KIBERNETIČKI NAPADI I KIBERNETIČKA SIGURNOST

Stanković, Vedran

Undergraduate thesis / Završni rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Karlovac University of Applied Sciences / Veleučilište u Karlovcu**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:128:927963

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-12-29**

VELEUČILIŠTE U KARLOVCU
Karlovac University of Applied Sciences

Repository / Repozitorij:

Repository of Karlovac University of Applied Sciences - Institutional Repository

zir.nsk.hr

dabar
DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Stručni studij sigurnosti i zaštite

Vedran Stanković

KIBERNETIČKI NAPADI

I

KIBERNETIČKA SIGURNOST

Završni rad

Karlovac, 2024.

Karlovac University of Applied Sciences

Safety and Protection Department

Profesional undergraduate study of Safety and Protection

Vedran Stanković

CYBER ATTACKS

AND

CYBER SECURITY

Final paper

Karlovac, 2024.

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Stručni studij sigurnosti i zaštite

Vedran Stanković

KIBERNETIČKI NAPADI

I

KIBERNETIČKA SIGURNOST

Završni rad

Mentor: Davor Kalem, mag. crim.

Karlovac, 2024.

VELEUČILIŠTE U KARLOVC

KARLOVAC UNIVERSITY OF APPLIED SCI
TrgJ.J.Strossmayera 9
HR-47000, Karlovac, Croatia
Tel. +385 - (0)47 - 843 - 510
Fax. +385 - (0)47 - 843 – 579

HRN EN ISO 9001:2009

VELEUČILIŠTE U KARLOVCU

Stručni studij sigurnosti i zaštite

Usmjerenje: Zaštita na radu Karlovac, 2024.

ZADATAK ZAVRŠNOG RADA

Student: Vedran Stanković Matični broj: 0248072646

Naslov: Kibernetički napadi i kibernetička sigurnost

Opis zadatka:

1. Opisati nastanak kibernetike i najvažnije pojmove vezane uz kibernetiku.
2. Pojasniti kibernetičku sigurnost, zakonsko određenje i tijela kibernetičke sigurnosti u Republici Hrvatskoj.
3. Definirati vrste kibernetičkih rizika i napada.
4. Analizirati najveće kibernetičke napada u svijetu i Republici Hrvatskoj.
5. Prikazati razvoj kibernetičke forenzike i kažnjiva djela vezana uz kompjutorski kriminalitet.
6. Prikazati razvoj kibernetičke forenzike i kažnjiva djela vezana uz kompjutorski kriminalitet.
7. Interpretirati sredstva koja koristi kibernetička forenzika.
8. Pojasniti mogućnosti poboljšanja kibernetičke sigurnosti u Republici Hrbvatskoj.

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
24. 02. 2024.	12. 7. 2024.	17. 07. 2024.

Mentor:
Davor Kalem, mag. crim.

Predsjednik Ispitnog povjerenstva:
Lidija Jakšić, mag. ing. cheming.

PREDGOVOR

Ovaj rad nastao je iz potrebe pisanja završnog rada za diplomski stručni studij Sigurnosti i Zaštite na Veleučilištu u Karlovcu.

Kao materijali korištene su knjige, brošure, internetske stranice koje se bave računalnom sigurnošću i proizvodnjom softvera za zaštitu računala od malicioznih napda.

Želim se zahvaliti svom mentoru gospodinu Davoru Kalemu, mag. crim. na savjetima i sugestijama prilikom pisanja ovog rada

Zahvaljujem se na velikoj potpori i razumijevanju svojoj obitelji. Hvala Vam što ste na svakom koraku bili i stajali uz mene.

SAŽETAK I KLJUČNE RIJEČI

U ovom radu cilj je pobliže objasniti što su kibernetički napadi, kako se mogu izvesti putem računalnih programa, kakvu štetu kibernetički napadi mogu napraviti za žrtvu, bila ona pojedinac ili veliko poduzeće, kako se obavljaju testiranja računalnih sustava, te načini pronalaska počinitelja kibernetičkog napada.

Ključne riječi: kibernetički napadi, kibernetička sigurnost, kibernetički rat, zlonamjerni programi, kibernetički kriminalitet, penetracijsko testiranje, adware, spyware, malware, ransomware, crv, scam

SUMMARY

In this final work, the goal is to explain in more detail what cyberattacks are, how they can be carried out through computer programs, how much damage cyberattacks can do to the victim, be it an individual or a large company, how computer systems are tested, and ways to find the perpetrator of a cyberattack.

Keywords: cyber attacks, cyber security, cyber war, malicious programs, cyber crime, penetration testing, adware, spyware, malware, ransomware, worm, scam

SADRŽAJ

1. UVOD

U kibernetičke prijetnje spadaju različiti oblici napada ili štetnih aktivnosti koje se provode putem računalnih sustava i interneta. Napadi se mogu izvoditi različitim načinima poput virusa[1],phishinga[2], ransomwarea[3], DDoS[4] napada i mnogih drugih. Sve ove prijetnje mogu nanijeti štetu pojedincima, tvrtkama i čak cijelim državama. Važno je biti svjestan potencijalnih prijetnji i poduzeti odgovarajuće mjere zaštite. Kibernetička sigurnost se odnosi na zaštitu računalnih sustava, mreža i podataka od kibernetičkih prijetnji. To uključuje implementaciju sigurnosnih mjera poput antivirusnih programa, firewalla, enkripcije podataka, sigurnosnih politika i obuka osoblja. Cilj je spriječiti neovlašteni pristup, oštećenje ili krađu podataka te osigurati integritet, povjerljivost i dostupnost informacija.

[1] Računalni virus je računalni program koji se može samostalno umnožavati te izvoditi radnje bez volje korisnika računala.
[2] Phising se odnosi na računalne prijevare u kojima napadač lažnim predstavljanjem pokušava potencijalnu žrtvu natjerati da nešto učini u njegovu korist. Napadači se za prijevare koriste elektroničkom poštom, servisima poput foruma, društvenih mreža, servisa za izravnu komunikaciju
[3] Ransomware je zlonamjerni program koji onemogućuje korištenje računala. Program šifrira datoteke na računalu ili onemogućuje korištenje tako da se pojavi početni ekran s određenom porukom koju nije moguće maknuti.
[4] DDoS napad cilja web-mjesta i poslužitelje ometanjem mrežnih usluga u pokušaju iscrpljivanja resursa aplikacije. Napadači iza tih napada preplavljuju web-mjesto nasumičnim prometom, što rezultira lošom funkcionalnošću web-mjesta ili potpunim izbacivanjem s mreže.

2. KIBERNETIKA

Riječ kibernetika dolazi od grčke riječi *κυβερνάω* što znači upravljam, kormilarim, a uveo ju je američki matematičar Norbert Wiener (1894. – 1964.) u djelu „Kibernetika“ (Cybernetics, 1984.). Bavio se tijekom II. svjetskog rata problemima vođenja letjelica. Došao je na zamisao da obradu informacija u elektroničkim napravama usporedi sa misaonim procesima kao u ljudskom mozgu. Predložio je okvire za jedinstvenu teoriju koja obuhvaća ponašanje kako ljudskih bića tako i strojeva.

Model sustava koji se pritom razmatra (kibernetički sustav) sastoji se od tri cjeline:

- podsustav osjetila kojima se prikupljaju informacije o trenutačnom stanju sustava,
- podsustav u kojem se iz prikupljenih informacija trenutačno stanje uspoređuje sa željenim stanjem i tako utvrđuje razlika (pogreška) i
- podsustav koji utječe na ponašanje sustava tako što smanjuje nastale razlike

U takvu je sustavu ostvarena povratna veza kao osnova stabilnoga djelovanja svih sustava. Primjer, kada čovjek želi dohvatiti neki predmet, tada postoji povratna veza koja obuhvaća vid, misaoni proces u mozgu i poticaj mišićima koji pokreću šaku prema predmetu. Zatvaranjem očiju, ta će se povratna veza prekinuti i postupak dohvaćanja predmeta bit će otežan. S vremenom se pokazalo da je početna zamisao o jednoj sveobuhvatnoj teoriji upravljanja i vođenja bila previše optimistična. Tim se problemom bave znanstvene discipline koje se velikim dijelom oslanjaju na primjenu informacijske i komunikacijske tehnologije. Kibernetika, kao naziv, uglavnom se rabi za studije ljudskoga živčanoga sustava i artefakata informacijske i komunikacijske tehnologije. Cjeloviti informacijski prostor ostvaren globalno umreženim računalima popularno se naziva kibernetičkim prostorom (engl. Cyberspace), a u znanstvenofantastičnoj literaturi naziv kiborg (od kibernetički organizam), biće kojemu su dodani umjetni organi ili dijelovi tijela.[1]

3. TERMINOLOŠKE DETERMINANTE

Sigurnost je jedno od egzistencijalnih pitanja. Bez sigurnosti nema opstanka niti za jednu zajednicu na svijetu. Najjednostavnija definicija sigurnosti je odsutnost od štetnih ugrožavanja. Cilj svake države je da bude sigurna, odnosno da država opstane što se naziva nacionalna sigurnost. Pojam nacionalne sigurnosti prvi se put spominje u Sjedinjenim Američkim Državama četrdesetih godina 20. stoljeća, ali intenzivnije se počeo koristiti na kraju Drugog svjetskog rata. Definicija nacionalne sigurnosti prema američkom novinaru Walteru Lippmanu glasi „nacija je sigurna u mjeri u kojoj nije u opasnosti da mora žrtvovati ključne vrijednosti da bi izbjegla rat te je sposobna, ako je izazovu, da ih zadrži pobjedom u takvom ratu". Osim Waltera Lippmana definiciju nacionalne sigurnosti dao je i Giacomo Luciani[5] prema kojoj je „nacionalna sigurnost sposobnost odolijevanja agresije izvana".[2]

3.1 Kibernetički prostor

Kibernetički prostor, odnos Cyberspace, označava sve ono što se odvija u virtualnom prostoru posredstvom globalno umreženih računala. Sam pojam cyberspace prvi je put u upotrebu stavio američki pisac William Gibson[6]. On je u svojoj knjizi izdanoj 1948. pod nazivom „Neuromancer", opisao što je cyberspace. Kibernetički prostor istovjetan je stvarnom prostoru jer se ljudi u njemu mogu družiti i komunicirati putem različitih društvenih mreža (npr. Facebook, X, YouTube, Instagram, LinkedIn i dr.) Od 2000. do 2010. broj ljudi koji koriste kibernetički prostor, odnosno internet, porastao s 360 milijuna na gotovo dvije milijarde korisnika. Osim za komunikaciju, kibernetički se prostor koristi i za druge aktivnosti kao npr. međunarodno poslovanje, trgovinu uslugama i robom, znanost i dr. Izuzev gospodarskih aktivnosti, kibernetički se prostor može koristiti i u vojne

[5] Giacomo Luciani vodeći je talijanski stručnjak za geopolitiku energije. Njegovi znanstveni interesi uključuju Političku ekonomiju Bliskog istoka i Sjeverne Afrike te Geopolitiku energije. Pomoćni je profesor na Institutu za diplomske studije međunarodnih i razvojnih studija u Ženevi i suvoditelj izvršnog magisterija za vodstvo u nafti i plinu na Institutu

[6] William Gibson, rođ. 17. ožujka 1948. u Conway-u, Južna Karolina, SAD). Pisac znanstvene fantastike koji je bio vođa žanrovskog cyberpunk pokreta.

svrhe pa je Združeni stožer oružanih snaga SAD-a u listopadu 2006. dao svoju definiciju kibernetičkog prostora: „područje koje karakterizira upotreba elektroničkog i elektromagnetskog dijapazona za pohranjivanje, modificiranje i razmjenjivanje podataka, putem mrežnih sustava i povezanih fizičkih infrastruktura". Uz sve prednosti koje daje u suvremenom svijetu, kibernetički prostor predstavlja i značajan sigurnosni izazov.

Sigurnosne prijetnje u kibernetičkom prostoru možemo podijeliti na četiri razine:

- prva razina je kibernetički kriminal,
- druga razina je kibernetička špijunaža,
- treća razina je kibernetički terorizam i
- četvrta razina je kibernetičko ratovanje.

Sve te ugroze su maliciozne, odnosno imaju zadatak naštetiti sustavima, npr. kritičnoj infrastrukturi, financijama, prometu, komunikacijama i ostalim osjetljivim sustavima. [2]

3.2 Kibernetička sigurnost

Kibernetička sigurnost tema je koja dugo zaokuplja pažnju znanstvenika, istraživača i ljudi iz poslovnog svijeta. Sve se više socijalnih interakcija odvija u kibernetičkim prostoru. To pokazuje i podatak da korisnici diljem svijeta pošalju preko 40 trilijuna e-poruka. Prema procjenama broj uređaja koji su bili spojeni na internet iznosio je oko 8,7 milijardi u 2012., dok je prema procjenama broj uređaja spojen na internet više od 62 milijarde u 2024 godini[3]. Iz tog razloga kibernetička sigurnost dobiva sve više na važnosti u svim segmentima života.

Sama ideja kibernetičke (cyber) sigurnosti počiva na tome kako naučiti, upravljati i osigurati nesmetano funkcioniranje informatičkog okruženja. Informatičko okruženje podrazumijeva tehnološke, organizacijske, društvene i ostale aspekte. Prema Središnjem državnom uredu za razvoj digitalnog društva Republike Hrvatske „kibernetička sigurnost obuhvaća skup procesa, mjera i standarda kojima se jamči određena razina pouzdanosti pri korištenju proizvoda i usluga u kibernetičkom prostoru, pri čemu sustavna zaštita računala i računalnih mreža, informatičke i informacijske infrastrukture". Kibernetička sigurnost postaje krucijalna stavka unutar nacionalne sigurnosti. U današnje vrijeme

kibernetičke prijetnje sve više u porastu, a napadi postaju sve napredniji i složeniji. Sama tipologija napada je različita, ali možemo reći da su to razni maliciozni programi, krađa osobnih i financijskih podataka, računalne prevare te zloupotreba raznih društvenih mreža. [2]

4. ZAKONSKO ODREĐENJE KIBERNETIČKE SIGURNOSTI

Sa danom 15. veljače 2024. godine, na snagu je stupio Zakon o kibernetičkoj sigurnosti.[7] Tim se zakonom u hrvatsko zakonodavstvo preuzima Direktiva Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibernetičke sigurnosti širom Unije.[8]

Zakonom o kibernetičkoj sigurnosti uređuju se:

- postupci i mjere za postizanje visoke zajedničke razine kibernetičke sigurnosti,
- kriteriji za kategorizaciju ključnih i važnih subjekata,
- zahtjevi kibernetičke sigurnosti za ključne i važne subjekte,
- posebni zahtjevi za upravljanje podacima o registraciji naziva domena i kontrola njihove provedbe,
- dobrovoljni mehanizmi kibernetičke zaštite,
- nadležna tijela u području kibernetičke sigurnosti i njihove zadaće i ovlasti,
- stručni nadzor nad provedbom zahtjeva kibernetičke sigurnosti,
- prekršajne odredbe,
- praćenje provedbe ovoga Zakona i druga pitanja od značaja za područje kibernetičke sigurnosti.

Cilj Zakona o kibernetičkoj sigurnosti je uspostavljanje sustava upravljanja kibernetičkom sigurnošću koji će osigurati djelotvornu provedbu postupaka i mjera za postizanje visoke razine kibernetičke sigurnosti u sektorima od posebne važnosti za nesmetano obavljanje ključnih društvenih i gospodarskih aktivnosti i pravilno funkcioniranje unutarnjeg tržišta.[4]

[7] Zakon o kibernetičkoj sigurnosti (NN 14/2024)
[8] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibernetičke sigurnosti širom Unije

4.1 Institucije Republike Hrvatske koje skrbe o kibernetičkoj sigurnosti i sigurnosti podataka

Institucije koja sudjeluju u borbi protiv kibernetičkih prijetnji su:

- Ured Vijeća za nacionalnu sigurnost
- Sigurnosno-obavještajna agencija
- Nacionalni CERT
- Zavod za sigurnost informacijskih sustava
- Ministarstvo unutarnjih poslova, Ravnateljstvo policije, Uprava kriminalističke policije, Kriminalističko-obavještajni sektor, Služba kibernetičke sigurnosti
- Agencija za zaštitu osobnih podataka

4.1.1 Ured Vijeća za nacionalnu sigurnost

Ured Vijeća za nacionalnu sigurnost središnje je državno tijelo za informacijsku sigurnost – hrvatski NSA (National Security Authority).[9] Ured koordinira i usklađuje donošenje i nadzire primjenu mjera i standarda informacijske sigurnosti u okviru područja sigurnosne provjere, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacijskih sustava i sigurnosti poslovne suradnje, te izdaje certifikate za fizičke i pravne osobe za pristup nacionalnim, NATO i EU klasificiranim podacima. [5]

4.1.2 Sigurnosno-obavještajna agencija

Sigurnosno-obavještajna agencija bavi se sustavnim prikupljanjem, analizom i obradom podataka koji su od značaja za nacionalnu sigurnost i koji su nužni za donošenje odluka značajnih za ostvarivanje nacionalnih interesa na području nacionalne sigurnosti. SOA nastoji otkriti i spriječiti radnje koje su usmjerene protiv neovisnosti i suvereniteta RH, nasilnog rušenja ustroja državne vlasti, protiv Ustavom i zakonima utvrđenih ljudskih

[9] NSA (National Security Authority) je nacionalna američka obavještajna agencije koja nadzire i analizira komunikaciju u državi, ali i u inozemstvu. NSA je odgovorna za globalno praćenje, prikupljanje i obradu informacija i podataka u obavještajne i protuobavještajne svrhe

prava i temeljnih sloboda te osnova gospodarskog sustava RH. SOA u inozemstvu prikuplja, analizira, obrađuje i ocjenjuje podatke političke, gospodarske, sigurnosne i vojne prirode koji se odnose na strane države, međunarodne vladine i nevladine organizacije, političke, vojne i gospodarske saveze, skupine i osobe, koji upućuju na namjere, mogućnosti, prikrivene planove i tajna djelovanja koja su usmjerena na ugrožavanje nacionalne sigurnosti. [6]

4.1.3 Nacionalni CERT

Nacionalni CERT (CERT.hr) dio je Hrvatske akademske i istraživačke mreže – CARNET . On je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj čiji je osnovni zadatak obrada računalno-sigurnosnih incidenata s ciljem očuvanja kibernetičke sigurnosti u Republici Hrvatskoj. CERT.hr se bavi incidentom ako se jedna od strana u incidentu nalazi u Republici Hrvatskoj. Osim toga, Nacionalni CERT je nadležni CSIRT[10] za pet sektora temeljem novog Zakona o kibernetičkoj sigurnosti). Radi se o sljedećim sektorima: bankarstvo, Infrastruktura financijskog tržišta, digitalna infrastruktura, istraživanje, te sustav obrazovanja. [7]

4.1.4 Zavod za sigurnost informacijskih sustava

Zavod za sigurnost informacijskih sustava (ZSIS) središnje je državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti državnih tijela Republike Hrvatske, koji obuhvaćaju standarde sigurnosti informacijskih sustava, sigurnosnu akreditaciju informacijskih sustava te upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka. Pored poslova sigurnosne akreditacije informacijskih sustava, Zavod za sigurnost informacijskih sustava nadležan je i za provedbu aktivnosti u svezi s upravljanjem kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka između državnih tijela i stranih država i organizacija kao i poslove

[10] CSIRT je kratica za Computer Security Incident Response Team, odnosno nadležno tijelo za prevenciju i zaštitu od kibernetičkih incidenata

istraživanja, razvoja i ispitivanja tehnologija namijenjenih zaštiti klasificiranih podataka te izdavanja uvjerenja za njihovu uporabu. [8]

4.1.5 Služba kibernetičke sigurnosti

Služba kibernetičke sigurnosti djeluje pod Ravnateljstvom policije, Uprava kriminalističke policije, Kriminalističko-obavještajni sektor. Sudjeluje u primjeni i razvoju nacionalnog zakonodavnog okvira kibernetičke sigurnosti, u aktivnostima i mjerama u svrhu povećanja sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora, u uspostavi učinkovitih mehanizama razmjene, ustupanja i pristupa podacima potrebnim za osiguravanje više razine opće sigurnosti u kibernetičkom prostoru. Aktivno djeluje na jačanju svijesti o sigurnosti svih korisnika kibernetičkog prostora, razvija usklađene obrazovne programe, potiče istraživanja i razvoj, radi na sustavnom pristupu međunarodnoj suradnji u području kibernetičke sigurnosti. Sustavno analizira, prati i izučava fenomenološki i etiološki aspekt kaznenih djela kibernetičkog kriminaliteta (kaznena djela protiv računalnih sustava, programa i podataka, kaznena djela protiv intelektualnog vlasništva, te kaznena djela iskorištavanja djece za pornografiju). Predlaže rješenja na planu podizanja razine učinkovitosti rada u suzbijanju kibernetičkog kriminaliteta, neposredno provodi složena kriminalistička istraživanja, obavlja poslove digitalne forenzike koji uključuju osiguranje, prikupljanje, obradu i analizu digitalnih dokaza. Pruža specijaliziranu potporu drugim policijskim jedinicama, surađuje s drugim ustrojstvenim jedinicama Ministarstva, tijelima državne uprave i pravnim osobama, policijama drugih zemalja i međunarodnim institucijama u svom djelokrugu rada. Sudjeluje u planiranju i izradi programa obuke i specijalizacije policijskih službenika, u izradi normativnih akata, izvješća i drugih stručnih materijala iz domene kibernetičkog kriminaliteta. [9]

4.1.6 Agencija za zaštitu osobnih podataka

Agencija za zaštitu osobnih podataka je samostalno i neovisno državno tijelo. Nadzire provedbu propisa o zaštiti osobnih podataka. Agencija je neovisno nadzorno tijelo i glede obrade osobnih podataka od strane nadležnih tijela u svrhu sprječavanja, istraživanja,

otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući i zaštitu od prijetnji javnoj sigurnosti i sprječavanje takvih prijetnji. [10]

5. KLASIFIKACIJA PRIJETNJI KIBERNETIČKE SIGURNOSTI

Definicija prijetnje može se definirati kao: „prijetnja, potencijalni uzrok neželjenog incidenta, koji može dovesti do štete na sistemu ili organizaciji, odnosno projektu.“ [11] Prijetnje su možebitni generator neizvjesnosti i ako nema prijetnji, nema ni ugroze za bilo koji sustav. Iz tog razloga potrebno je napraviti klasifikaciju prijetnji kako bi se kasnije na jednostavan način mogle identificirati. Prilikom identifikacije prijetnji bilo bi poželjno da se koriste tri vrste identifikacije: izvor prijetnji, lokacija i motivacija.

Kibernetički napadi se mogu izvesti u dvjema varijantama:

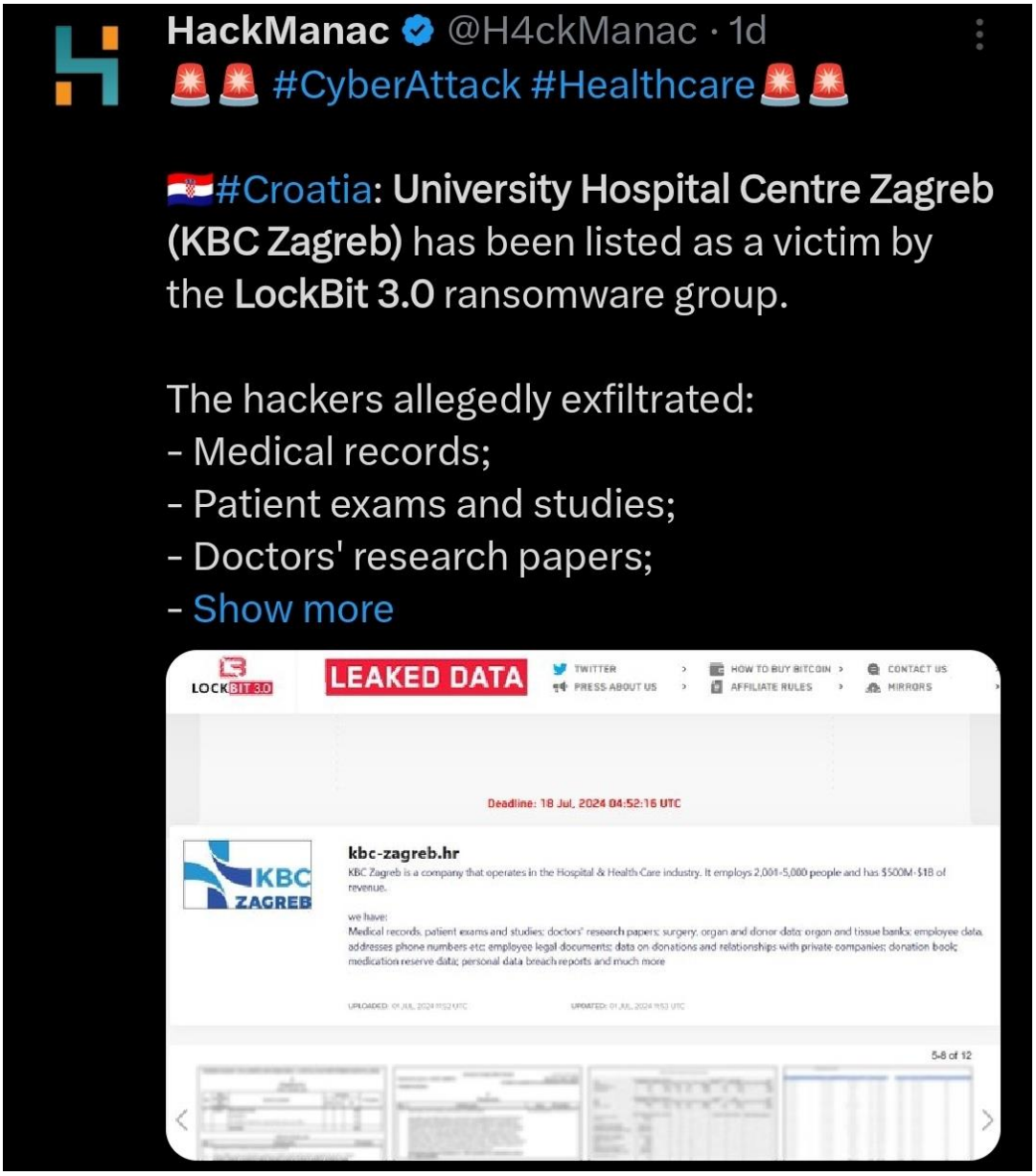
- napad na podatke i
- napad na nadzorne sustave ili operativne tehnologije.

Tijekom noći s 24. na 25. lipnja 2024. godine dogodio se kibernetički napad koji je bio usmjeren na Sveučilišni bolnički centar Zagreb (KBC Zagreb) u Hrvatskoj. Bolnica je morala zatvoriti cjelokupnu IT infrastrukturu. Napad je značajno oštetio digitalne sustave bolnice, uzrokujući velike probleme u radu i privremeno vraćanje na ručne procese. Predstavnici bolnice izjavili da osjetljivi podaci, iz bolničkog sustava, nisu ugroženi. Kompanija HackManac[11] objavila je na platformi X kako je Sveučilišni bolnički centar Zagreb žrtva LockBit 3.0[12] ransomware grupe. Hakeri su navodno preuzeli: medicinsku dokumentaciju, preglede i studije pacijenata, istraživačke radove liječnika, podatke s kirurgije, podatke o organima i darivateljima, podatke Banke organa i tkiva, podatke o zaposleniku, (adrese, telefonski brojevi), pravne dokumente zaposlenika, podatke o donacijama i odnosima s privatnim tvrtkama, knjigu donacija.[12]

---

[11] HackManac je globalna platforma sa sjedištem u Dubaiju koja pruža detaljne informacije o najnovijim računalnim napadima, uključujući imena *ransomware* grupa, žrtve i težinu napada

[12] LockBit 3.0 je zloglasna skupina kibernetičkih kriminalaca, poznata i kao LockBit Black, razvila je unosan poslovni model zasnovan na Ransomware-as-a-Service (RaaS) modelu, omogućujući čak i neiskusnim zlonamjernim akterima da pokrenu ransomware napade. Američki FBI smatra da je na čelu skupine 31-godišnji Rus, Dmitry Yuryevich Khoroshev. Potraga za njim i dalje traje.



Slika 1 objava Hackmanac-a o kibernetičkom napadu na KBC Zagreb, izvor: www.x.com

Dana 21. lipnja 2024. oko 12.20 dogodio se veliki mrežni incident u jugoistočnom dijelu kontinentalne Europe. Incident je rezultirao nestankom struje u elektroenergetskim mrežama Albanije, Crne Gore, Bosne i Hercegovine te djelomičnim nestankom struje u Hrvatskoj. Pogođeni distributeri električne energije, uz podršku susjednih distributera, vratili su napajanje svojim mrežama u roku od približno 2 sata s ciljem smanjenja utjecaja

poremećaja na potrošače. ENTSO-E [13] trenutno prikuplja sve relevantne tehničke podatke o ovom događaju od pogođenih distributera i pružit će više informacija što je prije moguće. [13]

Napad na nadzorne sustave također ostavljaju nesagledive posljedice i koriste se najčešće za ugrožavanje kritične infrastrukture jedne države (npr. voda, plin, električna energija, prometu i sl.). Takvi napadi izvode se putem interneta ili penetracijom u sustave nadzora odnosno operativnih tehnologija, koje su ključne za mnoge industrije danas. Dobar je primjer napad u ožujku 2000. kada je bivši zaposlenik putem interneta ušao u nadzorni sustav otpadnih voda u gradu Queenslandu u Australiji i preko pumpi pustio milijun litara otpadnih voda u sustav za pitku vodu. Taj slučaj je jedan od primjera kako se može na vrlo jednostavan način ugroziti zdravlje milijuna ljudi koji koriste pitku vodu. Šokantan je podatak da je nakon samo 45 pokušaja izvršio penetraciju u sustav i pustio otpadnu vodu u sustav pitke vode, dakle ostala 44 pokušaja nitko na vrijeme nije detektirao.[2]

[13] ENTSO-E je Europska mreža operatora prijenosnih sistema za električnu energiju

5.1 Kibernetički kriminal

Kibernetički kriminal najčešća je sigurnosna ugroza u kibernetičkom prostoru. Pojavljuje se sredinom sedamdesetih godina prošlog stoljeća kada dolazi do značajnijeg razvoja računala. Prva računala koja su bila razvijena bila su za upotrebu u vojne, znanstvene i tek nešto kasnije gospodarske svrhe. Ta činjenica je onemogućavala da se bilo tko izvan tih organizacija može baviti kibernetičkim kriminalom. Kibernetički kriminal obuhvaća prevare u kibernetičkom prostoru. Najčešći način kibernetičkog kriminala je prevara na internetskom bankarstvu, odnosno krađa s bankovnih kartica. Zarada od takve vrte kriminala penje se na oko 100 milijuna dolara godišnje. Osim prevare putem internet bankarstva, postoje i drugi oblici kibernetičkog kriminala. To su phishing napadi[14], socijalni inženjering[15], zlonamjerni računalni programi[16], keyloggersi[17] i ransomware.[18][2]

5.2 Kibernetička špijunaža

Kibernetički prostor je bitno područje svjetskog gospodarstva, ali za sobom nosi i sve veće ugoze za kibernetičku sigurnost. Cilj kibernetičke špijunaže je neovlašteno prikupljanje podataka u kibernetičkom prostoru. Kibernetičku špijunažu ne rade samo kriminalne skupine ili pojedinci, nego mogu biti države ili neke strane kompanije koje prikupljaju informacije. Razlozi prikupljanja informacija su dolazak do visokotehnoloških podataka, trgovina takvim informacijama trećim stranama koje bi takve informacije mogle iskoristit za vojnu i političku premoć. Problem je ako kibernetičku špijunažu koriste države

---

[14] Phising se odnosi na prijevare u kojima napadač lažnim predstavljanjem pokušava potencijalnu žrtvu natjerati da nešto učini u njegovu korist. Napadači se za prijevare koriste elektroničkom poštom, servisima poput foruma, društvenih mreža, servisa za izravnu komunikaciju

[15] Socijalni je inženjering niz tehnika pomoću kojih pojedinac, iskorištavanjem ljudskih pogrešaka i slabosti, utječe na drugog pojedinca kako bi ga naveo da učini nešto što nije u njegovom interesu. Socijalni se inženjering najčešće koristi u svrhu otkrivanja njihovih povjerljivih informacija ili dobivanja pristupa nekim drugim resursima do kojih napadač inače ne bi mogao doći.

[16] Zlonamjerni računalni programi dizajnirani su namjerom oštećenja ili onemogućavanja normalnog rad računala, mreže ili poslužitelja

[17] Keylogger je softver koji tajno prati i snima pritisnute tipke na tipkovnici. Oni također mogu biti i dijelovi hardvera, odnosno uređaji

[18] Ransomware je zlonamjerni program koji onemogućuje korištenje računala. Program šifrira datoteke na računalu ili onemogućuje korištenje tako da se pojavi početni ekran s određenom porukom koju nije moguće maknuti.

kako bi određene informacije iskoristile protiv neprijatelja. Tada je ugrožena sama nacionalna sigurnost te države. Metode koje se koriste u kibernetičkoj špijunaži slične su industrijskoj špijunaži. Primjer je ubacivanje malwara u računalnu infrastrukturu kompanija ili državnih institucija. Nakon što je malware ubačen u računalni sustav, on ondje prikuplja podatke o kompaniji ili državnoj instituciji. Također postoji i spyware, odnosno softver čija je namjena prikupljanje podatke o korisniku, te bez njegovog znanja pruzimanje kontrole nad zaraženim računalom. Jedan od najpoznatijih spywarea je Pegasus. Razvila ga je izraelska tvrtka s ciljem prikupljanja podataka o meti napada. Pegasus može snimati pozive i slike, prikupljati poruke i lozinke. Zanimljiva činjenica vezana za taj spyware je da ga je razvila izraelska tvrtka NSO, grupa za borbu protiv terorizma i kriminala, ali su zabilježeni i određeni slučajevi zloupotrebe tog softvera.[2]

2010. godine crv Stuxnet otkriven je u nuklearnom postrojenju u gradu Natanzu. Bio je dizajniran da uništi centrifuge koje je Iran koristio za obogaćivanje urana kao dio svog nuklearnog programa. Stuxnet je dizajniran da uništi centrifuge koje je Iran koristio za obogaćivanje urana kao dio svog nuklearnog programa. Većina urana koji se javlja u prirodi je izotop U-238. Međutim, fisibilni materijal koji se koristi u nuklearnoj elektrani ili oružju mora biti izrađen od nešto lakšeg U-235. Centrifuga se koristi za okretanje urana dovoljno brzo da odvoji različite izotope po težini do centrifugalne sile. Ove centrifuge su izuzetno osjetljive i nije neuobičajeno da se oštete tijekom normalnog rada. Kada Stuxnet zarazi računalo, provjerava je li to računalo povezano s određenim modelima programibilnih logičkih kontrolera (PLC-ova) koje proizvodi Siemens. PLC-ovi su način na koji računala komuniciraju i kontroliraju industrijske strojeve poput centrifuga urana. Ako se ne otkriju PLC-ovi, crv ne radi ništa, ako jesu, Stuxnet zatim mijenja programiranje PLC-ova, što rezultira nepravilnim okretanjem centrifuga, oštećujući ih ili uništavajući u tom procesu. Dok se to događa, PLC-ovi javljaju računalu kontrolera (pogrešno) da sve radi dobro, što otežava otkrivanje ili dijagnosticiranje onoga što se događa dok ne bude prekasno. Ured u Iranu (koji nije dio nuklearnog programa) doživljavao je tajanstvena ponovna pokretanja i plave ekrane smrti, koji su čak utjecali na računala sa svježim instaliranim operativnim sustavom. Nagađa se da su crv Stuxnet stvorile obavještajne

agencije Sjedinjenih Država i Izraela. Crv Stuxnet služio je kao alat za onesposobljavanje ili odgađanje iranskog programa razvoja nuklearnog oružja.[14]

Kibernetički terorizam odnosi se na upotrebu terorističkih metoda u kibernetičkom prostoru. Cilj mu je fizičko uništenje određenih uređaja, sustava uređaja ili nekog poslovnog procesa gdje postoje računalni sustavi. Prvim kibernetičkim terorističkim napadom smatra se napad na komunikacije veleposlanstva Šri Lanke. Od strane Oslobodilačkih tigrova tamilske domovine, odnosno frakcije Internet Black Tigers (IBT) u kolovozu 1997. godine napadnuta je službena komunikacija. Napad se odvijao na način da je slano oko 800 spam e-mailova što je rezultiralo onesposobljenom komunikacije veleposlanstva. Osim napada na vladine mrežne stranice[19], mete mogu biti i sustavi bolnica[20], nuklearnih postrojenja[21], elektrane[22], sustavi za kontrolu leta[23] i slično. Takvi napadi su postali sve učestaliji jer su znatno jeftiniji od klasičnih napada i ne zahtijevaju puno ljudi i opreme. Selidba terorističkih napada u kibernetički prostor postaje ozbiljna prijetnja svim državama. Kibernetički terorizam također može imati ozbiljne posljedice kao što su smrtni ishodi. Kritična infrastruktura u većini država nije na dovoljnoj razini sigurnosti, odnosno više se u laže u fizičko-tehničku zaštitu nego u kibernetičku zaštitu. Velika Britanija u svojoj strategiji nacionalne sigurnosti kibernetički terorizam uvrstila je kao ozbiljnu sigurnosnu prijetnju, te su izdvojili gotovo 650 milijuna funti na razdoblje od četiri godine za borbu i obranu od istog. Kibernetički terorizam postao stvarnost, ali i budućnost, i samo suradnja država može pomoći u borbi protiv te nove sigurnosne ugroze. Evolucija informacijske tehnologije jedan je od glavnih generatora gospodarstva svih država, ali i odgovornost da se spriječi možebitno zloupotrebljavanje. [2]

[19] 2007. godine kibernetički napad na Internet stranice estonske vlade, banaka, medija
[20] 2024. godine kibernetički napad na KBC Zagreb
[21] 2010. godine kibernetički napad na nuklearno postrojenje u gradu
[22] 2015. godine kibernetički napad na nacionalnu električnu mrežu u Ukrajini
[23] 2022. godine kibernetički napad na AHS Aviation Handling Services GmbH, Njemačka

5.3 Kibernetičko ratovanje

Kibernetičko ratovanje engl. cyberwarfare se može definirati kao rat koji se provodi pomoću računala i mreža koje ih povezuju, a sam rat provode države ili njihovi opunomoćenici protiv drugih država. Cilj kibernetičkog rata je poremetiti, uništiti ili uskratiti upotrebu vladinih i vojnih mreža. Jedan od zastrašujućih napada dogodio se 2007. godine na Estoniju. Nakon što je Estonija odlučila premjestiti spomenik sovjetskog vojnika iz parka u Talinu, čin je izazvao kibernetički napad na nju. Mete napadača, hakera, bile su važnije institucije za funkcioniranje države, pa su napadnute stranice vlade, medijske kuće, bankarski sustavi. Nakon kratkog vremena, 2008. godine dogodio se napad i na Gruziju. Radilo se o DDoS[24] napadima, engl. distributed denial-of-service attack. Kao i kod Estonije, napadnute su vladine stranice, odnosno onemogućiti građanima pristup bilo kakvim uslugama. Bio je to prvi napad koji je bio koordiniran s kopnenom invazijom na Gruziju. Ti napadi potaknuli su NATO savez da kibernetičko ratovanje istaknu kao ozbiljnu prijetnju za kritičnu infrastrukturu i druge segmente života, te zbog toga može ubuduće aktivirati članak 5. Washintonskog sporazuma [25] o obrani svojih članica.

Za razliku od ratovanja na kopnu, moru i zraku kibernetičko ratovanje ima svoje prednosti kao što su:

- niski operativni troškovi – znatno jeftinije od konvencionalnog ratovanja koje nosi enormne troškove,
- brisanje tradicionalnih granica – odvija se u kibernetičkom prostoru gdje nema granica i može doći izbilo kojeg dijela svijeta

[24] DDoS napad cilja web-mjesta i poslužitelje ometanjem mrežnih usluga u pokušaju iscrpljivanja resursa aplikacije. Napadači iza tih napada preplavljuju web-mjesto nasumičnim prometom, što rezultira lošom funkcionalnošću web-mjesta ili potpunim izbacivanjem s mreže

[25] Članak 5 Sjevernoatlantski ugovor (Washintonski sporazum sastavljen 4. travnja 1949 godine) objašnjava da je napad na jednu ili više zemalja potpisnica u Europi ili Sjevernoj Americi, napad na sve njih i zato se slažu da će u slučaju napada, svaka od njih, pozivajući se na pravo individualne ili zajedničke samoobrane iz članka 51 Povelje Ujedinjenih Naroda, pomoći potpisnici ili potpisnicama koje su napadnute, poduzimajući odmah, same i u skladu s drugim potpisnicama, korake koji se smatraju potrebnima, uključujući uporabu oružane sile, da bi povratile i održale sigurnost Sjevernoatlantskog područja

- nepripisivost odgovornosti – teško je ili nemoguće identificirati počinitelja i radi li se o unutarnjoj ili vanjskoj prijetnji,
- utjecaj na široku publiku – veliki odjek na percepciju sigurnosti

NATO je uveo pojam hibridnog rata, odnosno kombinaciju klasičnog ratovanja sa korištenjem informacijskih tehnologija u svrhu provedbe psiholoških operacija i zastrašivanja te upotrebu ne vojnih elemenata s ciljem širenja nesigurnosti i stvaranja unilateralne prednosti okupacijom ili aneksijom određenog područja. [2]

6. NAPADI ZLONAMJERNIM PROGRAMIMA

Zlonamjerni softver engl. malware je softver, bilo program ili datoteka, a dizajniran s namjerom oštećenja ili onemogućavanja normalnog rad računala, mreže ili poslužitelja. Može preuzeti kompletan ili djelomičan rad računala, računalnih sustava, tableta ili mobilnih uređaja. Vrste zlonamjernog softvera uključuju računalne viruse, crve, trojanske konje, ransomware i špijunski softver.[15] Ti zlonamjerni programi kradu, šifriraju i brišu osjetljive podatke, mijenjaju ili otimati osnovne računalne funkcije i nadziru aktivnosti računala krajnjih korisnika.[16] Napad zlonamjernim softverom može biti benigni, a može imati katastrofalne posljedice. Svake godine pokreću se milijuni napada zlonamjernim softverom na razne tvrtke, a svakodnevno se otkrije više od 500.000 novih zlonamjernih programa Takav softver omogućuje kriminalcima krađu novca i podataka, špijuniranje računalnih aktivnosti te oštećenje ili ometanje poslovanja.[17]

6.1 Adware

Adware je samostalan softverski program koji prikazuje oglase krajnjem korisniku u različitim oblicima: unutar samog programa ili putem skočnih prozora, kliznih oglasa, skočnih prozora preglednika, umetnutih oglasa ili izmijenjenog sadržaja web stranice. Adware nudi oglase sa sumnjivih stranica, a uglavnom se svode na prijevaru i prodaju nepostojećeg proizvoda. Na računalo se instalira najčešće sa besplatnim programima, a sve kako bi autori prekrili troškove izrade programa. Potajno može instalirati špijunski softver ili usporiti računalo stalnim prikazivanjem reklamnog sadržaja. Adware programe može se sa računala ukloniti samim deinstaliranjem programa putem operacijskog sustava, a također ga uklanjaju i razni antivirusni programi. [18]

Slika 2 Prikaz ekrana računala zaraženog adware-om, izvor: www.engadget.com

6.2 APT (Advanced Persistent Threat)[26]

Napredna ustrajna prijetnja (engl. Advanced Persistent Threat) odnosi se na organiziranu skupinu ljudi koja ima namjeru i sposobnost za ustrajan i djelotvoran napad određeni subjekt (naprimjer na vladu neke države). Izraz se koristi u kontekstu mrežnih napada, a može se koristiti i u kontekstu tradicionalnih načina špijunaže i napada. Izvršavanje APT napada zahtijeva više resursa od standardnog napada. Počinitelji su obično timovi iskusnih kibernetičkih kriminalaca koji imaju značajnu financijsku potporu. Neki APT napadi financiraju se od strane vlade i koriste se kao oružje za cyber ratovanje.

Točne definicije APT-a variraju. Iz izravnog prijevoda izraza APT može se zaključiti sljedeće:

- Advanced (napredan) - ljudi koji upravljaju prijetnjom koriste cijeli niz tehnika za sakupljanje podataka. Mogu uključivati tehnologije i tehnike koje se koriste za

[26] primjer APT napada je Stuxnet - crv korišten za napad na iranski nuklearni program

upade u računalne sustave, no uključuju i uobičajene načine skupljanja podataka (primjerice presretanje telefonskih poziva i satelitske snimke). Napadači često kombiniraju više metoda, alata i tehnika napada da bi došli do žrtve, ugrozili je i dobili pristup osjetljivim podacima.

- Persistent (ustrajan) - napadači pažnju posvećuju specifičnom zadatku. Oni ne traže informacije u svrhu financijske ili neke druge dobiti. To dovodi do zaključka da napadače nadzire neki vanjski subjekt. Napad se odvija uz stalni nadzor. Pritajeni i polagani napadi pokazali su se uspješnijima od stalnih velikih napada. Kad napadači izgube kontakt sa žrtvom obično će ga pokušati ponovno uspostaviti, najčešće uspješno. Jedan od glavnih napadačevih ciljeva je održavanje dugotrajnog pristupa resursima žrtve.
- Threat (prijetnja) - APT-ovi predstavljaju prijetnju jer posjeduju i sposobnosti i namjeru za napad. Napade izvode ljudi, za razliku od uobičajenih napada koji se temelje na automatiziranim dijelovima koda. Napadači imaju zadatak, te posjeduju odgovarajuće vještine, motivirani su, organizirani i odgovarajuće financirani.[19]

Napadi variraju ovisno o ciljevima, alatima i tehnikama kojima se napadači koriste, a također ovise o sposobnostima otkrivanja, identificiranja i obrane od strane žrtve. Prilikom napada napadači paze da ne budu otkriveni. Najčešće se prilikom napada koriste neotkriveni propusti u računalnim sustavima, programima ili operacijskim sustavima (eng. zero-day exploit). Industrija računalne sigurnosti u posljednjih nekoliko mjeseci sve više upozorava na opasnosti APT-a, posebice nakon što je tvrtka Google objavila da je bila žrtva mrežnog napada s izvorištem u Kini, a s ciljem krađe informacija.

Uspješan APT napad može se podijeliti u tri faze: infiltracija mreže, širenje prisutnosti napadača i izvlačenje prikupljenih podataka - sve bez otkrivanja.

1. Infiltracija mreže

Prva faza APT napada uključuje neovlašteni pristup mreži. Napadači često koriste tehnike socijalnog inženjeringa, kao što su e-poruke za krađu identiteta, kako bi ciljali pojedince na visokoj razini unutar organizacije. Te su e-poruke pažljivo izrađene kako bi

izgledale legitimno, često se pozivajući na tekuće projekte ili dolaze od pouzdanih članova tima.

2. Širenje prisutnosti napadača

Nakon što uđu u mrežu, napadači proširuju svoj pristup i prikupljaju kritične informacije. Oni mogu implementirati zlonamjerni softver za kretanje mrežom, mapiranje njegove strukture i dobivanje vjerodajnica kao što su nazivi računa i lozinke. To im omogućuje pristup vrijednim poslovnim podacima i uspostavljanje stražnjih vrata (engl. backdoor) za buduće napade.

3. Izvlačenje prikupljenih podataka

U završnoj fazi APT napada, cyber kriminalci izvlače ukradene podatke iz ugrožene mreže bez otkrivanja. Oni obično pohranjuju podatke na sigurno mjesto unutar mreže dok ne prikupe dovoljno da bi se izvlačenje isplatilo. Kako bi odvratili pažnju sigurnosnim timovima i povezali mrežne resurse, napadači mogu pokrenuti napade uskraćivanjem usluge (DoS) ili druge diverzantske taktike.[20]

6.3 Backdoor[27]

Stražnja vrata (eng. backdoor) odnosi se na bilo koju metodu kojom ovlašteni i neovlašteni korisnici mogu zaobići normalne sigurnosne mjere i dobiti pristup računalnim sustavima (tzv. root pristup), mreži ili softverskoj aplikaciji. Backdoor dolazi u obliku instaliranog programa ili promjena funkcija operacijskog sustava kao rootkit. Tom metodom cyber kriminalci kradu osobne i financijske podatke, instaliraju dodatni zlonamjerni softver i preuzimaju kompletan nadzor nad računalom, računalnim sustavom ili mrežom.

Zlonamjerni softver na stražnjim vratima općenito se klasificira kao trojan. Trojan je zlonamjerni računalni program koji se pretvara da je nešto što u stvari nije. Ima svrhu

[27] 2008. godine sve verzije OS-a Juniper Networks, od verzije 6.2.0 imale su backdoor koja su hakerima omogućavala administrativni pristup

isporuke zlonamjernog softvera, krađe podataka ili otvaranja stražnjih vrata na računalnom sustavu.[21]

6.4 Crv (engl. Worm)[28]

Računalni crvi su programi koji mogu sami sebe umnožiti, a šire se putem računalne mreže. Oni su samostalni programi koji se šire bez interakcije korisnika. Koriste računalnu mrežu kako bi s jednog računala zarazili drugo računalo. Nakon što je zarazio računalo izvršava određeni cilj kao što je instaliranje drugog zlonamjernog softvera, brisanje datoteka i korištenje i usporavanje propusnosti računalne mreže[22]

Crvi se mogu širiti na više načina:

Putem softverskih ranjivosti - neke varijante crva traže sigurnosne propuste na računalnim sustavima. Jednom kada se otkrije propust, on se infiltrira u taj sustav, a zatim obavlja svoje zlonamjerne aktivnosti.

Putem e-pošte - neke varijante crva mogu instalirati drugi zlonamjerni softver, poput backdoora. Na taj način računalo pretvara u bot i povezuje ga s botnet mrežom. Ta računala mogu slati neželjene e-poruke slučajnim ili ciljanim primateljima, a u privitku se nalazi datoteka sa crvom. Poslana neželjena pošta obično uključuje neke taktike socijalnog inženjeringa za veće šanse za infekciju.

Putem vanjskih uređaja - neke varijante crva mogu se kopirati na uređaje, kao što su USB vanjske memorije i vanjski tvrdi diskovi, koji se spajaju na već zaraženo računalo. Na taj način će se prenositi sa zaraženog računala na nezaraženo računalo.

[28] SQL Slammer iz 2003. bio je internetski crv koji je u 10 minuta zarazio otprilike 75 000 računala

Putem peer-to-peer (P2P)[29] mreža za dijeljenje datoteka - neki korisnici interneta znali su koristiti P2P aplikacije poput eMule[30] i Kazaa[31] za dijeljenje datoteka s prijateljima i obitelji. Međutim, takvu aktivnost iskorištavaju crvi. Crve u P2P mrežama teško je otkriti.

Preko društvenih mreža - neke varijante crva razmnožavale su se unutar poznatih društvenih stranica. Na primjer, na MySpace-u se je širio crv pod nazivom XSS.

Širenje putem socijalnog inženjeringa - podrazumijeva interakciju sa žrtvom. Autor crva lažima i različitim prijevarama pokušava žrtvu nagovoriti na njegovo pokretanje. Autor obično šalje e-mail poruku žrtvi u kojoj ga pokušava nagovoriti na preuzimanje i pokretanje izvršne datoteke crva. Osim slanja e-mail poruka, autori crva mogu slati i poruke na društvenim mrežama ili putem klijenata za trenutačnu razmjenu poruka.[23]

[29] P2P (peer-to-peer) slobodna razmjena informacija i datoteka među sudionicima mreže. Uslijed nemogućnosti primjerenog nadzora sudionika mreže i podataka, peer-to- peer mreže su iskorištene i za širenje zlonamjernih programa (virusa, crva, trojanskih konja, spyware programa, itd.) te za razmjenu zakonski zabranjenih sadržaja.

[30] eMule je aplikacija za P2P dijeljenje datoteka putem interneta

[31] Kazaa je aplikacija za P2P dijeljenje datoteka putem interneta

Slika 3 Prikaz e-poruke koja u privitku sadrži crva, izvor: www.malwarebytes.com

6.1 Malver (engl. Malware)

Malware je zloćudni softver koji napada operacijski sustav. Traži sigurnosne propuste operacijskog sustava ili sigurnosne propuste mreže da bi oštetio krajnjeg korisnika. Može tražiti novac od korisnika, sabotirati funkcionalnosti računala. Malware može ukrasti osjetljive podatke, kriptirati ili obrisati podatke, a može oštetiti rad samog operacijskog sustava čime računalo postaje neupotrebljivo. Vrste malware softver su: virus, crv, trojanski konj, spyware, zlonamjerni adware, crimeware, scareware, keylogger, rootkit Baš kao što prepoznamo prehladu po određenim simptomima, na sličan način možemo prepoznati i postojanje malware softvera na računalu.

Simptomi da je računalo zaraženo nekim od malwera su: računalo radi primjetno sporije, na zaslonu se pojavljuju reklame, pad operacijskog sustava, nagli nedostatak diskovnog prostora, u pregledniku se početna stranica primijenila bez da je to napravio korisnik, antivirusni program je isključen, ne može se pristupiti podatcima.[16]

6.2 Keylogger[32]

Hvatač (engl. Keylogger) je softver koji tajno prati i snima (sve) pritisnute tipke na tipkovnici. Oni također mogu biti i dijelovi hardvera, odnosno uređaji. Jedan od najpoznatijih ranih incidenata dogodio se sredinom 1970-ih, kada su sovjetski špijuni razvili nevjerojatno pametan hardverski keylogger koji je ciljao pisaće strojeve IBM Selectric u zgradama američkog veleposlanstva i konzulata u Moskvi i Sankt Peterburgu. Nakon instalacije, keyloggeri su mjerili jedva primjetne promjene u magnetskom polju svakog pisaćeg stroja dok se ispisna glava rotirala i pomicala za upisivanje svakog slova. U međuvremenu, sovjetska veleposlanstva odlučila su koristiti ručne pisaće strojeve, a ne električne za tipkanje povjerljivih podataka.[24]

Legitimni programi mogu imati funkciju keylogger softvera i pratiti pritisnute tipke kako bi pozvali specijalne programske funkcije ili za promjenu rasporeda tipki tipkovnice. Također, takav softver se može koristiti za kontrolu zaposlenika ili roditeljsku kontrolu djece. Zlonamjerna upotreba keyloggera podrazumijeva krađu povjerljivih podataka kao što su lozinke za pristup različitim servisima za plaćanje, brojevi kreditnih kartica itd. Keyloggeri predstavljaju specifičnu opasnost iz razloga jer nemaju namjeru izazvati štetu na zaraženom računalu, ali mogu nanijeti drugu štetu kao što je naprimjer financijska šteta. Podaci koje se keylogger softverom prikupe spremaju se u log datoteku koja se zatim putem e-pošte ili unaprijed definirane mrežne stranice ili baze podataka šalje napadaču.

Keylogger softver može se širiti na više načina: u e-mail privitcima, otvaranjem datoteka s otvorenih direktorija na P2P[33] mrežama, preko web preglednika (korištenjem neke njegove ranjivosti), preko drugog zlonamjernog softvera koji ima mogućnost preuzimanja s mreže.

---

[32] Zeus (2007) prikupljao korisnička imena, lozinke i bankovne podatke

[33] P2P (peer-to-peer) slobodna razmjena informacija i datoteka među sudionicima mreže. Uslijed nemogućnosti primjerenog nadzora sudionika mreže i podataka, peer-to- peer mreže su iskorištene i za širenje zlonamjernih programa (virusa, crva, trojanskih konja, spyware programa, itd.) te za razmjenu zakonski zabranjenih sadržaja.

Danas svi antivirusni alati imaju mogućnost detekcije keylogger softvera. Ali od njega se može zaštititi i na način da se kod pristupa servisima za plaćanje koriste jednokratne lozinke ili dvostruka autentifikacija. Također keyyloger softver ne bilježi unos preko virtualne tipkovnice koja se nalazi ugrađena u sam operacijski sustav Windows.[25]

Slika 4 Primjer keylogger softvera koji snima pritisnute tipke na tipkovnici, izvor: www.techtarget.com

6.3 Rootkit[34]

Rootkit je zlonamjerni softver koja napadaču omogućuje udaljenu administrativnu kontrolu nad računalom. Oni su posebno dizajnirani da budu nevidljivi na računalu kojeg zaraze. Rootkit može zaraziti računalo na više razina:

- aplikacijska razina – rootkit napada korisničke aplikacije na računalu. To su klasični trojanski konji i imaju smanjenu mogućnost skrivanja na sustavu,
- razina sistemskih biblioteka – na ovoj razini rootkit napada sistemske biblioteke mijenjajući njihov izvršni kod u radnoj memoriji računala,

[34] Rustock Rootkit (2006.) stvorio je jedan od najvećih botneta za slanje neželjene pošte. Procjene sugeriraju da je botnet sadržavao između 150 000 i 2,4 milijuna zaraženih računala.

- razina operacijskog sustava – rootkit se ubacuje duboko u jezgru operacijskog sustava. Ovo su najčešći rootkit softveri. Skoro ih je nemoguće otkriti budući da djeluju na istoj razini kao i operacijski sustav,
- razina upravitelja virtualnim strojem – zaobilazi operacijski sustav i nemoguće ga je otkriti iz njega,
- razina hardvera/ugrađenih programa – rootkit svoj izvršni kod implementira izravno u hardveru računala koristeći ugradbeni programski kod.

Najčešći rootkit softveri su oni koji djeluju na razini operacijskog sustava. Njihov razvoj je dugotrajan i tehnički zahtjevan. Kada zarazi računalo mogu proći mjeseci prije nego bude primijećen. Neki sigurnosni stručnjaci idu toliko daleko te ističu da je jedini način otklanjanja takvih rootkit softvera potpuno brisanje diska i reinstalacija cijelog sustava. Zbog toga su u borbi protiv takvih softvera učinkovite jedino mjere prevencije. Kod rootkit softvera posebno je važno pripaziti na: redovito ažuriranje cijelog operacijskog sustava, pažljivu instalaciju upravljačkih programa, potrebno je instalirati samo one upravljačke programe koji dolaze iz provjerenih izvora.[26]

6.4 Ransomware[35]

Ransomware je naziv za zlonamjerne programe koji onemogućuju korištenje računala. Kada se računalo zarazi ransomware programom, on šifrira datoteke ili onemogućuje korištenje tako da se pojavi početni ekran s određenom porukom koju nije moguće maknuti. Najčešće napada Word dokumente, te od korisnika traži otkupnina u zamjenu za daljnje normalno korištenje računala. Otkupninu se traži u uplati u obliku kripto valuta kako se ne bi mogla pratiti transakcija i otkriti počinitelj.

Ransomware koristi asimetričnu enkripciju. Ovo je kriptografija koja koristi par ključeva za šifriranje i dešifriranje datoteke. Javno - privatni par ključeva napadač jedinstveno generira za žrtvu. Privatni ključ se nalazi kod napadača, a ključ čini dostupan

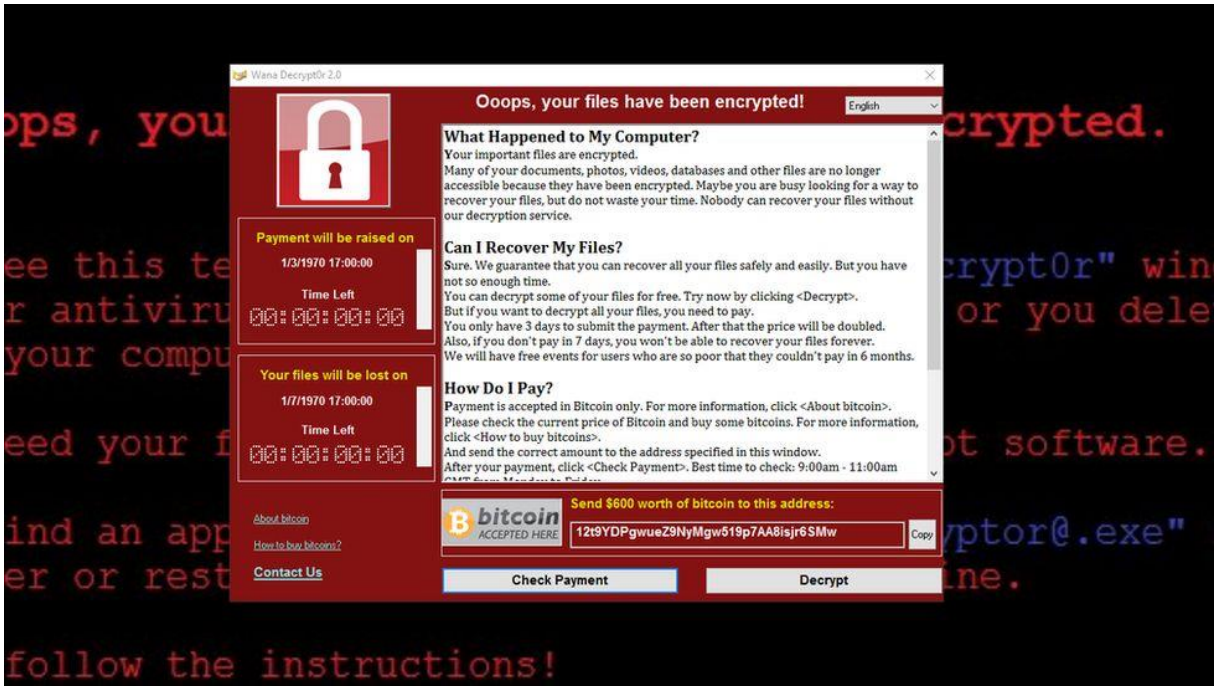
[35] WannaCry ransomware koji se može proširiti na druge uređaje na mreži napao je preko 200 000 računala u 150 zemalja

žrtvi nakon uplate otkupnine. U većini slučajeva, napadač nakon uplate otkupnine, žrtvi ne dostavlja privatni ključ, čime žrtvi čini dvostruku štetu.[27]

Najčešći način zaraze je na način da žrtva otvori privitak u elektroničkoj pošti, a koja se najčešće lažno predstavlja kao banka, internet trgovina i sl. Poveznica vodi na internet stranicu preko koje dolazi do zaraze računala. Također postoji način zaraze računala putem skočnih prozora u Internet pregledniku. Ti skočni prozori sadrže poruku kako je potrebno instalirati hitnu nadogradnju operacijskog sustava, nakon čega žrtva instalira zlonamjerni program na računalo. Kako se ransomware zlonamjerni program stalno modificira, antivirusni programi često isti ne mogu detektirati.

Koliko je ransomware opasan govori činjenica da su i u Hrvatskoj brojna poduzeća, ali i neka državna tijela bila zaražena ovim virusom (HT telekom, MORH, FINA, T- portal, KBC Zagreb, Orqa).[28]

Na više načina se može smanjiti zaraza računala ransomwareom: redovito ažuriranje operacijskog sustava, ažuriranje aplikacija instaliranih na računalu, ne otvarati poveznice u elektroničkim porukama koje su pristigle od sumnjivih pošiljatelja, instalacija antivirusnog alata i njegovo ažuriranje, preventivna instalacija nekog od anti-ransomware alata, ne otvarati razne reklamne poruke na Internet stranicama, periodičko kreiranje točke vraćanja, periodičko kreiranje sigurnosne kopije i njezina pohrana na vanjski disk ili poslužitelj.[29]



Slika 5 Prikaz poruke na računalu zaraženog ransomwareom pod imenom "WannaCry", izvor: www.bbc.com

6.5 Spyware

Spyware ili špijunski softver definiran je kao zlonamjerni softver dizajniran za instaliranje u računalo. On prikupljanje podataka o korisniku i prosljeđuje ih trećoj strani bez njegovog pristanka. Špijunski softver također se može odnositi na legitimni softver koji nadzire podatke u komercijalne svrhe poput oglašavanja. Međutim, zlonamjerni špijunski softver izričito se koristi za profitiranje od ukradenih podataka. Špijunski softver također utječe na performanse računala, računalne i internetske mreže, usporavajući njihov rad.

Zlonamjerni špijunski softver korak po korak poduzima radnje kako bi se instalirao na računalo i prikupljao podatke o korisniku, kao što su:

- infiltriranje – instalira se na korisnikovo računalo putem datoteka za instalaciju, zlonamjerne internetske stranice ili privitka elektroničke pošte
- nadzire i snima podatke - putem pritisnutih tipki na tipkovnici, snimanja zaslona i drugih kodova
- šalje ukradene podatke autoru špijunskog softvera koji će iste koristiti ili prodavati trećim stranama

Špijunski softver prikupljanje povjerljive podataka kao što su:

- lozinke i korisnička imena
- PIN-ovi bankovnih kartica
- brojevi kreditnih kartica
- bilježi pritisnute tipke na tipkovnici
- prati navike pregledavanja
- prikuplja adrese e-pošte[30]

7. OSTALE VRSTE NAPADA

7.1 Bot

Bot je skraćenica od Robot. Softverski program kojemu je namjena obavljanje određenog ponavljajućeg zadatka ili operacije. To su automatizirani procesi, koji imaju jasne pretpostavljene radnje koje trebaju izvršiti. Može obaviti jednostavne i kompleksne zadatke koji su mu definirani u samom programu. Programirani su tako da simuliraju ponašanje čovjeka, tj. imitira ponašanje stvarne osobe.

Bot može izvoditi različite radnje kao što su:

- Chatbot - automatizirani sistem za konverzaciju sa korisnicima. Ovaj bot može dati odgovore na određena pitanja, na različitim platformama. Ovisno o tome koliko je bot inteligentan, on može odgovarati na jednostavne i kompleksnije upite.
- Web crawlers - najpoznatiji je Googlebot. Ovaj bot posjećuje stranice i pregledava sadržaj koji je na njima objavljen. Vlasnicima internetskih stranica u cilju je da ih ovaj bot posjeti kako bi kasnije imali bolje rezultate pretraživanja. Postoje zli bot programi, koji pregledavaju objavljeni sadržaj, ali i onaj sadržaj koji bi trebao biti nedostupan široj publici.
- Social bot – slično kao Chatbot koji se koristi na društvenim mrežama. Upravlja nalozima društvenih mreža onih osoba koje imaju više otvorenih računa (profila)
- Malicious bot – zlonamjerni bot otkriva sadržaj koji nije za javnost. Šire sadržaj različitim metodama i pokušavaju zaobići različite sustave zaštite. da bi se domogli podataka.

Zlonamjerno korištenje bota je prikupljanje aktivnosti na Internet stranicama kojom se narušavaju Pravila o korištenju iste. Takve bot radnje su potencijalno opasne za vlasnike web sadržaja i njegove korisnike. Osim ciljanih napada uz pomoć bot aplikacija, vlasnici internetskih stranica ili druge internet infrastrukture (serveri, web aplikacija, i dr.) mogu osjetiti poteškoće u radu. Ako se prema nekom određenom serveru usmjeri veliki broj bot posjeta, može se opteretiti resurse koji dovode prestanka rada određenih servisa.

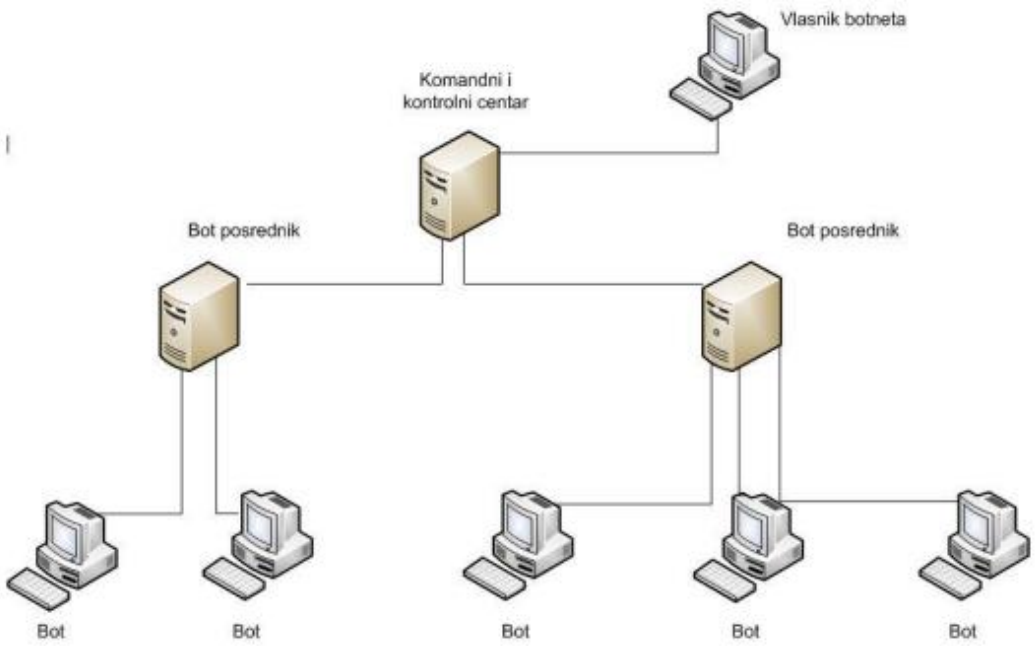
Napadi mogu biti ciljani i nasumični. Ciljani bot napadi definirani su kao DoS, ili DDoS napadi.[31]

7.2 Botnet

Botnet je skup računala koja su zaražena zlonamjernim programom koji omogućava osobi koja ga je stvorila određenu kontrolu nad zaraženim računalima. Korisnik tom prilikom nije svjestan da mu je računalo zaraženo i da sudjeluje u raznim zlonamjernim aktivnostima. Zaraženo računalno postaje zombi ili bot koji čeka instrukcije od glavnog računala (engl. Bot master). U počecima razvoje botneta njihova svrha bila je širenje spam poruka, dok su danas usmjereni na krađu osobnih podataka, bankovnih računa, provođenje napada i dr. Botneti zauzimaju veliki dio u cjelokupnom računalnom kriminalu i predstavljaju infrastrukturu pomoću koje se čini šteta korisnicima Interneta Europska unija pokrenula je projekt Advanced Cyber Defence Cetar čiji je zadatak izgraditi platformu za detekciju i uklanjanje botneta. Stvaratelji botnet mreža s vremenom smišljaju nove načine kojima poboljšavaju širenje svojih mreža, njihovo prikrivanje i onemogućuju njihovu detekciju.

Postoje dvije glavne vrste botneta: centralizirani i decentralizirani (P2P).

- Centralizirani botneti su vrsta botneta u kojoj su svi botovi povezani s jednim slojem komandnih i kontrolnih centara (engl. Command and control centar - C&C). Komandni i kontrolni centar stalno osluškuje i čeka na nova zaražena računala. Kad se ostvari komunikacija s novim botom on ga registrira u svojoj bazi, prati njegov status i šalje naredbe koje treba izvršiti. Upravitelj botneta komunicira s komandnim i kontrolnim centrom i na taj način upravlja cijelom mrežom.[32]



Slika 6 Prikaz centraliziranog botneta, izvor: www.cert.hr

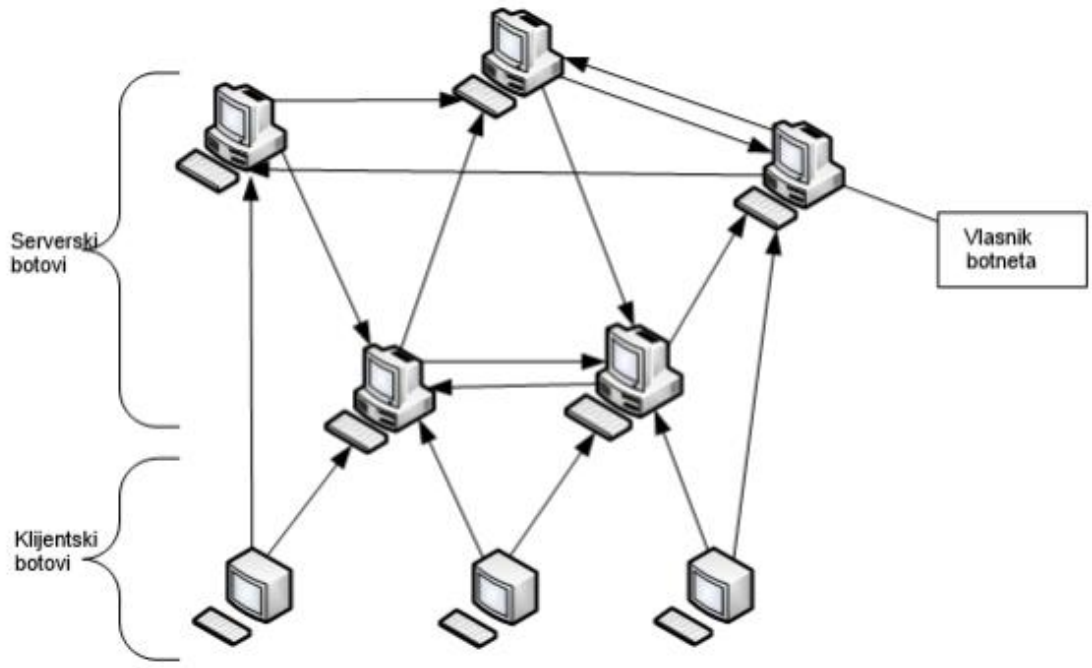
Način na koji botovi komuniciraju sa komandnim i kontrolnim centrom je najčešće preko HTTP[36] ili IRC[37] protokola što često omogućava prolaz paketa kroz sigurnosne uređaje (vatrozid, IPS i sl.). IRC (engl. Internet Relay Chat) protokol je dizajniran za tip komunikacije „jedan na više“ te se time ne ograničava broj korisnika unutar jednog komunikacijskog kanala. IRC pruža mogućnost direktne komunikacije i slanja naredbi samo određenim botovima. Drugi način komunikacije u botnet mreži je putem HTTP protokola. Zbog svoje prisutnosti na Internetu rijetko kad je blokiran i filtriran.

Decentralizirani (P2P) botneti se temelje na ideji da su svi botovi jednako važni kako bi se uklonila potreba za centralnim poslužiteljem. Računala koja se nalaze iza vatrozida ili posredničkih poslužitelja ne mogu prihvatiti dolazne konekcije, ali zato mogu

[36] HTTP (HyperText Transfer Protocol) je protokol na Internetu putem kojeg se prenose HTML dokumenti. Protokol, kao i svaki drugi protokol na Internetu, zahtijeva dva programa koja će se znati sporazumjeti. HTTP klijent program na jednoj strani i HTTP poslužitelj na drugoj strani. HTTP je najvažniji protokol na Internetu.

[37] Internet Relay Chat (IRC) je protokol za online komunikaciju koji omogućava realno vrijeme razgovora preko interneta.

inicirati komunikaciju. Nedostatak dolaznih konekcija od strane poslužitelja predstavlja problem u P2P infrastrukturi jer sprječava većinu botova da budu povezani s ostalim botovima. U centraliziranim botnetima nema ovog problema jer se botovi povezuju s poslužiteljem. Botovi koji su sposobni primati dolazne konekcije (ne nalaze se iza posredničkih poslužitelja, NAT-a ili vatrozida) se ponašaju kao poslužitelji i nazivaju se peerovi ili čvorovi.



Slika 7 Prikaz decentraliziranog (P2P) botneta, izvor www.cert.hr

Simptomi koji ukazuju da je računalo postalo dio botneta su:

- operacijski sustav je sporiji nego inače
- tvrdi disk radi stalno iako ne koristimo računalo
- dolazi do nestajanja ili promjene strukture datoteka
- kolege i prijatelji vam javljaju da su dobili mail koji niste poslali
- vatrozid vas obavještava da se neki program pokušava spojiti na Internet
- antivirusni ili drugi sigurnosni alat vas upozorava na sumnjive pojave[32]

7.3 CEO fraud i BEC (Bussiness Email Compromise)

CEO fraud je oblik poslovne prijevare gdje napadač lažira polje pošiljatelja kako bi izgledalo da je e-pošta poslana s legitimne adrese. Napadači se najčešće predstavljaju kao osoba na rukovodećoj poziciji (direktor, ravnatelj, dekan i dr.), te obično traže hitan prijenos određene svote novca na strani bankovni račun.

Business Email Compromise“ je oblik poslovne prijevare gdje napadač kompromitira korisnički račun nakon čega ulazi u komunikaciju između dva djelatnika (npr. nabava-dobavljač). Predstavlja se kao dobavljač, partner ili kupac i traži hitno plaćanje računa, uz izmjenu podataka u svoju korist na izvornom računu. Napadači se često znaju ubaciti u komunikaciju te nastaviti legitimnu korespondenciju sve do trenutka plaćanja računa, nakon čega šalju izmijenjene podatke o plaćanju.[33]

7.4 Dictionary napad

Napad brutalne sile u kojem napadači pokušavaju pogoditi korisničku lozinku za određeni mrežni račun prolaskom kroz popisu uobičajenih lozinki. Koriste se riječi, fraze i kombinacije brojeva. Kada je napad uspješan, napadač to iskorištava za pristup društvenim mrežama, bankovnim računima i ostalim datotekama.[34]

#	**Lozinka**
1	admin
2	123321
3	123456
4	decenija
5	12345678
6	tkalcevic1
7	Mucikapucika666
8	Grguras2
9	Dinamo.1967
10	kikokiko
11	grguras1
12	faithless23
13	deveroga
14	123456789
15	Mushyhush68
16	Istina12

17	000000
18	Mac123123
19	Vrgorac1
20	okaram4spomin

Tablica 1 Popis najčešćih lozinki hrvatskih korisnika u 2023. godini, izvor: www.bug.hr[35]

7.5 DoS (Denial of Service)

DoS (engl. Denial of Service) je kibernetički napad na računalni sustav (npr. web poslužitelj), a ima cilj uskraćivanja usluga (engl. denial of service). Time je npr. internetska stranica nedostupna. Napadač može pokrenuti DoS napad koristeći jedno računalo. Za razliku od DoS napada, DDoS (engl. Distributed Denial of Service) napad se pokreće sa više računala. Ta računala su fizički rasprostranjena diljem svijeta. Računala nisu u vlasništvu napadača, već drugih korisnika koji nisu svjesni da njihova računala sudjeluju u napadu. Tu skupinu računala nazivamo botnet. Botnet je skupina zaraženih računala koje nazivamo botovi. Njima napadač upravlja na daljinu Nakon što je računalo zaraženo, ono se spoji na komandni i kontrolni centar kako bi primalo nove naredbe od napadača. Malware koji je zarazio računalo, nastavlja se širiti na druga računala putem elektroničkih poruka ili koristeći ranjivost uređaja ili operacijskog sustava kojega želi zaraziti kako bi botnet stalno rastao. Komandni i kontrolni centar tada ima sve više računala pod kontrolom.

Zaštita od DDoS napada nije jednostavan jer je teško razlikovati legitimni promet od prometa uzrokovanog napadom. Trajanje napada ovisi o tome koliko je meta napada uložila u zaštitu od napada i koliko su napadači motivirani na napad. DDoS napad na računalne sustave može napraviti veliki financijsku štetu i naštetiti reputaciji kompanije, a time smanjiti i povjerenje korisnika.[36]

7.6 Hoax

Hoax je poruka elektroničke pošte koja sadrži neistiniti sadržaj. Ima cilj zastrašivanja ili dezinformiranja primatelja. Osoba koja je poslala poruku želi da se ta poruka proslijedi na što veći broj adresa elektroničke pošte. Pri tome ih primatelji

prosljeđuju internetom jer su uvjereni da time pomažu drugima. Hoaxi ne mogu uzrokovati oštećenja operacijskog sustava ili programa. Scam je ozbiljniji oblik hoaxa, često s ozbiljnim financijskim, pravnim ili drugim posljedicama za žrtvu.

Najčešće vrste hoaxa su:

- Hoaxi kao upozorenja o štetnim programima –sadrže lažna upozorenja na nove viruse i crve, trojanske konje ili druge oblike zlonamjernog koda.
- lanci sreće i zarade – primatelju se za prosljeđivanje hoaxa na određen broj adresa obećava novac ili neka druga nagrada. Lanci sreće mogu imati i prijeteći karakter. U tim slučajevima primatelja se upozorava da će ga zadesiti nesretan i neugodan događaj ukoliko primljenu poruku ne proslijedi na što veći broj adresa.
- lažni zahtjevi za pomoć – poruke kojima se izaziva suosjećanje prema nemoćnim osobama i djeci i poziva se na pomoć daljnjim prosljeđivanjem poruka. Primatelji ovakvih hoaxa rijetko odbijaju pomoći, te je zbog toga ova vrsta hoaxa veoma raširena.
- zastrašujući i prijeteći hoaxi – poruke koje upozoravaju na potencijalne opasnosti i pokušavaju zastrašiti primatelja. Moguće je da hoax sadrži i izravnu prijetnju primatelju kojem bi se trebalo nešto “strašno” dogoditi ako ne proslijedi primljeni e-mail na što više adresa.
- lažne peticije – poruke raznih sadržaja koje pozivaju na sakupljanje potpisa za nešto važno. Peticije mogu imati izmišljenu ili istinitu temu. Činjenica da je tema na koju se peticija odnosi istinita ne znači da je i sama peticija istinita. Često autori izmišljaju lažne peticije s istinitim temama kako bi uzrokovali pomutnju i potakli beskorisno trošenje tuđih vremenskih i računalnih resursa.
- kompromitirajući hoaxi – narušavaju ugled određenih organizacija ili osoba. Poruka sadrži lažne ili iskrivljene navode o određenim organizacijama, tvrtkama ili osobama i glavni im je cilj narušavanje nečijeg ugleda.[37]

7.7 Phishing

Phishing, riječ koja je nastala od engleske riječi za pecanje, fishing. Phising se odnosi na prijevare u kojima napadač lažnim predstavljanjem pokušava potencijalnu žrtvu natjerati da nešto učini u njegovu korist. Napadači koriste razne načine manipulacije kako bi od žrtve prikupili povjerljive podatke kao što su korisnička imena, lozinke, podatke sa bankovnih kartica, a sve u svrhu ostvarivanja imovinske koristi. Phishing poruke prenose se putem elektroničke pošte, a u poruci se nalazi poveznica koja vodi na lažne stranice banaka, servisa za elektroničko plaćanje i sl., a koja svojim izgledom podsjeća na originalnu internetsku stranicu. Napadači se osim elektroničke pošte koriste i drugim servisima poput foruma, društvenih mreža, servisa za izravnu komunikaciju. Društvene mreže su opasne jer sadrže podatke koji mogu poslužiti za krađu identiteta, ali i zbog činjenice da poruke dobivene od prijatelja mogu biti sa njihovih kompromitirani računa.

Najčešće metode phisinga su:

- jednostavni zahtjev - prema žrtvi napadač šalje elektroničku poruku da u odgovoru pošalje svoje osjetljive podatke elektroničkom poštom, kako bi se npr. provjerila nadogradnja sustava
- zlonamjerne poveznice - vode žrtvu na zlonamjernu internetsku stranicu
- zlonamjerna internetska stranica - može izgledati kao originalna stranica (npr. banke ili internetske trgovine), a služi za prikupljanje osobnih podataka, ostvarivanje financijske koristi ili neku drugu zlonamjernu radnju
- zlonamjerni skočni (engl. popup) prozor - prozora s poljima za unos povjerljivih podataka
- „tabnabbing“ – nova metoda koja koristi mogućnost internet preglednika. Preglednici obično imaju otvoreno nekoliko kartica istovremeno. Jedna se od neaktivnih kartica osvježi, ali sa zloćudnim sadržajem koji imitira legitimnu internetsku stranicu.

Phising se može izbjeći na način da se ne odgovara na elektroničke poruke koje dolaze od sumnjivih pošiljatelja, a u istima se traže osobni podatci, brojevi bankovnih kartica, korisnička imena, lozinke, te sumnjive poveznice na internetske stranice.[38]

7.8 Scam

Termin scam koristi se za opisivanje prijevare ili planova za izmamljivanje novca ili drugih vrijednosti od osoba koje ne sumnjaju da je riječ o prijevari. Scam je način za brzim ostvarivanjem zarade. Funkcionira na način da neka osoba ili grupa ljudi vara druge osobe ili grupe ljudi tako da im pruža lažne podatke prilikom davanja ponude ili nuđenja dogovora. Na meti su sve osobe, bez obzira na profesiju, godište, obrazovanje i prihode.

U Hrvatskoj bilježi se sve veći broj scam poruka kojima napadač pokušava zastrašiti potencijalnu žrtvu. U porukama se navodi žrtva odgovori na sudski poziv ili tužbu, nakon čega slijedi iznuda.[39]

POZIV NA SUD
Za potrebe pravne istrage
(2.3 Članak 191. Članak 153. Kaznenog zakona)

Moje ime je g. Nikola MILINA.
Glavni ravnatelj Hrvatske policije u suradnji s Europskim policijskim uredom (EUROPOL) za borbu protiv kriminaliteta informacijske i komunikacijske tehnologije, koji centralizira online izvješća.

Kontaktiramo vas nakon cyber-infiltracije, predmet ste nekoliko kaznenih progona zbog posjedovanja slike dječje pornografije - Cyber širenje - Dječja delinkvencija. Vaša IP adresa diskretno je istražena na internetu od strane Odjela za usklađenost s cenzurom Ministarstva unutarnjih poslova.

Imamo nekoliko stavki koje su zabilježene i dokaz su vaših kršenja. Od vas se traži da se oglasite putem e-pošte tako što ćete nam napisati svoja obrazloženja kako bismo ih stavili na ispitivanje i provjeru za procjenu sankcija.

Ovo unutar strogog roka od 72 sata. Nakon tog roka bit ćemo dužni svoje izvješće uputiti glavnom državnom odvjetniku g. Draženu Jeleniću radi pripreme tjeralice protiv Vas. Vaš će dosje također biti proslijeđen javnim medijima kako bi se spriječio vaš povratak i odvratili potencijalni kandidati od ove prakse. Na kraju navedenog postupka bit ćete registrirani kao seksualni prijestupnik.

Sada ste obaviješteni.

Srdačno,

M. Nikola MILINA
Glavni ravnatelj Hrvatske policije
Sjedalo : Zagreb

Approved

Slika 8 Primjer scam poruke, izvor www.cert.hr

7.9 Sniffing

Njuškanje (eng. sniffing) je presretanje i praćenje prometa na mreži. To se može učiniti pomoću softvera koji bilježi sve pakete podataka koji prolaze kroz određeno mrežno sučelje ili pomoću hardverskih uređaja izričito dizajniranih za tu svrhu.

Sniffing napad događa se kada napadač koristi sniffing program za presretanje i čitanje osjetljivih podataka koji prolaze kroz mrežu. Uobičajene mete za ove napade uključuju nešifrirane poruke e-pošte, vjerodajnice za prijavu i financijske informacije. U nekim slučajevima napadači također mogu koristiti alate za sniffing napade kako bi u pakete podataka ubacili zlonamjerni kod kako bi preuzeli ovlasti nad određenim računalom.

Postoje dvije vrste sniffing napada:

Pasivni sniffing napad

U pasivnom napadu, napadač prati promet koji prolazi kroz mrežu bez ometanja na bilo koji način. Ova vrsta napada može biti korisna za prikupljanje informacija o ciljevima na mreži i vrstama podataka (npr. vjerodajnice za prijavu, poruke e-pošte) koje prenose. Budući da ne uključuje nikakvo ometanje ciljnih sustava, također je manje vjerojatno da će izazvati sumnju od drugih vrsta napada.

Aktivni sniffing napad

U aktivnom napadu napadač šalje pakete podataka jednom ili na više računala na mreži. Na taj način dolazi do osjetljivih podataka. Korištenjem posebno izrađenih paketa napadači često mogu zaobići sigurnosne mjere koje bi inače zaštitile podatke od presretanja. Aktivno njuškanje također može uključivati ubacivanje zlonamjernog koda u računala koji napadačima omogućuje da preuzmu kontrolu nad njima ili ukradu osjetljive podatke.[40]

8. OBRANA OD KIBERNETIČKIH NAPADA

8.1 Penetracijsko testiranje

Penetracijsko testiranje (engl. pentest) je tehnika kojom se procjenjuje sigurnost računalnog sustava ili računalne mreže, najčešće neke tvrtke, koja se temelji na oponašanju stvarnog kibernetičkog napada. Prilikom testiranja etični haker izvodi različite vrste napada na metu, a te tehnike su jednake tehnikama stvarnih napada. Cilj mu je uočiti bilo kakvu ranjivost kojom može pristupiti sustavu, podacima za koju nema dozvolu, onemogućiti rad ostalim korisnicima, kao i preuzeti kontrolu nad ranjivim sustavom. Znanje, vještina i iskustvo etičkog hakera ovise o kvaliteti penetracijskog testiranja.

Sustav se smatra ako je zadovoljio kriterije koji jamče tajnost, dostupnost i integritet podataka. Tajnost podataka je stavka definirana korištenjem i pristupom informacija ovlaštenim korisnicima. Dostupnost osigurava kontrolu i mogućnost korištenja podataka, dok integritet podataka jamči konzistentnost procesa i valjanost podataka.

Penetracijski testovi ne moraju uvijek obuhvaćati cijelu mrežu. Mogu se usredotočiti na određene aplikacije, usluge i metodologije. Najčešće sa ta metoda koristi u velikim tvrtkama, te istima na taj način pomaže da pronađu način za implementaciju i nadogradnju sustava i da ne budu preopterećeni prilikom poslovanja.

U penetracijskom testiranju mogu se testirati: web-aplikacije, bežične mreže, fizička infrastruktura, socijalni inženjering.[41]

8.1.1 Testiranje web-aplikacije

Organizacije koriste testiranje penetracije web aplikacija kako bi spriječile napadače da iskoriste ranjivosti na aplikacijama okrenutim klijentu. Ovi testovi mogu varirati u složenosti zbog ogromne količine različitih preglednika, dodataka i proširenja koji svi dolaze u obzir prilikom pokretanja penetracijskog testa web aplikaciji. Ranjive web-aplikacije mogu ispustiti osjetljive podatke koji napadačima pomažu tijekom faze prikupljanja informacija o napadu ili dobiti pozadinski pristup određenoj aplikaciji.[42]

8.1.2 Testiranje bežične mreže

Rasprostranjenost bežične mreže (Wi-Fi-ja) čini ga atraktivnom metom i za znatiželjne prolaznike i za predane napadače. Penetracijski testeri mogu koristiti mnoge specijalizirane alate koji testiraju pouzdanost i sigurnost različitih bežičnih tehnologija. Sniffing alati i napadi deautentifikacije mogu se koristiti za preuzimanje kontrole nad bežićnom mrežom i preuzimanja podataka u mreži. Bežično penetracijsko testiranje također provjerava sigurnosne postavke na gostujućoj Wi-Fi mreži. Ako pravila pristupa nisu ispravno konfigurirana, a mreža za goste nije na vlastitom VLAN-u, napadač može potencijalno dobiti pristup privatnoj mreži putem bežične veze za goste.[42]

8.1.3 Testiranje fizičke infrastrukture

Nijedan sigurnosni softver ne može spriječiti nekoga da fizički uzme računalo poslužitelja. Napadači koriste socijalni inženjering kako bi se maskirali u tehničare, domare ili goste kako bi dobili fizički pristup osjetljivim područjima. U testu fizičke penetracije, vrata, brave i druge fizičke kontrole testiraju se kako bi se vidjelo koliko ih je lako zaobići.[42]

8.1.4 Socijalni inženjering

Napadači koriste socijalni inženjering kako bi prevarili zaposlenike tvrtke da im daju povlaštene informacije ili pristup organizaciji. Taj pristup može biti u obliku phishing, e-pošte, telefonskog poziva ili nekoga tko se fizički pretvara da je netko tko nije. Krajnja obrana od socijalnog inženjeringa je stručno i obučeno osoblje. Također se kontrolom ulaska za posjetitelje unutar tvrtke može spriječiti neovlašteni fizički pristup. Testovi socijalnog inženjeringa često se odvijaju putem e-pošte ili putem telefona. Softverske platforme mogu se koristiti za slanje lažnih poruka e-pošte i za krađu identiteta. Oni koji kliknu na poveznice u e-porukama ili odgovore na njih moraju proći obuku i informacijskoj sigurnosti.[42]

8.2 Faze procesa penetracijskog testiranja

Proces penetracijskog testiranja dijeli se u više faza

Slika 9 Faze procesa penetracijskog napada, izvor I. Zakarija et al: Primjena odabranog pristupa penetracijskom testiranju računalnih sustava[]

1. Faza planiranja

U fazi planiranja (engl. planning phase) odlučuje se metoda i opseg penetracijskog testiranja. Izvršitelj testiranja priprema strategiju napada, a naručitelj napada osigurava se od mogućih negativnih djelovanja testiranja. [43]

2. Faza izviđanja

U fazi izviđanja, koja je i najopsežnija, prikupljaju se informacije kao što su mrežni nazivi, domene, razni poslužitelji. Prikupljenim informacijama lakše se dolazi do potencijalnih ranjivosti.[43]

3. Faza napada

Faza napada je jezgra svakog penetracijskog testiranja. To je faza koja ne mora odmah biti uspješna. Ukoliko prvi pokušaj penetracije nije uspio, etički haker[38] odabire novi način napada.[44]

Faza napada sadrži dvije faze:

- dobivanje pristupa - koristi se napad na web aplikacije, ulaz na stražnja vrata, ubacivanje koda i dr. kako bi se otkrile ranjivosti sustava. Etični haker koristi tu ranjivosti kako bi ukrao podatke, presreo podatke i preuzeo kontrolu nad sustavom.[44]

- održavanje pristupa - cilj ove faze je vidjeti može li se ranjivost koristiti za postizanje trajne prisutnosti u sustavu. Ideja je oponašati napredne uporne prijetnje, koje često ostaju u sustavu mjesecima kako bi se ukrali najosjetljiviji podaci.[44]

4. Analiza

Nakon penetracijskog testiranja sastavlja se izvješće s rezultatima: specifične ranjivosti koje su iskorištene, osjetljivi podaci kojima je pristupljeno, vrijeme tijekom kojeg je etički haker mogao ostati u sustavu neotkriven. Sve te informacije se analiziraju od sigurnosnih stručnjaka kako bi se mogla postaviti odgovarajuća zaštita sustava od budućih napada.[43]

8.3 Standardi penetracijskog testiranja

8.3.1 Open Source Security Testing Methodology Manual (OSSTMM)

Open Source Security Testing Methodology Manual (OSSTMM) je priručnik koji u detalje opisuje proces penetracijskog testiranja. Cilj priručnika je definiranje stroge metodologije penetracijskog testiranja, pri čemu se moraju zadovoljiti tri uvjeta: konzistencija, ponovljivost i pouzdanost rezultata.

[38] Etički haker je stručnjak koji je fokusiran na napad na računalne sustave i dobivanje pristupa mrežama, aplikacijama, bazama podataka i drugim kritičnim podacima na zaštićenim sustavima. Za razliku od zlonamjernih hakera, etički hakeri rade uz dopuštenje vlasnika sustava i poduzimaju sve mjere opreza kako bi osigurali da rezultati ostanu povjerljivi

Open Source Security Testing Methodology Manual sadrži upute pomoću kojih se provodi iscrpno penetracijsko testiranje. Pokriva sva potrebna područja pritom pazeći na pridržavanje zakonskih odredbi. Priručnik sadrži šest dijelova: informacijska sigurnost, sigurnost procesa, sigurnost Internet tehnologija, sigurnost komunikacija, sigurnost bežičnih tehnologija i fizička sigurnost.

OSSTMM popisuje tehničke pojedinosti o tome što treba testirati i na koji način to treba učiniti, prije za vrijeme i nakon penetracijskog testiranja. Kako penetracijsko testiranje bilo usklađeno s OSSTMM standardom, testiranje mora pokriti sve module određenog poglavlja. Ukoliko ne postoji infrastruktura neophodna za izvođenje određenog penetracijskog testiranja, u konačnom izvješću se ta skupina označava oznakom: NOT APPLICABLE.[39][41]

8.3.2 National Institute of Standards and Technology (NIST) standard

Nacionalni institut znanosti i tehnologije Sjedinjenih Američkih Država (eng. National Institute of Science and Technology - NIST) napravio je dokument s nazivom Special Publication 800-42, Guideline on Network Security Testing. Taj dokument propisuje elemente penetracijskog testiranja sigurnosti u državnim organizacijama SAD-a. Dokumentom se identificiraju preduvjeti koji se moraju ispuniti za početak testiranja i preporuke prioriteta kojima se testiranje provodi. Dokument je usredotočen na aspekt mrežne sigurnosti, te se najviše posvećuje pažnja sustavima: vatrozidima (unutarnjim i vanjskim), usmjerivačima i preklopnicima, sustavima za zaštitu mrežnog okruženja sustavima, web, e-mail i ostalim aplikacijskim poslužiteljima, te ostalim poslužiteljima (DNS – Domain Name System , SMB – Server Message Block, NFS - Network File System, FTP - File Transfer Protocol i sl.)[41]

[39] NOT APPLICABLE ili skraćeno n/a u računalstvu se koristi kao oznaka za nedostatak vrijednosti ili nepoznatu vrijednost

8.3.3 Information Systems Security Assessment Framework (ISSAF)

Information Systems Security Assessment Framework (ISSAF) je strukturirani radni okvir koji sigurnost računalnog sustava organizira u različite domene. Opisuje specifične testove koji se provode. Uključuje opsežan skup sigurnosnih procedura, ali se smatra standardom u razvoju, te se nije preporučljivo pouzdati u njegove rezultate provođenja.[41]

8.4 Alati za provođenje penetracijskog testiranja

8.4.1 CoreImpact

CoreImpact je alat proizvođača Core Security Technologies[40]. Ima namjenu automatskog provođenja penetracijskog testiranja. Oponaša stvarni napad na mrežne poslužitelje, radne stanice, web aplikacije i krajnje sustave. Omogućava pronalazak ranjivosti i njezino ispravljanje prije nego se dogodi stvarni napad.

Njegove značajke su: provjera iskoristivih operacijskih sustava i servisa, mjerenje reakcije krajnjih korisnika na tzv. phishing i spear phishing napade, neželjene poruke i druge prijetnje elektroničke pošte i sl., testiranje sigurnosti web aplikacija i demonstraciju posljedica web-utemeljenih napada, razlikovanje pravih prijetnji od lažnih, konfiguriranje i testiranje učinkovitosti IDS (eng. Intrusion Detection System), IPS (eng. Intrusion Prevention System) sustava, vatrozida i sličnih infrastruktura, potvrdu sigurnosti nadogradnje, izmjena i zakrpa sustava te uspostavljanje i održavanje postupaka testiranja ranjivosti.

Alat također omogućava i analizu stanja sigurnosti u odnosu na tri najpoznatije metode napada:

---

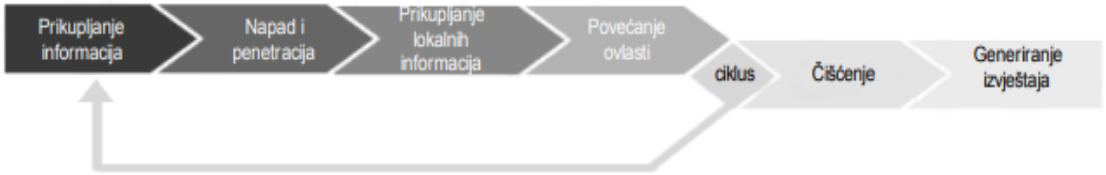
[40] Core Security Technologies američki je pružatelj rješenja za prevenciju kibernetičkih prijetnji i upravljanje identitetom koja tvrtkama pomažu proaktivno spriječiti, otkriti, testirati i pratiti rizike u svom poslovanju.

- probijanje mrežnih sustava obrane, uz pomoć napada osmišljenih za iskorištavanje ranjivosti u operacijskim sustavima i servisima instaliranim na poslužiteljima, kao i ranjivosti klijentskih aplikacija pokrenutih na stolnim računalima,
- prijevare od strane zaposlenika, dobavljača i drugih krajnjih korisnika, uz pomoć napada socijalnim inženjeringom temeljenim na porukama elektroničke pošte
- manipulaciju web aplikacija, radi pristupa podacima putem tzv. SQL injection napada ili napada uključivanjem udaljenih datoteka.

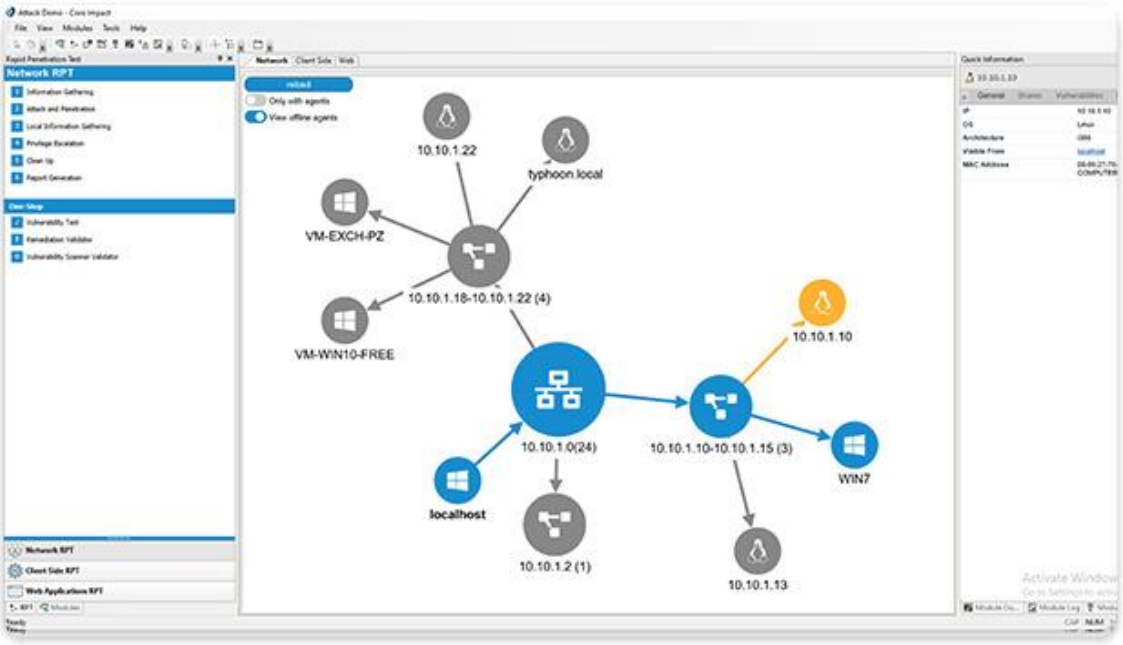
Najpoznatiji test CoreImpact alata je brzi penetracijski test (eng. Rapid Penetration Test) te se iz testa mogu dobiti informacije o:

- operacijskom sustavu i kritičnim servisima
- aplikacijama krajnjih točaka (web preglednici, čitače elektroničke pošte, komunikaciju u stvarnom vremenu (eng. instant messaging) i sl.
- sigurnosnim rješenjima krajnjih točaka (antivirusni alati, anti-phishing, anti-malware alati i sl.)
- informiranost krajnjih korisnika o napadima socijalnim inženjeringom, neželjenim porukama elektroničke pošte i dr.
- korištene web aplikacije, kao što su Internet bankarstvo
- prisutni IDS (eng. Intrusion Detection System) i IPS (eng. Intrusion Prevention System) sustavi, vatrozidi i drugi sigurnosni alati
- rezultate pretraživača ranjivosti
- sigurnosne politike

Rapid Penetration Test ima šest koraka: prikupljanje informacija, napad i penetracija, prikupljanje lokalnih informacija, povećanje ovlasti, čišćenje i generiranje izvještaja.[41]



Slika 10 Grafički prikaz RPT testa, izvor: www.cert.hr



Slika 11 Prikaz izgleda programa CoreImpact, izvor: www.coresecurity.com

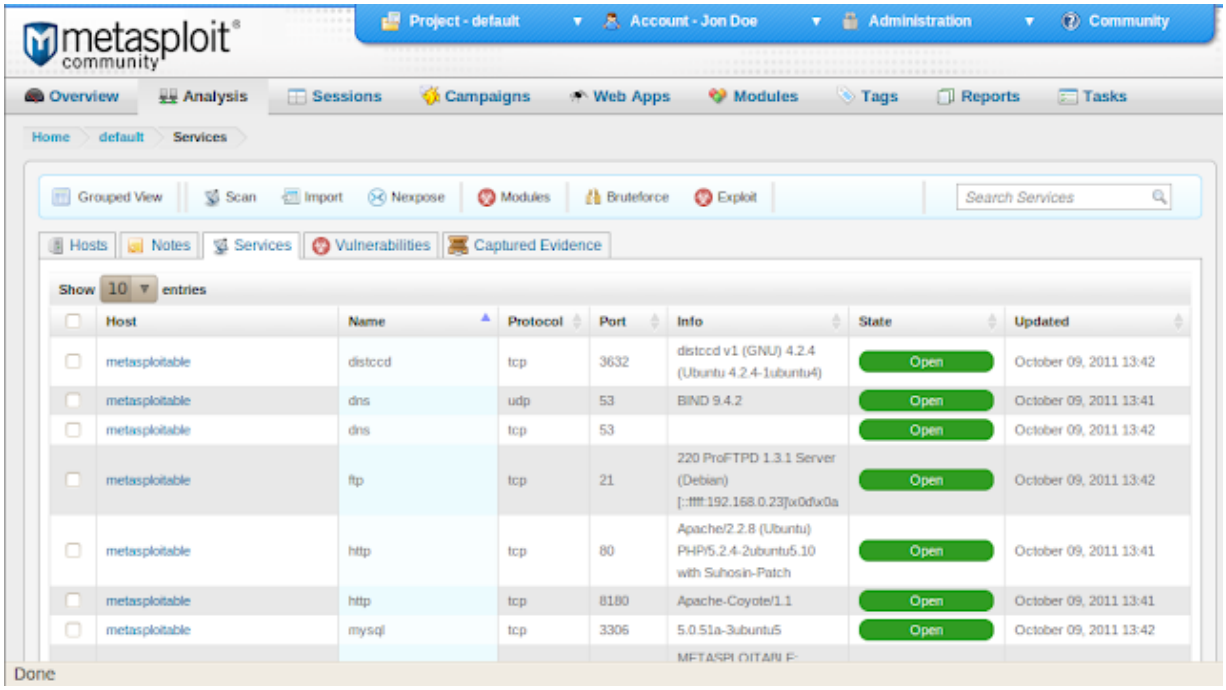
8.4.2 Metasploit

Metasploit je projekt otvorenog koda, a ima namjenu analize računalne sigurnosti. Osigurava informacije o sigurnosnim propustima i pomaže u izvođenju penetracijskog testiranja. Metasploit alat se može koristiti u zakonite i nezakonite svrhe. Alat koriste sigurnosni stručnjaci za izvođenje penetracijskog napada, administratori za provjeru instalacije zakrpi, proizvođači za testiranje ranjivosti. Metasploit alat sadrži biblioteke, module i korisnička sučelja pomoću kojih se konfigurira penetracijsko testiranje.[45]

Koraci iskorištavanja ranjivosti sustava korištenjem Metasploita su:

- odabir i konfiguracija kôda (eng. exploit) kojim se prodire u ciljni sustav uz iskorištavanje neke od poznatih ranjivosti
- provjera osjetljivosti ciljnog sustava na korištenu ranjivost

- Odabir i konfiguracija koda, čije će izvršavanje biti pokrenuto na ciljnom sustavu u slučaju uspješne zloporabe propusta
- odabir tehnike za kodiranje, tako da ga sustav za detekciju upada (IDS) ne uoči
- pokretanje izvođenja exploit koda[41]

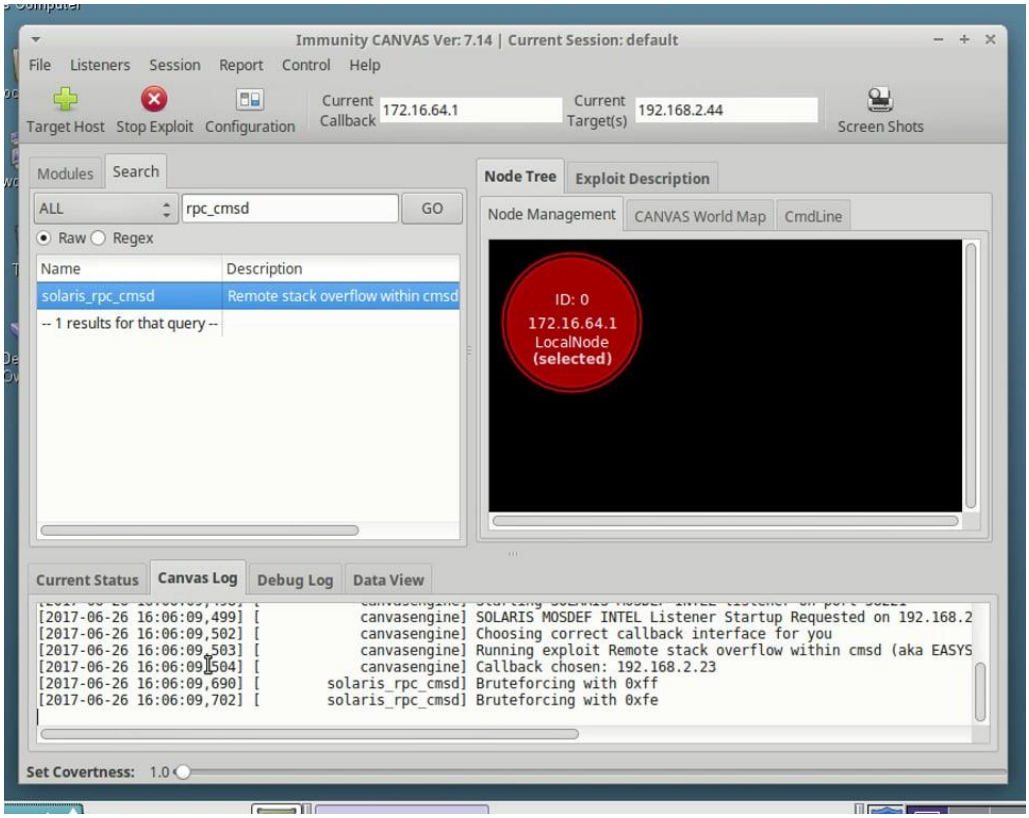


Slika 12 Prikaz izgleda programa Metasploit, izvor: www.thehackernews.com

8.4.3 Canvas

Canvas je komercijalni alat tvrtke Immunity[41], a koji se koristi za pomoć timovima koji provode penetracijsko testiranje. Sadrži bazu exploit kodova koja se redovito nadograđuje. Podržan je na platformama: Windows, Linux, Mac OS X i Python okruženjima (npr. mobiteli i Unix sustavi). Najveći prioritet alata je iskorištavanje ranjivosti velikog sigurnosnog rizika.[41]

[41] Imunity je američki proizvođač alata s kojima se provodi penetracijsko testiranje



Slika 13 Prikaz izgleda programa Canvas, izvor: www.immunityinc.com

8.5 Prednosti i nedostaci automatskog provođenja penetracijskog testiranja

Nekada se penetracijsko testiranje provodilo ručno. Provodili su ga ispitivači koji su imali veliko iskustvo, a koristili su vlastite kodove za zlouporabu. Ručno penetracijsko testiranje zahtijeva velike timove profesionalnih ljudi sa različitim vještinama, a što si organizacije koje provode testiranja ne mogu priuštiti.

Automatsko penetracijsko testiranje koristi alate koji su razvili timovi sigurnosnih stručnjaka. Alate mogu koristiti osobe koje imaju niži stupanj tehničkog znanja.

U tablici su prikazane prednosti i nedostaci automatskog i ručnog provođenja penetracijskog testiranja.[41]

	Ručno penetracijsko testiranje	Automatsko penetracijsko testiranje
PROCES TESTIRANJA	Radno-intenzivno, nedosljedno i sklono pogreškama, s nespecificiranim standardima kvalitete. Zahtijeva mnogo bitno različitih alata. Rezultati mogu značajno varirati od testa do testa. Općenito zahtjeva stručno sigurnosno osoblje za pokretanje testa i interpretaciju rezultata.	Brzo, jednostavno i sigurno. Eliminira pogreške zamornih ručnih zadataka. Centralizirano i standardizirano s ciljem dobivanja konzistentnih i ponovljivih rezultata. Jednostavno za korištenje i osigurava čiste izvještaje na temelju kojih se može reagirati.
MODIFIKACIJE MREŽE	Često se dogode mnoge izmjene na sustavu.	Sustavi se ne mijenjaju.
ISKORIŠTAVANJE, RAZVOJ I UPRAVLJANJE	Razvoj i održavanje baze zloporaba je vremenski skupo i zahtjeva značajnu stručnost. Javne zloporabe su sumnjive i nesigurne za pokretanje. Ponovno pisanje i unošenje koda je neophodno za višeplatformnu funkcionalnost.	Proizvođač proizvoda razvija i održava sve kodove te ih kontinuirano nadograđuje za postizanje maksimalne učinkovitosti. Kodove pišu profesionalci, temeljito ih testiraju i čine ih sigurnima za pokretanje. Pisani su i optimizirani za različite platforme i vektore napada.
ČIŠĆENJE	Ispitivač mora zapamtiti i poništiti sve izmjene. Nakon napada, mogu ostati otvorena stražnja vrata na sustavu.	Vodeći proizvodi nude iscrpno uklanjanje izmjena i stražnja vrata se nikad ne instaliraju.
STJECANJE I POVEĆANJE OVLASTI	Zahtjeva se izmjene sustava, budući da se kôd mora postaviti i prevesti na kompromitiranom računalu.	Korisnici mogu brzo prodrijeti dublje u mrežu. Kôd se nikad ne mora postavljati na ciljno računalo i testovi se mogu provesti udaljeno.
IZVJEŠTAVANJE	Zahtjeva značajan trud, bilježenje i uspoređivanje svih rezultata ručno. Svi izvještaji moraju biti generirani ručno.	Iscrpni prikaz prethodnih događaja i pronađenih mana generiraju se automatski i prilagodljivi su.
ZAPISIVANJE / ANALIZA	Spor, težak, često netočan proces.	Automatski se snima detaljno izvješće o svim aktivnostima.

OBUČAVANJE	Ispitivači moraju naučiti nestandardizirane, ad-hoc metode testiranja.	Korisnici mogu naučiti i instalirati alat za manje od jednog dana.

Tablica 2 Usporedba automatskog i ručnog penetracijskog testiranja, izvor: www.cert.hr

9. INTERNETSKA FORENZIKA

U posljednjim desetljećima industrija i vlade sve više koriste internet. Vlade koriste internet kako bi građanima i tvrtkama pružile javne usluge. Elektroničke državne usluge koje se pružaju građanima obično uključuju plaćanje poreza na dohodak, zahtijevanje i izdavanje osobne dokumentacije kao što su rodni i vjenčani listovi, izdavanje i obnavljanje vozačkih dozvola, sudjelovanje u izbornim procesima i tako dalje. Poduzeća postaju ovisna o internetu zbog komunikacije, pružanje svojih proizvoda i usluga kupcima i za donošenje novih poslovnih modela koji u potpunosti ovise o korištenju interneta. Tehnološki razvoj također ima "mračnu stranu": Budući da kriminal obično slijedi priliku, a Internet pruža mnoge nove mogućnosti, pojavljuju se novi zločini, kao i novi načini počinjenja "tradicionalnih zločina" pomoću novih tehnologija. Zbog "anonimnosti" kibernetičkih kriminalnih aktivnosti i činjenice da ta nova vrsta kaznenih djela nisu ograničena geografskim granicama, ona imaju dalekosežne posljedice. U umreženom svijetu, gdje su sve točke jednako udaljene od svih ostalih i dostupne su odasvud, načela pravnog sustava ne mogu svima nametnuti obveze da se pridržavaju svih zakona. Kao rezultat toga, vlade i poduzeća postaju sve osjetljiviji na prijetnje koje potječu s Interneta. Najčešća prijetnjama koja potječe s Interneta su zlonamjerni programi koji mogu ukrasti povjerljive informacije (u takve programe spadaju virusi, špijunski softver, crvi, trojanci). Također su česti phishing napadi, krađa identiteta, neželjena pošta, zapisivanje ključeva i napadi uskraćivanjem usluga.[46]

Zbog rasta kibernetičkog kriminala digitalna forenzika[42] postala je od iznimne važnosti. Istraga i prikupljanje odgovarajućih dokaza za kazneni progon često se pokazuje kao težak i složen zadatak. Usmjeravanje prijenosa kroz niz jurisdikcija kako bi se onemogućili pokušaji praćenja izvora ili opsežna upotreba kriptografskih tehnika kako bi podaci postali nerazumljivi, uobičajeni su koraci koje poduzimaju kriminalci kako bi

[42] Digitalna forenzika nastala je 1980.-ih godina kada je sve više ljudi počelo kupovati računala, a time su se i započeli izvršavati zločini putem računala. Do 1990.-ih, uspostavile su se temeljne tehnike i formalne metodologije za prikupljanje dokaza i istraživanje zločina. Forenzički alati su se razvijali tijekom godina prateći tehnologiju, a kako bi se olakšale istrage.

sakrili ili prikrili svoje aktivnosti. Internetska forenzika uključuje tehnike i metodologije za prikupljanje, čuvanje i analizu digitalnih podataka na Internetu u svrhu istrage i provedbe zakona. To je relativno nedavno područje istraživanja i prakse koje se razvilo kao rezultat sve većeg korištenja Interneta i kretanja kriminalnih aktivnosti. Također se tvrdi da su internetski forenzičari evoluirali kao odgovor hakerskoj zajednici.[46]

Internetska forenzika od velike je važnosti jer pomaže u razotkrivanju onoga što se dogodilo, te identificiranju i prikupljanju računalnih dokaza o počiniteljima.[47]

Internet je postao ne samo mjesto zločina, već i plodno tlo za primarne i sekundarne izvore dokaza. Forenzička istraga zahtijeva upotrebu discipliniranih istražnih tehnika za otkrivanje i analizu tragova dokaza koji su ostali nakon počinjenog kaznenog djela. Internetska forenzika uključuje priznavanje, prikupljanje i rekonstrukciju digitalnih dokaza i njihovo upravljanje na način koji ih čini dopuštenim u kaznenom progonu i u sudskim postupcima. Kao i druge forenzičke znanosti, internetska forenzika započinje prikupljanjem velikog broja intenzivno različitih varijabli ili atributa, a kulminira podudaranjem uzoraka među tim varijablama kako bi se individualizirali dokazi. Mrežna forenzika sve više zahtijeva i rezultira povezivanjem heterogenih skupova podataka koji se odnose na aktivnosti, koje se često događaju u više društvenih i poslovnih okruženja, te korelacijom digitalnih tragova sadržanih unutar i između različitih izvora podataka, kao što su web stranice, računalni dnevnici, internetske interesne grupe, internetske chat sobe.[46]

9.1 Kibernetički kriminalitet[43]

Elektroničko kazneno djelo definira se kao nezakonito djelo koje se provodi putem računala ili elektroničkih medija. Kibernetički zločin je zločin koji se provodi putem Interneta ili zločin čije je mjesto zločina internet. Kibernetički kriminalitet nisu nova

[43] U Glavi XXV Kaznenog zakona Republike Hrvatske opisana su kaznena djela protiv računalnih sustava, programa i podataka i to: „Neovlašteni pristup“, „Ometanje rada računalnog sustava“, „Oštećenje računalnih podataka“, „Neovlašteno presretanje računalnih podataka“, „Računalno krivotvorenje“, „Računalna prijevara“, „Zlouporaba naprava“, „Teška kaznena djela protiv računalnih sustava, programa i podataka“

kaznena djela. Puno slučajeva uključuje klasične vrste zločina u kojima kriminalci iskorištavaju računalnu snagu i dostupnost informacijama. Anonimnost koja se pruža putem Interneta potiče zločine koji uključuju korištenje računalnih sustava. Kriminalci vjeruju da postoji mala šansa da budu uhvaćeni i procesuirani za kazneno djelo. Kriminalci također sve više iskorištavaju hakerske tehnike i zlonamjerni kod. Kibernetički zločini mogu biti automatizirani (kao što su neželjena pošta, crvi, trojanci, virusi, špijunski softver) ili posebno ciljani, poput krađe vlasničkih informacija ili intelektualnog vlasništva, sabotaže itd.[46]

9.2 Prikupljanje digitalnih dokaza

Uz povećanu upotrebu Interneta, mogu se pronaći značajni dokumentarni dokazi o bilo kojem korisniku. Kada se istražuju kibernetički zločini, dokazi se mogu prikupiti iz više izvora. Pružatelji internetskih usluga obično vode opsežne zapisnike o aktivnosti korisnika, navodeći pristupne točke, korištene IP adrese, vrijeme početka i završetka veze itd. Ti se zapisi obično čuvaju od nekoliko dana, a mogu i godinu ili više. Većina pružatelja internetskih usluga također može učiniti podatke usmjerivača dostupnima za potrebe istrage kibernetičkih kaznenih djela. U budućnosti se očekuje da će tijela kaznenog progona zatražiti od pružatelja internetskih usluga pružanje još više informacija o korisnicima Interneta. Već postoje forenzičke sheme koje zahtijevaju pristup komunikacijskim podacima u stvarnom vremenu. Ostali izvori dokaza uključuju zapisnike sustava (elektroničke pošte, DHCP poslužitelji, vatrozidi), pa čak i internetska plaćanja.

Prema Zakonu o kaznenom postupku Republike Hrvatske pretraga[44] pokretnih stvari obuhvaća i pretragu računala i s njim povezanih uređaja, drugih uređaja koji služe prikupljanju, pohranjivanju i prijenosu podataka, telefonskim, računalnim i drugim komunikacijama i nositelja podataka. Na zahtjev tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu ili drugom uređaju ili nositelju podataka, te

[44] Zakon o kaznenom progonu (NN 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19, 126/19, 130/20, 80/22, 36/24), Glava XVIII, Dokazne radnje, Pretraga, od članka 240. do članka 260. ZKP-a

davatelj telekomunikacijskih usluga, dužni su omogućiti pristup računalu, uređaju ili nositelju podataka, te dati potrebne obavijesti za nesmetanu uporabu i ostvarenje ciljeva pretrage. Po nalogu tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu i drugim uređajima, te davatelj telekomunikacijskih usluga, dužni su odmah poduzeti mjere kojima se sprječava uništenje ili mijenjanje podataka.[46]

Predmeti koji se oduzimaju prema Kaznenom zakonu, ili koji mogu poslužiti pri utvrđivanju činjenica u postupku, privremeno će se oduzeti i osigurati njihovo čuvanje.

To se odnosi i na podatke pohranjene u računalima i s njim povezanim uređajima, te uređajima koji služe prikupljanju i prijenosu podataka, nositelje podataka i na pretplatničke informacije kojima raspolaže davatelj usluga., osim kada je prema zakonu privremeno oduzimanje predmeta zabranjeno. Podaci se na pisani zahtjev državnog odvjetnika moraju predati državnom odvjetniku u cjelovitom, izvornom, čitljivom i razumljivom obliku. Pri pribavljanju, snimanju, zaštiti i čuvanju podataka posebno će se voditi računa o propisima koji se odnose na čuvanje tajnosti određenih podataka.[46]

9.3 Tehnički izazovi za internetsku forenziku

Porast kibernetičkih kaznenih djela rezultirao je sve većom potrebom za razvojem internetskih forenzičkih tehnika i alata za otkrivanje napada. Osim potrebe da istražitelji razviju i primijene odgovarajuće alate i postupke za provođenje digitalnih istraga, postoji i širok raspon pitanja koja treba riješiti. To su pitanja koja obuhvaćaju tehničke, socijalne i pravne aspekte. Upotrebom ad hoc metoda i alata za pribavljanje digitalnih dokaza može se ograničiti pouzdanost i vjerodostojnost dokaza, posebno u postupku kaznenog progona u kojem se mogu osporiti i dokazi i postupci koji se upotrebljavaju za njihovo prikupljanje.

Tehnički izazovi uključuju raznolikost i heterogenost infrastrukture (različite platforme i različite primjene) i fizičke prepreke koje istražiteljima zabranjuju pristup izvorima dokaza (npr. tablice usmjeravanja u usmjerivačima). Praćenje dokaza putem Interneta također predstavlja poteškoće u provođenju analiza datuma i vremenskog okvira prikupljenih podataka. Da bi se primijenila većina forenzičkih modela, mora se pretpostaviti da se napad dogodio kako bi se primijenili određeni postupci u pokušaju otkrivanja i prikupljanja

relevantnih tragova. Vrsta i karakteristike napada moraju biti poznate i shvaćene kada se pokrene forenzička istraga.

Forenzički postupci obično zahtijevaju prikupljanje, pohranjivanje i analizu velikih količina podataka. To predstavlja visoke zahtjeve za sustave, a posebno u slučaju kibernetičkog kriminaliteta. Izazov za istražitelje su velike količine podataka, te dolazi do problema u odabiru značajnih ili relevantnih dijelova među njima. Kada se istražuju kibernetički zločini, podaci se moraju prikupljati dok računala i usmjerivači još rade, tzv. Proces otkrivanja uživo. Kriminalci često koriste širok raspon tehnika kako bi izbjegli istragu i kazneni progon. Tradicionalne antiforenzičke tehnike uključuju promjenu proširenja datoteka, softver za brisanje diskova, fizičko uništavanje medija, tehnike anonimizacije, korištenje besplatnog anonimnog pristupa internetu i besplatnih anonimnih internetskih i e-mail računa, kriptografiju i steganografiju. Korištenje enkripcije predstavlja značajne prepreke forenzičkim procesima. Kriminalci također često provode kriminalne aktivnosti iz zemalja u kojima se ne primjenjuju zakoni o računalnom kriminalu ili kibernetičkom kriminalu. Protiv osumnjičenog autora crva ILOVEYOU[45] nije bilo moguće poduzeti nikakve pravne radnje budući da je osumnjičeni bio smješten na Filipinima, koji u to vrijeme nisu imali zakonodavstvo protiv računalnog kriminala. Počinitelji koji provode kriminalne radnje putem Interneta često koriste kompromitirana računala u različitim zemljama kako bi izbjegli istragu, iskorištavajući različite zakone i pravne kodekse i postupke.[46]

[45] Crv ILOVEYOU poslan je sa Manile, Filipini dana 4. svibnja 2000. godine. Za pet sati se proširio Sjevernom Amerikom, Azijom i Europom putem e-poruka. Naziv poruke je bio „ILOVEYOU“ a u privitku datoteka koja je izgledala kao tekst. Nakon otvaranja privitka pokrenuo se crv koji je datoteke na računalu žrtve pretvorio u nove crve koji su se putem e-poruka dalje proširile na adrese koje je žrtva imala spremljene u adresaru.

9.4 Pravni izazovi za internetsku forenziku

Pravna pitanja koja se odnose na istragu i kazneni progon kibernetičkog kriminaliteta uključuju razlike u jurisdikcijama, postupanje s digitalnim dokazima, uvjete koji bi se trebali primjenjivati na zakonite istrage i zaštitu privatnosti pojedinaca.[46]

9.4.1 Digitalni podaci kao dokaz

Kibernetički kriminalitet i konvencionalni kriminal znatno se razlikuju i po počinjenju i u kaznenom progonu. Posebno je teško pratiti i istraživati kibernetički kriminalitet i kazneno goniti kriminalce u okviru postojećih pravnih sustava, koji su prilagođeni tradicionalnim vrstama kriminala. Nema otisaka prstiju i fizičke prisutnosti kod kibernetičkog kriminaliteta jer ne postoji fizička prisutnost počinitelja. Elektronički dokazi definiraju se kao sve informacije dobivene iz elektroničkog uređaja ili digitalnog medija koje služe za uvjeravanje istine o djelu. Elektronički dokazi se ne razlikuju suštinski od ostalih vrsta dokaza. Problemi se pojavljuju zbog krhkosti i prolaznosti mnogih oblika računalnih dokaza. Temeljno pitanje koje treba razmotriti jest mogu li se i u kojoj mjeri digitalni tragovi i računalni podaci tretirati kao dokumentarni dokazi. Provedba zakona je informacijski intenzivan proces u kojem agencije za provedbu zakona moraju prikupljati i tumačiti velike skupove podataka. Digitalne forenzičke istrage obično se koriste kao odgovor nakon događaja u kojem je izvršeno kazneno djelo. Dokazi se moraju izuzeti, ali u većini kaznenih djela iz područja kibernetike ne postoji u fizičkom obliku. Kibernetičke dokaze počinitelju je lakše uništiti ili izmijeniti bez očitih tragova. Digitalni dokazi su nestabilni jer se mogu lako uništiti neiskusnim pristupom i rukovanjem.

Dokazi prikupljeni preko mreže moraju imati sve atribute konvencionalnih dokaza. Prvenstveno mora biti pribavljen na zakonski način. Elektronski dokazi moraju biti nepobitni autentični, odnosno moraju biti povezani s kaznenim djelom. Utvrđivanje cjelovitosti i autentičnosti materijala na sudu zahtijeva standardne tehnike i metode za prikupljanje, čuvanje i prezentaciju pohranjenog materijala. Budući da su upotreba i rukovanje podacima i informacijama prikupljenima alatima za otkrivanje usko povezani sa standardizacijom, Europska komisija naglašava potrebu za stvaranjem tehničkih standarda kako bi se osiguralo da su prikupljeni podaci u skladu sa zahtjevima zakona

za uporabu takvih podataka u sudskim postupcima. Također je predloženo da se tehnička sredstva i metode podvrgnu neovisnom ispitivanju i certificiranju. Posebna pravila kaznenog postupka odnose se na pristup tijela kaznenog progona izvorima dokaza. Odgovarajući zakon regulira način na koji se činjenice mogu dokazati na sudovima. Kibernetički prostor otvara niz pitanja u vezi s primjenjivošću tih pravila. Dopuštenost dokaza iz računalnih evidencija na sudovima u velikoj mjeri ovisi o temeljnim načelima dokaza u dotičnoj zemlji. Dopuštenost digitalnih dokaza ključna je jer se u većini zemalja prisilne ovlasti primjenjuju samo na materijale koji bi bili dopušteni kao dokaz na suđenju.[46]

9.4.2 Traženje dokaza i nadležnosti

U tradicionalnom okruženju pretraživanje uključuje prikupljanje dokaza koji su u prošlosti zabilježeni ili registrirani u opipljivom obliku. U izvanmrežnoj pretrazi preduvjet za dobivanje zakonske ovlasti za pretraživanje jest postojanje razloga za vjerovanje da takvi podaci postoje na određenoj lokaciji i da će pružiti dokaze o određenom kaznenom postupku. Jedan aspekt upotrebe naloga za pretraživanje u okruženju kibernetičkog prostora odnosi se na zemljopisno područje primjene naloga koji je izdao sudac ili sud kojim se odobrava pristup digitalnim podacima. Digitalne forenzičke pretrage više se ne obavljaju na pojedinačnim uređajima s malim kapacitetima za pohranu podataka. Umjesto toga, prostor za potencijalne dokaze proširio se na mreže međusobno povezanih računala. Konvencijom o kibernetičkom kriminalitetu[46] uzeti su u obzir slučajevi da bi se zakonito odobreno pretraživanje na jednom mjestu potencijalno trebalo proširiti na međusobno povezane sustave koji se nalaze bilo gdje u nadležnosti istražnog tijela. Konvencijom se od država potpisnica zahtijeva da donesu zakonodavne i druge mjere koje mogu biti potrebne kako bi se osiguralo da ako njezina istražna tijela pretražuju (ili na sličan način pristupaju) određenom računalnom sustavu ili njegovom dijelu i imaju osnove vjerovati da su traženi podaci pohranjeni u drugom računalnom sustavu i da su

[46] donesena 23.11.2001. godine u Budimpešti, Mađarska. Od 27 država članica, Konvenciju je ratificiralo njih 26 – Irska ju je potpisala, ali je nije ratificirala. Konvencija se odnosi na suzbijanja kriminala s ciljem zaštite društva od kibernetičkog kriminala

takvi podaci zakonito dostupni početnom sustavu ili dostupni njemu, moraju moći hitno proširiti pretraživanje ili sličan pristup drugom sustavu. Često se podaci koji se pretražuju pohranjuju u opremi koja se nalazi u drugim državama. FBI je 2000. godine pristupio računalima u Rusiji putem Interneta i preuzeo podataka s računala kojima su se koristili optuženi hakeri Vasiliy Gorschkov i Aleksej Ivanov. Pitanja nadležnosti predstavljaju neke od najvećih izazova u borbi protiv kibernetičkog kriminaliteta. Mrežne granice presijecaju i nadilaze međunarodne granice. Nadležnost nad aktivnostima na internetu postala je jedno od glavnih bojišta za borbu za uspostavu vladavine prava u informacijskom društvu.

Međunarodna zajednica razvila je dugogodišnje metode za dobivanje i pružanje pravne pomoći. Ti su procesi, međutim, dugotrajni i često sadrže ograničenja u pogledu vrste pomoći koja se može dobiti. Pitanje kada je istražnom tijelu dopušteno jednostrani pristup podacima pohranjenima u drugoj državi, bez traženja uzajamne pomoći, bilo je pitanje o kojem su sastavljači Konvencije o kibernetičkom kriminalu dugo raspravljali.[47] Države članice u skladu s Konvencijom o kibernetičkom kriminalu prihvatile su prekogranični pristup pohranjenim računalnim podacima u dvije situacije: a) ako su podaci kojima se pristupa javno dostupni i b) ako je istražno tijelo pristupilo ili primilo podatke koji se nalaze izvan njegova državnog područja putem računalnog sustava u svojoj nadležnosti te je dobilo zakonitu i dobrovoljnu suglasnost osobe, koji ima zakonske ovlasti otkriti podatke ispitnom postupku putem tog sustava. Tko je osoba koja je zakonito ovlaštena za otkrivanje podataka može se razlikovati ovisno o okolnostima, prirodi osobe i dotičnom mjerodavnom pravu. Tvrdi se da izvan teritorijalno proširenje nadležnosti kaznenog postupka može ojačati suverenitet u transnacionalnom okruženju kibernetičkog prostora.[46]

[47] Policija prikupljanje podatke o stanju sigurnosti kao i druge podatke koji mogu doprinijeti uspješnom obavljanju policijskih poslova. Prikupljaju se podatci o počiniteljima kaznenih djela, prikrivačima, pomagačima, poticateljima te osobama za kojima se traga. Podaci se pohranjuju u pisanom ili digitalnom obliku na način koji osigurava njihovu trajnost i zaštitu od neovlaštenog pristupa.

9.4.3 Rudarenje podataka kao forenzički alat

Istražna tijela suočavaju se s potrebom izvlačenja relevantnih informacija iz velikog broja dokumenata. Moderni softverski alati za rudarenje podataka i teksta mogu se suočiti s izazovom stalnog povećanja količine dokumentacije i informacija koje nadležna tijela moraju obraditi. Tehnologija rudarenja podataka uključuje masovno prikupljanje podataka, skladišta podataka, statističku analizu i tehnike deduktivnog učenja te koristi ogromne količine podataka za izdvajanje informacija iz podataka, generiranje hipoteza i otkrivanje općih obrazaca. Stručnjaci za rudarenje podataka koriste informacijsku tehnologiju kako bi pronašli trendove i obrasce u gomili informacija koje potječu iz nekoliko izvora.

Informatizacija podataka i mogućnost pretraživanja cijelog teksta stvaraju neograničen broj načina postavljanja upita i sortiranja informacija. Informatizacijom i rudarenjem podataka mnogo je lakše pretraživati podatke, koji u početku nisu međusobno povezani, kombinirati ih i donositi nove informacije. Kombinacijom javno dostupnih podataka iz različitih izvora može se dobiti profil situacije ili ponašanja pojedinaca.

Alati za rudarenje podataka i teksta povećavaju rizik od prikupljanja podataka u sekundarne i često nepravilne svrhe. Važno je napomenuti da su tehnike rudarenja podataka potaknute sve većom javnom dostupnošću podataka i sve većom integracijom javnih internetskih podataka s postojećim privatnim skupovima podataka. Programi poput "Total Information Awareness" (TIA) u SAD-u, koji su nastojali koristiti rudarenje podataka za identifikaciju terorista, temelje se na čvrsto povezanom odnosu između vladinih baza podataka i baza podataka privatnog sektora. U tom kontekstu rudarenje podataka može dovesti do masovnog objedinjavanja informacija ne samo za počinitelje, već i za neograničeno velik broj pojedinaca. Prema riječima povjerenika za zaštitu podataka, aktivnosti rudarenja podataka zahtijevaju dodatne zaštitne mjere za uporabu tih podataka i praćenje uporabe tih operacija. Upotreba alata za rudarenje podataka i teksta trebala bi se temeljiti na posebnoj i odgovarajućoj pravnoj osnovi.[46]]

9.4.4 Forenzika i njihov utjecaj na privatnost

Upotreba forenzičkih metoda sama po sebi može predstavljati zadiranje u temeljno pravo građana na privatnost. Stoga zakonitost i dopuštenost elektroničkih dokaza na sudu ovise o poštovanju pravnih ograničenja i jamstava utvrđenih zakonodavstvom koje se odnosi na informacijsku i komunikacijsku privatnost. Materijalnim i postupovnim pravilima mora se osigurati da je prikupljanje i daljnja obrada elektroničkih dokaza u skladu s odredbama kojima se jamči zaštita podataka. Člankom 8. Europske konvencije[48] i člankom 7. Povelje Europske unije[49] o temeljnim pravima uređuje se zaštita privatnosti pojedinaca na razini EU-a. Istodobno, zaštita podataka u EU-u uređena je Direktivom 95/46/EZ, Direktivom 2002/58 i člankom 8. Zakonodavci moraju navesti postupke koje treba slijediti i uvjete koje treba ispuniti kako bi se istražio incident u području kibernetičkog kriminaliteta u skladu sa zahtjevima nužnosti i proporcionalnosti. Proporcionalnost, koja je ključno načelo europskog prava, zahtijeva daljnju procjenu nužnosti mjere i njezine prikladnosti za postizanje njezinih ciljeva. Cilj koji se želi postići mora se uravnotežiti s ozbiljnošću ako je uplitanje, koje treba procijeniti uzimajući u obzir, među ostalim, broj i prirodu pogođenih osoba te intenzivnost negativnih učinaka. Većina europskih zemalja regulira zakonitost istražnih aktivnosti općenito ili sektorskih zakona o zaštiti podataka. Relevantni pravni okvir znatno se razlikuje, posebno u usporedbi sa zemljama zajedničkog prava: razlike se ne odnose samo na materijalne pravne zahtjeve, već i na ustavnu pozadinu, pravni kontekst i zakonodavnu tehniku relevantnih odredaba. Upotreba forenzičkih metoda tijekom kaznene istrage obično podliježe relativno strogim postupovnim kontrolama i jamstvima, kao što je sudski nalog.[46]

[48] Konvencija za zaštitu ljudskih prava i temeljnih sloboda donesena 24.06.2013. godine u Strasbourgu, Njemačka
[49] Povelje Europske unije o temeljnim pravima, donesena 7.12.2000. godine u Nici, Italija

10. ZAKLJUČAK

U suvremenom svijetu, kibernetički napadi postaju sve složeniji i sofisticiraniji. Napadi ransomwareom su česti, a napadači šifriraju podatke i traže otkupninu za njihovo dešifriranje. Napadi phishingom se koriste lažnim e-porukama kako bi se korisnici prevarili da otkriju osobne ili financijske informacije. Napadi DDoS-om imaju za cilj preopteretiti mrežne resurse, što dovodi do nedostupnosti usluga. Napadi na softver i ranjivosti napadači iskorištavaju kako bi dobili neovlašten pristup sustavima ili podacima.

Kako u Europskoj uniji, a i u svijetu broj uređaja spojenih na Internet naglo raste, tako raste i opasnost od kibernetičkih napada. Kako većina uređaja koristi starije operativne sustave za koje proizvođači više ne izdaju zakrpe, takvi uređaji postaju laka meta kibernetičkih napada zbog svojih softverskih nedostataka.

I dan danas se dosta računala je pogonjeno starijim operacijskim sustavima Windows za koje se ne izdaju zakrpe. Za Windows XP nadogradnje su prestale sa danom 08. travnja 2014. godine. Operacijski sustav Windows 7 prestao je sa nadogradnjama 14. siječnja 2020. godine, dok za Windows 10 nadogradnje prestaju 14. listopada 2025. godine.

Računala sa takvim operacijskim sustavima, za koje su nadogradnje prestale predstavljaju veliku opasnost. Lako mogu postati meta napada i postati botovi ili čvorovi za daljnje kibernetičke napade.

Razni ransomwareom napadi događaju se češće na računalima koja nemaju instalirane zakrpe koje dolaze od proizvođača operacijskog sustava. Takvi napadi nanašaju veliku štetu poduzećima. Napadači traže otkupninu od žrtve kako bi im poslali ključ za dešifriranje podataka. Očajne žrtve, u nadi da će dobiti ključ i vratiti svoje podatke ili uspomene koje su godinama skupljali, uplaćuju tražene iznose, nakon čega od napadača ne dobivaju ključ, te osim gubitka podataka, poslovanja, gube i neku svotu novca.

Kako bi se smanjili kibernetički napadi bilo bi poželjno učiti iz tuđih iskustava, redovito ažurirati antivirusne programe, zakrpe, šifrirati i kopirati podatke na vanjske medije koje potom spremiti na sigurno mjesto, kod prijava na internetske stranice (npr. društvene

mreže, e-mail servise) koristiti zaporke koje imaju kombinaciju velikih i malih slova, brojeva i simbola kako bi se napad onemogućio. koristiti zaporke koje imaju kombinacije. Tvrtke bi trebale zaštititi informacije o svojim zaposlenicima, te iste educirati o opasnostima koje prijete od otvaranja e-poruka od nepoznatih pošiljatelja u kojima se nalaze privici ili poveznice na sumnjive stranice.

11. LITERATURA

[1] Hrvatska enciklopedija, Kibernetika, https://www.enciklopedija.hr/clanak/kibernetika pristupljeno 03.03.2024.g.

[2] **Damir Prskalo**, „*Kibernetička sigurnost kao ključna determinanta nacionalne sigurnosti Republike Hrvatske“,* Zbornik sveučilišta Libertas, 8, 2022

[3] IoT Connected Devices, Researchgate, https://www.researchgate.net/figure/IoT-Number-of-devices-worldwide-from-2015-to-2025-5_fig1_351075753 pristupljeno 01.07.2024.g.

[4] Objavljen je Zakon o kibernetičkoj sigurnosti (NN 14/2024), Cert.hr, https://www.cert.hr/objavljen-je-zakon-o-kibernetickoj-sigurnosti-nn-14-2024/ pristupljeno 03.07.2024.g.

[5] Republika Hrvatska, Ured vijeća za nacionalnu sigurnost, https://www.uvns.hr/hr/o-nama/djelokrug/informacijska-sigurnost-nsa pristupljeno 03.07.2024.g.

[6] Republika Hrvatska, Siguronosno-obvještajna agencija, https://www.soa.hr/hr/informacije/faq/ pristupljeno 03.07.2024. godine

[7] O Nacionalnom CERTu, Cert.hr, https://www.cert.hr/onama/ pristupljeno 03.07.2024. godine

[8] Republika Hrvatska, Zavod za sigurnost informacijskih sustava https://www.zsis.hr/default.aspx?id=13 pristupljeno 03.07.2024. godine

[9] Republika Hrvatska, Ministarstvo unutarnjih poslova, https://policija.gov.hr/uprava-kriminalisticke-policije/415 pristupljeno 03.07.2024. godine

[10] Agencija za zaštitu osobnih podataka, https://azop.hr/djelokrug/ pristupljeno 03.07.2024. godine

[11] **Ahić Jasmin i Nađ Ivan** *„Upravljanje rizikom u privatnoj sigurnosti“* Sarajevo: Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu, 2019. g.

[12] Ivan Podnar, Tko su HackManac, koji izvještava o napadu na KBC Zagreb i tko je ransomware grupa LockBit 3.0, BUG.hr, https://www.bug.hr/sigurnost/tko-su-hackmanac-koji-izvjestava-o-napadu-na-kbc-zagreb-i-tko-je-ransomware-42013 pristupljeno 02.07.2024.g.

[13] Grid incident report South-Eastern part of the Continental Europe power system, Entsoe, https://www.entsoe.eu/news/2024/06/21/grid-incident-report-south-eastern-part-of-the-continental-europe-power-system/ pristupljeno 02.07.2024.g.

[14] Josh Fruhlinger, Stuxnet explained: The first known cyberweapon, CSO, https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html pristupljeno 02.07.2024.g.

[15] Kinza Yasar, What is malware?, Techtarget https://www.techtarget.com/searchsecurity/definition/malware pristupljeno 05.03.2024.g.

[16] Što je malware i kojih 6 vrsta razlikujemo?, DIR.hr, https://dir.hr/sto-je-malware/ pristupljeno 26.03.2024.g.

[17] What Is Malware? Akami, https://www.akamai.com/glossary/what-is-malware pristupljeno 05.03.2024.g.

[18] Adware, Malwarebytes https://www.malwarebytes.com/blog/threats/adware pristupljeno 10.03.2024.g.

[19] *„Advanced Persistent Threat napadi“*, Centar Informacijske Sigurnosti, CIS-DOC-2011-11-031 Revizija 1.04

[20] Farah Amod, The 3 stages of an APT attack, Paubox https://www.paubox.com/blog/the-3-stages-of-an-apt-attack pristupljeno 10.03.2024.g.

[21] What is a backdoor?, Malwarebytes https://www.malwarebytes.com/backdoor pristupljeno 10.03.2024.g.

[22] O crvima, Cert.hr, https://www.cert.hr/crvi/ pristupljeno 24.03.2024.g.

[23] Worm, Malwarebytes, https://www.malwarebytes.com/blog/threats/worm pristupljeno 24.03.2024.g.

[24] What is a keylogger?, Malwarebytes https://www.malwarebytes.com/keylogger pristupljeno 06.03.2024.g.

[25] O keylogger softveru, Cert.hr https://www.cert.hr/keyloggeri/ pristupljeno 06.03.2024.g.

[26] O rootkit softveru, Cert.hr https://www.cert.hr/rootkitovi/ pristupljeno 06.03.2024.g.

[27] What Is Ransomware?, Trellix, https://www.trellix.com/security-awareness/ransomware/what-is-ransomware/ pristupljeno 17.04.2024.g.

[28] Ransomware - nemilosrdna prijetnja vašim podacima!, IDE3IT, https://ide3.hr/blog/it-price/ransomware-nemilosrdna-prijetnja-vasim-podacima

[29] Ransomware, Cert.hr, https://www.cert.hr/19795-2/ransomware/ pristupljeno 17.04.2024.g.

[30] Spyware: What It Is and How to Protect Yourself, Kaspersky, https://www.kaspersky.com/resource-center/threats/spyware pristupljeno 17.04.2024.g.

[31] Što je bot i koje 4 vrste botova znamo?, DIR.hr https://dir.hr/sto-je-bot/ pristupljeno 24.03.2024.g.

[32] *„Botneti“,* CARNet, NCERT-PUBDOC-2014-01-340

[33] [UPOZORENJE] U tijeku je kampanja poslovnih prijevara, Cert.hr, https://www.cert.hr/upozorenje-u-tijeku-je-kampanja-poslovnih-prijevara/ pristupljeno 24.03.2024.g.

[34] What is a Dictionary Attack?, Kaspersky, https://www.kaspersky.com/resource-center/definitions/what-is-a-dictionary-attack pristupljeno 24.03.2024.g.

[35] Sandro Vrbanus, Top 20 najčešćih lozinki hrvatskih korisnika u 2023. - manje smo neoprezni nego ostatak svijeta, BUG.hr, https://www.bug.hr/sigurnost/top-20-najcescih-lozinki-hrvatskih-korisnika-u-2023-manje-smo-neoprezni-nego-36597 pristupljeno 24.03.2024.g.

[36] *„Zaštita od DDoS napada“,* CARNet, CERT.hr-PUBDOC-2022-10-408

[37] Hoax, Cert.hr, https://www.cert.hr/19795-2/hoax/ pristupljeno 26.03.2024.g.

[38] Phising, Cert.hr, https://www.cert.hr/phishing/ pristupljeno 26.03.2024.g.

[39] Siniša Begović, Scam i Phishing – što su i kako se zaštititi?, Plavi ured, https://plaviured.hr/vodici/scam-phishing-sto-se-zastititi/ pristupljeno 17.04.2024.g.

[40] What Are Sniffing Attacks, and How Can You Protect Yourself?, Eccouncil, https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-are-sniffing-attacks/ pristupljeno 17.04.2024.g.

[41] *„Metodologija penetracijskog testiranja“*, CARNet, Revizija v1.0 CCERT-PUBDOC-2008-02-219

[42] What is Pentesting?, Hackerone, https://www.hackerone.com/knowledge-center/what-penetration-testing-how-does-it-work-step-step pristupljeno 20.04.2024.g.

[43] Penetration Testing, Imperva, https://www.imperva.com/learn/application-security/penetration-testing/ pristupljeno 20.04.2024.g.

[44] **Ivona Zakarija, Tomislav Domić, Vedran Batoš**, *„Primjena odabranog pristupa penetracijskom testiranju računalnih sustava“,* “Naše more” 60(1-2)/2013

[45] What is penetration testing?, IBM, https://www.ibm.com/topics/penetration-testing pristupljeno 20.04.2024.g.

[46] **Maria Karyda and Lilian Mitrou**, „*Internet Forensics: Legal and Technical Issues“,* University of the Aegean, Department of Information and Communication Systems Engineering, Karlovassi, Samos,GR 83200, Greece, 2007. g.

[47] **Krunoslav Antoliš**, *„Internetska forenzika i cyber terorizam“*, Polic. sigur. (Zagreb), godina 19. (2010), broj 1

[48] POPIS SLIKA

Stranica

[49] POPIS TABLICA

Stranica