Cyber kriminal i sustavi zaštite u moderno doba

Granđa Kozjak, Edita

VELEUČILIŠTE SUVREMENIH INFORMACIJSKIH TEHNOLOGIJA

STRUČNI DIPLOMSKI STUDIJ INFORMACIJSKIH TEHNOLOGIJA

Edita Granđa Kozjak

DIPLOMSKI RAD

CYBER KRIMINAL I SUSTAVI ZAŠTITE U MODERNO DOBA

Zagreb, listopada 2024.

Veleučilište suvremenih informacijskih tehnologija
10000 Zagreb, Ulica Vjekoslava Klaića 7

Studij:	Stručni diplomski studij informacijskih tehnologija smjer računalni sustavi
Student:	**Edita Granđa Kozjak**
Matični broj:	2019096

Zadatak diplomskog rada

Predmet:	Razvoj pouzdanih programa
Naslov:	**Cyber kriminal i sustavi zaštite u moderno doba**
Zadatak:	Istražiti povijest, vrste i kategorije kibernetičkog kriminala te sustave koji osiguravaju računalnu sigurnost. U praktičnom radu simulacijom prikazati način na koji hakeri iskorištavaju nedovoljno znanje žrtava te opisati potencijalnu štetu ako napadač uspije ostvariti svoj cilj.
Mentor:	Edmond Krusha, v. pred.
Zadatak uručen kandidatu:	19.10.2023.
Rok za predaju rada:	29.10.2024.
Rad predan:	_____

Povjerenstvo:

Jurica Đurić, v. pred.	član predsjednik	_____
Edmond Krusha, v. pred.	mentor	_____
mr. sc. Danijel Vještica Obradović, v. pred.	član	_____

SADRŽAJ

POPIS SLIKA

POPIS TABLICA

1. UVOD

Tehnologija danas, u digitaliziranom svijetu, okružuje ljudsku svakodnevicu. Fizičke, ali i pravne osobe, odnosno organizacije, izrazito se oslanjaju na tehnologiju, kako u privatnom, tako i poslovnom smislu.

Tehnologija, primjerice mobilni uređaji, pojedincu pruža pristup informacijama na dlanu, a poslovnim subjektima uvelike poboljšava komunikaciju s partnerima i klijentima te olakšava poslovanje. Komunikacija koja se prije nekoliko desetaka godina odvijala s pomoću pisama, kojima su bili potrebni dani da stignu primatelju, danas se obavlja u nekoliko klikova mišem te je pojedincu, ali i organizaciji, informacija dostupna unutar nekoliko sekundi. S rastom potrebe za što bržim pristupom informacijama i što većom količinom informacija, rastu i opasnosti od zlouporabe istih. Korisnici tehnologije, bilo u osobne ili poslovne svrhe, trebaju biti svjesni da podatci koji nisu adekvatno zaštićeni mogu biti zloupotrijebljeni.

Razumljivo je da u modernom dobu postoje sustavi koji običnog korisnika tehnologije, primjerice društvenih mreža, štite od moguće zloupotrebe. Međutim, u pojedinim slučajevima pokazalo se da ti sustavi zaštite nisu dovoljni zbog spretnosti i strategija koje se koriste za zlouporabu informacija stečenih od korisnika.

Moderan svijet, osim što nudi raznovrsne usluge putem tehnologija, također nudi i raznovrsne mogućnosti za zaštitu tehnologija koje se koriste. Često je slučaj da prosječni korisnici, koji nisu svjesni načina na koji njihovi osobni podaci mogu biti zloupotrijebljeni, ne iskazuju značajnu zabrinutost sve dok ne postane prekasno za provedbu zaštite nad tim podatcima. Također, često se primjećuje da organizacije, odnosno poslovni subjekti, premalo ulažu u sigurnost vlastitih podataka kao i podataka o zaposlenicima. Napredovanjem tehnologija i širenjem tehničkog znanja, posljedice kibernetičkog kriminala postaju sve očitije. U kontekstu zaštite bilo kakvih sustava, bilo za pojedinca ili organizaciju, nije moguće jamčiti potpunu sigurnost. Osim toga što se može dogoditi napad koji potencijalno izaziva štetu, otuđenje podataka ili izaziva nekakav drukčiji oblik štete, jednako tako i pojedinac može nesvjesno ili svjesno napraviti grešku koja se može smatrati kibernetičkim kriminalom.

U ovom diplomskom radu pokušat će se detaljnije pojasniti što je to kibernetički kriminal (*engl. cybercrime*), kako utječe na pojedinca i na poslovni svijet, odnosno organizacije, te koji su sustavi i mjere poduzete u modernom dobu za zaštitu od istoga. Za bolje razumijevanje teksta koristit će se u, pojedinom dijelu rada, tehnički engleski nazivi.

Za bolje razumijevanje ove teme, ključno je najprije razumjeti početak i razvoj ovakve vrste kriminala te početak zaštite od njega.

U prvom dijelu rada detaljnije će se posvetiti povijesti i razvoju kibernetičkog kriminala i sustava zaštite. Također, kibernetički kriminal kao pojava sama po sebi izazvao je niz drukčijih pojava u modernom dobu, poput osoba koje iskorištavaju slabosti sustava, kao što su hakeri. Nije pravilo da se nužno radi o zloupotrebi, moguće je da se tehnikama iskorištavanja sustava otkriju slabosti i problemi unutar raznih tehnologija, te tim znanjem osigurava pravovaljana zaštita istoga.

U ovom diplomskom radu također će se na stvarnim primjerima, uz utjecaj virusa COVID-19 te ratnih zbivanja u Ukrajini, prikazati kako kibernetički kriminal utječe na pojedinca i organizacije.

2. CYBER KRIMINAL I SUSTAVI ZAŠTITE

Kibernetički kriminal jedan je od najvećih i globalno najaktivnijih oblika kriminala današnjice. Pojavljuje se u različitim oblicima i nastavlja se razvijati.

Za pojam kibernetičkog kriminala (*engl. cybercrime*) postoji mnogo definicija, međutim, niti jedna od njih u potpunosti ne može obuhvatiti ovaj široki pojam. Najbolja definicija bila bi da je to zločin koji uključuje računalo i mrežu radi vlastite financijske ili neke druge vrste koristi, poput onesposobljavanja napadnutih računala ili nanošenja štete.

2.1. Povijest kibernetičkog kriminala

Činjenica je da se kroz povijest pokazalo kako postoje pojedinci ili skupine koji na ilegalne načine pokušavaju ostvariti korist ili nanijeti štetu drugima. Razvijanjem tehnologije razvija se i nova vrsta kriminala – kibernetički kriminal. Već se 60-ih godina prošlog stoljeća prvi put spominje korištenje računala u svrhu kriminalnih radnji, no kibernetički kriminal prošlog stoljeća uvelike se razlikuje od današnjeg.

Glavnu razliku čini internet, koji je stigao kasnije, te računala nisu bila spojena na mrežu. U početku su računala bila izrazito skupa, sastojala su se od iznimno velikih komponenti i zahtijevala posebne načine hlađenja. Upravo iz tih razloga sav računalni kriminal bio je povezan s kriminalom vezanim uz financijske investicije u računala.

Povijest kibernetičkog kriminala može se nazvati i poviješću hakiranja. Haker (*engl. hacker*) je osoba koja posjeduje izuzetna znanja u području informacijskih tehnologija i koristi svoja tehnička znanja za ostvarivanje ciljeva ili prelaženje prepreka.

Postoji nekoliko vrsta hakera:

- „White hat“ haker – Hakeri koji rade na zaštiti podataka od drugih hakera tako da pronalaze nesavršenosti sustava. Uglavnom ih zapošljavaju vlasnici sustava te zbog toga njihov rad nije protuzakonit.
- „Black hat“ haker – Hakeri sa zlim, odnosno lošim namjerama. Iskorištavaju, kradu i stvaraju financijsku korist od podataka. Njihov rad je ilegalan.
- „Grey hat“ haker – Hakeri ili eksperti računalne sigurnosti koji ponekad krše zakone i etičke standarde, ali većinom nemaju maliciozne namjere. Ovaj termin počeo se koristiti 90-ih godina prošlog stoljeća.

Za bolje shvaćanje pojma kibernetičkog kriminala, pojasniti će se dodatni pojmovi vezani uz njega, a u narednom tekstu detaljnije će se objasniti metode koje se koriste za izvršavanje određenih vrsta kibernetičkih napada.

2.2. Metode korištene za kibernetički kriminal

Može se reći da kibernetički kriminalci koriste skup alata ili metoda dizajniranih za kršenje informacijskih resursa u fazi njihovog stvaranja, obrade, pohrane i distribucije. U narednim potpoglavljima detaljnije će se definirati metode koje se koriste u kibernetičkom kriminalu.

2.3. Backdoor

„Backdoor“ je metoda za pristupanje računalnom sustavu ili kriptiranim podacima kojom se zaobilaze uobičajeni sigurnosni mehanizmi. Programer može stvoriti ovakvu metodu unutar aplikacije ili operativnog sustava radi popravljanja grešaka u sustavu ili drugih svrha, međutim, napadači često iskorištavaju postojeće metode ili ih instaliraju tijekom napada. U nekim slučajevima „crv“ ili „virus“ dizajniran je da iskoristi prednosti „backdoor-a“ stvorenog u prethodnom napadu. Ovo je vrsta zlonamjernog softvera koja zaobilazi ili negira uobičajene postupke provjere autentičnosti za pristup sustavu.

Ovom metodom kibernetičkog kriminala omogućen je udaljen pristup resursima unutar aplikacije, kao što su baze podataka i poslužiteljske datoteke. Time je počinitelju kriminala omogućeno udaljeno izdavanje sistemskih naredbi i ažuriranje zlonamjernog softvera.

Najčešće se koristi u svrhe:

- krađe podataka
- otmice poslužitelja
- uništavanja mrežne stranice
- pokretanja distribuiranih napada uskraćivanjem usluge (DDoS) *(engl. Distributed Denial of Service)*
- inficiranja posjetitelja mrežne stranice stranice
- napada na napredne trajne prijetnje (APT) *(engl. Advanced Persistent Threat)*.

Počinitelji koji koriste ovu metodu kibernetičkog kriminala najčešće identificiraju svoje mete pomoću skenera koji lociraju mrežne stranice sa zastarjelim komponentama ili lošom konfiguracijom. Nakon instaliranja „backdoora“ na temeljni poslužitelj, gdje je pristup mogući u bilo kojem trenutku, čak i ako je ranjivost zbog koje je omogućena njegova instalacija u međuvremenu uklonjena.

Nažalost, kada se infiltrira na računalo koje je napadnuto, vrlo ga je teško ukloniti. Otkrivanje ove metode na zaraženom računalu radi se uz pomoć skenera, odnosno antivirusnog programa za traženje poznatih programa koji su specifično dizajnirani da oštete računalo, ometaju njegov rad ili koji omogućuju neovlašten pristup operativnom sustavu *(engl. malware).* Međutim, ovaj proces sklon je pogreškama. Datoteke koje koristi „backdoor“ gotovo su uvijek maskirane

upotrebom pseudonima i zamaskiranog kôda, odnosno višestrukim slojevima enkripcije. Detekcija je dodatno otežana time što su mnoge aplikacije izgrađene na način da koriste dodatke trećih strana, a u većini su slučajeva vrlo ranjive.

2.4. Računalni virusi

Računalni virusi su posebni programi koji su ugrađeni u računalni softver s namjerom da uništavaju, iskrivljuju ili ometaju njegov rad. Mogu se prenositi preko komunikacijskih linija ili podatkovnih mreža. Osim toga, mogu se i sami reproducirati.

Postoji nekoliko tipova računalnih virusa, a osnovni su:

- boot resor virusi – infiltriraju se u Master Boot Record (resor tvrdog diska ili drugog medija za pohranu podataka koji sadrži kôd za pokretanje programa, obično operacijskog sustava)
- programski virusi – oni se aktiviraju izvršavanjem zaražene datoteke
- makro virusi – imaju mogućnost brisanja i kopiranja samih sebe te mijenjanja dokumenata, napisani su višim programskim makro jezikom.

Računalni virusi koriste tehnike prikrivanja. Svaki računalni „virus“ ima svoj potpis. Potpis je broj izveden iz niza teksta (algoritam ili hash) koji je jedinstven za određeni virus. Međutim, postoje razne tehnike kojima virusi mijenjaju svoje potpise. Njihov se algoritam prilikom svake zaraze sustava mijenja što programu za pronalaženje zlonamjernih programa izuzetno otežava detekciju virusa. Neke od tehnika su:

- „Stealth” tehnike – presreću zahtjeve koje program za pronalaženje virusa šalje prema operativnom sustavu te obmanjuju korisnika i antivirusni program
- polimorfni kôd – prilikom repliciranja, mijenja svoj kôd i duljinu te ga je teško detektirati
- metamorfni kôd – neki se virusi samostalno ponovno reprogramiraju mjenjajući time svoj kôd i potpis.

  Razlika između metamorfnog kôda i polimorfnog je u tome što metamorfni virus mijenja svoj kôd zadržavajući istu funkcionalnost dok polimorfni koristi tehnike šifriranja mjenjajući potpis.

Jedni od najozbiljnijih virusa do sada su:

- Word Concept (1995.) – makro računalni virus, prvi e-mail virus koji je inficirao Word dokumente. Godine 1996. bio je najrašireniji virus na svijetu, prisutan je još i danas
- Melissa (1999.) – računalni virus koji se sam slao svakome iz adresara računala. Prouzročena je šteta od otprilike 385 milijuna USD

- Michelangelo (1992.) – računalni virus koji je uzrokovao štetu na velikom broju računala
- Bubble boy (1999.) – prvi računalni virus koji se širio elektroničnom poštom
- Love bug (2000.) – poznatiji pod nazivom "I LOVE YOU" virus. Napravio je štetu od 8,75 milijardi USD te je u jednome danu zarazio 45 milijuna računala
- Code Red (2001.) – U samo devet sati zarazio je 250 000 računala. Procijenjena je šteta na 2,62 milijarde USD. Koristeći mane u sigurnosnom sustavu računala, pretvarao je računala u tzv. „zombije" koji odbijaju naredbe.

2.5. Trojanski konj

Zlonamjerni računalni program pod nazivom Trojanski konj, koji se preuzima na računalo prerušen kao legalan program, no nakon instalacije obavlja maliciozno djelovanje. Ima mogućnost izmjene operacijskog sustav na računalu koje je zaraženo radi ostvarivanja koristi od strane napadača. Najopasniji slučaj trojanskog konja je onaj kada omogućuje potpunu kontrolu napadaču nad zaraženim operacijskim sustavom. Time napadač može:

- koristiti zaraženo računalo kao dio „botnet" mreže, odnosno mreže zaraženih računala kojom napadač upravlja
- ukrasti povjerljive podatke sa zaraženog računala
- instalirati druge zlonamjerne programe na zaraženo računalo
- primati, modificirati i slati datoteke zaraženog računala
- zabilježiti svaku pritisnutu tipku koju korisnik unosi na svojoj tipkovnici
- pratiti aktivnosti korisnika računala
- koristiti memoriju tvrdog diska
- rušiti operacijski sustav zaraženog računala i izvoditi još mnoge druge radnje.

Kod ove metode kibernetičkog kriminala napadač ne mora nužno biti i osoba koja je računalo zarazila trojanskim konjem. Dovoljno je da otkrije da je računalo zaraženo trojanskim konjem te na taj način može preuzeti kontrolu nad zaraženim računalom. Trojanski konj širi se kao dio računalnog programa, preko ranjivih komponenti računalnog programa, putem e-mail privitka, preuzimanjem zaraženog programa te putem zlonamjernih mrežnih stranica s dinamičkim sadržajem. Naravno, postoje antivirusni i drugi programi koji su specijalizirani isključivo za zaštitu od trojanskih konja. Nažalost, ako je napadač imao pristup računalu putem trojanskog konja uklanjanje je složeno zbog toga što je potrebno detektirati sve promjene sustava koje je napadač napravio.

2.6. Sniffer

Sniffer se definira kao analizator prometa, odnosno program ili uređaj koji prati podatke koji se prenose preko mreže. Tradicionalno se koristi za legitimne funkcije upravljanja mrežom, no moguće ga je koristiti i tijekom kibernetičkog napada za krađu informacija. Postoje dvije glavne vrste tehnika: aktivno i pasivno analiziranje prometa. Vrsta tehnike koja se koristi ovisi o strukturi mreže koja se pokušava analizirati. Pasivno analiziranje prometa omogućuje napadaču da ne komunicira s metom, odnosno ciljanim računalom, već da se jednostavno spoji na mrežu i dohvaća pakete koje mreža šalje ili prima između dva računala, dok kod aktivnog analiziranja prometa napadač izravno komunicira s napadnutim računalom slanjem paketa i primanjem odgovora.

Za zaštitu od ovakve vrste napada i krađe podataka potrebno je koristiti snažan sigurnosni program ili koristiti VPN *(engl. Virtual Private Network)*, uslugu koja omogućuje kriptiranu vezu između računala i interneta.

2.7. DDoS napadi

Distribuirano uskraćivanje usluge *(engl. Distributed Denial of Service)* incidenti su usko povezani s botnetima, gdje hakeri, odnosno napadači, preuzimaju zapovjedništvo i kontrolu nad tisućama zaraženih uređaja povezanih s internetom, a zatim u koordiniranim napadima usmjeravaju sve te uređaje da istovremeno šalju zahtjeve prema cilju.

Primarno postoje tri vrste DDoS napada. Prva vrsta napada je ona kod koje se koriste velike količine prometa prema računalima koja su napadnuta ili sustavima kako bi se opteretili serveri zahtjevima.

Druga vrsta napada uključuje korištenje mrežnih paketa s ciljem oštećenja mrežne infrastrukture i alata za upravljanje njome. Ovu vrstu napada karakterizira napad na aplikacijski sloj organizacije. U konačnici, primarni cilj ovakvih napada je isti – onemogućavati servise ili mrežne resurse.

Zbog svoje kompleksnosti, vrlo je teško zaštititi se od ovakve vrste napada, naročito jer mnogi nisu svjesni da njihova računala mogu biti korištena u svrhu napada. Osobito su česti napadi na organizacije, odnosno poslovne subjekte. Dakako, organizacije mogu poduzeti mjere predostrožnosti te implementirati dodatne sustave i opremu koji će takve napade smanjiti, odnosno ublažiti štetu koju mogu izazvati.

2.8. E-mail Spoofing

E-mail spoofing je oblik kibernetičkog napada u kojem haker šalje elektroničku poštu (e-mail) koja je manipulirana izgledajući kao da potječe iz stvarnog izvora. Ovo je jedna od popularnijih

metoda koje se koriste za krađu identiteta jer je vjerojatnije da će korisnik otvoriti elektroničku poštu ako je pošiljatelj netko koga poznaje. Većina ovakvih lažnih poruka može se lako prepoznati, no neke vrste mogu uzrokovati ozbiljne probleme i sigurnosne rizike. Primjerice, lažna elektronička pošta koja se predstavlja kao poruka s poznate mrežne stranice za kupnju može od primatelja zatražiti pružanje osjetljivih podataka, poput financijskih informacija, kao što je broj kreditne kartice.

Osim za krađu identiteta napadači koriste lažnu elektroničku poštu i za:

- skrivanje identiteta lažnog pošiljatelja
- zaobilaženje filtera neželjene pošte i popisa blokiranih pošiljatelja
- pretvaranje da su dobivene informacije od strane pouzdane osobe, prijatelja ili kolege kako bi dobili osjetljive podatake
- pretvaranje da su dobivene informacije od strane pouzdane organizacije, primjerice od financijskih institucija, kako bi dobili pristup podacima o kreditnoj kartici
- za narušavanje ugleda pošiljatelja za kojeg se napadači predstavljaju
- pokretanje i širenje zlonamjernog računalnog programa skrivenog u privicima i
- pristup osjetljivim podacima koje prikupljaju treće strane.

2.9. Keylogging

Keylogging je način špijuniranja korisnika računala i uglavnom se koristi za dobivanje pristupa lozinkama i drugim povjerljivim informacijama putem prijevare. Snima svaki pritisak tipke na računalu. Alati za ovu vrstu napada mogu biti hardverski ili softverski, namijenjeni automatiziranju procesa zapisivanja pritiska tipki. Time se bilježe podaci poslani svakim pritiskom tipke u tekstualnu datoteku koja se kasnije može dohvatiti. Neki alati mogu snimiti sve na međuspremniku, aktivnosti poput kopiranja, izrezivanja i lijepljenja, pozive, GPS podatke te snimke mikrofona i kamere.

Vrste keylogginga su:

- softverski keyloggeri – sastoje se od aplikacija koje se moraju instalirati na računalo kako bi se ukrali podaci o pritiscima tipki. Najčešće se postavljaju na računalo kada korisnik preuzme zaraženu aplikaciju. Kada se zaraženi program instalira na računalo, prati svaki pritisak tipke u operativnom sustavu te bilježi putanje kroz koje svaki pritisak prolazi. Nakon što se pritisci tipki snime, automatski se prenose hakeru koji ih je postavio. Ovo je omogućeno putem udaljenog poslužitelja na koji su povezani zaraženi softver i haker. Haker dohvaća podatke prikupljene ovom vrstom napada te ih koristi kako bi otkrio razne informacije o korisniku, primjerice lozinke koje mogu omogućiti

pristup osjetljivim podacima unutar organizacije, privatnim financijskim podacima poput bankovnih računa i slično.

- hardverski keyloggeri – funkcioniraju slično kao i softverski keyloggeri, no najveća razlika je u tome što hardverski moraju fizički biti povezani s ciljanim računalom kako bi zabilježili korisničke pritiske na tipku. Iz tog je razloga u organizacijama vrlo važno pratiti tko ima pristup mreži i uređajima koji su na nju povezani. Nakon što hardverski zapisivač pritiska tipke završi s keyloggingom, pohranjuje podatke koje haker mora preuzeti s uređaja. Preuzimanje se može izvršiti tek nakon što je keylogger završio s bilježenjem pritisaka tipki, odnosno haker ne može doći do podataka dok keylogger radi. U nekim slučajevima haker može omogućiti pristup uređaju za keylogging putem Wi-Fi veze. Time je omogućeno dohvaćanje zabilježenih podataka preko mreže.

2.10. Tipovi kibernetičkog kriminala

Osim metoda i alata koji se koriste u kibernetičkom kriminalu, zbog svog širokog djelovanja kibernetički kriminal može se podijeliti u nekoliko tipova. Svaki tip djelovanja kibernetičkog kriminala ima istu svrhu, a ona uključuje ostvarivanje određene vrste koristi za pojedinca ili skupinu koja provodi kibernetički kriminal. Tipovi kibernetičkog kriminala su:

- krađa identiteta – korištenje podataka za identifikaciju pojedinca od strane nekog drugog (često stranca) bez dopuštenja ili znanja te osobe
- prijevara – koja se u pravnom smislu definira kao namjerno krivo predstavljanje činjenica u svrhu lišavanja nekoga vrijednog posjeda. Iako je prijevara ponekad sama po sebi kazneno djelo, češće je to element kaznenih djela, kao što je stjecanje novca lažnim pretvaranjem ili lažnim predstavljanjem
- zločini koji uključuju temeljne povrede osobne ili korporativne privatnosti – napadi na integritet informacija pohranjenih u digitalnom obliku i korištenje nezakonito dobivenih digitalnih informacija za ucjenjivanje poslovnih organizacija ili pojedinca
- piratstvo – ilegalna reprodukcije ili širenja materijala zaštićenog autorskim pravima, kao što su računalni programi, knjige, glazba i filmovi
- pranje novca – odnosno proces kojim kriminalci pokušavaju prikriti nezakonito podrijetlo i vlasništvo prihoda od svojih nezakonitih aktivnosti. Putem pranja novca kriminalci pokušavaju prihode od svojih zločina pretvoriti u sredstva naizgled legalnog podrijetla te
- krivotvorenje – proizvodnja lažnog novca radi zarade, vrsta krivotvorine u kojoj se nešto kopira kako bi se prevarilo tako što se to izdalo za originalni ili pravi artikl.

Ovo su specifični tipovi kibernetičkog kriminala koji su usmjereni na ciljane skupine, poput pojedinaca i poslovnih subjekata. Međutim, potrebno je spomenuti i da postoje vrste kibernetičkog kriminala unutar vladinih institucija, gdje se namjerno mijenjaju podaci radi profita ili političkih ciljeva. Vršenje ovih tipova kibernetičkog kriminala omogućeno je zbog anonimnosti koju pruža internet.

Svakim danom tehnologija se mijenja i prilagođava potrebama korisnika. Na razvoj tehnologije, osim potreba korisnika, utječu i razni drugi faktori, poput financijskih mogućnosti, znanja i slično. Međutim, u posljednjih nekoliko godina vidljivo je da na razvoj tehnologije utječu i „više" sile. Ubrzanim razvojem tehnologije raste i broj kibernetičkih napada, kao i sve veća potreba za sigurnošću.

U narednim potpoglavljima objasnit će se utjecaj virusa COVID-19 te rata u Ukrajini na porast kibernetičkog kriminala u Republici Hrvatskoj. Na ovim primjerima moći će se jasnije zaključiti kako „više" sile mogu utjecati na porast kibernetičkog kriminala.

2.11. Rast kibernetičkog kriminala izazvan COVID-19 virusom u Republici Hrvatskoj

Početkom 2020. godine započinje nova era za kibernetički kriminal. Svijet je zahvatio virus koji napada ljudsko tijelo. Zbog socijalnih mjera koje su stupile na snagu u svim zemljama pogođenim ovim virusom, raste potreba za povećanom digitalizacijom, odnosno za prelaskom svih sustava koje pojedinci ili organizacije koriste, a koji do tada nisu bili digitalni, u digitalni oblik. Sukladno tome, ubrzani razvoj tehnologija prati i porast kibernetičkog kriminala. Prema CERT-ovim izvještajima za 2019. i 2020. godinu, usporedit će se porast incidenata, odnosno kibernetičkih napada, prije i tijekom pandemije virusa COVID-19.

Nacionalni CERT *(engl. Computer Emergency Response Team)* je odjel Hrvatske akademske i istraživačke mreže – CARNET, koji ima za osnovni zadatak obrada računalno-sigurnosnih incidenata, odnosno kibernetičkih napada, koji ima za cilj očuvanje kibernetičke sigurnosti u Republici Hrvatskoj. Detaljnije pojašnjenje ove institucije bit će izloženo u narednom tekstu.

Kako bi se što bolje prikazao porast incidenata kibernetičkog kriminala, usporedit će se statistika incidenata prije i tijekom pandemije COVID-19.

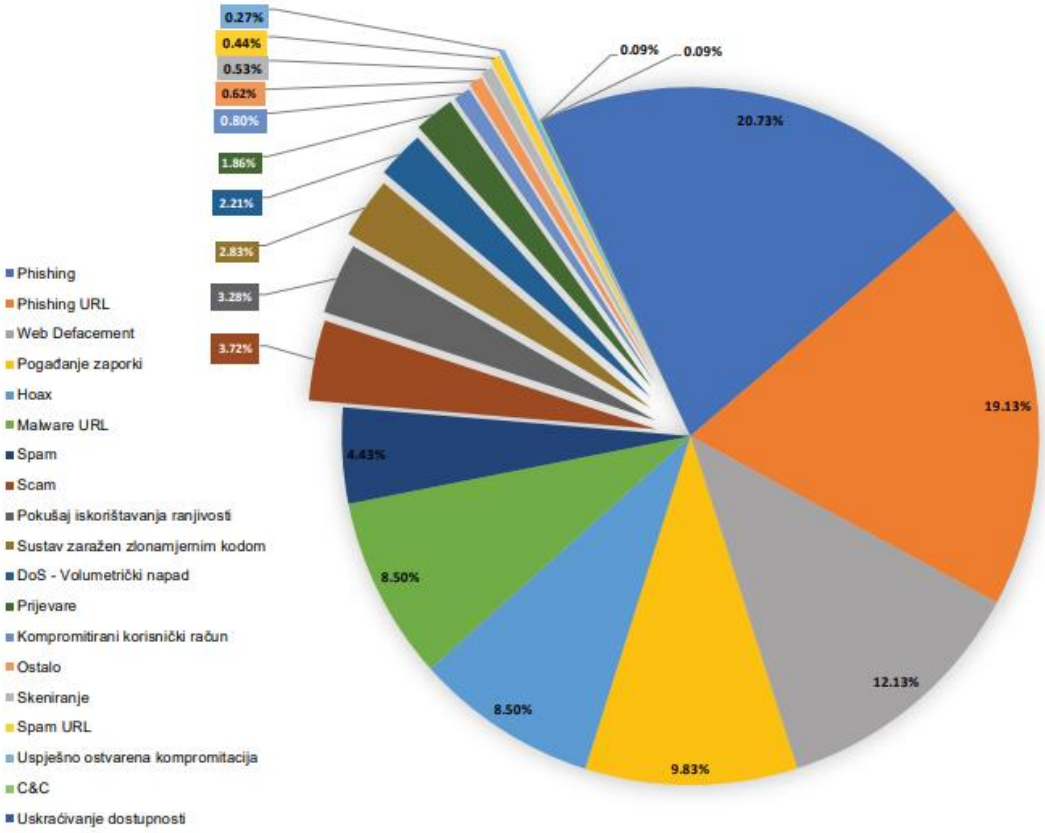
Kako bi se razumjeli statistički prikazi, u Tablica *1* pojašnjavaju se pojmovi korišteni unutar grafikona za statistički pregled incidenata.

Tablica 1. Pojmovnik

Kategorije incidenata	Opis
Web Defacement	Kompromitirana mrežna stranica s izmijenjenim sadržajem i izgledom.
Zaražen sustav zlonamjernim kôdom	Uključuje pametne telefone, računalo i slično.

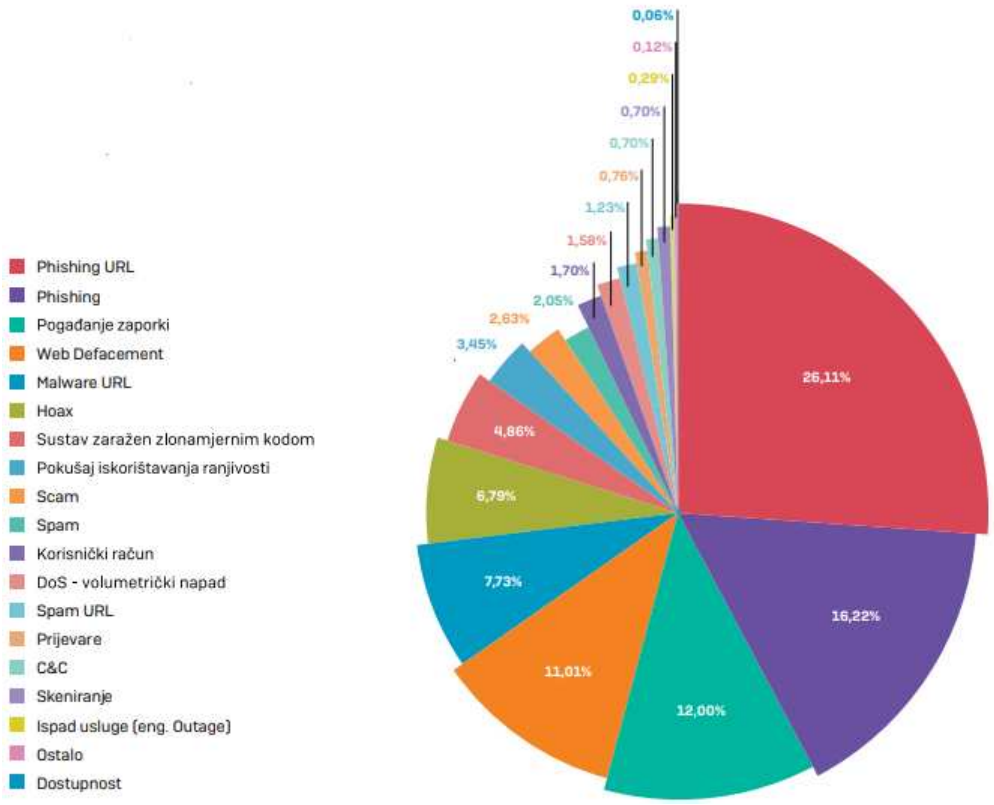
C&C	Upravljački poslužitelj za upravljanje i nadzor računala koji su dio botneta, može služiti za prikupljanje ukradenih podataka.
Korisnički račun	nesigurnost korisničkog računa koji pristupa nekom računalnom sustavu ili mrežnom servisu
Malware URL	Poveznica kojoj je krajnja točka neki zlonamjerni programski kod
Phishing URL	Poveznica do krivotvorene mrežnom stranice kako bi se ukrali podaci
Spam URL	Poveznica koja vodi do kompromitiranog mrežnog mjesta s ciljem postavljanja neovlaštenog reklamnog sadržaja.
Pogađanje zaporki	Neovlašteni pokušaji pristupanju računalnim sustavima pogađanjem zaporke.
Pokušaj iskorištavanja ranjivosti	Iskorištavanje mana računalnog sustava radi ostvarivanja neovlaštenog pristupa ili kako bi se utjecalo na tajnost i cjelovitost podataka.
Skeniranje	Neovlašteno automatizirano prikupljanje informacija o sustavima i računalnim mrežam.
Sniffing	Ilegalni pokušaji presretanja mrežnog prometa.
DoS – volumetrički napad	Napad s ciljem zagušenja mrežne propusnosti tako što šalje velike količine IP paketa.
DoS napad na aplikacijskom sloju	Slanje velikog broja zahtijeva sustavu s ciljem iskorištavanja propusta ili resursa sustava.
Ispad usluge	Neočekivani gubitak dostupnosti izazvan greškom u sustavu.
Spam	Neželjena elektronička pošta koja sadrži reklamni sadržaja
Hoax	Elektronička pošta neistinitog sadržaja s ciljem dezinformiranja ili zastrašivanja primatelja.
Phishing	Pokušaj navođenja pojedinca na odavanje povjerljivih podataka.
Scam	Navođenje pojedinca na odavanje povjerljivih podataka.

Slika *1* prikazuje statističke podatke, tj. postotke po tipu incidenata u 2019. godini, koji su otkriveni u sustavu za obradu incidenata prema Nacionalnom CERT-ovom godišnjem izvješću, odnosno incidente prije pojave virusa COVID-19 u Republici Hrvatskoj.



Slika 1. Tip raspodjela incidenata u 2019. godini (CERT, 2021)

Prvi zabilježeni slučaj virusa COVID-19 u Republici Hrvatskoj dogodio se u veljači 2020. godine, a u ožujku iste godine donose se mjere za ograničavanje kretanja. Za usporedbu se uzima naredna godina, tj. prva godina pojave virusa COVID-19. Slika *2* prikazuje postotke incidenata po tipu u 2020. godini, koji su otkriveni u sustavu za obradu incidenata prema Nacionalnom CERT-ovom godišnjem izvješću za 2020. godinu.



Slika 2. Tip raspodjela incidenata u 2020. godini (CERT, 2021)

Navedeni grafikoni prikazuju incidente u Republici Hrvatskoj prije i početkom pojave virusa COVID-19 u Republici Hrvatskoj.

Prema Nacionalnom CERT izvješću, za vrijeme 2020. godine obrađeno je i zaprimljeno 1710 prijava koje se klasificiraju kao sigurnosni - računalno incidenti. Čelni tipovi incidenata su phishing, pogađanje zaporki i phishing URL. Najistaknutija promjena u 2020. godini odnosi se na općenito velik broj prijavljenih incidenata. Za razliku od 2019. godinu, Nacionalni CERT zaprimio je i razradio 66% više incidenata u 2020. godini.

Tijekom 2020. godine broj prijava incidenata rastao je, a tokom ožujka pojavili su se sigurnosno-računalni izgredi vezani uz pandemiju COVID-19. Obrađena je phishing kampanja povezana s COVID-19, u kojoj se pošiljatelj predstavljao kao Svjetska zdravstvena organizacija, a sadržaj elektroničke pošte uključivao je zlonamjeran privitak. Stupanjem na snagu mjera rada od kuće u svim organizacijama koje su to mogle omogućiti, DDoS napad prijavljen je na login.aaiedu.hr, mrežnog sjedište, smješteno na mrežnom poslužitelju Sveučilišnog računskog centra, time je uzrokovao poteškoće u radu svih sustava koje koriste prijavu putem navedenog serivsa.

Tokom travnja iste godine zabilježene su i neke phishing kampanja sa zlonamjernim privicima, u kojima se sadržaj poruka odnosio na COVID-19. Maliciozni sadržaj u privicima uglavnom je

bio korišten u svrhu krađe osjetljivih korisničkih podataka. Zaprimljena je obavijest koja je sadržavala indikatore kompromitacije zlonamjernog softvera tematski vezanog uz COVID-19, kasnije prozvanog „CoViper“. Također, od velikih organizacija odnosno hrvatskih banaka stigle su prijave phishing kampanja usmjerene na njihove korisnike s ciljem krađe podataka.

Tijekom svibnja phishing kampanje su zabilježene sa zlonamjernim privicima, u kojima se maliciozan sadržaj odnosio na COVID-19, no u nešto manjem broju nego u prethodnom mjesecu. Također, Nacionalni CERT zaprimio je prijavu od vanjskog izvora o kompromitiranim korisničkim računima pod njegovom nadležnošću.

U lipnju je Nacionalni CERT zaprimio prijavu o ilegalnim stranicama na kojima se nalazio sadržaj kopiran sa stranica stvarnih tijela javne vlasti. Na jednoj od njih napadač se predstavljao kao autorizacijska infrastruktura. Na tim ilegalnim stranicama su se nalazile poveznice do Google obrazaca gdje su traženi osobni podaci korisnika (uključujuć i lozinku).

U rujnu je bila zabilježena phishing kampanja vezana uz COVID-19, u kojoj se pošiljatelj predstavljao kao Ministarstvo zdravlja. "Od" polje bilo je namješteno i glasilo je „Ministarstvo zdravlja Hrvatska“. Privitak poruke elektroničke pošte sadržavao je .zip datoteka koja je sadržavala zlonamjerni LokiBot infostealer.

Krajem prosinca zabilježen je povećan broj ucjenjivačkih lažnih poruka kojima je pošiljatelj pokušavao iznuditi novčanu korist od primatelja. Metoda kojom je pošiljatelj pokušavao ostvariti financijsku dobit temeljila se na prijetnji objavljivanjem osjetljivih snimaka primatelja koji je zaprimio ucjenjivačku poruku, ako žrtva ne izvrši uplatu u vrijednosti Bitcoina. Kako bi sadržaju poruke učinio što uvjerljivijom, pošiljatelj je lažirao adresu pošiljatelja kako bi bila istovjetna adresi primatelja.

Također, više od 23.000 baza podataka postalo je javno dostupno time postajeći jedan od najvećih slučajeva curenja podataka. Vjeruje se da je kolekcija baza došla s privatnog hakerskog foruma kojeg mnogi koriste u svrhu prikupljanja što većeg broja adresa elektroničke pošte, korisničkih imena i lozinki u obliku čistog teksta. Kolekcija se sastoji od više od 226 milijuna jedinstvenih korisničkih računa.

2.12. Rat u Ukrajini

Osim što je svijet pogođen virusom COVID-19, u trenutku pisanja ovog rada odvijaju se ratna zbivanja u Ukrajini koja utječu na cijeli svijet, uključujući i područje kibernetičkog kriminala te kibernetičke sigurnosti. Moderno doba omogućilo je i moderan način ratovanja, a u ovom konkretnom slučaju, osim ratovanja u fizičkom svijetu, vodi se i rat na mreži.

James Andrew Lewis, viši potpredsjednik i direktor programa strateških tehnologija u CSIS-u *(engl. Center for Strategic and International Studies)*, napisao je preliminarni izvještaj o

kibernetičkom napadu na Ukrajinu. U njemu se osvrnuo na javno dostupne informacije o kibernetičkom napadu na Ukrajinu te na nastojanja napadača čiji je cilj bio poremetiti usluge i instalirati destruktivne zlonamjerne programe na mreže. Napadi su uključivali krađu identiteta, odbijanje usluge i iskorištavanje programskih mana.

Primarne mete u ovim napadima bile su mrežne stranice financijske institucije, telekomunikacijskih usluga i pružatelji energenata, ukrajinske vlade i mediji. Do srpnja 2022. godine, najveća kibernetička šteta nastala ovim napadima nije utjecala samo na Ukrajinu, nego i šire. Najveći poremećaj bio je napad na satelit Viasat Inc's KA-SAT, koji pruža širokopojasne internetske usluge širom Europe.

Kao što je već spomenuto u ovom radu, kibernetički napadi mogu se koristiti i u političke svrhe. U ovom konkretnom slučaju koriste se za postizanje političkih ciljeva ometanjem financijskih institucija, širenjem dezinformacija, ometanjem energetskih sustava, prijevoza i vladinih službi, i dr. Prema raspoloživim podacima, napadači su uspjeli prodrijeti u vojnu komunikaciju te su pokušali širiti dezinformacije. Na primjeru stvarnoga rata može se primijetiti koliko snažan utjecaj kibernetički kriminal može imati na stvarni svijet i koliko može utjecati na milijune ljudi. U ovom konkretnom slučaju postoje javno dostupne informacije o kibernetičkim napadima tijekom ratnih zbivanja, a u nastavku su navedene po mjesecima:

- listopad 2021. godine – Prema vremenskim oznakama u kôdu, zlonamjerni softver Issacwiper nastao je 19. listopada 2021. godine, a potom je raspoređen u ukrajinske mreže vlade u veljači 2022. godine.
- studeni 2021. godine – Započeo je razvoj kloniranih nrežnih stranica ukrajinske vlade sa zlonamjernim softverom i ugrađenim poveznicama na lažnim mrežnim lokacijama. Smatra se da je ova aktivnost povezana s drugim distribuiranim napadom uskraćivanja usluge (DDoS) u veljači 2022. protiv ukrajinskog bankarskog sektora i vladinih mrežnih stranica.
- prosinac 2021. godine – Razvijen je „Hermeticwiper“ zlonamjerni softver, prema najstarijoj vremenskoj oznaci koda, koristi se u veljači 2022. u napadu protiv financijskih organizacija i ukrajinskih vladinih ugovarača.
- prosinac 2021. godine – Dolazi do „phishing“ napada na Državnu migracijsku službu Ukrajine.
- prosinac 2021. godine – Razvijen je zlonamjerni program koji se koristi u ožujku i travnju u phishing napadima.

- prosinac 2021. godine – Zabilježena je kompromitacija mreže nuklearne organizacije sigurnosti. Hakeri su ukrali podatke iz ove organizacije do ožujka 2022. godine.
- siječanj 2022. godine – Hakeri su postavili destruktivni zlonamjerni softver (WhisperGate) maskiran kao ransomware na brojnim sustavima ukrajinske vlade, neprofitnih organizacija i organizacija informacijske tehnologije.
- siječanj 2022. godine – Hakeri su napali oko 70 ukrajinskih državnih mrežnih stranica, srušivši nekoliko njih, te narušili stranice Ministarstva vanjskih poslova. Rušenje je uključivalo prijeteću poruku Ukrajincima i obavijest o izlaganju osobnih podataka, što je kasnije opovrgnuto od strane Ukrajinskog centra za strategiju komunikacijske i informacijske sigurnosti.
- siječanj 2022. godine – Hakeri su phishingom napali zapadnu vladinu agenciju koja djeluje u Ukrajini.
- veljača 2022. godine – Hakeri su napali ukrajinsku energetsku kompaniju špijunskim zlonamjernim softverom putem phishing napada.
- veljača 2022. godine – Hakeri su slali phishing e-poštu u ime ukrajinskih državnih tijela sa zlonamjernim softverom maskiranim kao softver za prevođenje ukrajinskog jezika.
- veljača 2022. godine – Hakeri su napali ukrajinski bankarski sektor i vladine mrežne stranice nizom DDoS napada, čime su izazvali privremeno isključivanje mrežnih stranica.
- veljača 2022. godine – Novine *The Times* izvještavaju kako su hakeri ciljali na ranjivosti u više od 600 kritičnih infrastrukturnih institucija i Ministarstva obrane u Kijevu u pokušaju kompromitiranja podataka i ometanja usluge.
- veljača 2022. godine – Hakeri su ciljali mrežne stranice ukrajinskog bankarskog sektora i ukrajinske vlade DDoS napadom, čineći neka mjesta nedostupnima. Ovo je bio drugi DDoS napad na ukrajinske banke i vladine mrežne stranice unutar dva tjedna.
- veljača 2022. godine – Hakeri su postavili destruktivni malware (HermeticWiper) kako bi se uništilo oko 300 sustava u više od desetak financijskih, vladinih, energetskih, informatičkih i poljoprivrednih institucija.
- veljača 2022. godine – Hakeri su postavili kriptor datoteka na mrežu poljoprivredne tvrtke.
- veljača 2022. godine – Hakeri su napali novine *Kyiv Post* DDoS napadom, zbog čega je njihova mrežna stranica bila izvan mreže.

- veljača 2022. godine – Hakeri su postavili destruktivni zlonamjerni softver (IsaacWiper) na ukrajinsku državnu mrežu.
- veljača 2022. godine – Hakeri su phishing napadom napali članove europske vlade uključene u koordinaciju logistike izbjeglica koje bježe iz Ukrajine.
- veljača 2022.godine – Hakeri su destruktivnim zlonamjernim softverom napali kompaniju za satelitske komunikacije Viasat, onemogućivši komunikaciju modema s KA-SAT satelitom Viasat Inc. Napad je utjecao na povezanost diljem Ukrajine i Europe, jer taj satelit omogućuje pristup internetu korisnicima u više zemalja.
- veljača 2022.godine – Hakerska skupina ciljala je visoko pozicionirane Ukrajince kroz phishing napad, s namjerom preuzimanja računa na društvenim medijima i širenja dezinformacija o ukrajinskim snagama.
- veljača 2022. godine – Hakeri su napali ukrajinsku graničnu kontrolnu postaju destruktivnim zlonamjernim softverom, prisilivši službenike da ručno obrađuju izbjeglice koje prelaze u Rumunjsku.
- ožujak 2022. godine – Hakeri su napali najmanje 30 ukrajinskih sveučilišnih mrežnih stranica.
- ožujak 2022. godine – Hakeri su 9. ožujka i 24. veljače napali telekom operatera Triolan, utječući na mrežnu povezanost.
- ožujak 2022. godine – Hakeri su napali veliku televizijsku tvrtku destruktivnim računalnim programom (DesertBlade).
- ožujak 2022. godine – Hakeri su ciljali Ukrajince phishing napadom kako bi postavili zlonamjerni softver koji ugrožava korisničke podatke.
- ožujak 2022. godine – Hakeri su napali ukrajinsku istraživačku instituciju.
- ožujak 2022. godine – Ukradeni su podaci od organizacije za nuklearnu sigurnost.
- ožujak 2022. godine – Hakeri su ciljali mrežu Vinasterisk, utječući na povezanost u zapadnoj Ukrajini.
- ožujak 2022. godine – Hakeri su postavili destruktivni zlonamjerni softver (CaddyWiper) u ukrajinskim organizacijama.
- Ožujak 2022. godine – Hakeri su napali medijsku tvrtku Ukraine 24 iz Kijeva kako bi lažno izvijestili da je predsjednik Zelensky najavio predaju Rusiji. Predsjednik Zelensky kasnije je objavio video u kojem navodi da je poruka lažna.
- ožujak 2022. godine – Hakeri su phishing napadom napali sustave ukrajinskih državnih tijela.

- ožujak 2022.godine – Hakeri su napali nekoliko ukrajinskih novinskih kuća, nagrđujući platforme simbolima zabranjenima u Ukrajini.
- ožujak 2022. godine – Hakeri su postavili destruktivni zlonamjerni softver (DoubleZero) usmjeren na ukrajinska poduzeća.
- ožujak 2022. godine – Hakeri su napali internetsku stranicu Ukrajinskog Crvenog križa, što je uzrokovalo njenu nefunkcionalnost nekoliko sati.
- ožujak 2022. godine – Hakeri su ciljali ukrajinske organizacije phishing napadom. Zlonamjerni program prenosi backdoor koji hakerima omogućuje pristup i kontrolu nad podacima sustava.
- ožujak 2022. godine – Hakeri su ciljali Ukrajinu phishing napadom s elektroničkom poštom koja je sadržavala dokument sa zlonamjernim softverom, maskiranim kao da dolazi iz Nacionalne policije Ukrajine.
- ožujak 2022. godine – Hakeri su napali pružatelja usluga prijevoza i logistike sa sjedištem u zapadnoj Ukrajini.
- ožujak 2022. godine – Hakeri su koristili WordPress mrežne stranice za ciljanje 10 mrežnih stranica prilikom više DDoS napada, uključujući ukrajinske vladine agencije, tijela za pružanje savjeta i rješenja o specifičnim političkim i ekonomskim problemima, te financijske stranice.
- ožujak 2022. godine – Hakeri su napali Ukrtelecom, jednog od najvećih pružatelja telekomunikacijskih usluga u Ukrajini, što je uzrokovalo pad povezanosti u zemlji na 13% prijeratne razine. Stručnjaci iz Državne službe za specijalnu zaštitu komunikacija i informacija Ukrajine uspostavili su vezu u roku od nekoliko sati od napada.
- ožujak 2022. godine – Hakeri su ciljali ukrajinske organizacije i pojedince phishing napadom. Prijevara elektroničkom poštom tvrdila je da dolazi iz Ministarstva obrazovanja i znanosti Ukrajine, a zlonamjerni softver omogućavao je hakerima pristup osjetljivim podacima i identifikacijskim informacijama korisnika.
- travanj 2022. godine – Hakeri su phishingom pokušali pristupiti računima i napali Telegram račune te račune na društvenim mrežama dužnosnika ukrajinske vlade.
- travanj 2022. godine – Hakerska grupa ciljala je nekoliko ukrajinskih medijskih organizacija u pokušaju da dobije dugoročni pristup mrežama i prikupi osjetljive informacije. Microsoft je preuzeo kontrolu nad sedam internetskih domena kako bi ublažio ove napade.

- travanj 2022. godine – Hakeri su napali ukrajinsko energetsko postrojenje, CERT-UA i pomoć privatnog sektora uglavnom su osjetili pokušaje gašenja trafostanica u Ukrajini.
- travanj 2022. godine – Hakeri su DDoS napadom napali ukrajinsku državnu poštu, nekoliko dana nakon objavljivanja nove markice u čast ukrajinskog pograničnog čuvara. Napad je utjecao na sposobnost agencije da vodi svoju internetsku trgovinu.
- travanj 2022. godine – Hakeri su stvorili lažnu Facebook stranicu pod nazivom *Ukrajina 24*, tražeći od korisnika da unesu svoje osobne podatke i podatke o plaćanju.
- travanj 2022. godine – Hakeri su upotrijebili kompromitiranu elektroničku poštu ukrajinske vlade u phishing napadu.
- travanj 2022. godine – Hakeri su ciljali ukrajinska državna tijela phishing napadom.
- svibanj 2022. godine – Hakeri su pokrenuli phishing napad pod krinkom navodnog CERT-UA, koristeći zlonamjerni softver koji ugrožava korisničke podatke.
- svibanj 2022. godine – Hakeri su pokrenuli phishing napad kako bi dobili pristup podacima za autentifikaciju. Elektronička pošta upozoravala je primatelje na nadolazeći kemijski napad kako bi ih uvjerila da otvore privitak pun zlonamjernog softvera.
- lipanj 2022. godine – Hakeri su ciljali ukrajinske državne organizacije phishing napadom.
- lipanj 2022. godine – Hakeri su ciljali medijske organizacije u Ukrajini phishing napadom.

Ove informacije pružaju uvid u kolikoj mjeri kibernetički napadi mogu utjecati na funkcioniranje jedne države te koliko zlonamjerne namjere mogu koristiti pojedincima koji ih provode.

Prema prethodno navedenim informacijama, primjećuje se da su napadači za svaki napad imali jasan cilj: izazivanje panike među građanima kroz širenje dezinformacija, onemogućavanje normalnog rada institucija ključnih za redovno funkcioniranje države ili ometanje rada drugih institucija čija je uloga od presudne važnosti za zajednicu. Osim napada na organizacije i institucije, vidljivi su i napadi koji direktno utječu na pojedince, poput krađe financijskih i osobnih podataka, koji se kasnije mogu koristiti u zlonamjerne svrhe te time nanijeti štetu.

2.13. Sustavi zaštite

Sustavi zaštite ili kibernetička sigurnost predstavljaju praksu zaštite mreža, sustava i programa od informatičkih napada koji su pojašnjeni u prethodnom tekstu. Uspješna kibernetička sigurnost temelji se na više slojeva zaštite raspoređenih po računalima, mrežama, programima ili podacima koji se namjeravaju zaštititi. Unutar organizacije, procesi, ljudi, i tehnologija bi se

trebale međusobno nadopunjavati kako bi se stvorila učinkovita zaštita od kibernetičkih napada. Za osiguravanje dobre sigurnosti potrebna su četiri mehanizma koja čine cjelinu: politika, koja definira ciljeve osiguravanja sustava. Mehanizmi uključuju prava pristupa i osiguravanje sigurnosti hardvera te prakse koje omogućuju provođenje željene politike. Uvjerenje se odnosi na pouzdanost mehanizama implementiranih za sigurnost. Također, važan je poticaj i motivacija ljudi koji održavaju i osiguravaju sustav kako bi ga zaštitili od prijetnji.

Ovisno o veličini organizacije, potrebno je uspostaviti upravljanje kibernetičkom sigurnošću unutar organizacije. Ključno je da rukovodstvo organizacije kibernetičku sigurnost smatra značajnim poslovnim rizikom. Postoje dobrovoljni okviri koji se mogu koristiti za procjenu rizika i primjenu najboljih povezanih praksi. Primjerice, Nacionalni institut za standarde i tehnologiju *(engl. National Institute of Standards and Technology)* definira pet istodobnih i kontinuiranih funkcija:

- identifikacija – razvijanje organizacijskog razumijevanja za upravljanje rizikom kibernetičke sigurnosti u vezi sa sustavima, ljudima, imovinom i podacima
- zaštita – razvijanje i implementacija odgovarajućih zaštitnih mjera u organizaciji kako bi se osigurala zaštita podataka organizacije, ali i pojedinaca
- detektiranje – razvijanje i implementacija mehanizama za prepoznavanje kibernetičkog napada
- odgovor – razvijanje i implementacija mehanizama za poduzimanje radnji vezanih uz incidente kibernetičke sigurnosti
- oporavak – razvijanje i implementacija mehanizama za planove otpornosti i vraćanje svih usluga i podataka koji su bili narušeni zbog kibernetičkog napada.

Sustavi zaštite uključuju razne mehanizme i radnje poduzete u svrhu zaštite informacija. Prema Zakonu o informacijskoj sigurnosti Republike Hrvatske, „Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podataka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda“, dok su „mjere informacijske sigurnosti opća pravila zaštite podataka koja se provode na fizičkoj, tehničkoj ili organizacijskoj razini.“

Na temelju Konvencije Vijeća Europe o kibernetičkom kriminalu iz 2001. godine („Budimpeštanska konvencija“), prvog međunarodnog ugovora o kibernetičkom kriminalu, Republika Hrvatska 2002. godine donosi odluku o proglašenju zakona temeljenog na ovoj konvenciji.

Konvencija Vijeća Europe o kibernetičkom kriminalu razlikuje četiri vrste računalnog kriminala, definiranih kao kriminal protiv integriteta, dostupnosti, povjerljivosti računalnih podataka i sustava:

1. Članak 2. – nezakoniti pristup: Svaki nezakoniti i namjerni pristup računalnom sustavu ili njegovom dijelu.
2. Članak 3. – protuzakonito presretanje: Svako protupravno namjerno presretanje nejavnih prijenosa računalnih podataka unutar, iz ili prema računalnom sustavu.
3. Članak 4. – ometanje podataka: Svako nezakonito oštećenje, izmjena, povreda ili brisanje računalnih podataka.
4. Članak 5. ometanje sustava: Svako ozbiljno nezakonito ometanje rada računalnog sustava unošenjem, oštećenjem, uništavanjem, prijenosom, izmjenom ili brisanjem računalnih podataka.

Sljedeći čimbenici mogu se identificirati kao čimbenici koji utječu na rast kibernetičkog kriminala:

- povećanje informatizacije unutar svih dijelova društva, bilo putem društvenih mreža ili poslovnih sustava koje koriste pojedinci i poslovni subjekti, no bez adekvatnog povećanja sigurnosti
- tehnološko i znanstveno napredovanje koje povećava vjerojatnost da se miroljubive tehnologije koriste kao sredstva štete, što kreatori tih tehnologija nisu predvidjeli
- terorizam ubrzano postaje posebna vrsta informacijske prijetnje; teroristi koriste suvremene informacijske sustave za komunikaciju i prikupljanje informacija. Većina modernih terorističkih akata osmišljena je ne samo da prouzrokuje materijalnu štetu i prijetnju ljudskim životima, već i informacijski i psihološki šok. Takvim utjecajem na velike mase ljudi stvara se povoljno okruženje za postizanje terorističkih ciljeva
- digitalna nejednakost, prisutna u zemljama koje su izgubile informacijsku utrku, može se koristiti kao sredstvo manipulacije protiv pojedinih država.

2.14. Tipovi kibernetičke sigurnosti

Kako bi se pojedinac ili organizacija mogli zaštititi, ili barem to pokušali, postoje različite razine unutar sustava koje je potrebno osigurati. Svaki sustav je jedinstven, no svi sustavi su u pravilu vrlo slični po svojoj izvedbi. Primjerice, mrežna stranica ima korisničko sučelje putem kojeg se korisnici njome koriste, no u pozadini postoji programski kôd koji omogućuje funkcionalnost i rad stranice. Mrežna stranica može imati različita pravila, poput dozvola za posebne korisnike koji imaju pristup određenim dijelovima stranice, dok ostali nemaju ista

prava. Bilo koji sustav mora imati implementirane sigurnosne mehanizme kako bi se osigurala povjerljivost podataka. Kibernetička sigurnost je širok pojam, no postoji nekoliko tipova kibernetičke sigurnosti koji čine cjelinu. U narednom tekstu detaljnije će se objasniti tipovi kibernetičke zaštite.

2.15. Sigurnost mreže

Mrežna sigurnost ključna je za zaštitu podataka i informacija, očuvanja sigurnosti zajedničkih podataka u organizacijama, pouzdanog pristupa i performansa mreže kao i zaštitu od kibernetičkih napada. Postoji nekoliko tipova sigurnosti mreže poput:

- vatrozid *(engl. firewall*) – kontrolira dolazni i odlazni promet na mrežama prema unaprijed definiranim sigurnosnim pravilima. Njegova svrha je sprječavanje neovlaštenog vanjskog prometa koji nema izvor iz privatne mreže.
- segmentacija mreže – arhitektonski pristup koji dijeli mrežu na više segmenata, odnosno manjih mreža, pri čemu svaki segment djeluje kao vlastita mreža. Ovaj način omogućuje mrežnim administratorima kontrolu protoka prometa između manjih mreža na temelju definiranih pravila.
- kontrola pristupa – definira tko (ljudi, grupe ili uređaji) ima pristup mrežnim aplikacijama i sustavima, čime se sprječava neželjeni pristup.
- VPN (*engl. Virtual Private Network*) s udaljenim pristupom – pruža udaljeni i siguran pristup mreži tvrtke zaposlenicima ili klijentima. Virtualna privatna mreža stvara tunel između organizacije i udaljenog korisnika te osigurava šifriranje mrežnog prometa.
- ZTNA (*engl. Zero trust network access*) – pristup mreži s nultim povjerenjem, poznat i kao programski definirani perimetar *(engl. Software Defined Perimeter, SDP)*, skup je tehnologija i funkcionalnosti koje omogućuju siguran pristup internim aplikacijama za udaljene korisnike. Djeluje tako da pristup osjetljivim podatcima i mreži nikada nije implicitan, a pristup se odobrava s najmanjim potrebnim privilegijama.
- sigurnost elektroničke pošte – odnosi se na sve procese, proizvode i usluge dizajnirane za zaštitu računa i sadržaja e-pošte od vanjskih prijetnji.
- prevencija gubitka podataka (*engl. Data loss prevention*) – metodologija kibernetičke sigurnosti koja kombinira tehnologiju i najbolje prakse za sprječavanje izlaganja osjetljivih informacija izvan organizacije.
- sustav za sprječavanje upada (*engl. Intrusion Prevention System*) – tehnologije koje sprječavaju ili otkrivaju sigurnosne napade na mreže, kao što su iskorištavanje poznatih ranjivosti, napadi uskraćivanjem usluge i napadi brutalnom silom.

- sandboxing – praksa kibernetičke sigurnosti u kojoj se programski kôd ili datoteka pokreću u sigurnom, izoliranom okruženju koje oponaša radno okruženje korisnika. Ovaj sustav promatra datoteku ili kôd dok se izvršava i traži zlonamjerno ponašanje kako bi spriječio prijetnje da dopru do mreže.

2.16. Sigurnost u oblaku

Organizacije sve više prihvaćaju računalstvo u oblaku, stoga je potrebno poduzeti odgovarajuće mjere sigurnosti. U osnovi postoje tri kategorije odgovornosti u ovoj vrsti sigurnosti, a to su:

- odgovornost na pružatelju – odnosi se na zaštitu same infrastrukture, uključujući pristup, krpanje i konfiguraciju fizičkih poslužitelja te fizičke mreže na kojoj se izvode računalne instance, pohrana i drugi resursi.
- odgovornost na korisniku – uključuje upravljanje korisnicima i njihovim pravima pristupa, zaštitu računa u oblaku od neovlaštenog pristupa, zaštitu i šifriranje podataka na računu.
- odgovornost ovisno o modelu usluge – odgovornosti koje ovise o tome je li riječ o infrastrukturi kao usluzi *(engl. Infrastructure as a Service)*, platformi kao usluzi *(engl. Platform as a Service)* ili softveru kao usluzi *(engl. Software as a Service)*, kao što je e-pošta u oblaku.

2.17. Sigurnost krajnjih točaka

Sigurnost krajnjih točaka *(engl. Endpoint security)* odnosi se na praksu osiguravanja krajnjih ili ulaznih točaka korisničkih uređaja, kao što su prijenosna računala, stolna računala, i mobilni uređaji, od zlonamjernih napada. U organizacijama je ova vrsta sigurnosti ključna za zaštitu podataka, kako poslovnih tako i privatnih.

2.18. Sigurnost mobilnih uređaja

Sigurnost mobilnih uređaja bitna je za organizacije koje svojim zaposlenicima osiguravaju službene mobilne uređaje, ali i za fizičke osobe. Zbog svoje kompleksnosti, podijeljena je u nekoliko razina, a to su:

- aplikacijska – zlonamjerni program može biti razvijen kao aplikacija koju korisnici nesvjesno instaliraju na svoje uređaje. Mobilna sigurnosna rješenja trebala bi moći otkriti i blokirati preuzimanje tih zlonamjernih aplikacija.
- mreža – ranjivosti mreže na koju je uređaj spojen mogu se iskoristiti za krađu podataka ili isporuku zlonamjernog sadržaja. Mobilna sigurnost uključuje blokiranje ovih napada na razini mreže.

- operativni sustav – operativni sustavi iOS i Android mogu sadržavati ranjivosti koje se mogu iskoristiti za promjenu konfiguracija uređaja. Mobilna sigurnost uključuje procjene rizika u stvarnom vremenu, praćenje konfiguracija i druge alate za otkrivanje i sprječavanje iskorištavanja ranjivosti uređaja.

2.19. Sigurnost Internet stvari

Internet stvari *(engl. Internet of Things, IoT)* odnosi se na bilo koju fizičku imovinu povezanu s mrežom koja nije računalo. Unatoč brojnim prednostima i inovacijama koje IoT tehnologija omogućuje, međusobna povezanost pametnih uređaja predstavlja značajan izazov za poduzeća u smislu ozbiljnih sigurnosnih rizika koji proizlaze iz nenadziranih i nezaštićenih uređaja povezanih s mrežom.

Internet stvari, zbog svoje jedinstvenosti, predstavljaju izazov u osiguravanju njihove sigurnosti od napada. Svaki uređaj je jedinstven i ima vlastite postavke. Ranjivosti IoT tehnologija koje se mogu procijeniti i zaštititi su:

- neadekvatne zadane postavke – IoT uređaji koji dolaze s tvorničkim postavkama mogu uključivati zadane lozinke i druge postavke koje se ne mogu promijeniti.
- nemogućnost nadogradnje – kod nekih IoT uređaja ponekad je nemoguće ažurirati vatrozid ili druge sigurnosne postavke uređaja.
- korištenje neprikladne tehnologije – neadekvatno korištenje operacijskog sustava na uređaju može stvoriti ranjivosti koje se kasnije mogu iskoristiti.

U svrhu zaštite od kibernetičkih napada, postoje zakoni i institucije koje se bave kibernetičkom sigurnošću, kako pojedinaca, tako i organizacija. Detaljnije definiranje takvih institucija bit će pojašnjeno u idućem potpoglavlju.

2.20. Nacionalni CERT

Nacionalni CERT *(engl. Computer Emergency Response Team)*, osnovan sukladno Zakonu o informacijskoj sigurnosti, odjel je Hrvatske akademske i istraživačke mreže – CARNET. Obrada računalno-sigurnosnih incidenata s ciljem očuvanja kibernetičke sigurnosti u Republici Hrvatskoj je osnovni cilj. Prema Zakonu o informacijskoj sigurnosti, usklađivanje postupanja u slučaju računalno-sigurnosnih incidenata na javnim informacijskim sustavima nastalih u Republici Hrvatskoj ili u drugim zemljama i organizacijama jedna je od glavnih zadaća CERT-a je, kada su povezani s Republikom Hrvatskom. U djelokrugu svojih djelovanja, CERT provodi reaktivne i proaktivne mjere. Proaktivnim mjerama nastoji se ublažiti ili spriječiti moguće štete. One podrazumijevaju:

- praćenje računalno-sigurnosnih tehnologija – praćenje razvoja u području sigurnosnih tehnologija i promicanje novih znanja
- sigurnosne obavijesti – u cilju sprječavanja šteta, praćenje stanja na području računarske sigurnosti i objavljivanje sigurnosnih obavijesti
- promicanje informacija iz područja računarske sigurnosti – prikupljanje i promicanje bitnih informacija u obliku dokumenata, uputa i preporuka
- unaprjeđenije svijesti o značenju računarske sigurnosti – obrazovanje javnosti i podizanje svijesti o važnosti računarske sigurnosti
- obuka i edukacija o računalnoj sigurnosti – provođenje edukativnih aktivnosti za određene ciljne skupine.

Reaktivne mjere podrazumijevaju djelovanje na incidente u Republici Hrvatskoj koji mogu ugroziti računarske sigurnosti javnih informacijskih sustava. Te mjere podrazumijevaju:

- sigurnosna upozorenja – na temelju dobivenih informacija o incidentima izdaju se upozorenja vezana uz računalnu sigurnost
- sigurnosne preporuke – priprema, obrada, i prikupljanje sigurnosnih smjernica o nesavršenosti informacijskih sustava te njihova javna distribucija i arhiviranje
- koordinacija rješavanja značajnih incidenata – suradnja u rješavanja incidenata u koje je uključena minimalno jedna strana iz Republike Hrvatske.

3. SIMULACIJA NAPADA

U ovom poglavlju prikazat će se najčešće korištene metode cyber napada u digitalnom svijetu – phishing, DDoS i keylogging napadi. Ovi napadi, iako tehnički različiti, predstavljaju ozbiljne prijetnje sigurnosnim informacijskim sustavima, ciljajući kako na osobne korisnike, tako i na velike organizacije. Simulacije su napravljene isključivo u edukativne svrhe. Za potrebe ove simulacije koriste se dva virtualna stroja koja međusobno komuniciraju, na kojima se izvode simulacije pomoću Kali Linuxa i Ubuntua.

3.1. Simulacija phising napada

Postoje okruženja koja omogućuju testiranje i simuliranje napada. Cilj ovih okruženja je osvijestiti pojedince i organizacije o važnosti računalne zaštite, kao i o utjecaju kibernetičkog kriminala. Rad obuhvaća različite vrste kibernetičkih napada koji iskorištavaju neznanje pojedinaca ili ranjivosti sustava. Potreba za izvođenjem ove simulacije je pokazati koliku štetu pojedinac može nanijeti, bilo u privatne ili poslovne svrhe, izvođenjem jedne vrste napada. U ovoj simulaciji pojedinac, odnosno žrtva, izlaže riziku svoje osobne podatke, uključujući korisničko ime i lozinku jedne mrežne stranice.

Primjerice, ako je žrtva zaposlenik organizacije koja obrađuje i radi s osjetljivim podacima, poput banke, može se nanijeti izuzetno velika šteta, ne samo pojedincu nego i organizaciji te svim klijentima koji surađuju s tom organizacijom. Zaposlenik banke koji koristi svoje korisničko ime i lozinku za pristup internom sustavu, a primi ovakvu vrstu phishing elektroničke pošte na svoju službenu adresu, može nesvjesno omogućiti hakeru pristup internom sustavu. Naravno, to se događa ako zaposlenik ne prepozna da je riječ o phishing elektroničkoj pošti. Haker tada može dobiti pristup internom sustavu te, koristeći ukradene podatke, iskoristiti pristup za rad s osjetljivim podacima.

U ovoj simulaciji bit će prikazano kako haker dolazi do osjetljivih podataka na mrežne stranici koja svojim korisnicima omogućava korištenje programa za grafički dizajn, editiranje video uradaka, fotografija i slično.

Za izvedbu simulacije phishing napada bilo je potrebno osigurati okruženje koje napadači koriste kako bi iskoristili neznanje svojih žrtava.

U ovom konkretnom slučaju korišten je Kali Linux, Linux distribucija namijenjena etičkom hakiranju, testiranju probojnosti sustava i digitalnoj forenzici. Sadrži brojne programe za testiranje ranjivosti te se može pokrenuti uz pomoć virtualnog programa za virtualizaciju operativnih sustava ili s računalnog tvrdog diska. Za potrebe ove simulacije, Kali Linux je pokrenut s računalnog tvrdog diska te sadrži minimalnu instalaciju.

Nakon instalacije svih potrebnih programa za ispravan rad Kali Linuxa, koristi se alat pod nazivom Blackeye.

Blackeye je alat otvorenog kôda koji služi za phishing napade. Ovaj alat sadrži predloške za krađu identiteta nekoliko desetaka najpopularnijih mrežnih stranica. Predlošci mrežnih stranica dizajnirani su u PHP *(engl. Hypertext Preprocessor)* jeziku, stoga je bilo potrebno instalirati i PHP servis koji omogućava ispravno pokretanje stranica kako bi se simulacija mogla provesti. Pokretanjem alata hakeru se otvara izbornik s predlošcima stranica koje se mogu priložiti u elektroničkoj pošti namijenjenoj žrtvi.

Kako bi bilo moguće pristupiti mrežnoj stranici, bilo je potrebno osigurati servis koji to omogućava. U ovom slučaju korišten je Ngrok, koji pokreće klijentski proces na računalu, stvara privatni tunel prema usluzi i zaobilazi vatrozid. Tunel koji uspostavlja je siguran i može prenositi podatke samo na lokalni host porta koji je haker otvorio.

Pri pokretanju Ngrok servisa na odabranom portu generira se URL *(engl. Uniform Resource Locator)*, koji se prosljeđuje žrtvi.

3.2. Simulacija DDoS napada

Distribuirani napadi uskraćivanja usluge predstavljaju jednu od najčešćih i najopasnijih prijetnji u današnjem digitalnom svijetu. Ovi napadi koriste se za preopterećivanje mrežnih resursa, servera ili aplikacija generiranjem velike količine prometa s više izvora.

Za potrebe ove simulacije korišteni su Kali Linux, koji služi kao „napadač“, te Ubuntu, koji služi kao „cilj“. Oba sustava konfigurirana su u virtualnom okruženju, što omogućuje sigurno testiranje i promatranje napada bez opasnosti za stvarne mreže.

Tijekom simulacije koristit će se alat za praćenje prometa kako bi se detaljno analiziralo ponašanje „cilja“, Wireshark.

Cilj ove simulacije je prikazati štetan učinak ovakve vrste napada na stvarne sustave te onemogućavanje normalnog rada sustava koji su cilj napadača.

3.3. Simulacija Keyloggin napada

Cilj simulacije Keylogginga bio je prikazati kako se pomoću praćenja tipki može doći do osjetljivih podataka cilja, kao što su lozinke i korisnička imena. Keyloggeri su zlonamjerni alati koji neprimjetno prate svaki pritisak tipki na tipkovnici i bilježe ih u datoteku, omogućujući napadaču pristup povjerljivim informacijama poput vjerodajnica za prijavu na različite mrežne stranice.

Za potrebe ove simulacije korišten je Kali Linux kao „napadač“ te Ubuntu kao „cilj“. Napadač je na ciljanom sustavu instalirao keylogger koji je pratio unos tipki na tipkovnici, što je

omogućilo snimanje korisničkih podataka unesenih na ciljanom računalu. Ova simulacija naglašava koliko lako napadači mogu doći do povjerljivih informacija ako žrtva nije svjesna postojanja zlonamjernog softvera.

4. PRAKTIČAN RAD - SIMULACIJA NAPADA

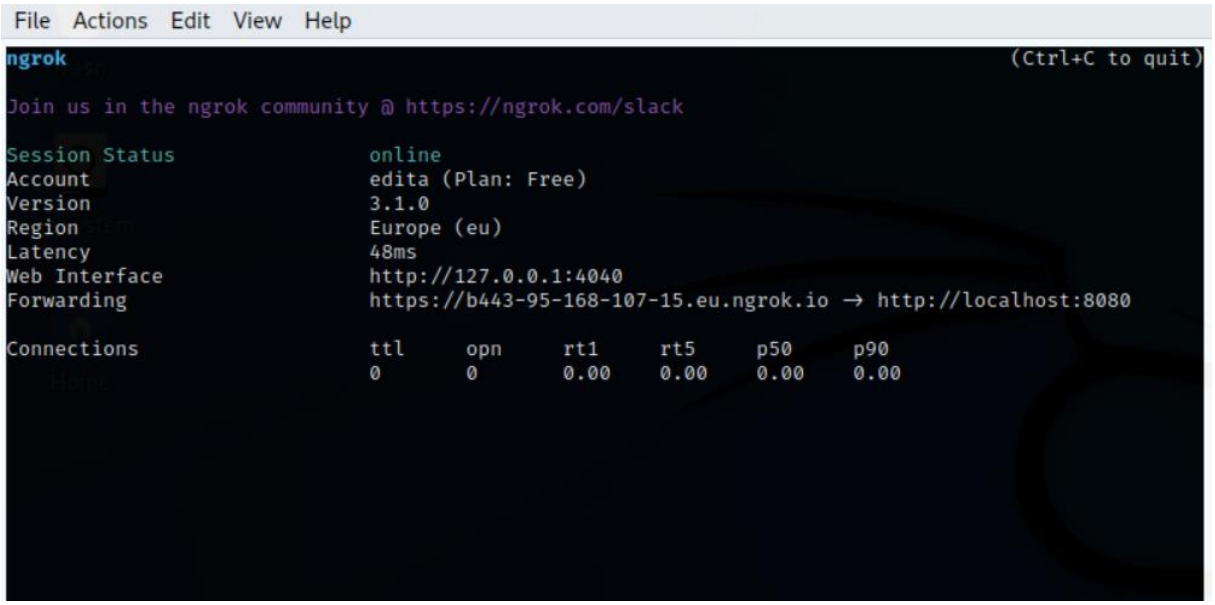
U ovom praktičnom radu prikazat će se simulacija nekoliko prethodno opisanih vrsta napada.

4.1. Phising napad

Ova simulacija prikazuje phishing napad čiji je cilj doći do osobnih podataka žrtve prilikom prijave na lažnu stranicu poslanu putem elektroničke pošte, uključujući korisničko ime, lozinku, IP adresu i korisničkog agenta.

Ova simulacija biti će prikazana na jednoj od poznatih mrežnih stranica. Kako bi se lakše koristili s Kali Linuxom, naredbom `kex -win -s` se pokreće GUI (*engl. Graphical user interface).*

U jednom terminalu pokreće se naredba ngrok s odabranim portom. U svrhu ove simulacije pokreće se naredba `ngrok http 8080` te se otvara sljedeći prikaz (Slika *3*).



Slika 3. Prikaz generiranog URL-a ngrok serivsom

Kao što se može vidjeti putem Ngrok servisa, generiran je URL koji haker šalje svojoj žrtvi kako bi pribavio željene podatke nakon što ih žrtva upiše.

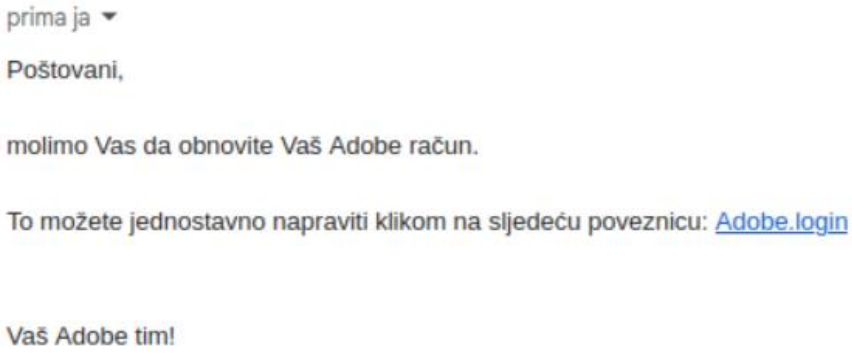
Naredna slika (Slika *4*) prikazuje generirane predloške koje je moguće odabrati kako bi se poslali korisniku. Naravno, haker može generirati vlastiti izgled stranice i koristiti ga, no u ovoj simulaciji koristit će se jedna od predefiniranih stranica.

```
┌──(edchad㉿N007415)-[~/blackeye-im/sites]
└─$ ls
adobe     devianart  icloud          microsoft  playstation  spotify        verizon
amazon    dropbox    instafollowers  myspace    protonmail   stackoverflow  vk
apple     facebook   instagram       netflix    reddit       steam          wifi
badoo     github     line            origin     shopify      tiktok         wordpress
bitcoin   gitlab     linkedin        paypal     shopping     twitch         yahoo
create    google     messenger       pinterest  snapchat     twitter        yandex
```

Slika 4. Predlošci mrežnih stranica unutar alata Blackeye

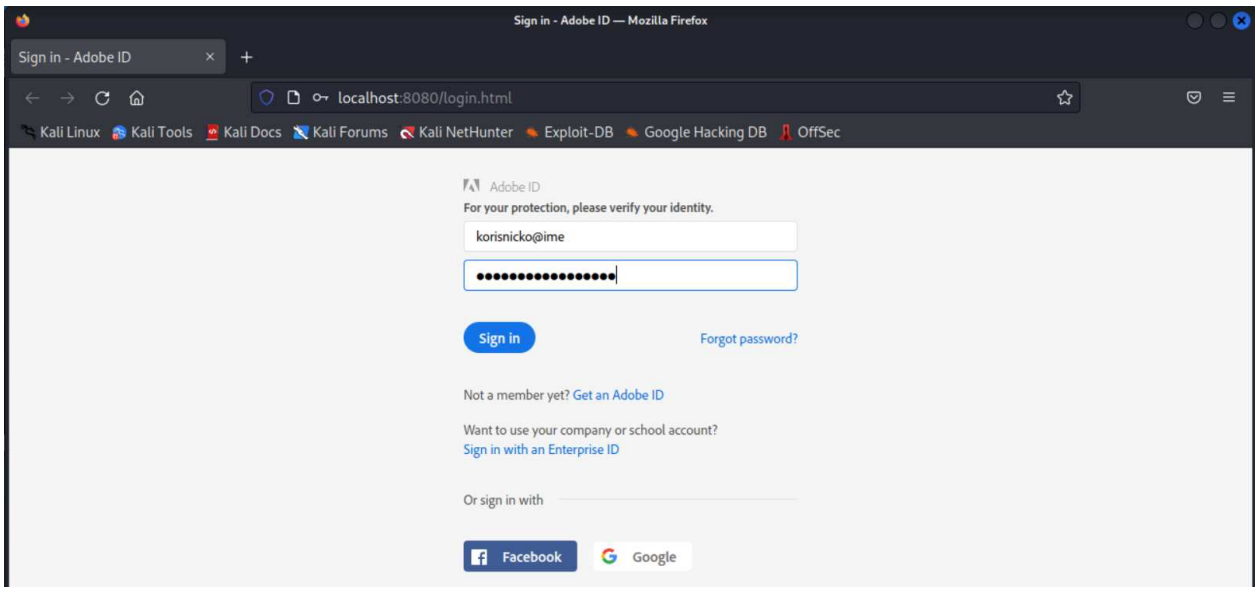
Predefinirana stranica za ovu simulaciju je Adobe. Potrebno je pozicionirati se u tu datoteku, pokrenuti PHP servis i dodijeliti mu port koji je zauzet Ngrok servisom.

Slika *5* prikazuje primjer elektroničke pošte koju žrtva zaprimi sa zamaskiranim URL-om, osmišljenim da izgleda kao legitimna poruka od neke institucije ili pojedinca, s ciljem da haker dođe do podataka.



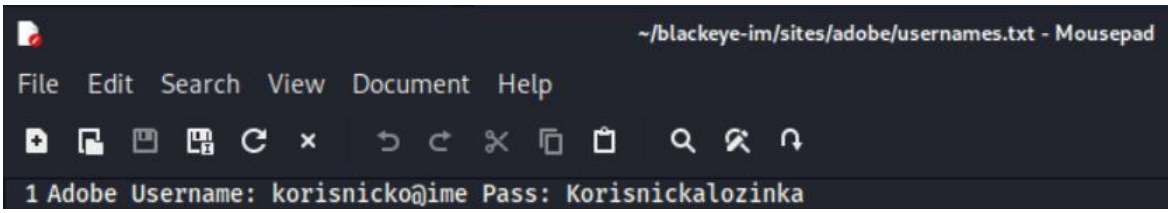
Slika 5. Phisnig elektronička pošta

Nakon što žrtva klikne na link, otvara joj se prikaz stranice koja služi za unos korisničkih podataka, kao što prikazuje naredna slika (Slika *6*).



Slika 6. Izgled phishing stranice

Nakon što korisnik upiše svoje podatke i pritisne gumb „Sign in“, automatski biva preusmjeren na pravovaljanu stranicu, dok se njegovi podaci u međuvremenu pohranjuju u posebnu tekstualnu datoteku, kao što prikazuje naredna slika (Slika *7*).



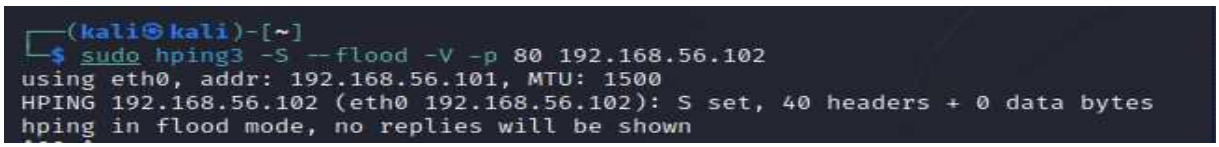
Slika 7. Korisnički podaci žrtve

Osim što napadač uspješno dolazi do korisničkih podataka, poput korisničkog imena i lozinke, također dolazi do IP adrese *(engl. Internet Protocol)*, koja je jedinstvena adresa za identifikaciju uređaja na internetu ili unutar interne mreže. Također, napadač dobiva podatke o korisničkom agentu *(engl. User Agent)*, koji identificiraju aplikaciju, operacijski sustav i verziju preglednika korisnika. Naredna slika (Slika *8*) prikazuje IP adresu i podatke o korisničkom agentu.

Slika 8. IP adresa i podaci o korisničkom agentu

4.2. DDoS napad

DDoS simulacija prikazuje kako napadač onemogućuje mrežne resurse ciljanog sustava te u velikoj mjeri ometa rad na njemu.



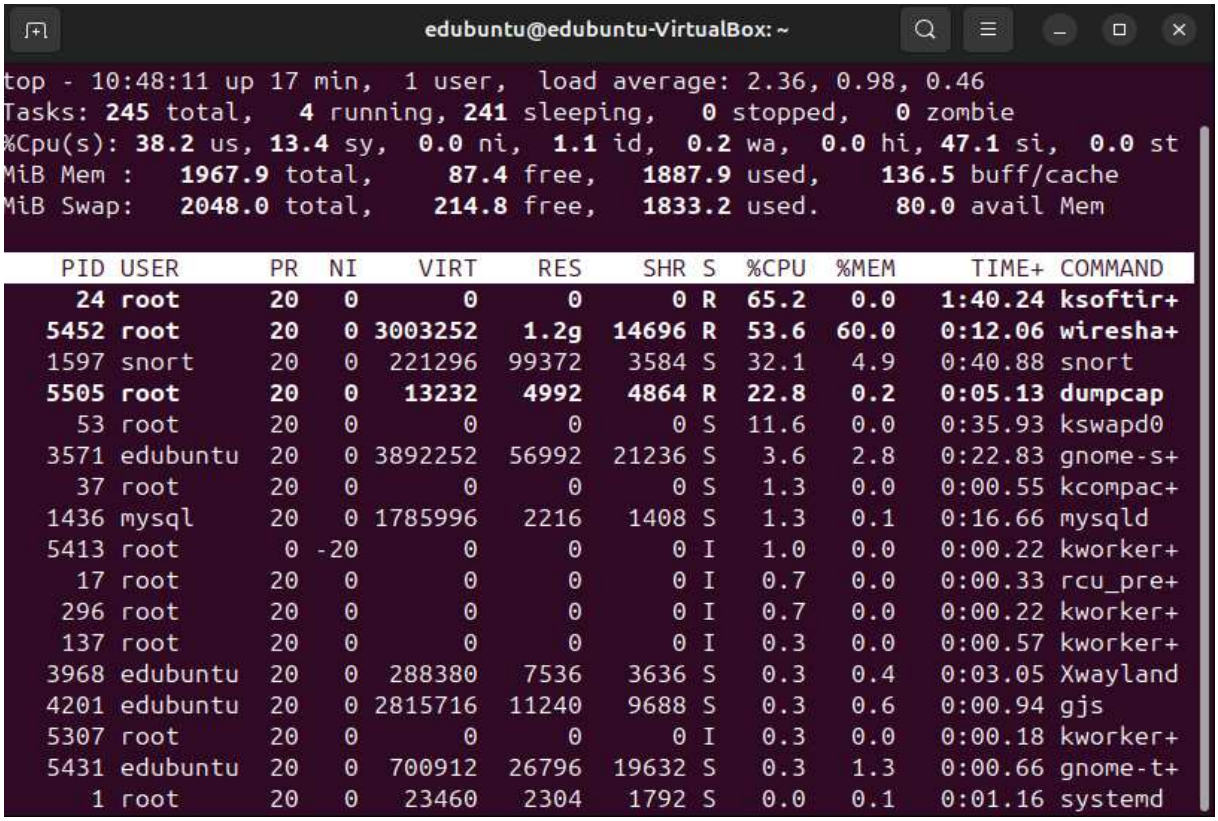
Slika 9. Pokretanje DDoS napada

Slika *9* prikazuje kako na napadačkom sustavu izgleda pokretanje napada.

Potrebno je pojasniti oznake naredbe `sudo hping3 -S --flood -V -p 80 192.168.56.102` riječ kako bi se moglo bolje razumijela ova simulacija:

- sudo označava da se naredba pokreće kao „root“ korisnik unutar Linux sustava
- hping3 je alat koji može slati prilagođene TCP/IP pakete
- -S se koristi za slanje TCP SYN paketa
- --flood uzrokuje slanje velikog broja paketa što je brže moguće
- -V omogućava prikaz detaljnog izlaza
- -p 80 usmjerava napad na port 80, koji je HTTP port
- 192.168.56.102 je IP adresa ciljanog sustava.

Na ciljanom sustavu, Ubuntu, pokreće se naredba `top` kako bi se vidio utjecaj napada na performanse sustava.

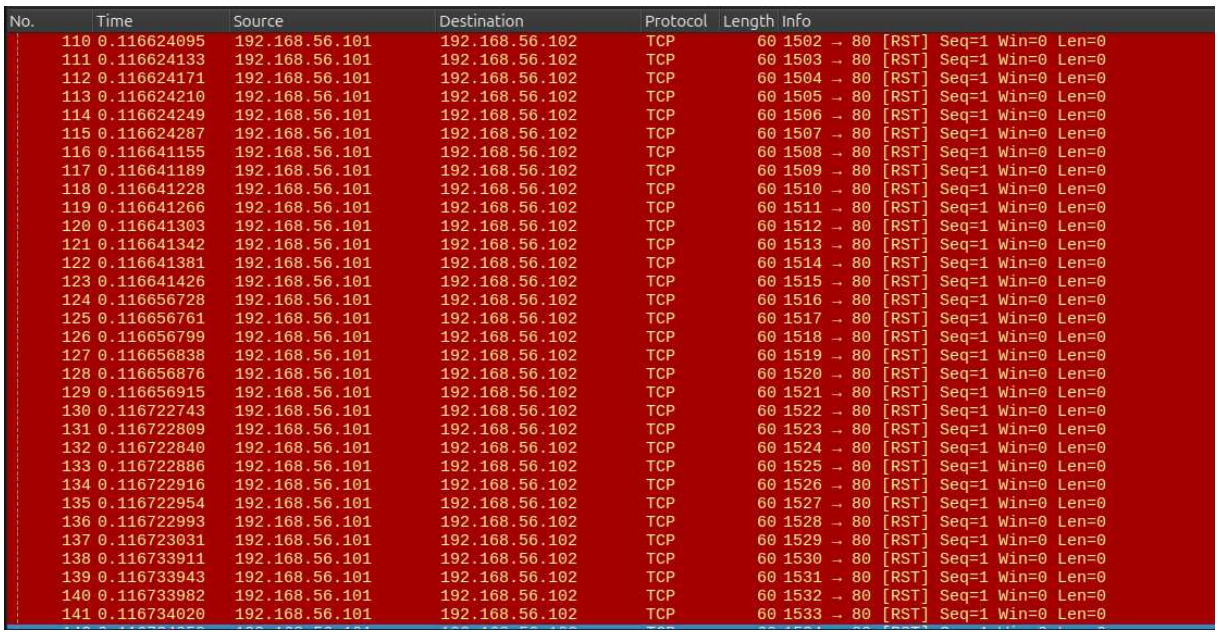


Slika 10. Prikaz resursa ciljanog sustava

Osim dodatnih podataka koji su prikazani, detaljnije će se pojasniti samo oni koji pokazuju kako napad, koji je u trenutku pokretanja ove naredbe u izvedbi, utječe na sustav.
Kako bi se bolje razumijela slika, potrebno je najprije pojasniti oznake:

- PID označava jedinstveni identifikacijski broj svakog procesa u sustavu.
- USER prikazuje korisničko ime korisnika koji je pokrenuo proces.
- PR označava prioritet procesa, koji određuje koliko CPU *(engl. Central Processing Unit)* vremena proces dobiva.
- NI je vrijednost „nicenessa“ procesa; vrijednost može biti između -20, što predstavlja najveći prioritet, i 19, što predstavlja najniži prioritet.
- VIRT prikazuje ukupnu količinu virtualne memorije koju proces koristi.
- RES prikazuje stvarnu memoriju koju proces trenutno koristi u fizičkoj memoriji.
- SHR prikazuje količinu zajedničke memorije koju proces koristi.
- S prikazuje trenutno stanje procesa.

Kao što se može vidjeti, u ovom slučaju proces s PID-om 24 (kernel soft interrupt daemon) koristi 65,2% CPU-a zbog intenzivnog mrežnog prometa, odnosno DDoS napada koji se izvršava u trenutku pokretanja naredbe `top` na Ubuntu sustavu.
PID 5452 označava da Wireshark koristi 56,6% CPU-a i 60% fizičke memorije, odnosno 1,2 GB. Ovo je veoma bitan podatak u analizi ovog napada, jer se tijekom napada koristi alat Wireshark, koji služi za analizu paketa poslanih iz napadačkog u ciljani sustav. Ova dva aktivna procesa tijekom napada zauzimaju značajan dio resursa ciljanog sustava, što rezultira onemogućavanjem normalnog rada na tom sustavu.
Osim navedenih procesa koji koriste velike količine resursa, na ciljanom sustavu mogu se primijetiti i neki drugi procesi prema istim principima.
Uz pomoć naredne slike (Slika *11*) prikazuje se analiza podataka koji se šalju iz napadačkog sustava prema ciljanom sustavu. Wireshark je alat koji služi za analizu paketa i pokreće se na ciljanom sustavu, prikazujući pakete koji pristižu te s koje adrese dolaze.



No.	Time	Source	Destination	Protocol	Length	Info
110	0.116624095	192.168.56.101	192.168.56.102	TCP	60	1502 → 80 [RST] Seq=1 Win=0 Len=0
111	0.116624133	192.168.56.101	192.168.56.102	TCP	60	1503 → 80 [RST] Seq=1 Win=0 Len=0
112	0.116624171	192.168.56.101	192.168.56.102	TCP	60	1504 → 80 [RST] Seq=1 Win=0 Len=0
113	0.116624210	192.168.56.101	192.168.56.102	TCP	60	1505 → 80 [RST] Seq=1 Win=0 Len=0
114	0.116624249	192.168.56.101	192.168.56.102	TCP	60	1506 → 80 [RST] Seq=1 Win=0 Len=0
115	0.116624287	192.168.56.101	192.168.56.102	TCP	60	1507 → 80 [RST] Seq=1 Win=0 Len=0
116	0.116641155	192.168.56.101	192.168.56.102	TCP	60	1508 → 80 [RST] Seq=1 Win=0 Len=0
117	0.116641189	192.168.56.101	192.168.56.102	TCP	60	1509 → 80 [RST] Seq=1 Win=0 Len=0
118	0.116641228	192.168.56.101	192.168.56.102	TCP	60	1510 → 80 [RST] Seq=1 Win=0 Len=0
119	0.116641266	192.168.56.101	192.168.56.102	TCP	60	1511 → 80 [RST] Seq=1 Win=0 Len=0
120	0.116641303	192.168.56.101	192.168.56.102	TCP	60	1512 → 80 [RST] Seq=1 Win=0 Len=0
121	0.116641342	192.168.56.101	192.168.56.102	TCP	60	1513 → 80 [RST] Seq=1 Win=0 Len=0
122	0.116641381	192.168.56.101	192.168.56.102	TCP	60	1514 → 80 [RST] Seq=1 Win=0 Len=0
123	0.116641426	192.168.56.101	192.168.56.102	TCP	60	1515 → 80 [RST] Seq=1 Win=0 Len=0
124	0.116656728	192.168.56.101	192.168.56.102	TCP	60	1516 → 80 [RST] Seq=1 Win=0 Len=0
125	0.116656761	192.168.56.101	192.168.56.102	TCP	60	1517 → 80 [RST] Seq=1 Win=0 Len=0
126	0.116656799	192.168.56.101	192.168.56.102	TCP	60	1518 → 80 [RST] Seq=1 Win=0 Len=0
127	0.116656838	192.168.56.101	192.168.56.102	TCP	60	1519 → 80 [RST] Seq=1 Win=0 Len=0
128	0.116656876	192.168.56.101	192.168.56.102	TCP	60	1520 → 80 [RST] Seq=1 Win=0 Len=0
129	0.116656915	192.168.56.101	192.168.56.102	TCP	60	1521 → 80 [RST] Seq=1 Win=0 Len=0
130	0.116722743	192.168.56.101	192.168.56.102	TCP	60	1522 → 80 [RST] Seq=1 Win=0 Len=0
131	0.116722809	192.168.56.101	192.168.56.102	TCP	60	1523 → 80 [RST] Seq=1 Win=0 Len=0
132	0.116722840	192.168.56.101	192.168.56.102	TCP	60	1524 → 80 [RST] Seq=1 Win=0 Len=0
133	0.116722886	192.168.56.101	192.168.56.102	TCP	60	1525 → 80 [RST] Seq=1 Win=0 Len=0
134	0.116722916	192.168.56.101	192.168.56.102	TCP	60	1526 → 80 [RST] Seq=1 Win=0 Len=0
135	0.116722954	192.168.56.101	192.168.56.102	TCP	60	1527 → 80 [RST] Seq=1 Win=0 Len=0
136	0.116722993	192.168.56.101	192.168.56.102	TCP	60	1528 → 80 [RST] Seq=1 Win=0 Len=0
137	0.116723031	192.168.56.101	192.168.56.102	TCP	60	1529 → 80 [RST] Seq=1 Win=0 Len=0
138	0.116733911	192.168.56.101	192.168.56.102	TCP	60	1530 → 80 [RST] Seq=1 Win=0 Len=0
139	0.116733943	192.168.56.101	192.168.56.102	TCP	60	1531 → 80 [RST] Seq=1 Win=0 Len=0
140	0.116733982	192.168.56.101	192.168.56.102	TCP	60	1532 → 80 [RST] Seq=1 Win=0 Len=0
141	0.116734020	192.168.56.101	192.168.56.102	TCP	60	1533 → 80 [RST] Seq=1 Win=0 Len=0

Slika 11. Wireshark analiza podatkovnog prometa

Kao što se može primijetiti unutar Wireshark alata, tijekom napada vidljivo je da se u kratkom vremenskom razdoblju s izvorne IP adrese 192.168.56.101, koja pripada Kali Linux virtualnoj napadačkoj mašini, šalje velika količina podataka. Kako bi se bolje razumjela slika, potrebno je pojasniti oznake koje se na njoj nalaze.

- No. označava broj paketa.
- Time označava vrijeme u kojem je paket poslan.
- Source označava IP adresu napadačkog sustava.
- Destination označava IP adresu ciljanog sustava.
- Protocol označava protokol na koji je usmjeren napad.
- Length označava ukupnu dužinu paketa u bajtovima.
- Info prikazuje sažetu informaciju o specifičnom paketu i relevantnim podacima.

Vidljivo je da se s napadačkog sustava IP adrese 192.168.56.101 u razmaku od nekoliko milisekundi šalje velik broj paketa na ciljani sustav IP adrese 192.168.56.102.

Budući da je prilikom pokretanja naredbe s napadačkog sustava definirano da će se ciljati port 80, koji je HTTP port, uz oznaku RST koja signalizira prekid veze jer paketi ne prenose podatke, ovom simulacijom prikazuje se kako se u kratkom vremenskom razdoblju onemogućuje rad na ciljanim sustavima.

4.3. Keylogging napad

Potreba za simulacijom keylogginga proizlazi iz potrebe da se prikaže kako napadač može doći do osjetljivih podataka na ciljanom sustavu. Nakon svih potrebnih konfiguracija na Ubuntu

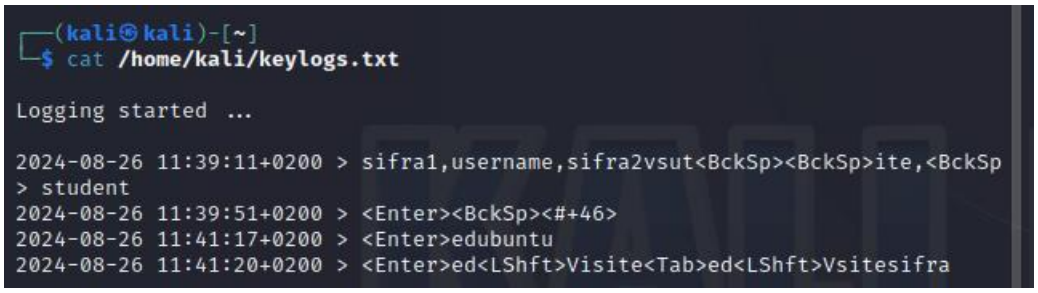
stroju, pokreće se naredba `sudo logkeys --start --output /tmp/keylogs.txt` koja omogućava da se svaki pritisak na tipkovnicu zabilježi u tekstualnu datoteku *keylogs.txt*. Tijekom simulacije uneseni su razni podaci na Ubuntu sustavu koje između ostalog sadrže i lozinke.

Kako bi napadač preuzeo keylogs.txt datoteku koristi se naredba `scp edubuntu@192.168.56.102 tmp/keylogs.txt /home/kali/.`

Kako bi se bolje razumjela ova naredba, potrebno je pojasniti njezinu sintaksu:

- scp označava "secure copy", alat za sigurno kopiranje datoteka između dva sustava putem SSH protokola.
- edubuntu@192.168.56.102 je korisničko ime i IP adresa udaljenog sustava s kojeg se datoteka kopira. U ovom slučaju, datoteka se kopira s korisnika „edubuntu“ na ciljanom sustavu.
- :/tmp/keylogs.txt označava putanju do datoteke koju je potrebno kopirati s udaljenog sustava (u ovom slučaju datoteka *keylogs.txt* koja se nalazi u direktoriju /tmp).
- /home/kali/ označava lokalni direktorij na napadačevom sustavu gdje će datoteka biti pohranjena nakon kopiranja.

Uz pomoć ove naredbe, napadač preuzima tekstualnu datoteku u kojoj su spremljeni svi pritisci na tipkovnici Ubuntu sustava. Naredna slika (Slika *12*) prikazuje *keylogs.txt* datoteku na Kali Linux sustavu.



Slika 12. Prikaz keylogs.txt datoteke

Na napadačkom sustavu, Kali Linuxu, pokretanjem naredbe `cat /home/kali/keylogs.txt` pregledavaju se podaci koji su preuzeti s Ubuntu sustava, gdje se može vidjeti da je svaki pritisak tipke na tipkovnici zabilježen. U ovoj datoteci mogu se vidjeti korisnička imena i lozinke za pristup određenim mrežnim stranicama.

5. ZAKLJUČAK

Ljudsku svakodnevicu okružuje tehnologija, bilo da je pojedinac toga svjestan ili ne. U digitalnom svijetu, gdje se pojedinci, ali i organizacije, uvelike oslanjaju na korištenje tehnologije za obavljanje svakodnevnih procesa, pojavljuje se i opasnost od iskorištavanja podataka koje te tehnologije koriste, kao i potreba za njihovom zaštitom.

Kroz razvoj tehnologije i kontinuirani rast potrebe pojedinaca za sustavima koji omogućuju bolje funkcionalnosti i brži pristup željenim podacima, često dolazi do propusta.

U ovom radu prikazano je kako je tijekom pojave COVID-19 virusa u Republici Hrvatskoj, zbog veće potrebe za digitalizacijom sustava, porastao i broj incidenata, odnosno napada koji su iskorištavali ranjivosti sustava. Usporedbom podataka iz godine prije početka pandemije COVID-19 i godine kada je došlo do zatvaranja i ograničavanja rada pojedinih ustanova, jasno se primjećuje porast broja kibernetičkih napada. Povećana potreba za digitalizacijom sustava dovela je do naglog porasta, a time je, možda zbog greške ili namjernog zanemarivanja, sigurnost sustava bila nedovoljno zaštićena.

Osim utjecaja COVID-19 virusa, na stvarnom primjeru rata vidljiv je utjecaj kibernetičkog kriminala, ali i računalne sigurnosti, i to ne samo na pojedinca ili organizaciju, već i na cijelu državu.

Rat u Ukrajini i podaci prikupljeni o kibernetičkim napadima tijekom pisanja ovog rada pokazuju koliku ključnu ulogu računalna sigurnost ima u obrani jedne zemlje. Tijekom čitanja poglavlja o ratu u Ukrajini može se primijetiti da su kibernetički napadi sustavno izvedeni kako bi onesposobili bitne sustave ključne za rad državnih ustanova. Osim onesposobljavanja ključnih ustanova, kibernetički napadi imaju za cilj širenje masovne panike i dezinformacija. Kada se to promatra na razini jedne države, jasno je da imaju utjecaj od najviših državnih institucija, poput vojske, pa sve do civila.

Od postanka prvog računala koje je imalo mogućnost spajanja na mrežu, postoje pojedinci koji, zbog vlastite koristi ili zadovoljstva, pokušavaju prouzročiti štetu. Nažalost, dok haker ne pokuša iskoristiti neki dio sustava na novi način, ne može se osigurati pravovaljana računalna zaštita. To se posebno primjećuje kod IoT tehnologija, koje svojom jedinstvenošću predstavljaju izazov za računalnu sigurnost.

Tijekom istraživanja ove tematike ukazala se prilika za simulacije kibernetičkih napada. Simulacijama napada se ukazuje se na problematiku da pojedinci često ne obraćaju pozornost na detalje te da veliku ulogu u računalnoj sigurnosti ima znanje o njoj. Pojedinac svojim neznanjem može prouzročiti veliku štetu, ili da je riječ o osobnim podacima koje izlaže

napadaču ili o podacima organizacije. Osim utjecaja pojedinca na vlastitu digitalnu sigurnost, kao i sigurnost organizacije, ostalim napadima prikazuje se kako oni utječu na ciljani sustav i koje ranjivosti iskorištavaju kako bi ometali daljnji rad pojedinca ili organizacije.

Odgovornost za računalnu sigurnost i osiguravanje osobnih podataka tijekom korištenja računala leži na pojedincu. Pojedinac koji koristi računalo mora biti upoznat ne samo s prednostima koje računalo pruža, već i s rizicima kojima izlaže sebe i druge. Osim odgovornosti pojedinca, jednaku odgovornost snose i organizacije koje koriste različite sustave kako bi osigurale zaštitu podataka kojima se služe.

U praktičnom dijelu ovog rada pokazano je koliko je, nažalost, lako postati napadač, ali i žrtva.

LITERATURA

1. https://amazoniainvestiga.info/index.php/amazonia/article/view/1548/1541 (pristupljeno 10.4.2022.)
2. https://www.britannica.com/topic/cybercrime (pristupljeno 10.4.2022.)
3. https://www.fbi.gov/investigate/cyber (pristupljeno 10.4.2022.)
4. https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=LEGISSUM%3Al14560 (pristupljeno 17.4.2022.)
5. https://www.techtarget.com/searchsecurity/definition/cybercrime (pristupljeno 17.4.2022.)
6. https://www.imperva.com/learn/application-security/backdoor-shell-attack/ (pristupljeno 17.4.2022.)
7. https://www.cert.hr/virusi/ (pristupljeno 17.4.2022.)
8. https://hr.wikipedia.org/wiki/Ra%C4%8Dunalni_virus (pristupljeno 10.5.2022.)
9. CERT,(2022) statistika, https://www.cert.hr/statistika/ (pristupljeno 10.5.2022.)
10. https://www.techtarget.com/searchsecurity/definition/email-spoofing (pristupljeno 10.5.2022.)
11. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html (pristupljeno 10.5.2022.)
12. https://www.ncsc.gov.uk/section/information-for/large-organisations (pristupljeno 20.6.2022.)
13. https://hr.wikipedia.org/wiki/Pandemija_COVID-19_u_Hrvatskoj (pristupljeno 20.6.2022.)
14. https://hr.wikipedia.org/wiki/Nacionalni_CERT (pristupljeno 20.6.2022.)
15. https://www.cert.hr/wp-content/uploads/2020/01/GI-NCERT-2019-FIN.pdf (pristupljeno 24.6.2022.)
16. https://www.cert.hr/wpcontent/uploads/2021/02/Carnet_Cert_godisnji_izvjestaj_2020_0402-3.pdf (pristupljeno 24.6.2022.)
17. https://www.imperva.com/learn/application-security/website-defacement-attack/ (pristupljeno 10.7.2022.)
18. https://duplico.io/kibersigurnost-u-2021-godini/ (pristupljeno 10.7.2022.)
19. https://gatefy.com/blog/what-malicious-url/ (pristupljeno 10.7.2022.)
20. https://plaviured.hr/vodici/scam-phishing-sto-se-zastititi/ (pristupljeno 15.7.2022.)

21. https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/# (pristupljeno 15.7.2022.)
22. https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/ (pristupljeno 15.7.2022.)
23. https://www.checkpoint.com/cyber-hub/network-security/what-is-ips/ (pristupljeno 1.8.2022.)
24. https://www.ibm.com/topics/mobile-security (pristupljeno 1.8.2022.)
25. https://www.checkpoint.com/solutions/iot-security/ (pristupljeno 1.8.2022.)
26. https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-security.html (pristupljeno 1.8.2022.)
27. https://www.csis.org/people/james-andrew-lewis (pristupljeno 15.8.2022.)
28. https://en.wikipedia.org/wiki/James_Andrew_Lewis (pristupljeno 15.8.2022.)
29. https://www.csis.org/people/james-andrew-lewis (pristupljeno 15.8.2022.)
30. https://csiswebsiteprod.s3.amazonaws.com/s3fspublic/publication/220616_Lewis_Cyber_War.pdf?S.iEKeom79InugnYWlcZL4r3Ljuq.ash (pristupljeno 1.9.2022.)
31. Dejan Košutić, (2012), 9 Steps to Cybersecurity The Manager's Information Security Strategy Manual
32. Lawrence C. Miller, (2016), Cybersecurity for dummies
33. Godišnje izvješće o radu nacionalnog vijeća za kibernetičku sigurnost i operativno-tehničke koordinacije za kibernetičku sigurnost za 2021. godine – Ured vijeća za nacionalnu sigurnost
34. Ross J. Anderson , Security Engineering, A guide to Building Dependable Distributed Systems Second Edition
35. https://hr.wikipedia.org/wiki/Kali_Linux (pristupljeno 20.9.2022.)
36. https://www.geeksforgeeks.org/blackeye-phishing-tool-in-kali-linux/ (pristupljeno 20.9.2022.)

SAŽETAK

Diplomski rad temelji se na istraživanju tematike kibernetičkog kriminala i sustava zaštite. Rad pojašnjava povijest i nastanak kibernetičkog kriminala, njegove vrste i kategorije. Osim kibernetičkog kriminala, obrađuje se tematika sustava zaštite koji služe za računalnu sigurnost. Nakon obrade teorijskog dijela, ukazala se potreba prikazati kroz simulaciju kako hakeri iskorištavaju neznanje svojih žrtava te pojasniti moguću štetu koja može nastati u slučaju da napadač ostvari svoj cilj.

Ključne riječi: sigurnost, kriminal, mreža, incidenti, sustavi, haker

SUMMARY

This thesis is based on research into cybercrime and protection systems. The paper explains the history and origin of cybercrime, as well as its types and categories. In addition to cybercrime, the topic of protection systems that ensure computer system security is also covered. After addressing the theoretical part, the need arose to demonstrate, through simulation, how hackers exploit their victims' lack of knowledge and to clarify the potential damage that can occur if the attacker achieves their goal.

Keywords: security, crime, network, incidents, systems, hackers