lu,mt,nl,pl,pt,ro,sk,si,es,se

Sveukupni broj skeniranih portova iznosi 453 964.



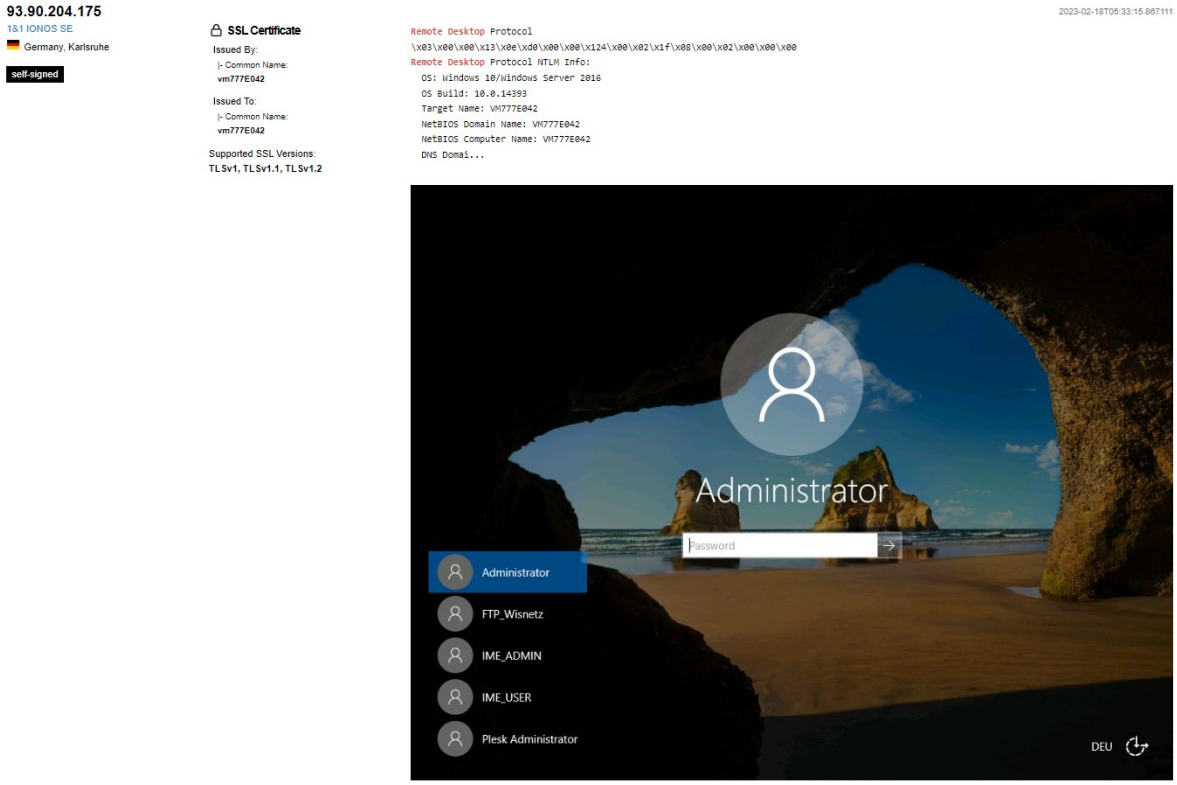
Slika 5.3: Otvoreni RDP (3389) portovi

Bitno je napomenuti da unatoč tome što su portovi otvoreni, većina dobivenih rezultata je dodatno zaštićena Windows prijavom na korisničke račune.

Pretragom rezultata uočeno je da je pomoću alata Shodan Images na mnogim uređajima uspješno snimljena snimka zaslona.

remote desktop "port:3389" has_screenshot:true

country:at,be,bg,hr,cy,cz,dk,ee,fi,fr,de,gr,hu,ie,it,lv,lt,lu,mt,nl,pl,pt,ro,sk,si,es,se



Slika 5.4 Snimka zaslona uređaja pristupanog RDP-om

Od pronađenih 453 956 rezultata, na 162 241 skeniranih uređaja, odnosno 35,74% snimljena je snimka zaslona.

SMB (engl. *Server Message Block*) protokol [18] je mrežni protokol za dijeljenje podataka koji omogućuje dijeljenje podataka, kao i pristup podacima, datotekama i uređajima u mreži. SMB je protokol aplikacijskog sloja OSI modela koji radi na TCP/IP konekciji (port 445) i radi po principu klijent – server.

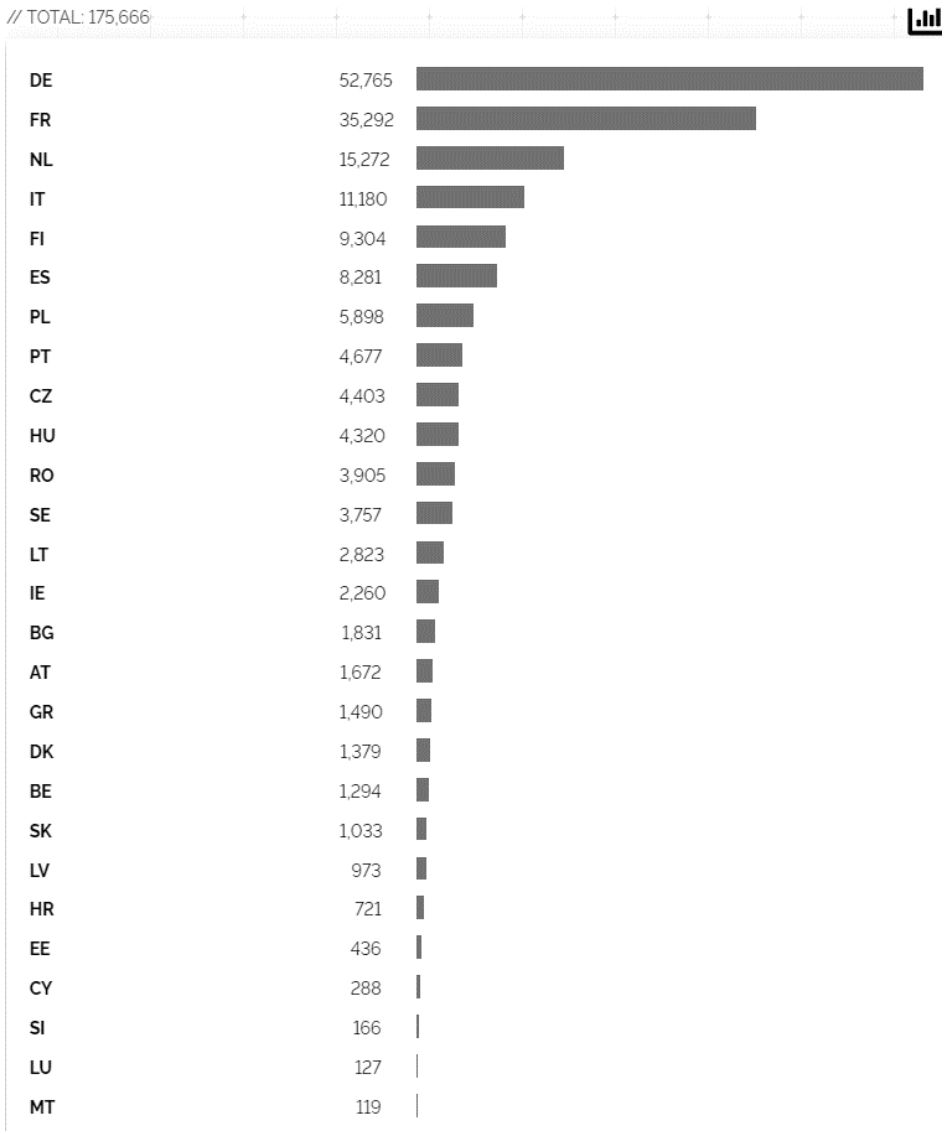
Primarni korak za sigurno korištenje SMB protokola je podešavanje autentikacije i enkripcije na serverskoj strani. U suprotnom, napadaču mogu biti dostupni svi dijeljeni podaci.

Kroz Shodan je napravljena analiza uređaja koji imaju otvorene portove 445 u zemljama EU.

smb port:445

country:at,be,bg,hr,cy,cz,dk,ee,fi,fr,de,gr,hu,ie,it,lv,lt,lu,mt,nl,pl,pt,ro,sk,si,es,se

Navedeni filter prikazuje 175 666 pronađena uređaja.



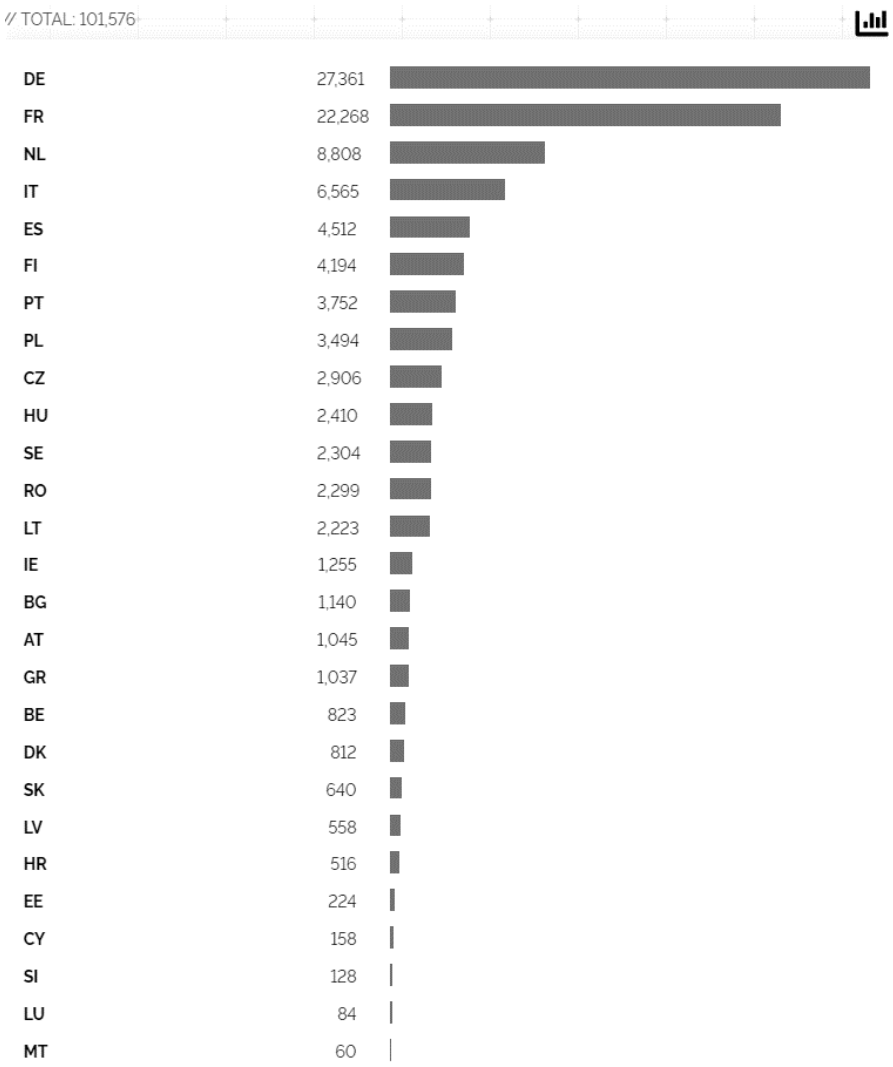
Slika 5.5: Otvoreni SMB (445) portovi

Kroz određeni niz godina pojavljivali su se sigurnosni napadi „Remote Code Execution (RCE)“ koji su iskorištavali ranjivosti SMB protokola prve verzije (SMBv1). Pri iskorištavanju navedenih ranjivosti, napadač bi dobio mogućnost izvršavanja kodova na kompromitiranim serverima. Nakon navedenih napada, ranjivosti su zakrpane, ali se korištenje SMBv1 protokola i dalje smatra rizičnim te se ne preporučuje.

Od prethodno dobivenih rezultata provjereno je koliko uređaja koristi prvu verziju SMB-a [10].

"SMB Version: 1" port:445

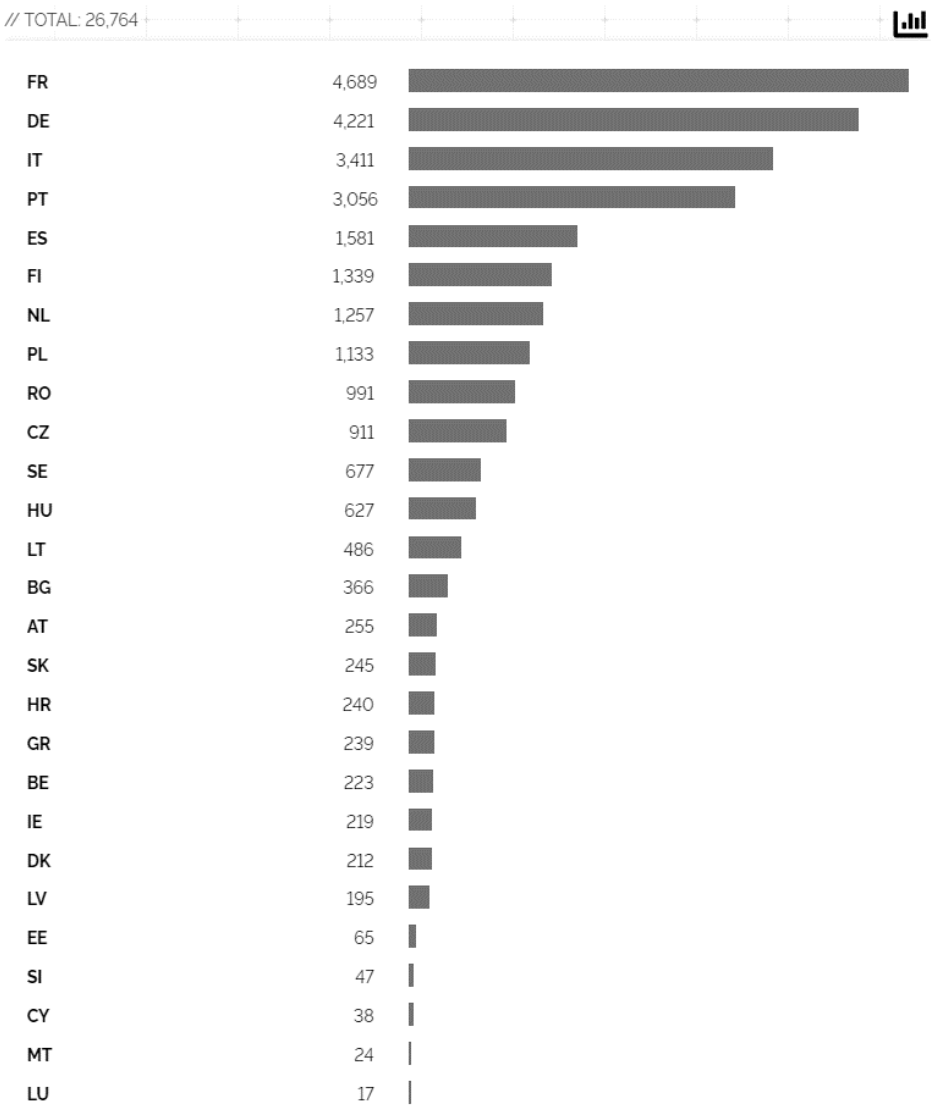
country:at,be,bg,hr,cy,cz,dk,ee,fi,fr,de,gr,hu,ie,it,lv,lt,lu,mt,nl,pl,pt,ro,sk,si,es,se



Slika 5.6: SMB protokoli prve verzije

Kako je ranije već navedeno, da bi se podaci zaštitili, na serverskoj strani nužno je podesiti autentikaciju. Kreiran je upit koji pronalazi koliko uređaja nema podešenu autentikaciju. [26]

"authentication: disabled" port:445
country:at,be,bg,hr,cy,cz,dk,ee,fi,fr,de,gr,hu,ie,it,lv,lt,lu,mt,nl,pl,pt,ro,sk,si,es,se



Slika 5.7: Otvoreni SMB portovi s nepodešenom autentikacijom

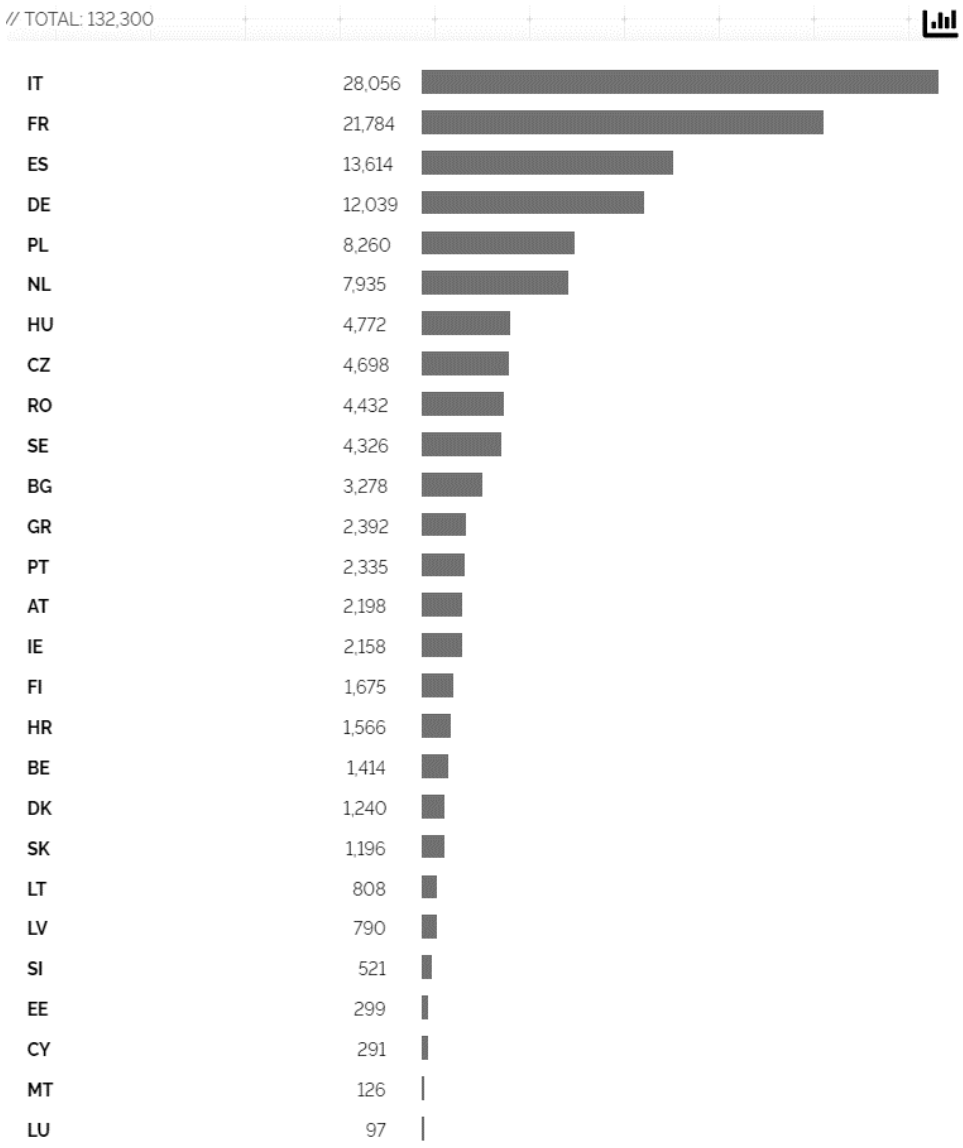
Od pronađenih 26 764 rezultata, skoro polovica, točnije 10 000 nalazi u Francuskoj i Njemačkoj.

Telnet je alat [19] koji omogućuje pristup udaljenom uređaju isključivo kroz komandno sučelje. Alat radi po principu klijent – server te je komunikacija omogućena u oba smjera. Pristup udaljenom računalu ostvaruje se preko TCP/IP protokola kroz port 23.

Najveću sigurnosnu prepreku predstavlja činjenica da Telent radi u *clear text* načinu rada, što znači da nikakav promet nije kriptiran uključujući i korisničko ime i lozinku.

Kroz Shodan upit analiziran je broj uređaja koji koriste Telnet, odnosno koji imaju otvoren port 23:

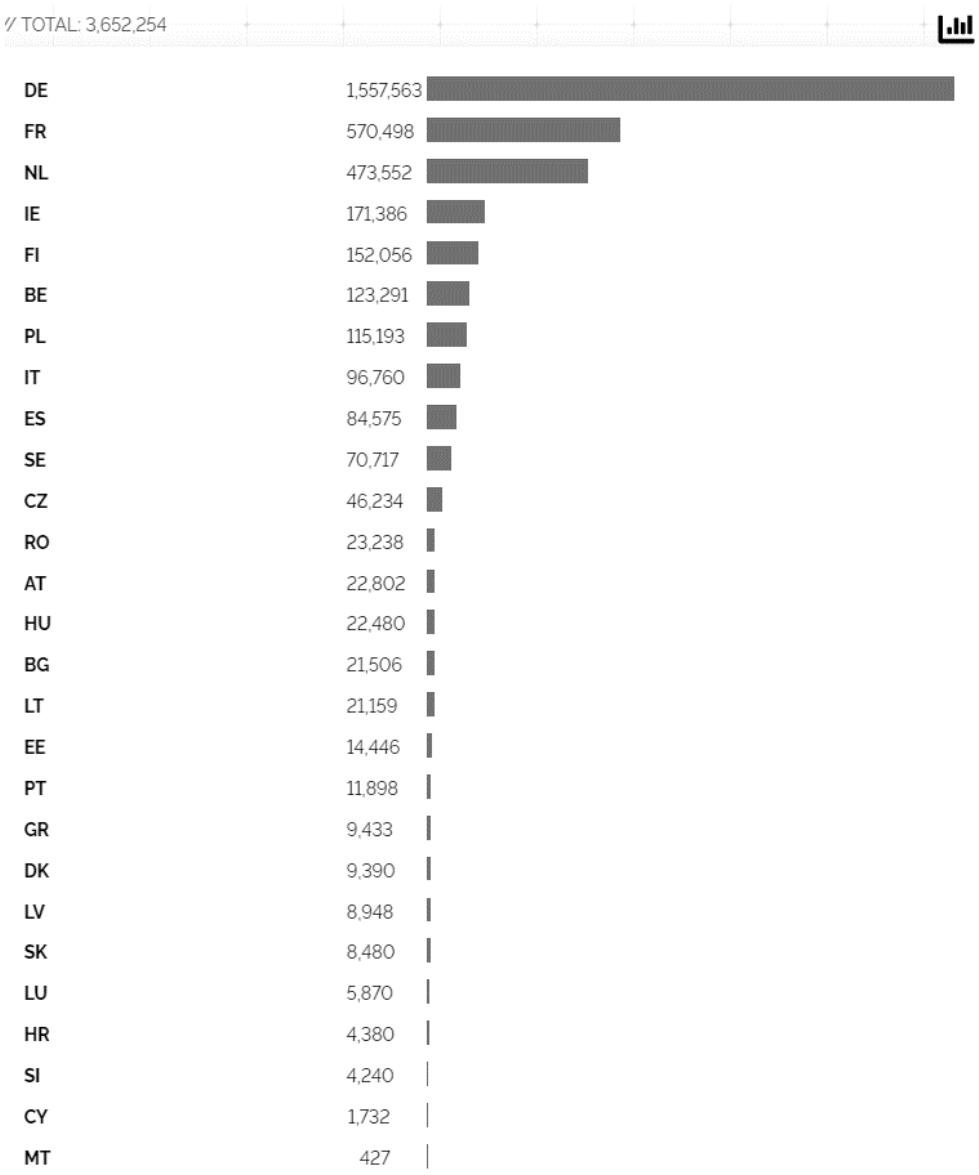
port:23 country:at,be,bg,hr,cy,cz,dk,ee,fi,fr,de,gr,hu,ie,it,lv,lt,lu,mt,nl,pl,pt,ro,sk,si,es,se



Slika 5.8: Otvoreni Telnet portovi (23)

Kao alternativa Telnetu, savjetuje se korištenje SSH (engl. *Secure Shell*) protokola kojim se korisnici povezuju na udaljena računala sigurnim putem te je sav promet kriptiran. Radi boljeg prikaza rezultata te komparacije za dva navedena protokola, kreiran je upit za Open SSH protokol koji radi na portu 22.

port:22 product:"OpenSSH"
country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se



Slika 5.9 Otvoreni portovi (22) OpenSSH protokola

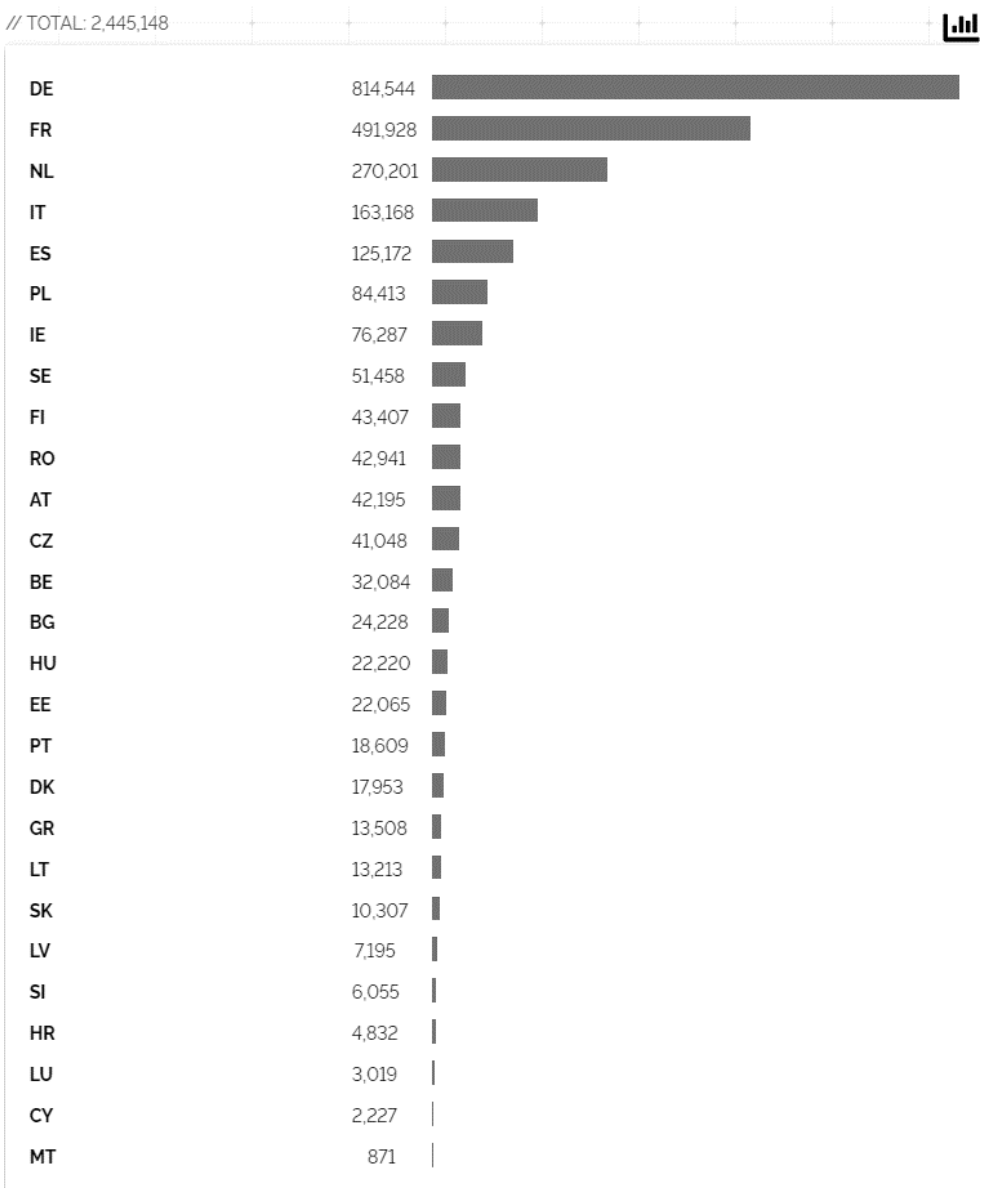
SSL (engl. *Secure Sockets Layer*) protokol [14] je sigurnosni protokol koji omogućuje sigurni prijenos podataka i njihovu enkripciju. SSL je zadužen za autentikaciju između dva uređaja kroz proces rukovanja (engl. *handshake*) i potvrdu njihovih identiteta čime se osigurava integritet podataka njihovim digitalnim potpisivanjem.

SSL certifikat je digitalni certifikat koji izdaje CA (engl. *Certification Authority*) radi potvrđivanja identiteta web servera i njegovog javnog ključa. Točnije, kada klijent pošalje HTTPS zahtjev web serveru, web server mu šalje javni ključ i SSL certifikat potpisan od strane CA. Nakon primitka SSL certifikata, provjerava se njegova valjanost i ukoliko se potvrdi da javni ključ doista pripada web serveru, klijent i server razmjenjuju ključeve nakon čega započinje sigurna komunikacija.

Istaknuvši važnost korištenja ispravnih SSL certifikata[15], kroz Shodan je kreiran upit za SSL certifikate koji nisu valjani, odnosno koji su istekli.

ssl.cert.expired:true

country:at,be,bg,hr,cy,cz,dk,ee,fi,fr,de,gr,hu,ie,it,lv,lt,lu,mt,nl,pl,pt,ro,sk,si,es,se



Slika 5.10 Istekli SSL certifikati

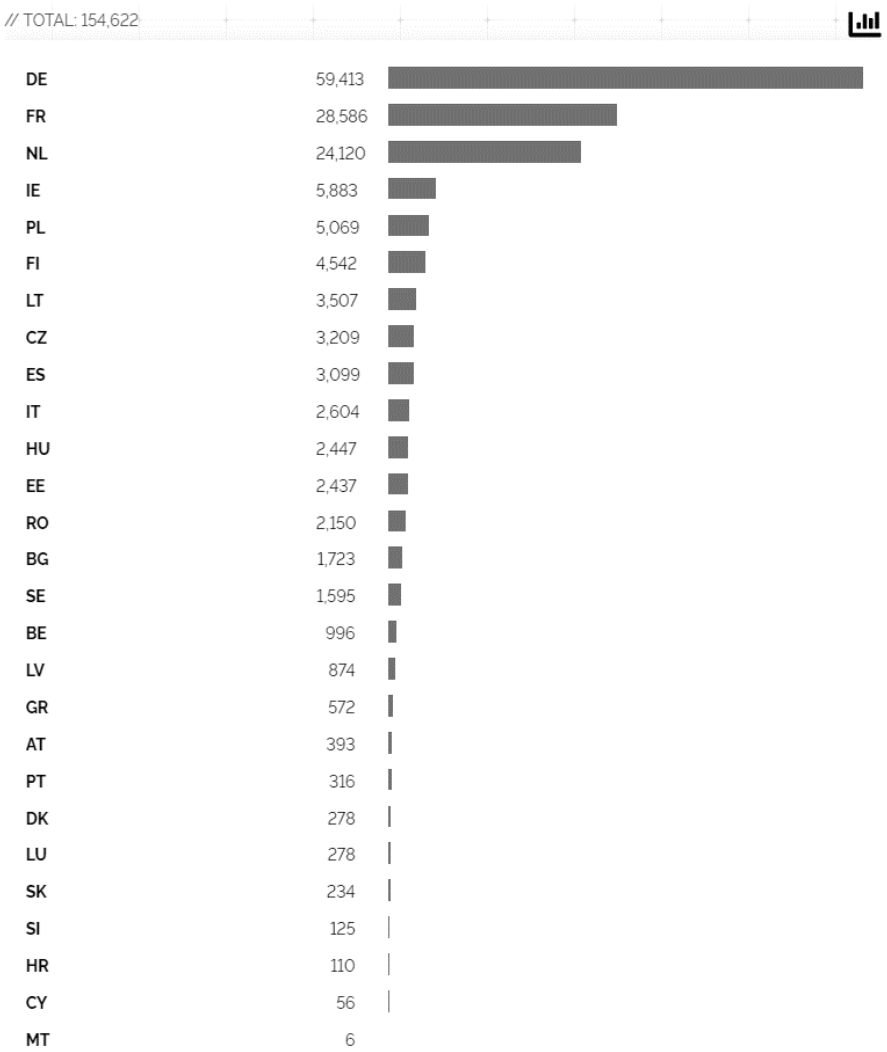
SSL certifikati koje izdaje i potpisuje pojedinac zovu se samoizdani certifikati (engl. *self-signed)* certifikati. Takvi certifikati se najčešće koriste u internim i privremenim okruženjima. Da bi *self-signed* certifikati bili valjani, oni se moraju ručno instalirati na uređaj. Korištenje takvih certifikata smatra se rizičnim jer ukoliko dođe do kompromitacije

korijenskog certifikata, zaduženog za izdavanje svih ostalih certifikata, svaki sustav koji ga je koristio postaje ranjiv.

Shodan nudi mogućnost pretraživanja *self-signed* certifikata s filterom tag:self-signed. Licenca dodijeljena za izradu ovog projekta ne dozvoljava takvu vrstu filtera, ali postoji drugi način pretrage *self-signed* certifikata po organizaciji koja je izdala certifikat, odnosno po nazivu certifikata.

Primjerice, sljedeći filter pretražuje *self-signed* certifikate za example.com.[27]

ssl.cert.issuer.cn:example.com ssl.cert.subject.cn:example.com
country:at,be,bg,hr,cy,cz,dk,ee,fi,fr,de,gr,hu,ie,it,lv,lt,lu,mt,nl,pl,pt,ro,sk,si,es,se

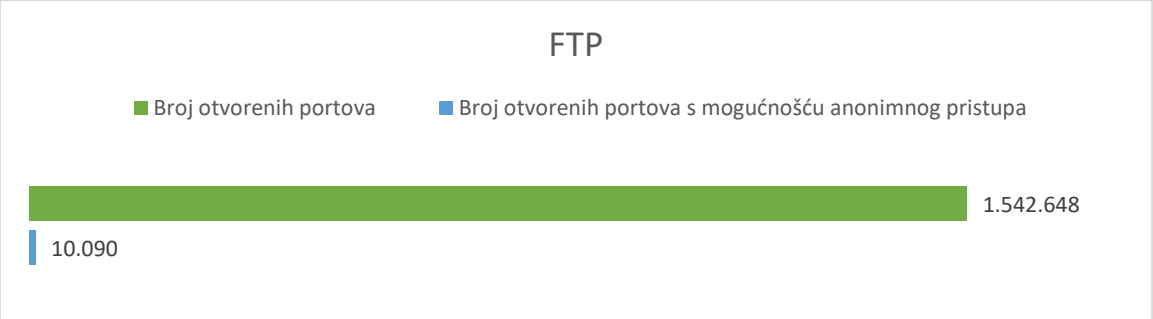


Slika 5.11 *Self-signed* certifikati za example.com

5.1.2. Komparacija rezultata

Nakon odrađenih analiza utvrđeno je stanje ranjivosti pojedinih protokola za države Europske Unije. U ovom dijelu rada odrađena je komparacija dobivenih rezultata te je prikazan odnos pojedinih protokola s pojedinim ranjivostima. Također su istaknute države s najboljim i najlošijim rezultatima.

Analizom FTP protokola prvo su skenirani svi otvoreni portovi u zemljama Europske Unije, zatim je izvršen upit za navedene portove koji imaju mogućnost anonimnog pristupa. Kroz graf je prikazan odnos otvorenih portova u odnosu na ranjivost omogućenu anonimni pristupom.



Izvršavanjem upita za FTP protokol od sveukupnih pronađenih 1 542 648 rezultata, u Njemačkoj se nalazi 35,76% rezultata. Analizom ranjivosti FTP protokola, odnosno analizom FTP protokola s mogućnošću anonimnog pristupa, utvrđeno je da je u Njemačkoj 0,47% skeniranih uređaja ranjivo. Rezultati dobiveni za Njemačku dvostruko su veći od Francuske koja je druga po redu s dobivenim rezultatima. Najmanje skeniranih uređaja detektirano je u Crnoj Gori, s 423 rezultata, odnosno 0,02% od ukupnih rezultata te s dva pronađena rezultata uspješnog anonimno povezivanja, što čini 0,47% njihovih uređaja ranjivim. Hrvatska se nalazi pri dnu ljestvice s 3 663 rezultata od kojih 0,6% ima mogućnost anonimnog pristupa.

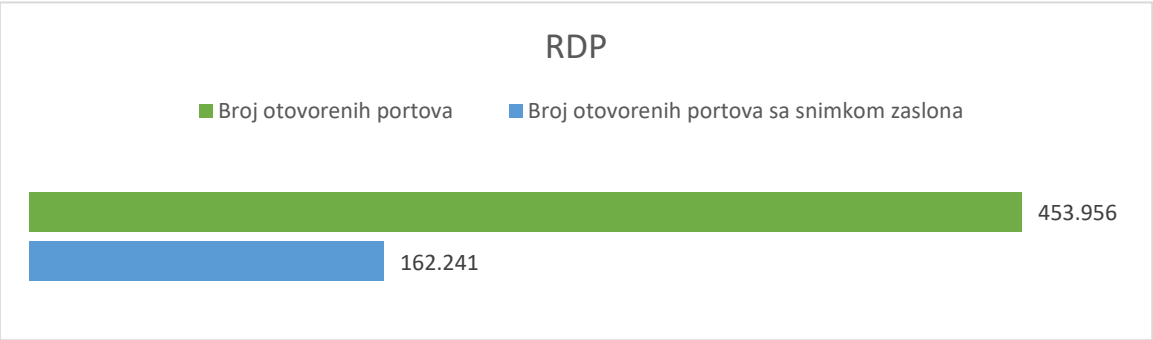
Obzirom da određene države imaju veći broj stanovnika te samim time je očekivan i veći broj uređaja spojenih na Internet, odrađena je normalizacija dobivenih rezultata za dva najveća i dva najmanja rezultata, kao i za Hrvatsku. Sljedeća tablica prikazuje normalizaciju pronađenih rezultata u odnosu na broj Internet korisnika kako bi se dobio vjerniji prikaz rezultata.[25]

Tablica 5.1 Normalizacija rezultata - FTP protokol

Država	Broj Internet korisnika	Otvoreni FTP portovi	Postotak otvorenih portova u odnosu na broj Internet korisnika (%)	Otvoreni FTP portovi s mogućnošću anonimnog pristupa	Postotak ranjivih portova u odnosu na broj Internet korisnika (%)
Njemačka	79,127,551	551,723	**0,6972**	2,608	**0,0032**
Francuska	60,421,689	253,507	**0,4195**	1,336	**0,0022**
Cipar	1,320,400	1,991	**0,1508**	8	**0,0006**
Crna Gora	547,000	423	**0,0773**	2	**0,0004**
Hrvatska	3,787,838	3,663	**0,0967**	22	**0,0006**

Analizom normaliziranih rezultata, uviđa se da je broj skeniranih otvorenih portova, kao i broj ranjivih portova i dalje najveći u Njemačkoj.

Pretragom uređaja koji imaju otvoren port 3389 za RDP protokol pronađeno je 453 956 rezultata od kojih čak 35,74% ima snimljenu snimku zaslona. Grafičkim prikazom utvrđen je odnos tih analiziranih rezultata.



Daljnjom analizom dobivenih rezultata utvrđeno je ponovno vodstvo Njemačke koja sadržava 34,27% ukupnog rezultata. U Njemačkoj je, kao i u analizi FTP protokola, skenirano dvostruko više uređaja od države koja se nalazi druga na ljestvici, u ovom slučaju Nizozemske. Zadnja država na tablici je ponovno Crna Gora sa 220 skeniranih rezultata, što

iznosi 0,04% ukupnog rezultata. Za Hrvatsku je pronađeno 1 856 rezultata, što čini 0,4% ukupno skeniranih portova.

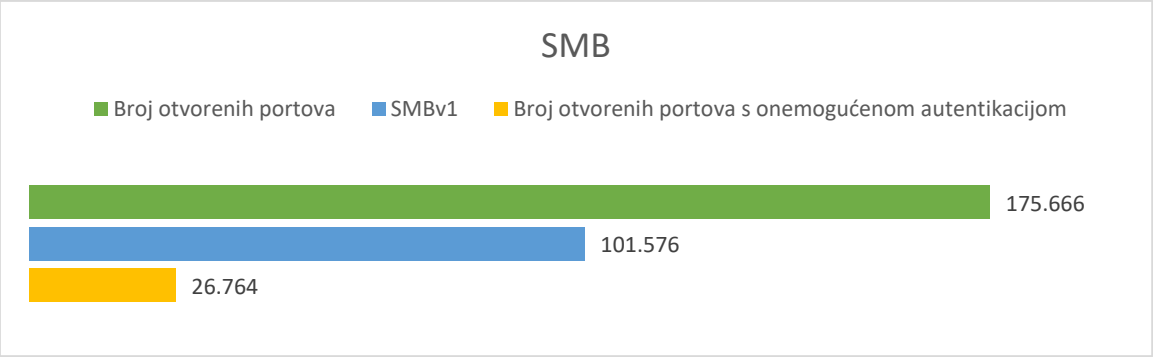
Sljedeća tablica prikazuje normalizaciju pronađenih rezultata u odnosu na broj Internet korisnika.

Tablica 5.2 Normalizacija rezultata - RDP protokol

Država	Broj Internet korisnika	Otvoreni RDP portovi	Postotak otvorenih portova u odnosu na broj Internet korisnika (%)
Njemačka	79,127,551	155,578	**0,1966**
Nizozemska	16,383,879	79,507	**0,4852**
Cipar	1,320,400	478	**0,0362**
Crna Gora	547,000	220	**0,0402**
Hrvatska	3,787,838	1,856	**0,0489**

Uvidom u normalizirane rezultate, vidljivo je da Njemačka ima manji postotak otvorenih RDP portova u odnosu na Nizozemsku iako je u Njemačkoj skenirano dva puta više otvorenih RDP portova. Također tablica 5.2 prikazuje podjednake dobivene rezultate u Hrvatskoj i Crnoj Gori.

Analizom SMB protokola odrađeni su upiti za sveukupni broj otvorenih portova, broj portova koji koriste SMBv1 te broj otvorenih portova s onemogućenom autentikacijom. Kroz graf je prikazan odnos rezultata navedenih parametara.



Kao i u prethodne dvije analize, skeniranjem SMB protokola, utvrđeno je da Njemačka ima najveći broj rezultata, od skeniranih 175 666 od kojih je 51,85% SMB prve verzije i 7,99%

rezultata s nepodešenom autentikacijom. Iako je u Njemačkoj pronađeno najviše sveukupnih rezultata, Francuska, koja se nalazi na drugom mjestu s 35 292 rezultata, ima najviše rezultata u analizi onemogućene autentikacije te je 63,09% nesigurno zbog korištenja SMBv1. 13,28% dobivenih rezultata u Francuskoj ima onemogućenu autentikaciju na SMB protokolima. Na zadnjem mjestu ljestvice ponovno se nalazi Crna Gora s 119 rezultata, od kojih je 50,42% je prve verzije te samo 20,16% s onemogućenom autentikacijom. Hrvatska ima 721 skenirana SMB protokola čime zauzima 22. mjesto u ukupnom poretku. Od navedenog 721 rezultata, čak 71,56% ih je SMB prve verzije i 33,28% s onemogućenom autentikacijom.

Sljedeća tablica prikazuje normalizaciju pronađenih rezultata u odnosu na broj Internet korisnika.

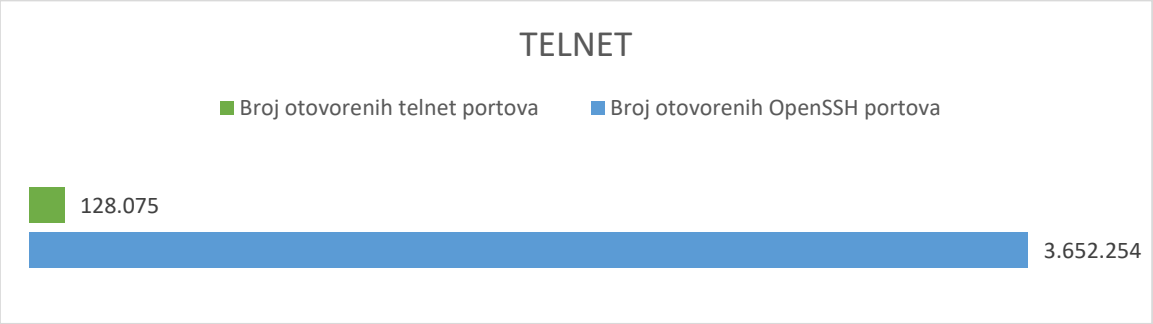
Tablica 5.3 Normalizacija rezultata - SMB protokol

Država	Broj Internet korisnika	Postotak otvorenih SMB portova u odnosu na Internet korisnike (%)	Postotak otvorenih SMB portova prve verzije u odnosu na Internet korisnike (%)	Postotak otvorenih SMB portova s onemogućenom autentikacijom u odnosu na Internet korisnike (%)
Njemačka	79,127,551	0,0667	0,0345	0,0053
Francuska	60,421,689	0,0584	0,0368	0,0069
Luksemburg	636,565	0,0232	0,0153	0,0026
Crna Gora	547,000	0,0043	0,0109	0,0044
Hrvatska	3,787,838	0,0190	0,0136	0,0063

Tablicom normalizacije uočeni su djelomično vjerniji rezultati ranjivosti SMB protokola. U odnosu na korisnike Interneta u pojedinoj državi, u Njemačkoj se nalazi najviše skeniranih SMB portova, ali je u Francuskoj najviše ranjivosti. Francuska ima najviše SMBv1 ranjivosti, kao i najveći postotak SMB portova s onemogućenom autentikacijom. Od navedenih država, Hrvatska iza Francuske ima najveći postotak ranjivosti za onemogućenu

autentikaciju, dok su u državama s manjim brojem Internet korisnika i manji postotci ranjivih uređaja.

Za analizu Telenta, skenirani su i portovi koji koristi OpenSSH. Obzirom da se ne preporučuje korištenje Telneta, odnosno da se savjetuje korištenje SSH protokola, odnos između dobivenih rezultata je zadovoljavajući. Korištenje OpenSSH alata je značajno učestalije od Telneta, što je i vidljivo na sljedećem grafu.



Izvršavanjem upita za uređaje koji koriste Telnet, pronađeno je 132 300 rezultata. Na prvom mjestu ljestvice rezultata po državama nalazi se Italija koja sadrži 21,2% ukupnog rezultata. Zadnje mjesto zauzima Luksemburg sa samo 97 rezultata, odnosno 0,07%. U Hrvatskoj je pronađeno 1 556 otvorenih telnet portova koji sadržavaju 1,18% ukupno skeniranih portova. Obzirom da je SSH, kao sigurna alternativa Telnetu, poznat i često korišten protokol, pronađeni rezultati Telent portova bi trebali biti manji, odnosno očekivani udio za pojedine države bi trebao biti manji.

Tablica 5.4 Normalizacija rezultata - Telnet i SSH

Država	Broj Internet korisnika	Postotak otvorenih Telnet portova u odnosu na Internet korisnike (%)	Postotak otvorenih SSH portova u odnosu na Internet korisnike (%)
Italija	54,798,299	0,0512	0,1765
Francuska	60,421,689	0,0360	0,9442
Luksemburg	636,565	0,0152	0,9221
Crna Gora	547,000	0,0230	0,0780
Hrvatska	3,787,838	0,0413	0,1156

Tablicom normalizacije skeniranih Telnet i SSH portova, detektiran je najveći postotak Telnet portova u Italiji, iza koje slijedi Hrvatska. Normalizacijom SSH rezultata vidljivo je da Francuska u donosu na broj Internet korisnika ima najveći postotak korištenja SSH protokola što znatno utječe na sigurnost uređaja spojenih na Internet u cijeloj državi.

Analizom SSL protokola, odnosno SSL certifikata pronađena je značajan broj rezultata, točnije 2 445 148 certifikata koji su istekli. Veliki udio tih rezultata, točnije 814 544 (33,35%) nalazi se u Njemačkoj. Najveći broj certifikata koje su korisnici izdali sami, odnosno *self-signed* certifikata za domenu example.com, također je skenirano u Njemačkoj, gdje je pronađeno 38,42% takvih certifikata. U Crnoj Gori skenirano je 0,03% isteklih certifikata što je vidno manji rezultat od svih drugi država. Pri analizi isteklih SSL certifikata, Hrvatska se pozicionirala pri dnu ljestvice s 0,19% ukupno pretraženih certifikata. Za *self-signed* certifikate za example.com, u Hrvatskoj je prepoznato 110 rezultata, što čini 0,07% ukupno pronađenih rezultata.

Tablica 5.5 Normalizacija rezultata - SSL certifikati

Država	Broj Internet korisnika	Istekli certifikati u odnosu na Internet korisnike (%)	Self-signed certifikati za example.com u odnosu na Internet korisnike (%)
Njemačka	79,127,551	1,0294	0,0750

Francuska	60,421,689	0,8141	0,0473
Cipar	1,320,400	0,4071	0,0042
Crna Gora	547,000	0,1592	0,0011
Hrvatska	3,787,838	0,1275	0,0029

Normalizacijom dobivenih rezultata predstavljena je tablica u kojoj je postotak isteklih certifikata u odnosu na Internet korisnike u Njemačkoj značajno veći od drugih država. Iza Njemačke, nalazi se Francuska s nešto manjim postotkom, ali i dalje dovoljno velikim u odnosu na druge države. Također je vidljivo da od navedenih rezultata, Hrvatska ima najmanji postotak isteklih certifikata.

5.1.3. Preporuke za zaštitu od napada

Analizom ranjivosti uređaja po određenim protokolima, utvrđeno je da postoji velik broj uređaja koji su nezaštićeni i koji mogu biti kompromitirani. Korisnici ne moraju nužno imati podatke koji su povjerljivi ili osjetljivi, ali narušavaju privatnost podataka. Obzirom da se radi o protokolima koji se učestalo koriste, postoji niz sigurnosnih preporuka za zaštitu od napada.

Ranije u radu je uočeno da određeni broj FTP servera dozvoljava anonimnu prijavu, stoga je prvi korak u sigurnosnoj zaštiti da se onemogući anonimna prijava, odnosno da se forsira autentikacija na serverima. Obzirom da FTP protokol sam po sebi nije siguran protokol jer ne kriptira podatke, preporučljivo je korištenje sigurne verzije protokola – FTPS (FTP Secure) ili SFTP (SSH FTP) [20]. FTPS je nadograđena verzija FTP-a koja koristi SSL/TLS za enkripciju podataka, SFTP je nadograđeni FTP koji radi na SSH konekciji. Oba protokola prenose kriptirane podatke, ali je razlika u tome što je FTPS baziran na FTP-u i dalje koristi TCP port 21, za razliku od SFTP koji je baziran na SSH-u i koristi TCP port 22. Za razliku od FTPS protokola, SFTP ne nudi mogućnost anonimnih prijava na server.

Kao što je ranije spomenuto u radu, korištenjem RDP protokola korisnici se izlažu potencijalnim *BruteForce* napadima gdje napadači automatiziranim alatima pokušavaju odgonetnuti lozinku korisničkog računa. Prvi korak pri zaštiti RDP protokola je postavljanje jakih, odnosno kompleksnih lozinki i podešavanje sustava tako da je dopušten samo određen broj pogrešno unesenih lozinki, nakon čega se korisnički račun zaključava. Korisnicima se

savjetuje redovno ažuriranje softvera jer ažurirane verzije softvera mogu sadržavati zakrpe potencijalnih ranjivosti. Također je, pri zaštiti RDP protokola, potrebno uzeti u obzir ograničavanje pristupa i konekcija na vatrozidima (engl. *firewall*) za RDP port 3389 [12].

Kako je i prikazano analizom, neki uređaji nemaju podešenu autentikaciju za SMB protokol. Kao prva sigurnosna preporuka, autentikacija je nužan korak u osiguravanju uređaja. Nadalje, korištenje SMB protokola prve verzije nije preporučljivo zbog određenih sigurnosnih ranjivosti koje su navedenu ranije u radu, nego se preporuča korištenje zadnje SMB verzije.

Sav promet koji koristi Telnet nije kriptiran i nije siguran, stoga se savjetuje izbjegavanje korištenja Telenta u svim slučajevima. Kao alternativa Telnetu, dobra praksa je korištenje SSH protokola jer je sav promet kriptiran, uključujući i podatke za prijavu. OpenSSH je alat koji omogućuje korisnicima spajanje na udaljeno računalo uz enkripciju podataka i sigurni prijenos između uređaja.

SSL protokol se smatra zastarjelim protokolom i sigurnosni stručnjaci savjetuju korištenja SSL protokola za TLS protokol koji je nadograđena verzija SSL-a i osigurava siguran pristup web serverima. Obzirom da je u radu odrađena analiza isteklih certifikata te da je pronađen značajan broj rezultata, korisnicima se naglašava važnost korištenja ispravnih certifikata i njihova obnova. Podešavanjem automatske obnove certifikata izbjeći će se dio ranjivosti vezanih za SSL certifikate. Korištenje certifikata koji korisnici kreiraju i izdaju sami, odnosno self-signed certifikata potencijalno može ugroziti pojedine korisnike, ali i cijeli sustav, stoga se savjetuje izbjegavanje korištenja istih. Pri kreiranju Internet stranica, korisnici imaju mogućnost korištenja besplatnih SSL certifikata koji će potvrditi njihov identitet. Ukoliko se koriste self-signed certifikati, nužan je korak osigurati da napadač ne može doći do korijenskog certifikata jer bi u suprotnom bili ugroženi sva tijela kojima je izdao certifikat.

5.2. Analiza sigurnosnih ranjivosti Web kamera i uređaja za ispis

Većina korisnika pri konfiguraciji privatnih okruženja ostavlja predefinirane postavke uređaja, što osim predefiniranih korisničkih imena i lozinki, uključuje i omogućenost pojedinih servisa i otvorenost portova prema Internetu. Povezivanjem uređaja na Internet i

nepravilnom sigurnosnom konfiguracijom, uređaji dovode u opasnost cijelo lokalno okruženje. Obzirom da su web kamere i uređaji za ispis, uređaji koji se najčešće mogu pronaći u privatnim okruženjima, a povezani su na Internet, u ovom dijelu rada odrađena je analiza njihovih ranjivosti.

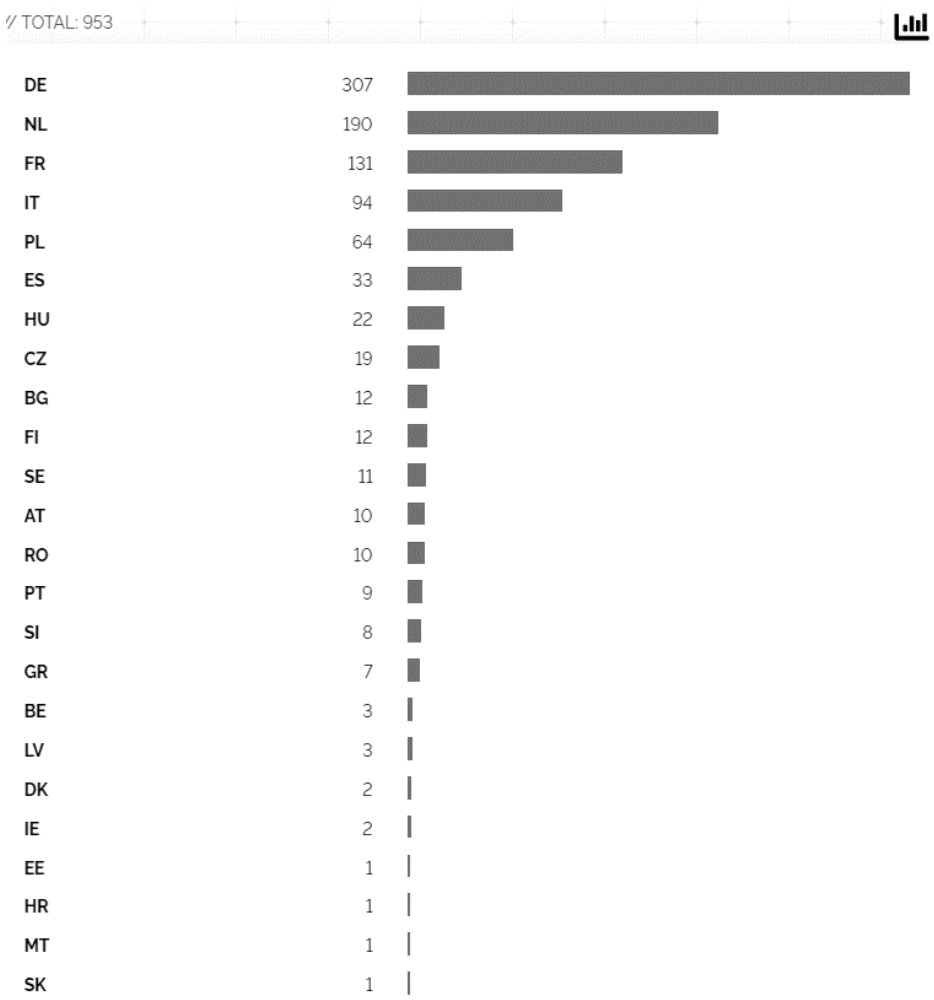
5.2.1. Analiza ranjivosti uređaja

IP kamere su digitalne kamere koje šalju video snimke u obliku signala mrežnim putem. Web kamere su povezane na lokalnu mrežu žičnim ili bežičnim putem.

Iz sigurnosnih aspekata, problematika web kamera je korištenje neažuriranih i zastarjelih softvera, kao i korištenje predefiniranih pristupnih podataka ili nekorištenje istih. Osim toga, sigurnosni rizik također predstavlja mogućnost drugih uređaja u lokalnoj mreži da prepoznaju web kamere.

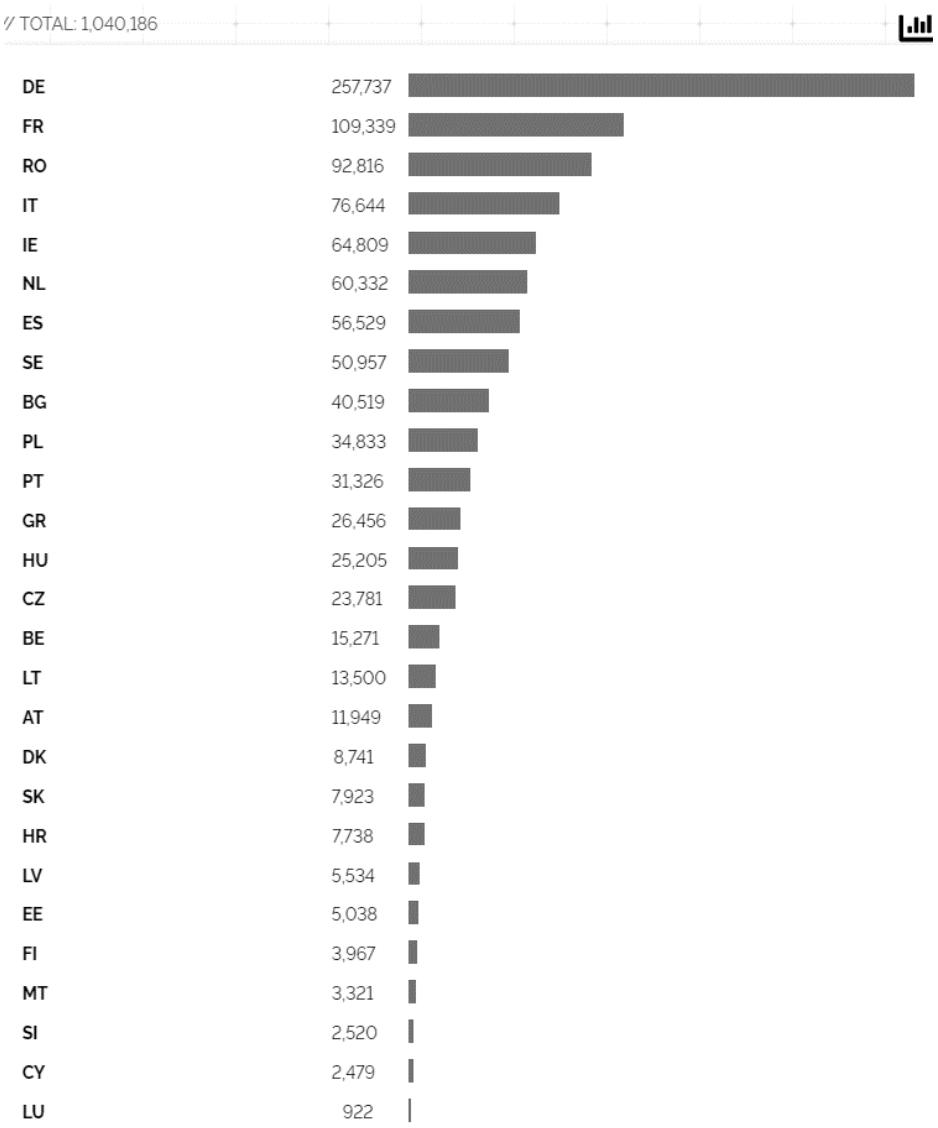
Koristeći Shodan pretražene su web kamere spojenih na Internet na području Europske Unije. Obzirom da uz studentsku licencu, dodijeljenu za pisanje ovog rada, nije moguće pretraživati uređaje po oznakama, za upite web kamera, korištenje su pojedine ključne riječi kao što su „webcam“ i „camera“[28].

webcam country:at,be,bg,hr,cy,cz,dk,ee,fi,fr,de,gr,hu,ie,it,lv,lt,lu,mt,nl,pl,pt,ro,sk,si,es,se



Slika 5.12 Pretraga web kamera filterom "webcam"

camera country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se

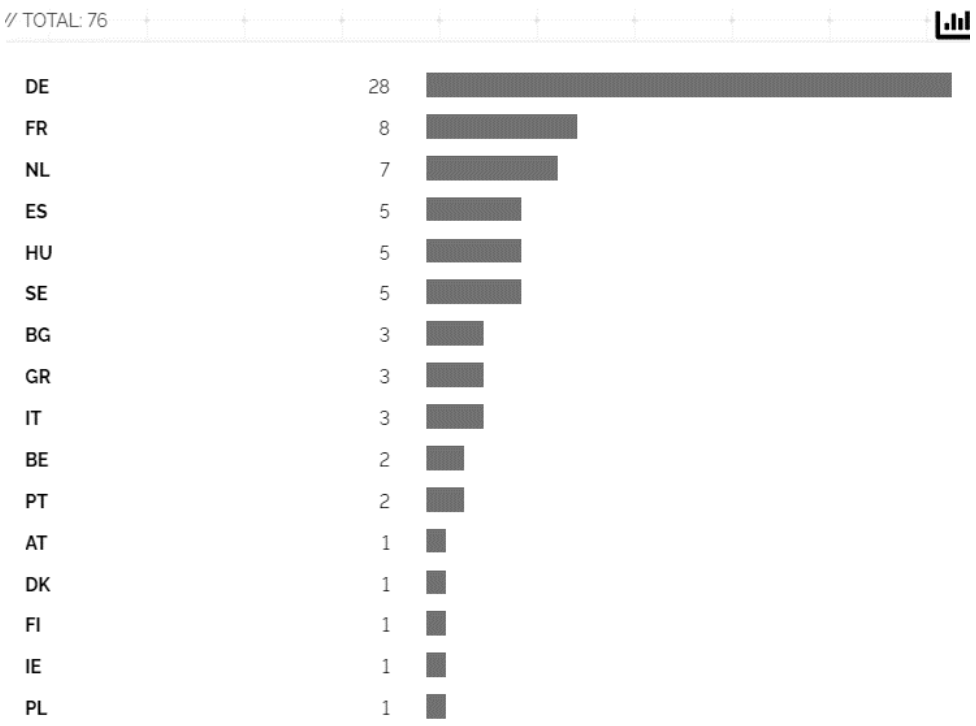


Slika 5.13 Pretraga web kamera filterom "camera"

Obzirom da bez korištenja oznaka, navedeni filteri ne izbacuju doista sve web kamere, kreirani su dodatni upiti koji specificiraju pretrage za pojedine proizvođače web kamera. Kroz prethodno kreirane upite, izdvajaju se sljedeći proizvođači softvera: webcamXP, Yawcam, GeoVision (GeoHttpServer) i Netwave.

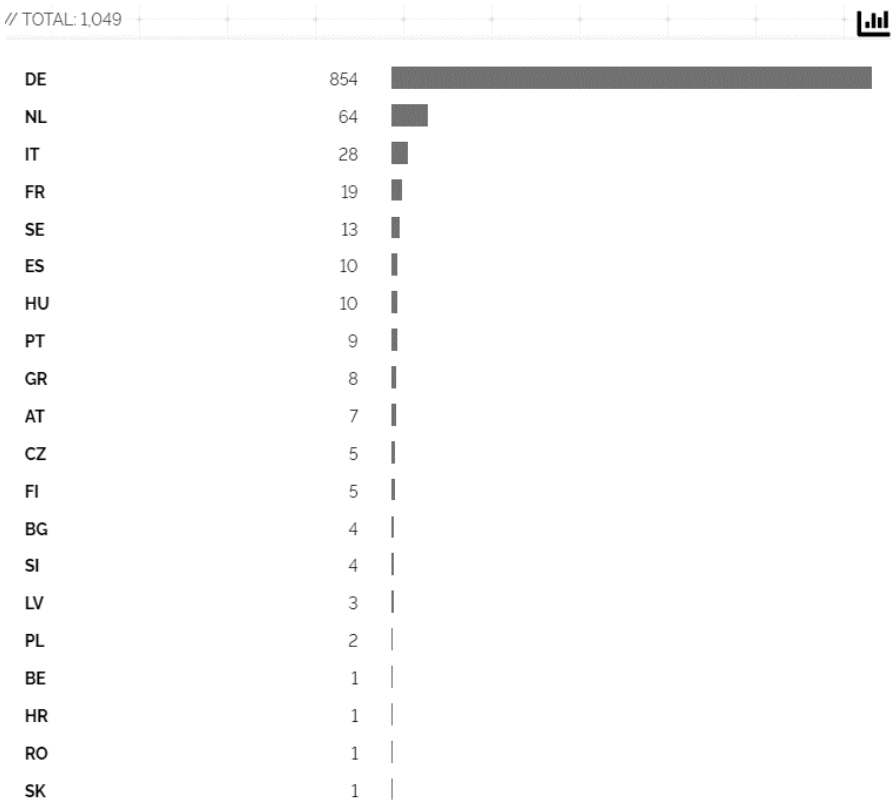
"server: webcamxp"

country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se



Slika 5.14 webcamXP web kamere

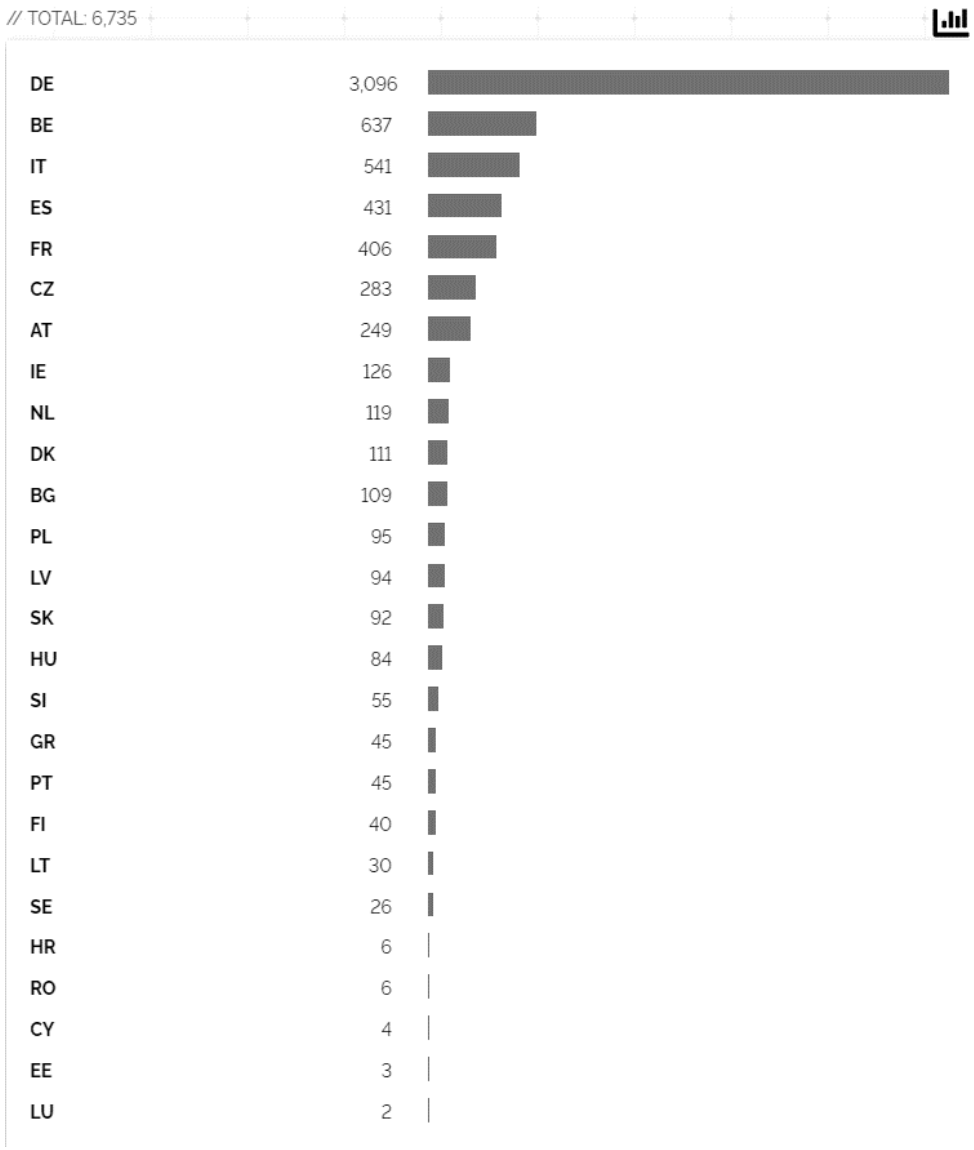
yawcam country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se



Slika 5.15 yawcam web kamere

"server: GeoHttpServer"

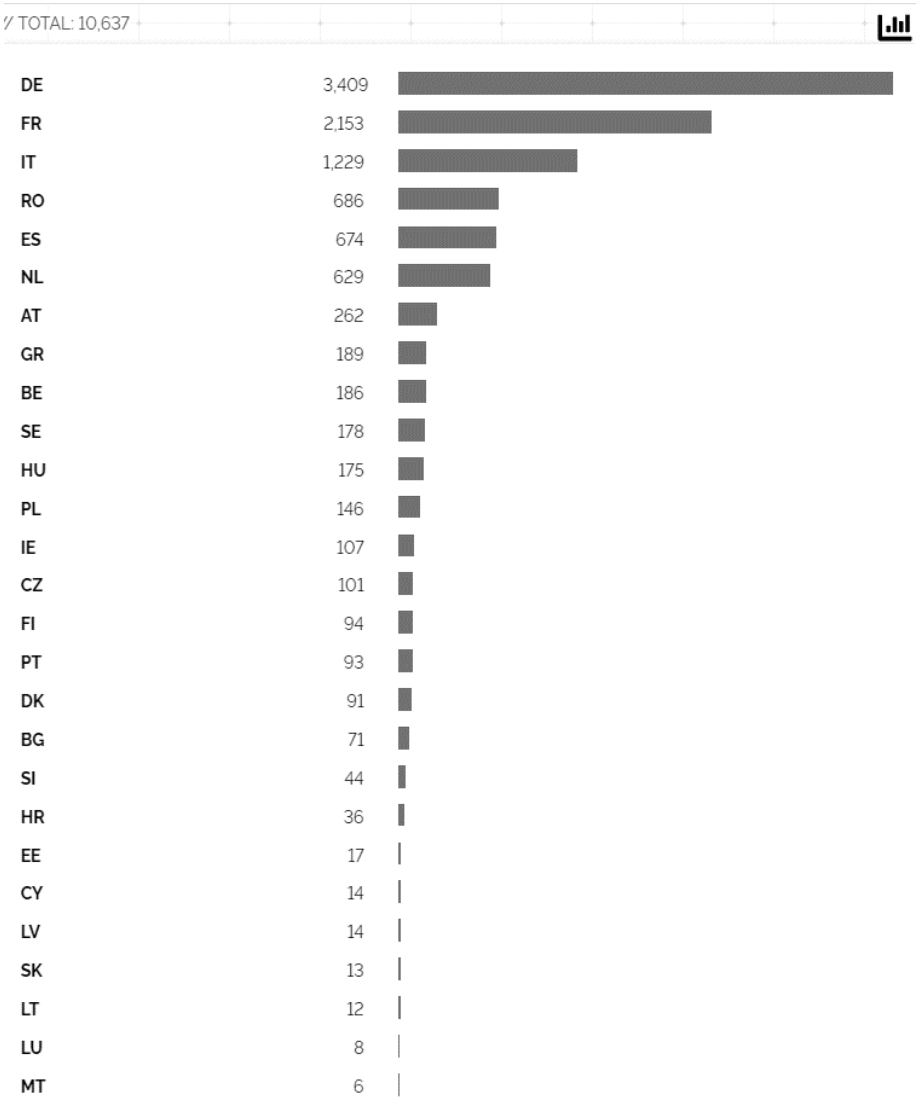
country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se



Slika 5.16 GeoVision web kamere

"server: Netwave IP camera"

country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se



Slika 5.17 Netwave web kamere

Kroz prethodno odrađene analize, vidljiva je popularnost, odnosno učestalost korištenja pojedinih web kamera.

Pojedine web kamere zaštićene su korisničkim imenom i lozinkom, dok se ostalima pristupa anonimno.

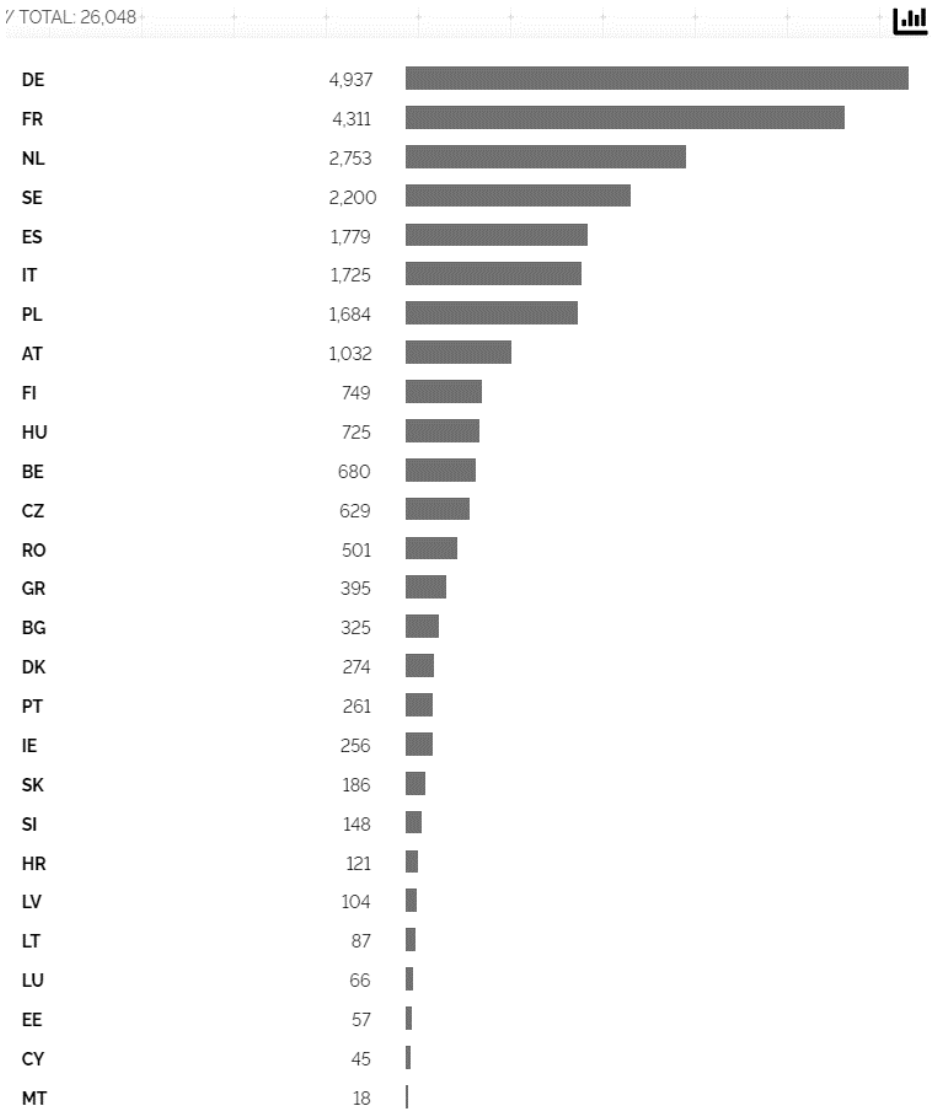
Od detektiranih 953 „webcam“ web kamera, za 81 kameru postoji kreirana snimka zaslona, što znači da je pristup web kameri dopušten svima, bez potrebe za unosom korisničkih podataka.

Uređaji za ispis smješteni su u skoro svakom poslovnom uredu, kao i u kućnim okruženjima. Ulaganjem u sigurnost lokalne mreže, često se izostavlja činjenica da su uređaji za ispis

povezani na Internet te da predstavljaju sigurnosnu prijetnju, kao i svaki drugi uređaj te samim time predstavljaju sigurnosne prijetnje za ostatak lokalne mreže u kojoj se nalaze.

IPP (engl. *Internet Printing Protocol*) je protokol [11] aplikacijskog sloja OSI modela koji radi na portu 631. Svi moderni uređaji za ispis koji su povezani na mrežu koriste IPP protokol za vezu između samog uređaja i odgovarajućeg softvera. Koristeći IPP protokol, softver šalje naredbe uređaju za ispis te protokol uređaju omogućuje informacije o funkcijama uređaja, pojedinim stanjima samog uređaja te zadacima koje uređaj obavlja. Sljedećim upitom pretraženi su uređaji koji imaju otvoren IPP port 631.

port:631 country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se

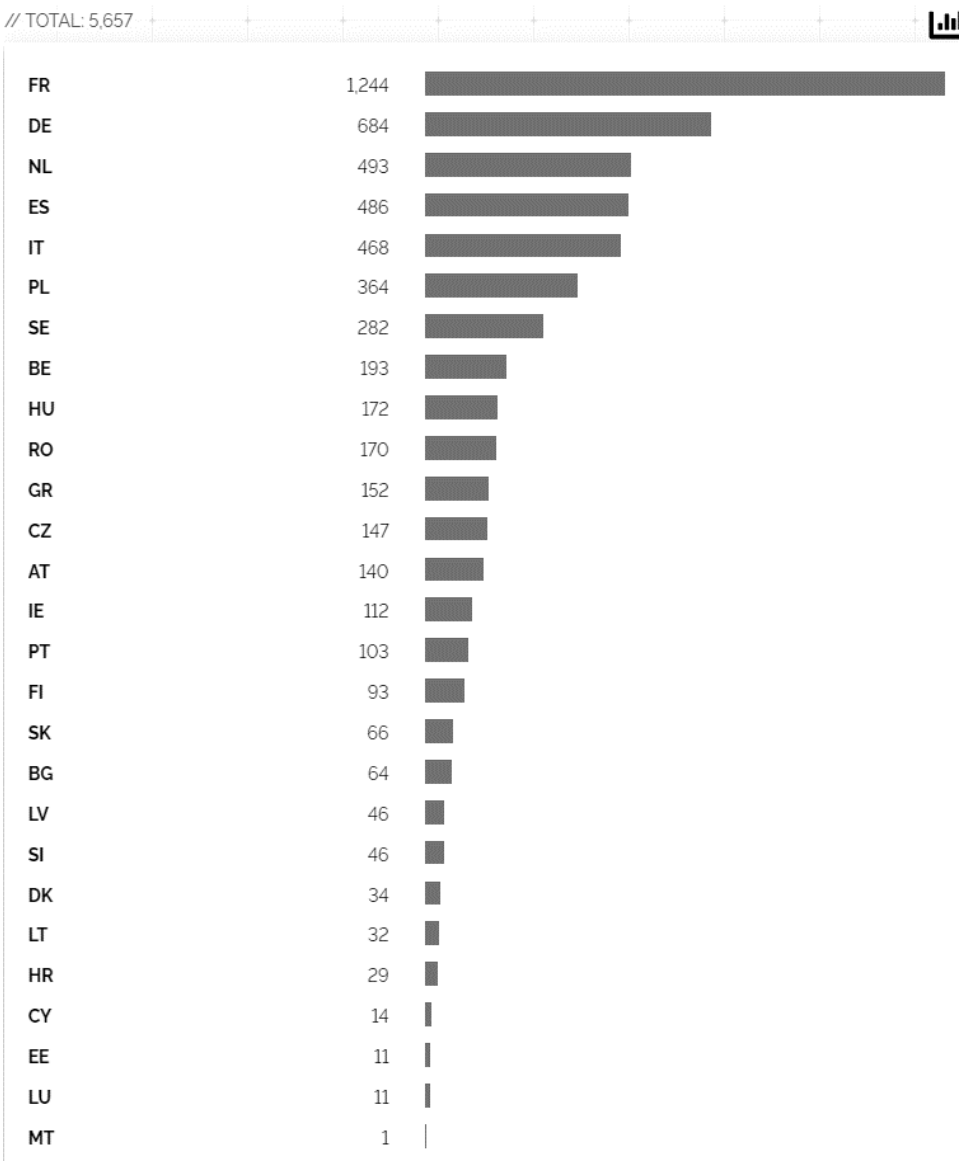


Slika 5.18 Otvoreni IPP (631) portovi

Obzirom da dio dobivenih rezultata vraća rezultat „404 Not Found“ ili neki od drugih HTTP odgovora o statusu, izveden je dodatni upit koji pretražuje uređaje za ispis dostupne putem HTTP protokola s HTTP statusom „200 OK“.

port:631 "200 OK"

country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se



Slika 5.19 Otvoreni IPP portovi (631) - HTTP status "200 OK"

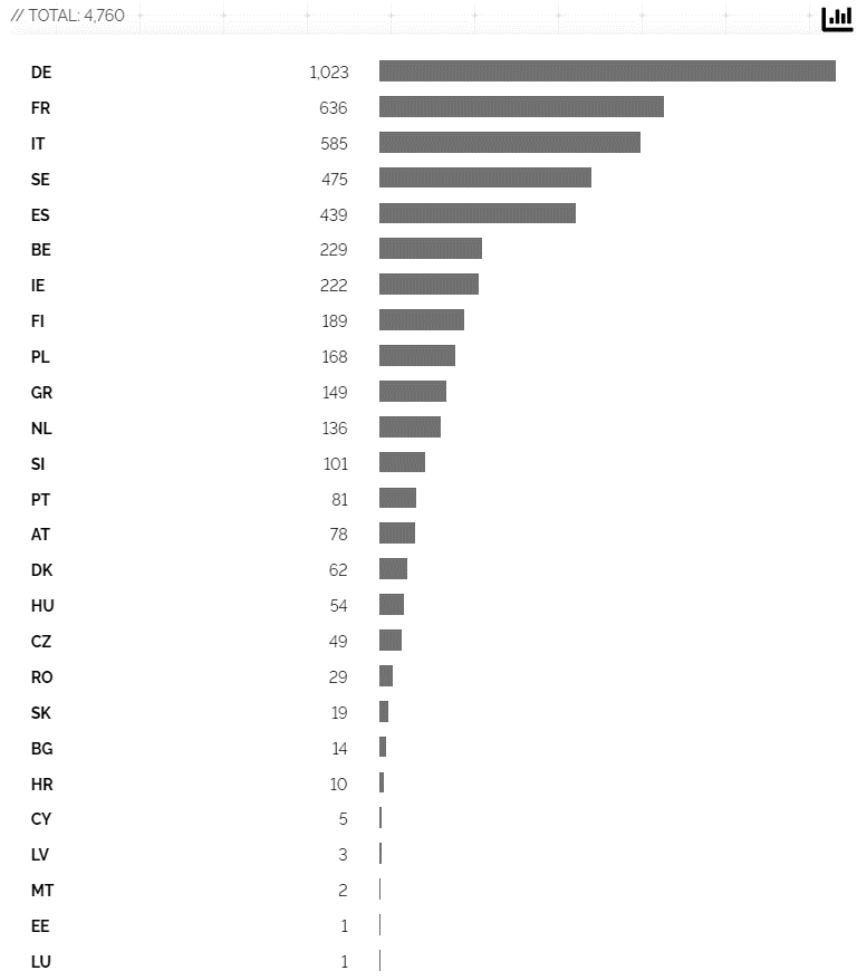
Pregledom dobivenih rezultata, uočljivo je da se broj rezultata znatno smanjio kada su se u obzir uzeo HTTP status. Pojedini uređaji zahtijevaju autentikaciju za pristup uređaju za ispis, ali i određeni dio skeniranih uređaja daje omogućen pristup.

U ostatku analize neće se uzimati u obzir uređaji s ostalim HTTP statusima, odnosno radit će se upiti samo za uređaje za ispis koji su dostupnim putem HTTP protokola.

U ovom dijelu analize, kreirani su upiti za najčešće korištene modele uređaja za ispis u kućnim i uredskim okruženjima, odnosno za HP, Epson, Lexmark i Canon uređaje za ispis.

Jedni od najpoznatijih i najčešće korištenih uređaja za ispis su marke HP. HP uređaji za ispis koji koriste HTTP protokol, pretraženi su sljedećim filterom:

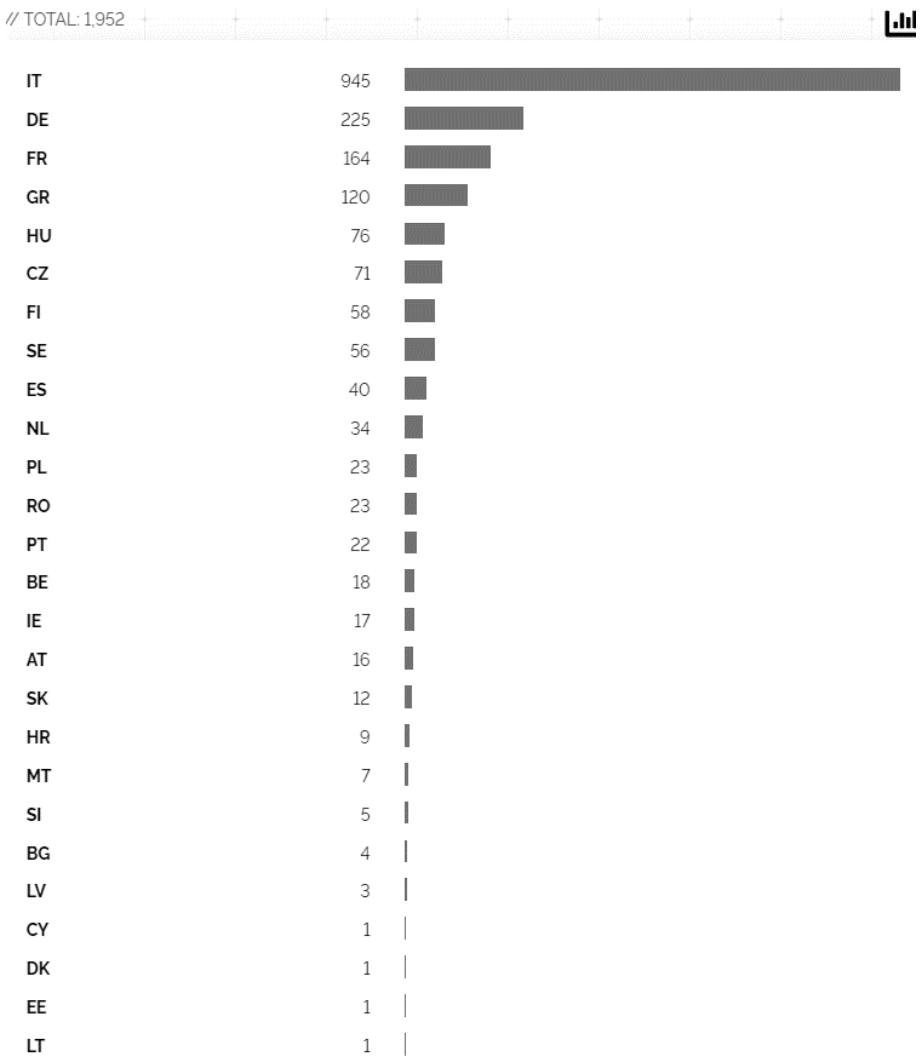
"Server: HP HTTP Server" "200 OK"
country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se



Slika 5.20 HP uređaji za ispis - HTTP status "200 OK"

Istim principom pretraženi su Epson uređaji za ispis kojima se može pristupiti putem HTTP protokola.

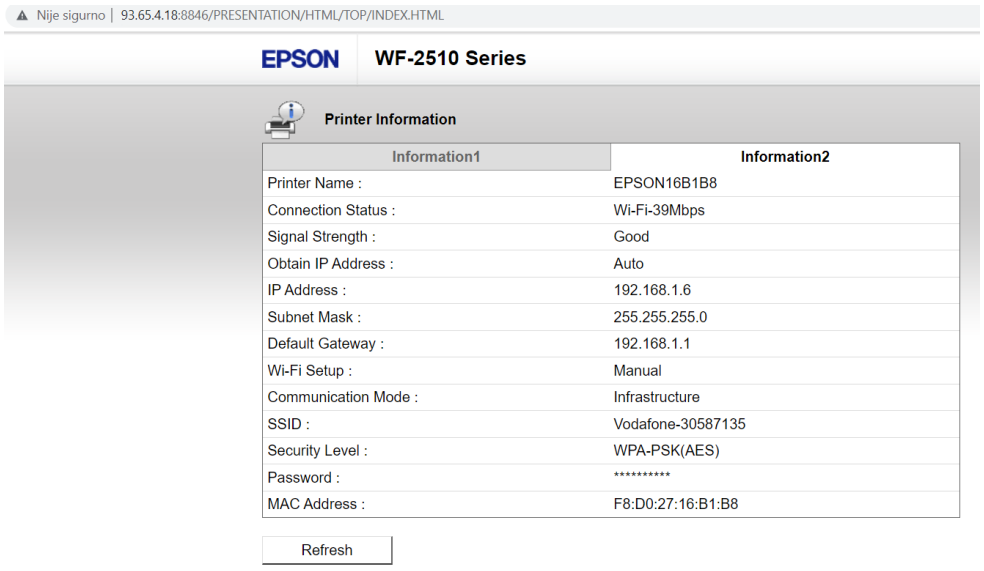
"Server: Epson" "200 OK"
country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se



Slika 5.21 Epson uređaji za ispis - HTTP status "200 OK"

Od ukupno pronađenih 2 559 rezultata, 1952 ih je sa HTTP statusom „200 OK“.

Dobiveni rezultati preusmjeravaju na HTTP stranice uređaja za ispis. Na slici X, vidljive se specifikacije uređaja, kao što su informacije o WiFi-u i MAC adresa uređaja.

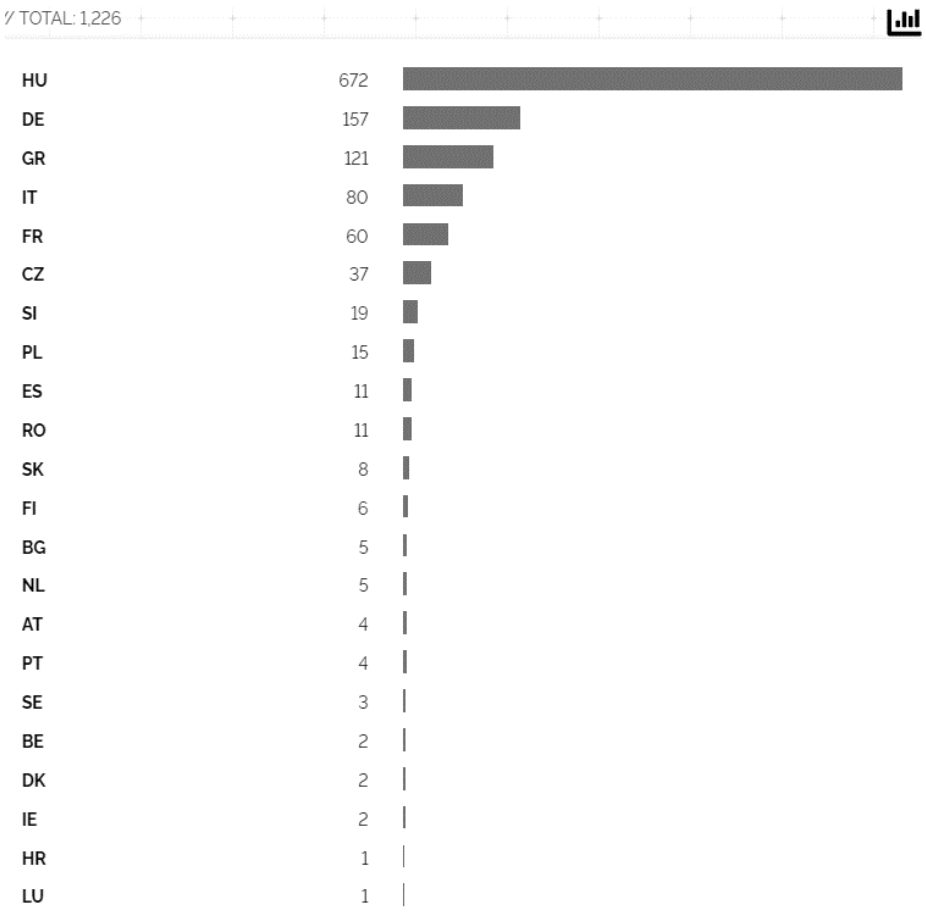


Slika 5.22 Pristup Epson uređaju za ispis

Za Lexmark uređaje za ispis pronađeno je 1 226 rezultata kojima se može pristupiti putem HTTP protokola od ukupnih 1 402 rezultata.

"Server: Lexmark" "200 OK"

country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se

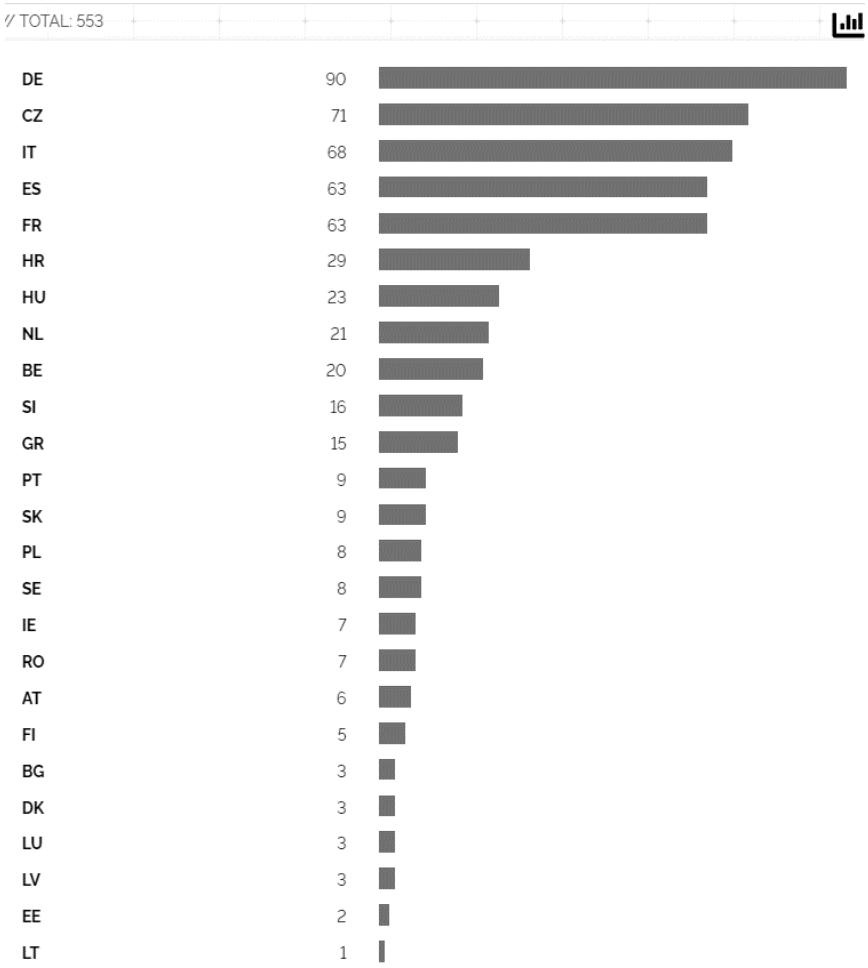


Slika 5.23 Lexmark uređaji za ispis - HTTP status "200 OK"

Posljednja analiza uređaja za ispis radi upite za Canon uređaje.

"Server: Canon HTTP Server" "200 OK"

country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se



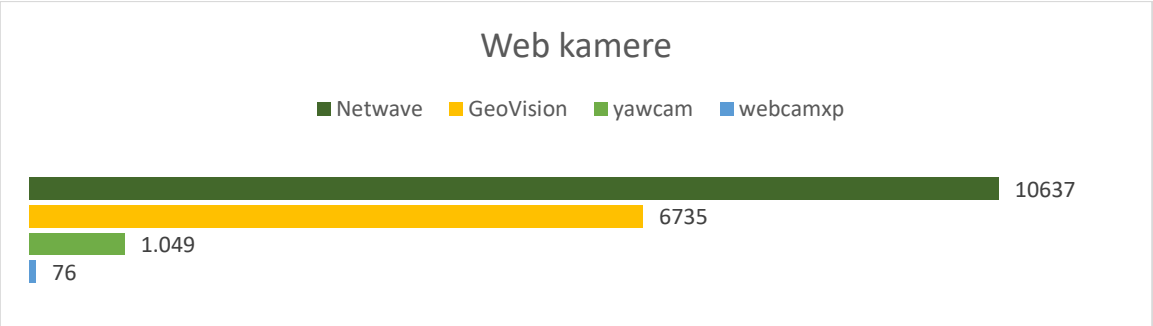
Slika 5.24 Canon uređaji za ispis - HTTP status "200 OK"

Od ukupnih 1 065 Canon uređaja za ispis, 553 rezultata vraća HTTP status „200 OK“, što je zanemareni rezultat za polovicu Canon uređaja za ispis.

5.2.2. Komparacija rezultata

Za analizu ranjivih web kamera korišteni su filteri „webcam“ i „camera“ kako bi se dobio uvid u dostupnost web kamera na Internetu u državama Europske Unije. Kreiranjem upita najviše rezultata je skenirano u Njemačkoj, Francuskoj i Nizozemskoj što je u odnosu na broj stanovnika i broj Internet korisnika, djelomično očekivani rezultat. Obzirom da tim filterima nisu obuhvaćene sve web kamere izložene na Internetu, analiza je produljena kreiranjem upita za pojedine proizvođače softvera za web kamere.

Sljedeći graf prikazuje broj skeniranih rezultata u ovisnosti o proizvođaču softvera.



Obzirom da je već navedeno da je broj skeniranih uređaja veći u državama koje imaju više Internet korisnika, kreirana je tablica normalizacije rezultata u kojoj su dobiveni rezultati uspoređeni s brojem Internet korisnika. U tablicu su uvrštene Netwave web kamere jer je skeniranjem zaključeno da su te web kamere najučestalije.

Tablica 5.6 Normalizacija rezultata - web kamere

Država	Broj Internet korisnika	Postotak „webcam“ rezultata u odnosu na Internet korisnike (%)	Postotak „camera“ rezultata u odnosu na Internet korisnike (%)	Postotak Netwave web kamera u odnosu na Internet korisnike (%)
Njemačka	79,127,551	0,0004	0,3257	0,0043
Francuska	60,421,689	0,0002	0,1809	0,0035
Luksemburg	636,565	0	0,0698	0,0012
Cipar	1,320,400	0	0,1877	0,0011
Hrvatska	3,787,838	0,00002	0,2043	0,0009

Normalizacijom rezultata najviše je skeniranih sveukupnih web kamera u Njemačkoj, kao i Netwave web kamera. Iako je na Cipru pronađen manji broj uređaja, u odnosu na broj Internet korisnika, u postotku je manje ranjivih uređaja u Hrvatskoj.

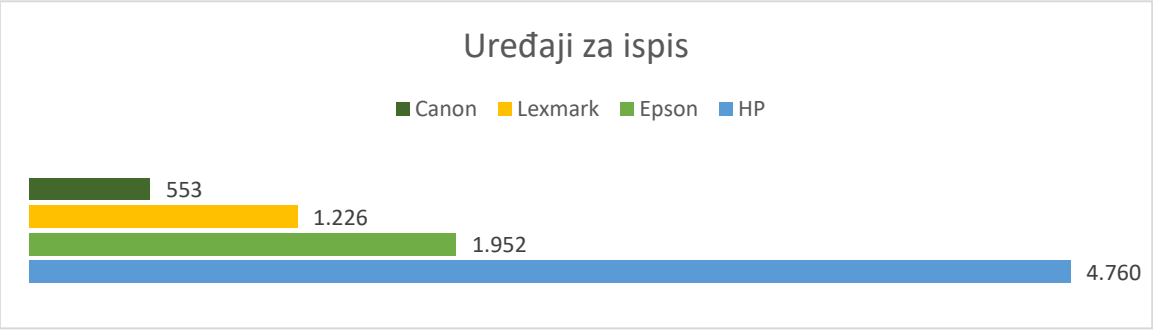
Za analizu uređaja za ispis skeniran je port 631 koji koristi protokol IPP. Uvidom u dobivene rezultate najviše uređaja je pronađeno u Njemačkoj (4 973) i Francuskoj (4 311). U odnosu na broj Internet korisnika u navedenim državama, rezultat IPP protokola u Njemačkoj iznosi 0,0008%, a u Francuskoj 0,0020%, iz čega je vidljivo da je u Francuskoj veći postotak izloženih uređaja za ispis. Najmanji broj skeniranih uređaja za ispis pronađen je u Crnoj

Gori, gdje je 18 uređaja skenirano na Internetu, što je u usporedbi s brojem Internet korisnika, rezultat od 0,0001%. U Hrvatskoj je skeniran 121 uređaj, odnosno 0,0007% u odnosu na broj Internet korisnika.

Tablica 5.7 Normalizacija rezultata - uređaji za ispis

Država	Broj Internet korisnika	Otvoreni IPP portovi u odnosu na Internet korisnike (%)	Postotak „HP“ uređaja u odnosu na Internet korisnike (%)	Postotak „Epson“ uređaja u odnosu na Internet korisnike (%)
Njemačka	79,127,551	0,0008	0,0012	0,0002
Francuska	60,421,689	0,0020	0,0010	0,0002
Italija	54,798,299	0,0008	0,0010	0,0017
Luksemburg	636,565	0,0017	0,0001	0
Crna Gora	547,000	0,0001	0,0003	0,0012
Hrvatska	3,787,838	0,0007	0,0002	0,0002

Kako bi se produbila analiza uređaja za ispis, odrađeni su upiti za pojedine proizvođače uređaja za ispis, odnosno proizvođače softvera koji su najčešće korišteni u državama Europske Unije. Grafičkim prikazom vidljiva je usporedba pojedinih proizvođača uređaja za ispis.



Analizom HP uređaja za ispis u zemljama Europske Unije pronađen je 5 341 rezultat od kojih je 4 760 (89,12%) uređaja dostupno putem HTTP protokola. Najviše odgovarajućih upita pronađeno je za Njemačku koja sadrži 21,89% ukupnog rezultata, odnosno po tablici

normalizacije 0,0012%. Samo je jedan skeniran HP uređaj u Luksemburgu, što je u odnosu na broj Internet korisnika rezultat od 0,0001%. U Hrvatskoj je skenirano deset HP uređaja za ispis, što u odnosu na broj korisnika iznosi 0,0002%.

Za Epson uređaje za ispis najviše rezultata, čak 48,41% je skenirano u Italiji. Drugi po redu rezultat je 225 skeniranih Epson uređaja u Njemačkoj, što je skoro četiri puta manje od broja uređaja u Italiji. Po samo jedan skenirani Epson uređaj za ispis nalazi se u Litvi, Estoniji, Danskoj i Cipru. U Hrvatskoj je skenirano devet uređaja, što je u odnosu na broj Internet korisnika, rezultat od 0,0002%.

Izvršavanjem upita za Lexmark uređaje za ispis pronađeno je samo 1 226 rezultata, od kojih je više od polovice (54,81%) skenirano u Mađarskoj. Lexmark uređaji za ispis pronađeni su u samo 22 države Europske Unije, čime se može zaključiti da nisu korišteni u velikoj mjeri. Samo jedan uređaj skeniran je u Hrvatskoj i Luksemburgu.

Najmanje pronađenih uređaja za ispis je proizvođača Canon za koje je skenirano samo 553 uređaja. Najveći broj (90) skeniranih uređaja je u Njemačkoj.

5.2.3. Preporuke za zaštitu od napada

Velik broj korisnika pri prvom korištenju web kamere, kao i uređaja za ispis ostavlja predefinirane korisničke podatke za prijavu ili uopće ne podešavaju iste. Primarni korak pri zaštiti od potencijalnih napada je postavljanje snažnih i kompleksnih lozinki koje će napadaču onemogućiti jednostavan pristup. Ukoliko uređaji imaju mogućnost postavljanja više faktorske autentikacije, preporuka ih je konfigurirati.

Kompanije koje proizvode web kamere i uređaje za ispis i stavljaju ih na tržište, mogu detektirati pojedine ranjivosti uređaja te ih „zakrpati“ novom nadogradnjom softvera. Korisnicima bi trebali redovno ažurirati softver u svrhu izbjegavanja potencijalnih napada.

Web kamere, kao i uređaji za ispis mogu biti bežično povezani s ostatkom mreže. Ukoliko je to slučaj, sigurnosna preporuka je uključiti WPA2 enkripciju na uređajima te ih na taj način dodatno zaštiti.

Obzirom da su uređaji za ispis kroz lokalnu mrežu povezani na Internet, sigurnosni stručnjaci savjetuju izoliranje navedenih uređaja od interneta na način da se ACL listama (engl. *Access Control List*) ograniči pristup na određene subnete te da se onemogući usmjeravanje prometa prema internetu čime uređaji za ispis postaju dostupni samo u lokalnoj mreži.

Predefiniranom konfiguracijom na uređajima za ispis omogućeni su pojedini servisi, kao što su Telnet ili FTP, čije su ranjivosti prikazane u prethodnom poglavlju. Korištenjem navedenih servisa, napadač može dobiti pristup uređajima za ispis, stoga se savjetuje onemogućavanje tih servisa, kao i ostalih servisa koji nisu potrebni za obavljanje funkcija samog uređaja.

Korištenjem IPP protokola, predefinirano nije uključena enkripcija te se uređajima za ispis kod web pristupa koristi HTTP protokol. IPPS je sigurna verzija IPP protokola koja koristi SSL na portu 443, čime je korisnicima omogućen siguran pristup uređajima i njihova funkcija ispisivanja.

5.3. Analiza sigurnosnih ranjivosti servisa Memcached i DNS

DoS (engl. *Denial of Service*) napadi su napadi u kojima se enormnom količinom mrežnog prometa uskraćuje usluga klijentima te je zaštita od DoS napada postao veliki izazov za sigurnosne stručnjake. Napadač će izvršiti napad na način da presretne komunikaciju između klijenta i servera te umjesto servera klijentu šalje podatke. Osim velike količine podataka, napadač klijentu može servirati i maliciozni sadržaj pod krinkom legitimnog odgovora na klijentski zahtjev. Pojedini servisi sadrže sigurnosne mane kojima napadač može presresti komunikaciju i kompromitirati sustav. U ovom dijelu rada predstavljeni su servisi Memcached i DNS te je odražena analiza njihovih ranjivosti.

5.3.1. Analiza ranjivosti

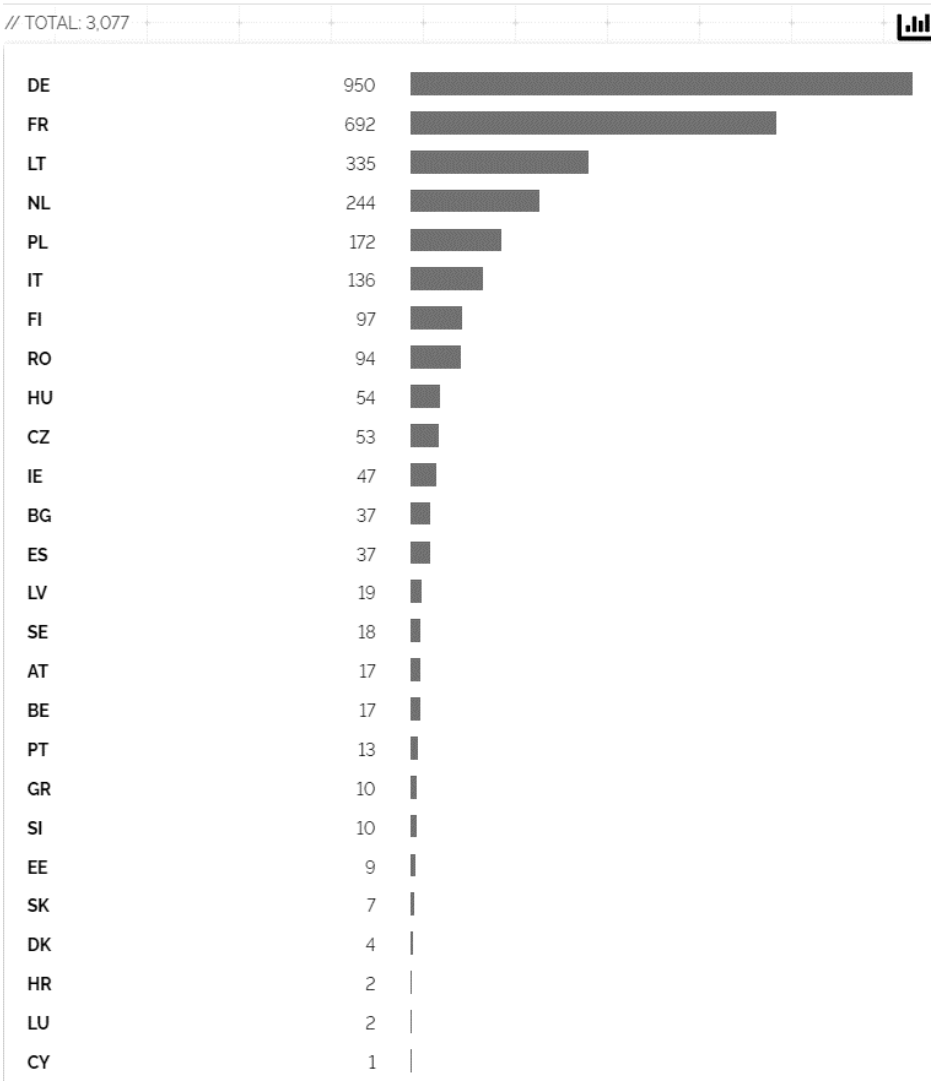
Memcached je mehanizam [22] otvorenog koda koji prikuplja podatke i pohranjuje ih u dinamičku memoriju. Pohranjivanjem podataka u međuspremnik nastoji se ubrzati proces dohvaćanja podataka iz baze, kao i njihovo posluživanje.

Memcached serveri imaju mogućnost rada na UDP protokolu (port 11211), koji po svom načinu rada šalje i prima podatke neovisno o drugoj strani konekcije, odnosno neovisno o tome je li konekcija s druge strane prihvaćena i jesu li podaci pristigli na odredište ili ne. Zbog te mogućnosti Memcached serveri koji koriste UDP su ranjivi te potencijalno dolazi do DoS napada.

Napadač *spoofa* ranjivi Memcached server, odnosno u ime žrtve šalje zahtjeve za podacima serveru. Memcached server će u tom slučaju preopteretiti žrtvu mrežnim prometom i velikim količinama podataka, nakon čega dolazi do nemogućnosti korištenja usluge.

Za analizu Memcached servera u zemljama EU, koji rade na portu 11211, pronađeno je ukupno 3 154 rezultata, od kojih gotovo svi (3 077) koriste UDP port 11211.

udpport:"11211" product:"Memcached"
country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se



Slika 5.25: Memcached serveri (udpport 11211)

Za Memcached servere koji rade na portu 11211, pronađeno je ukupno 3 154 rezultata.

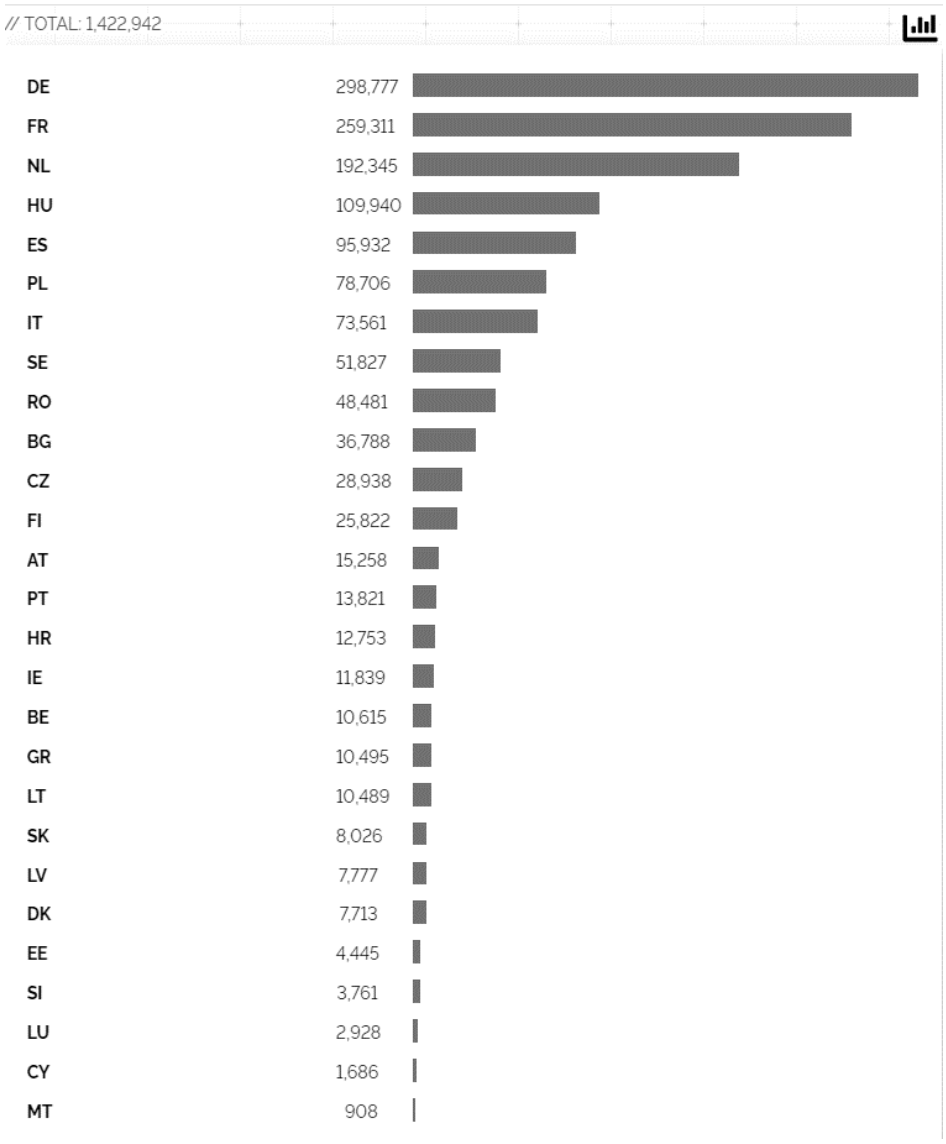
DNS (engl. *Domain Name System*) prevodi imena domena u IP adrese te radi na portu 53. Prilikom pristupanja klijenta web stranici, DNS upiti se izvršavaju na dva načina: iterativno

i rekurzivno[23]. Iterativni DNS upit radi na principu da se DNS upiti izvršavaju dok god klijent ne dobije traženi zapis, na način da svaki DNS server koji nema navedeni zapis, vraća informaciju klijentu o drugom DNS serveru.

Rekurzivni DNS serveri izvršavaju upite tako da šalju upite drugim DNS serverima te na kraju kada dobiju odgovarajući DNS zapis, dostavljaju klijentu.

Skeniranjem otvorenih DNS portova, pronađeno je 1 422 942 rezultata u državama Europske Unije.

"port: 53" country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se



Slika 5.26 Otvoreni DNS portovi

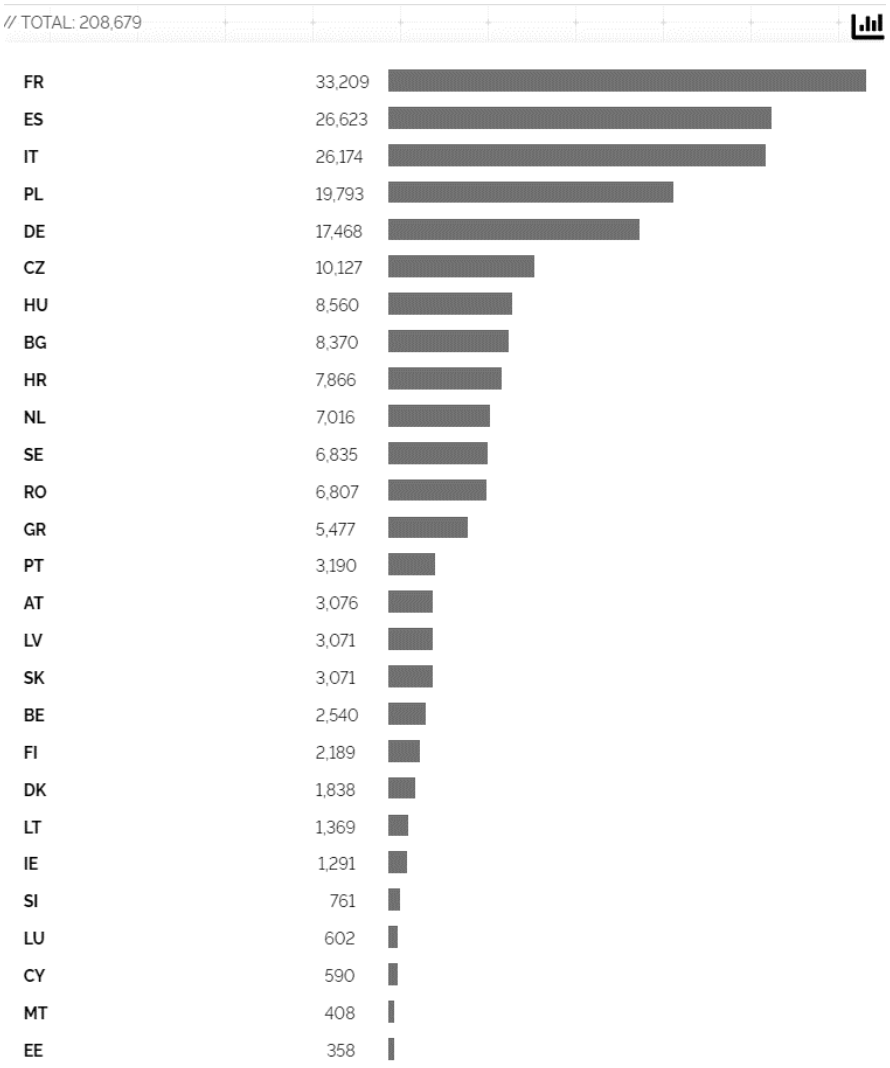
Obzirom da rekurzivni DNS koristi predmemoriju (engl. *cache*) u kojemu pohranjuje prethodne izvršene upite, rekurzivni DNS server je brži za razliku od iterativnog no, zbog principa na kojemu radi, DNS je pogodan za pojedine napade.

Jedan od napada je DNS cache poisoning napad u kojemu napadač presretne komunikaciju između klijenta i DNS servera. Na traženi klijentski upit, napadač prosljeđuje informacije te ga potencijalno usmjerava na malicioznu web stranicu. Obzirom da DNS server koristi cache, tu informaciju će proslijediti i drugim klijentima te potencijalno zaraziti cijeli sustav.

Kroz Shodan su pretraženi uređaji koji imaju omogućen rekurzivni DNS.

"port: 53" Recursion: Enabled

country:at,be,bg,cz,dk,de,ee,ie,gr,es,fr,hr,it,cy,lv,lt,lu,hu,mt,nl,pl,pt,ro,si,sk,fi,se



Slika 5.27 Omogućen rekurzivni DNS po državama

5.3.2. Komparacija rezultata

Za Memcached servere koji rade na portu 11211, pronađeno je ukupno 3 154 rezultata, od kojih gotovo svi (3 077) koriste UDP port 11211. Najveći broj skeniranih otvorenih UDP portova pronađeno je u Njemačkoj, gdje se nalazi 31,19% Memcached servera i Francuskoj gdje se nalazi 22,48% ukupnih rezultata. Najmanji broj skeniranih rezultata nalazi se na Cipru, gdje je skeniran samo jedan otvoreni port. Pregledom skeniranih rezultata u Hrvatskoj pronađena su dva Memcached servera s UDP portom 11211.

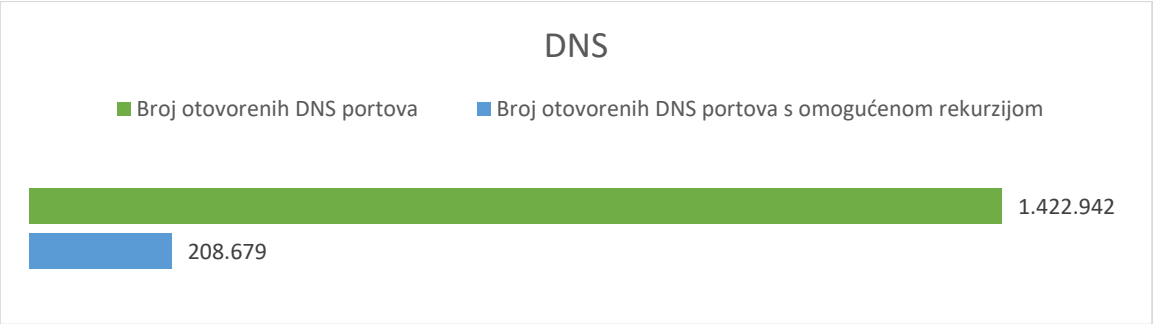
Da bi se dobio djelomično vjerniji prikaz rezultata, kreirana je tablica normaliziranih rezultata za države s najvećim i najmanjim brojem pronađenih rezultata te s rezultatima u Hrvatskoj.

Tablica 5.8 Normalizacija rezultata - Memcached

Država	Broj Internet korisnika	Postotak otvorenih UDP portova 11211 u odnosu na Internet korisnike (%)
Njemačka	79,127,551	0,0012
Francuska	60,421,689	0,0011
Litva	2,603,900	0,0128
Luksemburg	636,565	0,0003
Cipar	1,320,400	0,0001
Hrvatska	3,787,838	0,0001

U Njemačkoj je skenirano 950 otvorenih 11211 portova što u usporedbi s brojem Internet korisnika iznosi 0,0012%, dok je u Litvi skenirano skoro tri puta manje otvorenih portova (335) te je u usporedbi s brojem Internet korisnika to rezultat od 0,0128%, čime je zaključeno da je Litva po ovoj kategoriji ranjivosti, nesigurnija.

Analizom DNS servisa u državama Europske Unije, skenirano je 1 422 942 otvorenih portova. Skeniranjem ranjivih portova, odnosno portova na kojima je podešen rekurzivni DNS, uočeno je da 14,66% DNS servisa koristi rekurzivne upite.



Analizom skeniranih rezultata uočeno je da se najveći broj otvorenih DNS portova nalazi u Njemačkoj te da je od 298 777 portova, 5,84% ranjivo. Pregledom dobivenih rezultata za Francusku, u kojoj je detektiran najveći broj rekurzivnih DNS-ova, uočeno je da je 12,8% sveukupno skeniranih portova u Francuskoj nesigurno. Iako je u Crnoj Gori pronađen najmanji broj rezultata, njih 908, čak 44,93% od njih ih je ranjivo. Najmanje pronađenih DNS portova s omogućenom rekurzijom pronađeno je u Estoniji te je naspram DNS portova u toj državi ranjivo samo 8% skeniranih rezultata.

U Hrvatskoj je skeniranjem DNS portova pronađeno 12 753 otvorenih DNS portova od kojih je 61,83% s omogućenom rekurzijom, čime se Hrvatska pozicionirala visoko na ljestvici.

Tablica 5.9 Normalizacija rezultata - DNS

Država	Broj Internet korisnika	Postotak otvorenih DNS portova u odnosu na Internet korisnike (%)	Broj otvorenih rekurzivnih DNS portova u odnosu na Internet korisnike (%)
Njemačka	79,127,551	0,3775	0,0220
Francuska	60,421,689	0,4291	0,0549
Španjolska	43,509,182	0,2204	0,0612
Crna Gora	547,000	0,1659	0,0745
Estonija	1,276,521	0,3482	0,0280
Hrvatska	3,787,838	0,3366	0,2076

Normalizacijom rezultata po broju Internet korisnika u državama Europske Unije, uočeno je da je po analizi rekurzivnih DNS servisa Hrvatska nezaštićenija od Njemačke, Francuske i

Španjolske u kojima je skenirano najviše otvorenih DNS portova. Iako je u Njemačkoj pronađeno najviše otvorenih DNS portova, samo 5,84% ih je nesigurno te je u usporedbi s brojem Internet korisnika rezultat manji nego u drugim državama.

5.3.3. Preporuke za zaštitu od napada

Analizom ranjivosti Memcached servera, utvrđeno je da određeni broj servera koristi UDP protokol za pohranu i pristup predmemoriranim podacima te da je time napadačima omogućen pristup serveru koji rezultira napadom uskraćivanja usluge (engl. Denial of service). Za zaštitu Memcached servera potrebno je povezati server s lokalnim sučeljem (127.0.0.1) te onemogućiti korištenje UDP protokola čime bi se sav promet odvijao koristeći TCP protokol na portu 11211. Za zaštitu od napada, preporučljivo je podesiti vatrozide tako da se na Memcached serverima dopusti pristup samo određenim uređajima, odnosno IP adresama klijentskih strana.

Omogućavanjem rekurzivnog DNS servera se DNS upiti izvršavaju brže, prvenstveno zato što rekurzivni DNS koristi međuspremnik čime se dohvaćanje DNS upita olakšava te je klijentima uvijek dostavljena samo konačna informacija. Unatoč tomu, korištenje rekurzivnog DNS servera predstavlja sigurnosni rizik, kako za pojedine klijent, tako i za cijeli sustav jer napadač može presresti komunikaciju te klijenta usmjeriti na malicioznu stranicu. Sigurnosni stručnjaci savjetuju izbjegavanje korištenja rekurzivnog DNS-a, odnosno njegovo onemogućavanje na sustavu čime će se znatno ojačati sigurnost i izbjeći mogućnost napada uskraćivanja usluge.

Zaključak

Razvoj tehnologija i porast broja uređaja povezanih na Internet doveli su do porasta sigurnosne izloženosti istih. Većina privatnih korisnika uređaje spojene na Internet ostavlja s predefiniranom konfiguracijom i predefiniranim pristupnim podacima, što predstavlja značajne sigurnosne prijetnje, kao i sigurnosne izazove protiv istih. Posebice kada se radi o uređajima iz kategorije Internet stvari kojima je svrha olakšati svakodnevni život korisnika, no da bi to zaista i bilo tako, potrebno je imati svijest da su svi ti uređaji javno dostupni i da predefinirane postavke ne mogu biti zadovoljavajuće rješenje.

Paralelno sa razvojem tehnologija, razvijana je i inteligencija čija je primarna svrha prikupljanje podataka o svim dostupnim i javnim uređajima na internetu – OSINT. Premda je OSINT često korišten s negativnim namjerama, potrebno je iskoristiti sve beneficije te inteligencije kako bi se pronašle ranjivosti i osigurale se. Jedan od OSINT alata korisnih u pretraživanju svih uređaja spojenih na Internet je Shodan, pretraživač koji je u stanju pronaći uređaje poput desktop računala pa sve do nuklearne elektrane. Rad prikazuje Shodan pretragu svih europskih država po protokolima FTP, RDP, SMB, Telnet i SSL te analizu dobivenih rezultata. Obzirom da broj pronađenih rezultata ovisi i o broju stanovnika pojedine države, odnosno broju korisnika Interneta, u radu je odrađena normalizacija istaknutih podataka. Potom su pretražene sve Web kamere i uređaji za ispis u Europi, analizirane su ranjivosti pristupa uređajima i dane preporuke za zaštitu od napada. Analizirani su servisi Memcached i DNS, gdje je uočeno da postoji oko milijun i pol otvorenih DNS portova u državama Europske Unije.

Popis kratica

IoT	*Internet of Things*	Internet stvari
OSINT	*Open Source Intelligence*	inteligencija otvorenih izvora podataka
FTP	*File Transfer Protocol*	protokol za prijenos datoteka
RDP	*Remote Desktop Protocol*	protokol za udaljene uređaje
SMB	*Server Message Block*	protokol za dijeljenje podataka
TCP	*Transmission Control Protocol*	transportni protokol
UDP	*User Datagram Protocol*	transportni protokol
IP	*Internet Protocol*	Internet protokol
SSL	*Secure Sockets Layer*	sigurnosni protokol prijenosa podataka
CA	*Certification Authority*	certifikacijsko tijelo
HTTP(S)	*HyperText Transfer Protocol (Secure*)	web protokol
IPP	*Internet Printing Protocol*	protokol uređaja za ispis
DoS	*Denial of Service*	uskraćivanje usluge
DNS	*Domain Name System*	sustav imenovanja domenskih imena

Popis slika

Popis tablica

Literatura

[1] J. MATHERLY, "THE COMPLETE GUIDE TO SHODAN: COLLECT. ANALYZE. VISUALIZE. MAKE INTERNET INTELLIGENCE WORK FOR YOU", FEBRUARY 28, 2016

[2] N. A. Hassan, "Digital Forensics Basics: A Practical Guide Using Windows OS", February 25, 2019

[3] B. GENGE, C. ENĂCHESCU, "SHOVAT: SHODAN-BASED VULNERABILITY ASSESSMENT TOOL FOR INTERNET-FACING SERVICES" HTTPS://ONLINELIBRARY.WILEY.COM/DOI/EPDF/10.1002/SEC.1262 (ACCESSED 2022)

[4] B. RADVANOVSKY, "PROJECT SHINE", 10TH SANS ICS SECURITY SUMMIT, FEBRUARY 23-24, 2015.

[5] "ANALYSIS OF VULNERABILITIES IN MQTT SECURITY USING SHODAN API AND IMPLEMENTATION OF ITS COUNTERMEASURES VIA AUTHENTICATION AND ACLS" HTTPS://IEEEXPLORE.IEEE.ORG/DOCUMENT/8554472 (ACCESSED MAY 10, 2022

[6] Y. CHEN, "EXPLORING SHODAN FROM THE PERSPECTIVE OF INDUSTRIAL CONTROL SYSTEMS" HTTPS://IEEEXPLORE.IEEE.ORG/STAMP/STAMP.JSP?ARNUMBER=9072175 (ACCESSED DECEMBER 4 2022)

[7] H. AL-ALAMI, A. HADI, "VULNERABILITY SCANNING OF IOT DEVICES IN JORDAN USING SHODAN" HTTPS://IEEEXPLORE.IEEE.ORG/DOCUMENT/8277814 (ACCESSED MAY 10, 2022)

[8] A. ALBATAINEH, I. ALSMADI, "IOT AND THE RISK OF INTERNET EXPOSURE: RISK ASSESSMENT USING SHODAN QUERIES" HTTPS://IEEEXPLORE.IEEE.ORG/DOCUMENT/8792986 (ACCESSED MAY 10, 2022)

[9] „WHAT IS SHODAN? HOW TO USE IT & HOW TO STAY PROTECTED" HTTPS://WWW.SAFETYDETECTIVES.COM/BLOG/WHAT-IS-SHODAN-AND-HOW-TO-USE-IT-MOST-EFFECTIVELY/ (ACCESSED MAY 9, 2022)

[10] „TOP SHODAN DORKS" HTTPS://SECURITYTRAILS.COM/BLOG/TOP-SHODAN-DORKS (ACCESSED NOVEMBER 27, 2022)

[11] „HOW TO USE THE INTERNET PRINTING PROTOCOL" HTTPS://WWW.PWG.ORG/IPP/IPPGUIDE.HTML DORKS (ACCESSED FEBRUARY 20, 2023)

[12] „SECURING REMOTE DESKTOP (RDP) FOR SYSTEM ADMINISTRATORS" HTTPS://SECURITY.BERKELEY.EDU/EDUCATION-AWARENESS/SECURING-REMOTE-DESKTOP-RDP-SYSTEM-ADMINISTRATORS(ACCESSED FEBRUARY 20, 2023)

[13] „NETWORK PRINTER SECURITY BEST PRACTICES" HTTPS://SECURITY.BERKELEY.EDU/EDUCATION-AWARENESS/NETWORK-PRINTER-SECURITY-BEST-PRACTICES(ACCESSED FEBRUARY 18, 2023)

[14] „WHAT IS SSL? | SSL DEFINITION" HTTPS://WWW.CLOUDFLARE.COM/LEARNING/SSL/WHAT-IS-SSL/(ACCESSED FEBRUARY 18, 2023)

[15] „Dangers of Using Self-Signed Certificates“ https://securitytrails.com/blog/dangers-of-using-self-signed-certificates(accessed February 20, 2023)

[16] „What is Maltego? | How to use it for Information Gathering.“ https://www.cybervie.com/blog/what-is-maltego-how-to-use-it-for-information-gathering/(accessed February 21, 2023)

[17] „FTP (File Transfer Protocol)“ https://www.techtarget.com/searchnetworking/definition/File-Transfer-Protocol-FTP(accessed February 17, 2023)

[18] „What is the SMB protocol?“ https://nordvpn.com/blog/what-is-smb/(accessed February 20, 2023)

[19] „Introduction to TELNET“ https://www.geeksforgeeks.org/introduction-to-telnet/(accessed February 21, 2023)

[20] „SFTP vs. FTPS: Understanding the 8 Key Differences“ https://www.spiceworks.com/tech/networking/articles/sftp-vs-ftps/(accessed February 24, 2023)

[21] „What Is SMB Protocol and Why Is it a Security Concern?“ https://cybersophia.net/articles/what-is/what-is-smb-protocol-and-why-is-it-a-security-concern/#Security_Issues_and_Concerns(accessed February 19, 2023)

[22] „Memcached DDoS attack“ https://www.cloudflare.com/learning/ddos/memcached-ddos-attack/(accessed February 24, 2023)

[23] „What is recursive DNS?“ https://www.cloudflare.com/learning/dns/what-is-recursive-dns/(accessed February 22, 2023)

[24] „Metagoofil – Tool to Extract Information from Docs, Images in Kali Linux“ https://www.geeksforgeeks.org/metagoofil-tool-to-extract-information-from-docs-images-in-kali-linux/(accessed February 22, 2023)

[25] „Internet User Statistics & 2022 Population for the 53 European countries and regions“ https://www.internetworldstats.com/stats4.htm(accessed February 24, 2023)

[26] „Ultimate OSINT with Shodan: 100+ great Shodan queries“ https://www.osintme.com/index.php/2021/01/16/ultimate-osint-with-shodan-100-great-shodan-queries/(accessed February 19, 2023)

[27] „Awesome Shodan Search Queries“ https://github.com/jakejarvis/awesome-shodan-queries/blob/main/readme.md#network-attached-storage-nas(accessed February 19, 2023)

[28] „Shodan Dorks“ https://github.com/humblelad/Shodan-

DORKS/BLOB/MASTER/README.MD#WINDOWS-RDP-PASSWORD(ACCESSED FEBRUARY 19, 2023)