CYBER NAPAD, VRSTE CYBER NAPADA I ADEKVATNA ZAŠTITA PODATAKA I KORISNIKA

Nehad Gaši, MA; Internacionalni univerzitet Travnik u Travniku, Fakultet informacionih tehnologija Travnik; nehad.gasi@iu-travnik.com
Dina Vrebac, BA; Internacionalni univerzitet Travnik u Travniku, Fakultet informacionih tehnologija Travnik; dina.vrebac@iu-travnik.com
Amira Trako, BA; Internacionalni univerzitet Travnik, Fakultet politehničkih nauka Travnik; amira.trako@iu-travnik.com

Pregledni članak

SAŽETAK

Danas smo svjedoci vremena u kojem se čak i ratovi u svijetu između različitih država odvijaju u digitalnom formatu. U današnjem okruženju u kojem kibernetički broj napada neprestano raste, niko se više ne može oslanjati na tradicionalni način zaštite poput antivirusnih softvera I softvera za otkrivanje malicioznih softvera. Cyber kriminal obuhvata skup krivičnih djela gdje se kao objekat izvršenja i kao sredstvo za izvršenje krivičnog djela koriste računari, računarske mreže, računarski podaci, kao i njihovi produkti u materijalnom i elektronskom obliku. Postalo je jasno da instalirani antivirusni program ne garantuje potpunu sigurnost korisnika ili informacionog sistema. Prije svega, postavlja se pitanje da li su svi računari i uređaji na sasvim propisan način zaštićeni najnovijom verzijom antivirusnog programa. Samo kontinuirano praćenje pokrivenosti endpoint okoline je jako izazovno za IT administratore. Čak i ako postoji instalirani antivirusni softver sa zadnjim update-om virusne detekcije, detekcija i prevencija sofisticiranih napada dodatni su izazovi. U pravilu, IT administratori koji su odgovorni za održavanje I sifurnost Sistema, neće dobiti trenutni uvid u to što se događa ili historijski pregled što se dogodilo prilikom nekog sigurnosnog napada.

Ključne riječi: *cyber, criminal, email, računar, antivirus, malware, IT, informacioni sistem, kompjuterski criminal*

CYBER ATTACK, TYPES OF CYBER ATTACK AND ADEQUATE PROTECTION OF DATA AND USERS

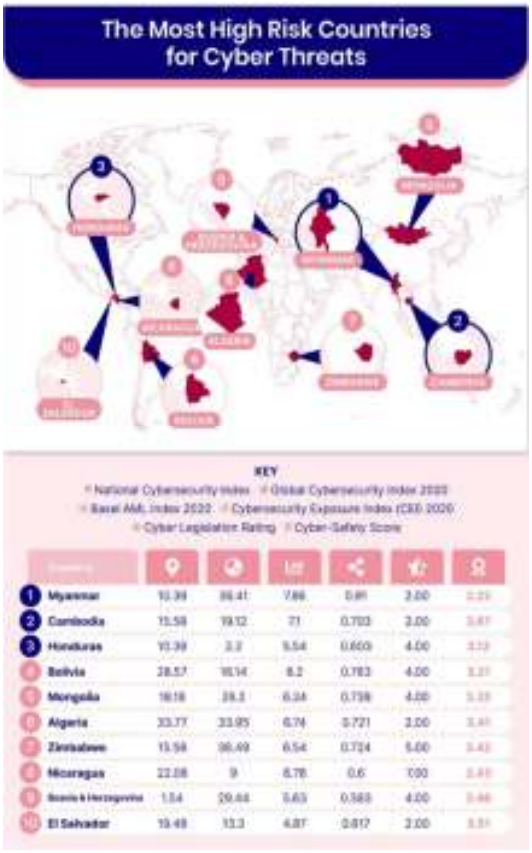
ABSTRACT

Today we are witnessing a time in which even wars in the world between different states are taking place in a digital format. In today's environment where the number of cyberattacks is constantly growing, no one can rely on traditional protection such as antivirus software and malware detection software anymore. Cybercrime includes a set of criminal offenses where computers, computer networks, computer data, as well as their products in material and electronic form are used as the object of execution and as a means of committing the crime. It became clear that the installed anti-virus program does not guarantee the complete security of the user or the information system. First of all, the question arises whether all computers and devices are properly protected by the latest version of the antivirus program. Just continuously monitoring the coverage of the endpoint environment is very challenging for IT administrators. Even if there is installed antivirus software with the latest update of virus detection, detection and prevention of sophisticated attacks are additional challenges. As a rule, IT administrators who are responsible for the maintenance and security of the System, will not get an immediate insight into what is happening or a historical overview of what happened during a security attack.

Keywords: *cyber, criminal, email, computer, antivirus, malware, IT, information system, computer crime*

1 CYBER KRIMINAL

Cyber kriminal je kriminal koji se izvršava u cyber (računarskom) prostoru I svijetu. Cyber criminal obuhvata sve radnje koje nisu dozvoljene u "realnom svijetu" .Ova vrsta kriminala raste najbrže od svih vrsta kriminala zbog stalnog rasta broja „inovativnih" oblika kriminalnih radnji koje se ćine pomoću računara. Na početku, cyber kriminal je bio kriminal koji se odnosio samo na zarazu računara ili sistema, međutim danas cyber kriminal je jedan od najopsnijih vrsta kriminala, a razlog toga je što je kompletno društvo prešlo na digitalnu sfreu, odnosno svo poslovnje se odvija u digitalnom načinu. Prema Globalnom izvješću o cyber kriminalu koje provodi kompanija SEON na rang listi sigurnosti pri samom dnu tabele je BiH, na 86. poziciji, od ukupno 94 zemlje obuhvaćene ovim izvještajem.[37]



Slika 1.: Zemlje sa najviše kibernetičkih napada
Izvor: https://seon.io/resources/global-cybercrime-report/

Cyber kriminal javlja se u raznim oblicima, koji imaju za cilj krađu podataka, ali i nanošenje velike štete. Najćešće se cyber napad realizuje putem malicioznih programa (virusa ili malware-a). Riječ je o štetnim programi koje cyber kriminalci koriste kako bi pristupili računarima i na taj način nanjeli velku štetu. Svi cyber napadi se javljaju u sljedećim oblicima:

1.1 Virusi/trojanci

Virus trojanac ili popularni naziv trojanski konj maliciozni je virusni program koji se koristi da bi zarazio sistem računara i na njemu napravio zlonamjerne aktivnosti. Obično se trojanski konj koristi za krađu

[37] Global Cybercrime Report: Which Countries Are Most at Risk? 2022 - SEON – datum pristupa 29.12.2022.

personalnih podataka, širenje drugih vrsta virusa ili jednostavno rečeno, za poremećaj performansi računara. Uz to, hakeri ih najčešće koristite za dobivanje daljinskog pristupa željenom računaru, inficiranje određenih fajlova i nanošenje štete samom sistemu. Čim se trojanac ubaci u računar, on će se početi skrivati svojoj žrtvi. Trojanci su veoma slični pravim virusima i zato ih je vrlo teško detektovati. Zbog toga bi se trebali oslanjati na najnovije antivirusne programe koji su updateovani sa zadnjom virusnom detekcijom. U početku, kad su trojanci nastali, oni nisu bili napravljeni da se mogu samostalno širiti internetom. Međutim novije verzije trojanskog konja u sebi imaju dodatnu komponentu koja može omogućiti njihovo vema brzo I neprimjetno umnožavanje. Aktivnost svakog trojanskog konja ovisi o namjerama njihovog autora, odnosno hakera koji je taj trojanski konj ubacio u system zaraženog računara. [38]

Aktivnosti koje mogu uzrokovati trojanci

- Inficiranje odnosno zaraza, koruptiranje i pisanje preko već postojećih fajlova, sistemskih komponenti i instaliranih aplikacija. Oni također mogu uništiti kompletan sistem brisanjem jako važnih sistemskih fajlova ili čak formatiranjem hard diska.
- Krađa financijskih podataka, kao što su brojevi kreditnih kartica, podaci za logiranje, passwordi, vrijedni lični dokumenti i ostale korisnikove osjetljive informacije.
- Praćenje korisnika i svakog pritiskanja tipke koje korisnik napravi na tastaturi. Trojanac također može uzeti "screenshot" i pokrenuti neku drugu aktivnost za krađu specifične informacije.
- Slanje svih prikupljenih podataka na unaprijed definisanu email adresu, upload tih podataka na unaprijed određeni FTP server ili prebacivanje istih uz pomoć sporedne internet konekcije udaljenom hostu.
- Instaliranje stražnjih vrata (backdoor) ili aktivacija vlastite komponente koja će dopustiti udaljenom napadaču da preuzme kontrolu nad kompromitiranim računarom I sistemom.
- Ostavljanje i instaliranje drugih parazita u vidu raznih skrivenih programa.
- Uskraćivanja usluga ili resursa (DoS, Denial of Service) ili drugih mrežnih napada protiv udaljenih hostova ili slanje pretjerane količine email poruka da bi se internet saobraćajem preplavili unaprijed definisani računari.
- Instaliranje skrivenih FTP servera koje mogu koristiti zlonamjerne osobe za ostvarivanje različitih ilegalnih ciljeva.
- Terminiranje antivirusnog programa. Trojanski konj može isto tako onemogućiti usluge i funkcije sistema i tako spriječiti standardne sistemske alate u normalnom funkcioniranju.
- Blokiranje korisnikovog pristupa web stranicama I pretraživaćima i izvorima gdje se mogu pronaći neka moguća riješenja sigurnosnih problema.
- Prikazivanje nepoželjnih komercijalnih oglasa i pop-up reklama.
- Degradiranje konekcije na internet, kao i brzine računala. Također može smanjiti sigurnost sistema i tako prouzročiti njegovu nestabilnost.

1.2 Spyware/Adware

Adware je zlonamjerni softver koji automatski prikazuje reklame na mreži kako bi ostvario prihod za svog autora. Oglasi se mogu pojaviti u korisničkom interfejsu softvera, na ekranu tokom procesa instalacije ili u pretraživaču. Iako adware nije uvijek opasan, u nekim slučajevima može biti dizajniran za analizu posjećenih internetskih stranica, predstavljanje reklamnog sadržaja,

[38] https://virusi.hr/trojanci/ - datum pristupa 29.12.2022.

instaliranje dodatnih programa i preusmjeravanje vašeg pretraživača na nesigurne stranice. Može čak sadržavati trojanske konje i špijunski softver. Adware može biti u paketu sa softverom ili igrom koju korisnik želi. U mnogim slučajevima, tokom instalacije paket će pristupiti serveru treće strane koji isporučuje najnoviji adver ili dodatak bez dodirivanja disk jedinice. Osim toga, isti instalateri reklamnog softvera mogu oteti mehanizam isporuke i mogu se koristiti za isporuku mnogo većeg zlonamjernog softvera.

Spyware je špijunski softver je zlonamjerni softverski kod koji se tajno pokreće na računaru, prikuplja informacije o korisniku i njegovim navikama pretraživanja, a zatim te informacije prenosi nazad udaljenom entitetu. Umjesto da ometa rad uređaja, špijunski softver cilja osjetljive informacije i može dati udaljeni pristup hakerima. Svrha špijunskog softvera je prikupljanje informacija o osobi ili organizaciji bez njihovog znanja i prenošenje tih informacija drugom subjektu radi finansijske dobiti. Zbog toga se špijunski softver često koristi za krađu finansijskih ili ličnih podataka. Jedna specifična vrsta špijunskog softvera je keylogger, koji snima korisnikove pritiske tipki kako bi otkrio lozinke i druge lične podatke. To ga čini prijetnjom visoke ozbiljnosti.[39]

1.3 Ransomware

Ransomware je vrsta napada zlonamjernog softvera u kojem napadač zaključava i šifrira podatke žrtve, važne datoteke, a zatim zahtijeva plaćanje za otključavanje i dešifriranje podataka. Ova vrsta napada koristi prednosti ljudskih, sistemskih, mrežnih i softverskih ranjivosti kako bi zarazila žrtvin uređaj – koji može biti računar, štampač, pametni telefon, nosivi terminal, POS terminal ili druga krajnja tačka.

Primjeri ransomware virusa

Postoje hiljade vrsta ransomware malvera. U nastavku navodimo nekoliko primjera zlonamjernog softvera koji su imali globalni utjecaj i uzrokovali veliku štetu.

1.3.1 WannaCry

WannaCry je ulazni ransomware koji iskorištava ranjivost u Windows SMB protokolu, i ima mehanizam samoproširenja koji mu omogućava da zarazi druge mašine. WannaCry je upakovan kao dropper, samostalni program koji izdvaja aplikaciju za šifrovanje/dešifrovanje, datoteke koje sadrže ključeve za šifrovanje i Tor komunikacioni program. Nije zamućen i relativno ga je lako otkriti i ukloniti. U 2017. WannaCry se brzo proširio u 150 zemalja, pogađajući 230.000 računara i procjenjujući štetu od 4 milijarde dolara.

1.3.2 Cerber

Cerber je ransomware-as-a-service (RaaS) i dostupan je za korištenje cyber kriminalcima, koji izvode napade i šire svoj plijen s programerom zlonamjernog softvera. Cerber radi tiho dok šifrira datoteke i može pokušati spriječiti pokretanje antivirusnih i Windows sigurnosnih funkcija, kako bi spriječio korisnike da obnove sistem. Kada uspješno šifrira datoteke na mašini, prikazuje napomenu o otkupnini na pozadini radne površine.

1.3.3 Locky

Locky je u stanju da šifrira 160 tipova datoteka, prvenstveno datoteka koje koriste dizajneri, inženjeri i testeri. Prvi put je

[39] https://www.cisco.com/c/en/us/products/security/adware-vs-spyware.html#~how-adware-and-spyware-work – datum pristupa 27.12.2022.

objavljen 2016. godine. Prvenstveno se distribuira pomoću kompleta za eksploataciju ili krađe identiteta – napadači šalju e-poruke koje podstiču korisnika da otvori Microsoft Office Word ili Excel datoteku sa zlonamjernim makroima ili ZIP datoteku koja instalira zlonamjerni softver nakon ekstrakcije.

1.3.4 Cryptolocker

Cryptolocker je objavljen 2017. godine i zahvatio je preko 500.000 računara. Obično inficira računare putem e-pošte, stranica za dijeljenje datoteka i nezaštićenih preuzimanja. Ne samo da šifrira datoteke na lokalnom računalu, već može skenirati i mapirane mrežne diskove i šifrirati datoteke u koje ima dozvolu za pisanje. Nove varijante Crypolocker-a mogu izbjeći naslijeđeni antivirusni softver i firewall.

1.3.5 Petya i Not Petya

Petya je ransomware koji inficira mašinu i šifruje cijeli hard disk, pristupajući glavnoj tabeli datoteka (MFT). Ovo čini cijeli disk nepristupačnim, iako stvarne datoteke nisu šifrirane. Petya je prvi put viđena 2016. godine, a širila se uglavnom putem lažne poruke za prijavu za posao koja povezuje sa zaraženom datotekom pohranjenom u Dropboxu. To je uticalo samo na Windows računare. Petya zahtijeva od korisnika da pristane da mu da dozvolu za izmjene na nivou administratora. Nakon što se korisnik složi, ponovo pokreće računar, prikazuje lažni ekran pada sistema, dok počinje šifriranje diska iza scene. Zatim prikazuje obavijest o otkupnini. Originalni Petya virus nije bio vrlo uspješan, ali nova varijanta, nazvana NotPetya od strane Kaspersky Labsa, pokazala se opasnijom. NotPetya je opremljena mehanizmom razmnožavanja i može se širiti bez ljudske intervencije.

NotPetya se prvobitno širila koristeći backdoor u računovodstvenom softveru koji se široko koristi u Ukrajini, a kasnije je koristio EternalBlue i EternalRomance, ranjivosti u Windows SMB protokolu. NotPetya ne samo da šifrira MFT već i druge datoteke na hard disku. Dok šifrira podatke, oštećuje ih na takav način da se ne mogu oporaviti. Korisnici koji plate otkupninu zapravo ne mogu dobiti nazad svoje podatke.[40]

1.3.6 Ryuk

Ryuk inficira mašine putem phishing emailova ili preuzimanja. Koristi dropper, koji izdvaja trojanac na žrtvinoj mašini i uspostavlja stalnu mrežnu vezu. Napadači tada mogu koristiti Ryuk kao osnovu za naprednu trajnu prijetnju (APT), instalirajući dodatne alate kao što su keyloggeri, izvodeći eskalaciju privilegija i bočno kretanje. Ryuk je instaliran na svakom dodatnom sistemu kojem napadači dobiju pristup. Nakon što napadači instaliraju trojanac na što je moguće više mašina, aktiviraju ransomware ormarića i šifriraju datoteke. U napadnoj kampanji zasnovanoj na Ryuku, aspekt ransomware-a je samo posljednja faza napada, nakon što su napadači već napravili štetu i ukrali datoteke koje su im potrebne.

1.3.7 GrandCrab

GrandCrab je objavljen 2018. On šifrira datoteke na korisnikovoj mašini i zahtijeva otkupninu, a korišten je za pokretanje napada iznuđivanja zasnovanih na ransomware-u, gdje su napadači prijetili da će otkriti navike žrtava da gledaju pornografiju. Postoji nekoliko verzija, a sve su namjenjene Windows mašinama. Besplatni dekriptori su danas dostupni za većinu verzija GrandCrab-a.

[40] https://www.imperva.com/learn/application-security/ransomware/ - datum pristupa 03.01.2023.

1.4 Scareware

Scareware je zlonamjerni softver koji vara korisnike računara da posjete web stranice koje su zaražene zlonamjernim softverom. Također poznat kao softver za obmanu, lažni softver za skeniranje ili softver za prevaru, scareware može doći u obliku iskačućih prozora. Ovo se pojavljuje kao legitimna upozorenja kompanija za antivirusni softver i one tvrde da su datoteke vašeg računara zaražene. Toliko su pametno urađeni da se korisnici plaše da plate naknadu za brzu kupovinu softvera koji će riješiti problem tzv. Međutim, ono što na kraju preuzimaju je lažni antivirusni softver koji je zapravo zlonamjerni softver namijenjen krađi ličnih podataka žrtve. Prevaranti također koriste druge taktike, kao što je slanje neželjene pošte za distribuciju scarewarea. Jednom kada se taj e-mail otvori, žrtve se onda zavaravaju da kupuju bezvrijedne usluge. Nasjedanje na ove prevare i objavljivanje podataka o vašoj kreditnoj kartici otvara vrata za buduće zločine krađe identiteta. Scareware obično prati obrazac. Iskačući prozori vas iznenada upozoravaju da su na vašem računaru pronađene opasne datoteke ili pornografija i nastaviće da se pojavljuju sve dok ne kliknete na dugmad koja „uklanjaju sve pretnje“ ili se od vas ne zatraži da se registrujete za antivirusni softver. Pop-up prevare su dizajnirane da izgledaju kao prave poruke upozorenja. Koristeći taktiku društvenog inženjeringa, često se pojavljuju iskačući prozori zastrašujućih programa:[41]

- Imitiraju logotipe legitimnih antivirusnih programa i koristite imena koja zvuče slično;
- Prikazuju snimak ekrana "zaraženih" datoteka na vašem računaru;
- Prikazuju traku napretka koja pokazuje da se vaš računar "skenira";
- Sadrži trepereće crvene slike;
- Koristite VELIKA slova i uskličnike, uz upozorenja da djelujete brzo ili odmah.

1.5 Fišing (phishing)

Napadi krađe identiteta su lažna komunikacija za koju se čini da dolazi iz pouzdanog izvora, ali koja može ugroziti sve vrste izvora podataka.[42] Napadi mogu olakšati pristup vašim mrežnim nalozima i ličnim podacima, dobiti dozvole za modifikaciju i kompromitaciju povezanih sistema – kao što su terminali na prodajnim mjestima i sistemi za obradu narudžbi – i u nekim slučajevima oteti cijele računarske mreže dok se ne isporuči naknada za otkupninu. Ponekad su hakeri zadovoljni dobijanjem vaših ličnih podataka i informacija o kreditnoj kartici radi finansijske dobiti. U drugim slučajevima, phishing email poruke se šalju radi prikupljanja podataka za prijavu zaposlenika ili drugih detalja za korištenje u zlonamjernijim napadima na nekoliko pojedinaca ili određenu kompaniju. Phishing je vrsta cyber napada o kojoj bi svi trebali naučiti kako bi se zaštitili i osigurali sigurnost e-pošte u cijeloj organizaciji.

1.5.1 Kako phishing funkcioniše?

Phishing počinje lažnom email poštom ili drugom komunikacijom dizajniranom da namami žrtvu. Poruka je napravljena tako da izgleda kao da dolazi od pošiljaoca od povjerenja. Ako to zavara žrtvu, nju nagovaraju da daju povjerljive informacije - često na web stranici za prevare. Ponekad se zlonamjerni softver također preuzima na ciljni računar. Cyber kriminalci počinju tako što identifikuju grupu pojedinaca na koje žele da ciljaju. Zatim kreiraju email poštu i tekstualne poruke koje izgledaju kao legitimne, ali zapravo sadrže opasne

[41] https://usa.kaspersky.com/resource-center/definitions/scareware - datum pristupa 03.01.2023.

[42] https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~types-of-phishing-attacks – datum pristupa 27.12.2022.

linkove, priloge ili mamce koji navode njihove mete da poduzmu nepoznatu, rizičnu akciju. ukratko:

- Prevaranti često koriste emocije poput straha, radoznalosti, hitnosti i pohlepe kako bi natjerali primaoce da otvore priloge ili kliknu na linkove.
- Phishing napadi su dizajnirani da izgledaju kao da dolaze od legitimnih kompanija i pojedinaca.
- Cyber kriminalci kontinuirano inoviraju i postaju sve sofisticiraniji.
- Potreban je samo jedan uspješan phishing napad da bi se kompromitirala vaša mreža i ukrali vaši podaci, zbog čega je uvijek važno razmisliti prije nego što kliknete.

1.5.2 Vrste phishing napada

1.5.2.1 Spear phishing

Spear phishing cilja određene pojedince umjesto široke grupe ljudi. Na taj način napadači mogu prilagoditi svoju komunikaciju i izgledati autentičnije. Spear phishing je često prvi korak koji se koristi za prodor u odbranu kompanije i izvođenje ciljanog napada. Prema Institutu SANS, 95% svih napada na poslovne mreže rezultat je uspješnog phishinga.[43]

1.5.2.2 Microsoft 365 phishing

Metode koje koriste napadači za pristup Microsoft 365 nalogu email pošte prilično su jednostavne i postaju najčešće. Ove phishing kampanje obično imaju oblik lažne e-pošte od Microsofta. E-poruka sadrži zahtjev za prijavu, u kojem se navodi da korisnik treba da resetuje svoju lozinku, da se nije nedavno prijavio ili da postoji problem sa nalogom na koji treba obratiti pažnju. Uključen je URL koji mami korisnika da klikne kako bi riješio problem.

1.5.2.3 Kompromis poslovne e-pošte (BEC)

BEC je pažljivo planirani i istraženi napadi koji se lažno predstavljaju kao izvršni dobavljač ili dobavljač kompanije.

1.5.2.4 Lov na kitove

Kada napadači krenu na "veliku ribu" poput generalnog direktora, to se zove kitolov. Ovi napadači često provode dosta vremena na profilisanje cilja kako bi pronašli pogodan trenutak i sredstva za krađu akreditiva za prijavu. Lov na kitove je od posebnog značaja jer su rukovodioci na visokom nivou u mogućnosti da pristupe velikom broju osetljivih informacija kompanije.

1.5.2.5 Fiš na društvenim mrežama

Napadači često istražuju svoje žrtve na društvenim mrežama i drugim stranicama kako bi prikupili detaljne informacije, a zatim planiraju svoj napad u skladu s tim.

1.5.2.6 Voice phishing

Voice phishing ili "vising" je oblik društvenog inženjeringa. To je lažni telefonski poziv dizajniran za dobivanje osjetljivih informacija kao što su vjerodajnice za prijavu. Na primjer, napadač može nazvati pretvarajući se da je agent podrške ili predstavnik vaše kompanije. Novozaposleni su često ranjivi na ove vrste prevara, ali one se mogu dogoditi svakome - i postaju sve češće.

[43] https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~types-of-phishing-attacks – datum pristupa 27.12.2022.

2 TRI NIVOA ZAŠTITE OD CYBER NAPADA

U dosadašnjem istraživanju sigurnosti na internetu I zaštiti podataka, poznato je da samo antivirusni program nije dovoljan, ali postavlja se pitanje što ustvari organizacije trebaju poduzeti kako bi poboljšale svoju zaštitu. Kako bi dobile najveću vrijednost od sigurnosnih riješenja, organizacije se moraju fokusirati na glavne izvore rizika, odnosno tri nivoa zaštite.[44]

2.1 Zaštita korisnika od malicioznog sadržaja uz XDR: Od osobnog računara do emaila

Content zaštita pretpostavlja pravovremenu detekciju zlonamjernog sadržaja, automatsku korelaciju događaja i kontekstualizaciju detekcije – od endpoint računara do email saobraćaja. Umjesto individualnih detekcija, govorimo o novoj poboljšanoj tehnologiji – XDR (Extended Detection and Response) -koja pruža efikasan odgovor na današnje moderne prijetnje. XDR donosi automatizaciju i samim time olakšava analizu podataka.

Kad postoji sumnja na prijetnju, korisnik vrlo lako može pristupiti historijskoj listi događaja i saznati što je dovelo do uzbune. Istovremeno se eliminira potreba za pretragom log zapisa iz različitih izvora, štedi se vrijeme i dobiva se pravi uvid u rizike koji proizlaze iz pojedine detekcije (ili kombinacije detekcija) malicioznog sadržaja. Iako su XDR rješenja donedavno bila rezervirana samo za organizacije s "dubljim džepom", danas je XDR jednako dostupan i malim i srednjim preduzećima. Umjesto da se oslanjaju na klasični anti-virus, firme će uz XDR spojiti više proizvoda u jedinstven alat i značajno smanjiti rizike. Ovakvim se rješenjem jednostavno upravlja i automatski se eliminira potrebno vrijeme analize. XDR, uveliko olakšava analizu prijetnji u e-mail saobraćaju, na cjelokupnoj mreži, u cloud (oblak) infrastrukturi i, naravno, na samim endpoint računarima korisnika.

Rastom broja javno dostupnih pristupnih tačaka u organizaciju (VPN, SSL VPN, RDP…), ali i sve većim brojem as-a-service web aplikacija, rastu i prilike za ulaz napadača u organizaciju. Krađa identiteta je zato jedan od glavnih pravaca napada za dobivanje neovlaštenog pristupa IT sistemu. Potreba za udaljenim pristupom u toku COVID pandemije povećala je površinu napada mnogih organizacija. Pritom je posao napadača olakšan ako se koriste passwordi bez dodatnih provjera ili faktora (npr. certifikat, one time password, itd). Situaciju olakšava i ne korištenje upravljanih identiteta za pristup svim poslovnim aplikacijama.

Rješenja za upravljanje identitetima donose multi-faktorsku autentifikaciju i single sign-on (SSO). Od korisnika traže što manje oslanjanje na lozinke. Aplikacije trebaju biti dostupne s bilo kojeg mjesta, što je posebno došlo do izražaja tijekom pandemije. Njihovo korištenje pritom treba biti sigurno za organizaciju. Isto tako, administratori trebaju vidjeti ko je i kada pristupio kojoj aplikaciji. Rješenja za multi-faktorsku autentifikaciju smanjuju ulogu passworda, pa tako i neovlašten pristup računima i računarima.[45]

2.2 Edukacija zaposlenika o cyber prijetnjama

Zadnji nivo obrane organizacije od napada je zaposlenik. Naime, u mnogim se slučajevima sve svodi na to hoće li ili ne zaposlenik kliknuti na link ili na poslani prilog u e-mailu. Educiranost o napadima, posebno onima koji se isporučuju putem

[44] https://mreza.bug.hr/kako-se-zastititi-od-cyber-napada-u-tri-tocke/ - datum pristupa 29.12.2022.

[45] https://pcpress.rs/tri-nivoa-zastite-od-cyber-napada/ - datum pristupa 29.12.2022.

email pošte, ključna je u stvaranju otpornosti organizacije na proboje I na neovlaštene upade. Velike organizacije su tradicionalno ovakve probleme rješavale uz sistemsku edukaciju zaposlenika o sigurnosnim prijetnjama. Međutim, tradicionalne SAT (Security Awareness Training) inicijative podrazumijevaju dovoljno novca i vremena, a to su ograničeni resursi. I to napadači dobro znaju i iskorištavaju.

ZAKLJUČAK

U ovom radu prikazali smo detaljno šta je to cyber kriminal, koje su najzastupljenije vrste cyber kriminala. U prvom dijelu rada prikazana je I tablica sa brojem yber napada u svijetu, I vidjeli smo da mi kao država smo na 86. mjestu po broju napada koji se odvijaju na računarskim mrežama i podacima korisnika. Prikazani su problemi koje cyber napadi uzrokuju i vrste virusa koje hakeri koriste da bi došli do podataka I iznude novca kako bi te iste podatke vratili vlasniku. Također prikazana je jedna oj najjačih vrsta virusnog napada, to jest ransomware virus koji dovodi do totalnog uništenja podataka korisnika i zaključavanja svih datoteka.

Objašnjena su i tri nivoa zaštite od cyber napada. Sva tri nivoa su detaljno objašnjena i zaključeno je da samo jedan nivo zaštite nije sasvim dovoljan za potpunu sigurnost, nego da je potrebna kombinacija zaštita. I na kraju kao najvažnije od svega je da podignemo svjest kako zaposlenika, tako i ostalih korisnika interneta i digitalnih uređaja jer niko u potpunosti nije zaštićen.

LITERATURA

Knjige:

1) Mary Aiken (2017) -The Cyber Effect
2) Monnappa K A (2019) - Zaštita od zlonamernih programa (Malware analysis)
3) Erik Kol (2021) - Onlajn-opasnost kako zaštititi sebe i voljene od zle strane interneta
4) Bruce Schneier (2019) - DATA I GOLIJAT: nevidljivi rat za prikupljanje vaših podataka i kontrolu vašeg života
5) Alexey Kleymenov, Amr Thabet (2019) - Mastering Malware Analysis
6) Dr. Erdal Ozkaya (2019) - Cybersecurity: The Beginner's Guide
7) Victor Marak (2015) - Windows Malware Analysis Essentials

Internet stranice:

- https://seon.io
- https://virusi.hr
- https://www.cisco.com/c/en/us/products/security/adware-vs-spyware.html
- https://www.imperva.com
- https://usa.kaspersky.com/resource-center/definitions/scareware
- https://mreza.bug.hr
- https://pcpress.rs

1 CYBER ATTACK

Cyber crime is crime that is committed in cyber (computer) space and the world. Cyber criminal includes all actions that are not allowed in the "real world". This type of crime is growing the fastest of all types of crime due to the constant increase in the number of "innovative" forms of criminal actions that are committed using computers. In the beginning, cybercrime was a crime related only to the infection of a computer or system, but today cybercrime is one of the most serious types of crime, and the reason for this is that the entire society has moved to the digital sphere, that is, all business is conducted in a digital way. . According to the Global Report on Cybercrime conducted by the SEON company, BiH is at the very bottom of the security ranking, in the 86th position, out of a total of 94 countries included in this report.[46]

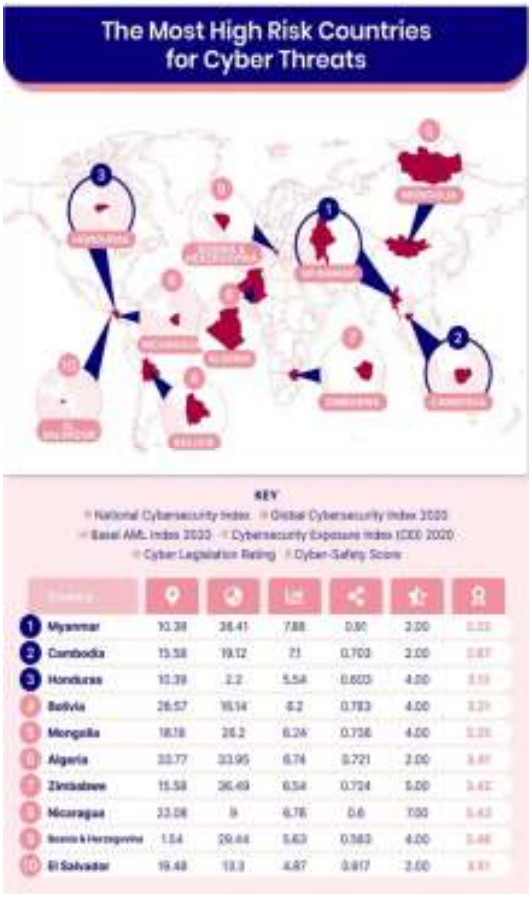


Figure 1.: Countries with the most cyber attacks
Source:https://seon.io/resources/global-cybercrime-report/

Cyber crime occurs in various forms, which aim to steal data, but also to cause great damage. Most often, a cyber attack is carried out through malicious programs (viruses or malware). These are malicious programs that cybercriminals use to access computers and thus cause great damage. All cyber attacks occur in the following forms:

1.1 Viruses/trojans

A Trojan virus or popularly known as a Trojan horse is a malicious virus program that is used to infect a computer system and perform malicious activities on it.

[46] Global Cybercrime Report: Which Countries Are Most at Risk? 2022 - SESSION- access date 29.12.2022.

Typically, a Trojan horse is used to steal personal data, spread other types of viruses, or simply put, to disrupt computer performance. In addition, hackers most often use them to gain remote access to the desired computer, infect certain files and cause damage to the system itself. As soon as the Trojan is inserted into the computer, it will start hiding from its victim. Trojans are very similar to real viruses and therefore very difficult to detect. Therefore, you should rely on the latest antivirus programs that are updated with the latest virus detection. In the beginning, when Trojans were created, they were not designed to spread independently over the Internet. However, newer versions of the Trojan horse have an additional component in them that can enable their very fast and imperceptible multiplication. The activity of each Trojan horse depends on the intentions of its author, that is, the hacker who inserted the Trojan horse into the system of the infected computer.[47]

Activities that can be caused by Trojans

- Infecting, corrupting and writing over already existing files, system components and installed applications. They can also destroy the entire system by deleting very important system files or even formatting the hard drive.
- Theft of financial data, such as credit card numbers, login data, passwords, valuable personal documents and other sensitive user information.
- Tracking the user and every keystroke the user makes on the keyboard. The Trojan can also take a "screenshot" and run some other activity to steal specific information.
- Sending all collected data to a predefined email address, uploading that data to a predefined FTP server or transferring it to a remote host with the help of a secondary Internet connection.
- Installing a backdoor or activating a proprietary component that will allow a remote attacker to take control of a compromised computer and system.
- Leaving and installing other parasites in the form of various hidden programs.
- Denial of Service (DoS) or other network attacks against remote hosts or sending excessive email messages to flood predefined computers with Internet traffic.
- Installing hidden FTP servers that can be used by malicious persons to achieve various illegal goals.
- Termination of the antivirus program. A Trojan horse can also disable system services and functions and thus prevent standard system tools from functioning normally.
- Blocking the user's access to web pages and search engines and sources where some possible solutions to security problems can be found.
- Showing unwanted commercial ads and pop-up ads.
- Degradation of Internet connection and computer speed. It can also reduce the security of the system and thus cause its instability.

1.2 Spyware/Adware

Adware is malicious software that automatically displays advertisements online to generate revenue for its author. Ads may appear in the user interface of the software, on the screen during the installation process or in the browser. Although adware is not always dangerous, in some cases it can be designed to analyze the websites you visit, present advertising content, install additional programs and redirect your browser to unsafe sites. It may even contain Trojan horses and spyware. Adware can be bundled with the software or game that the user wants. In many cases, during installation the package will access a

[47] https://virusi.hr/trojanci/- access date 29.12.2022.

third-party server that delivers the latest adware or plugin without touching the drive. Besides,

Spyware is spyware is malicious software code that secretly runs on a computer, collects information about a user and their browsing habits, and then transmits that information back to a remote entity. Instead of interfering with the device, spyware targets sensitive information and can give remote access to hackers. The purpose of spyware is to collect information about a person or organization without their knowledge and transmit that information to another entity for financial gain. Because of this, spyware is often used to steal financial or personal information. One specific type of spyware is a keylogger, which records a user's keystrokes to reveal passwords and other personal information. This makes it a high-severity threat.[48]

1.3 Ransomware

Ransomware is a type of malware attack where the attacker locks and encrypts the victim's data, important files, and then demands payment to unlock and decrypt the data. This type of attack takes advantage of human, system, network and software vulnerabilities to infect a victim's device – which could be a computer, printer, smartphone, wearable terminal, POS terminal or other endpoint.

Examples of ransomware viruses

There are thousands of types of ransomware malware. Below are a few examples of malware that have had a global impact and caused a lot of damage.

1.3.1 WannaCry

WannaCry is an inbound ransomware that exploits a vulnerability in the Windows SMB protocol, and has a self-expansion mechanism that allows it to infect other machines. WannaCry is packaged as a dropper, a standalone program that extracts an encryption/decryption application, files containing encryption keys, and the Tor communication program. It is not cloudy and is relatively easy to detect and remove. In 2017, WannaCry spread rapidly to 150 countries, affecting 230,000 computers and causing an estimated $4 billion in damage.

1.3.2 Cerberus

Cerber is a ransomware-as-a-service (RaaS) and is available for use by cybercriminals, who carry out attacks and spread their loot with the malware developer. Cerber runs silently while encrypting files and may try to prevent antivirus and Windows security features from starting, to prevent users from restoring the system. When it successfully encrypts files on the machine, it displays a ransom note on the desktop background.

1.3.3 Locky

Locky is able to encrypt 160 file types, primarily files used by designers, engineers and testers. It was first published in 2016. Primarily distributed using exploit or phishing kits – attackers send emails that prompt the user to open a Microsoft Office Word or Excel file with malicious macros or a ZIP file that installs malware after extraction.

1.3.4 Cryptolocker

Cryptolocker was released in 2017 and infected over 500,000 computers. It usually infects computers via email, file sharing sites, and unprotected downloads. It not only encrypts files on the local computer, but can also scan mapped network drives and encrypt files to which it has write

[48] https://www.cisco.com/c/en/us/products/security/adware-vs-spyware.html#~how-adware-and-spyware-work– access date 27.12.2022.

permission. New variants of Crypolocker can bypass legacy antivirus software and firewalls.

1.1.1. Petya and Not Petya

Petya is a ransomware that infects a machine and encrypts the entire hard drive, accessing the Master File Table (MFT). This makes the entire drive inaccessible, even though the actual files are not encrypted. Petya was first seen in 2016 and spread mainly through a fake job application message linking to an infected file stored in Dropbox. It only affected Windows computers. Petya requires the user to agree to grant him permission to make changes at the administrator level. After the user agrees, it restarts the computer, displays a fake system crash screen, while behind-the-scenes disk encryption begins. It then displays a ransom note. The original Petya virus was not very successful, but a new variant, dubbed NotPetya by Kaspersky Labs, has proven to be more dangerous.

NotPetya initially spread using a backdoor in accounting software widely used in Ukraine, and later exploited EternalBlue and EternalRomance, vulnerabilities in the Windows SMB protocol. NotPetya not only encrypts MFT but also other files on the hard drive. While encrypting data, it damages it in such a way that it cannot be recovered. Users who pay the ransom cannot actually get their data back.[49]

1.3.5 Ryuk

Ryuk infects machines via phishing emails or downloads. It uses a dropper, which extracts the Trojan on the victim's machine and establishes a persistent network connection. Attackers can then use Ryuk as the basis for an Advanced Persistent Threat (APT), installing additional tools such as keyloggers, performing privilege escalation and lateral movement. Ryuk is installed on every additional system that attackers gain access to. After the attackers install the Trojan on as many machines as possible, they activate the locker ransomware and encrypt the files. In a Ryuk-based attack campaign, the ransomware aspect is only the last stage of the attack, after the attackers have already done the damage and stolen the files they need.

1.3.6 GrandCrab

GrandCrab was released in 2018. It encrypts files on a user's machine and demands a ransom, and was used to launch ransomware-based extortion attacks, where attackers threatened to reveal victims' pornography viewing habits. There are several versions, all of which are intended for Windows machines. Free decryptors are available today for most versions of GrandCrab.

1.4 Scareware

Scareware is malware that tricks computer users into visiting websites that are infected with malware. Also known as scamware, fake scanware, or scamware, scareware can come in the form of pop-ups. These appear as legitimate warnings from antivirus software companies and they claim that your computer's files are infected. They are so cleverly done that users are afraid to pay a fee for the quick purchase of software that will solve the problem of the so-called. However, what they end up downloading is fake antivirus software that is actually malware designed to steal the victim's personal information. Scammers also use other tactics, such as spamming to distribute scareware. Once that email is opened, victims are then tricked into buying worthless services.

[49] https://www.imperva.com/learn/application-security/ransomware/- date of access 03.01.2023.

Falling for these scams and releasing your credit card information opens the door for future identity theft crimes. Scareware usually follows a pattern. Pop-ups suddenly warn you that dangerous files or pornography have been found on your computer and will continue to appear until you click the "remove all threats" buttons or you are asked to register for antivirus software. Pop-up scams are designed to look like real warning messages. Using social engineering tactics, scary program pop-ups often appear: Pop-ups suddenly warn you that dangerous files or pornography have been found on your computer and will continue to appear until you click the "remove all threats" buttons or you are asked to register for antivirus software. Pop-up scams are designed to look like real warning messages. Using social engineering tactics, scary program pop-ups often appear: Pop-ups suddenly warn you that dangerous files or pornography have been found on your computer and will continue to appear until you click the "remove all threats" buttons or you are asked to register for antivirus software. Pop-up scams are designed to look like real warning messages. Using social engineering tactics, scary program pop-ups often appear:[50]

- They mimic the logos of legitimate antivirus programs and use names that sound similar;
- They show a screenshot of the "infected" files on your computer
- They display a progress bar indicating that your computer is "scanning";
- Contains flashing red images
- Use CAPITAL letters and exclamation points, with warnings to act quickly or immediately.

1.5 Phishing (phishing)

Phishing attacks are fraudulent communications that appear to come from a trusted source, but can compromise all types of data sources.[51]Attacks can facilitate access to your online accounts and personal information, gain permissions to modify and compromise connected systems – such as point-of-sale terminals and order processing systems – and in some cases hijack entire computer networks until a ransom payment is delivered. Sometimes hackers are content to get your personal and credit card information for financial gain. In other cases, phishing emails are sent to collect employee login information or other details for use in more malicious attacks on a few individuals or a specific company. Phishing is a type of cyber attack that everyone should learn about in order to protect themselves and ensure email security throughout the organization.

1.5.1 How does phishing work?

Phishing begins with a fake email or other communication designed to lure the victim. The message is made to look like it's coming from a trusted sender. If this fools the victim, they are tricked into providing confidential information - often on a scam website. Sometimes malware is also downloaded to the target computer. Cybercriminals start by identifying a group of individuals they want to target. They then create email and text messages that look legitimate but actually contain dangerous links, attachments, or lures that trick their targets into taking an unknown, risky action. in short:

- Scammers often use emotions like fear, curiosity, urgency and greed to get

[50] https://usa.kaspersky.com/resource-center/definitions/scareware- date of access 03.01.2023.

[51] https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~types-of-phishing-attacks– access date 27.12.2022.

recipients to open attachments or click on links.

- Phishing attacks are designed to look like they are coming from legitimate companies and individuals.
- Cybercriminals are continuously innovating and becoming more sophisticated.
- It only takes one successful phishing attack to compromise your network and steal your data, which is why it's always important to think before you click.

1.5.2 Types of phishing attacks

1.5.2.1 Spear phishing

Spear phishing targets specific individuals instead of a broad group of people. In this way, attackers can tailor their communication and appear more authentic. Spear phishing is often the first step used to penetrate a company's defenses and launch a targeted attack. According to the SANS Institute, 95% of all attacks on business networks are the result of successful phishing.[52]

1.5.2.2 Microsoft 365 phishing

The methods used by attackers to gain access to a Microsoft 365 email account are quite simple and are becoming more common. These phishing campaigns usually take the form of fake emails from Microsoft. The email contains a login request, stating that the user needs to reset their password, hasn't logged in recently, or that there is an account issue that needs attention. A URL is included that entices the user to click to fix the problem.

1.5.2.3 Business Email Compromise (BEC)

BEC is a carefully planned and researched attack that impersonates an executive supplier or company supplier.

1.5.2.4 Whaling

When attackers go after "big fish" like a CEO, it's called whaling. These attackers often spend a lot of time profiling a target to find an opportune moment and means to steal login credentials. Whaling is of particular importance because high-level executives are able to access a large amount of sensitive company information.

1.5.2.5 Phish on social networks

Attackers often research their victims on social media and other sites to gather detailed information and then plan their attack accordingly.

1.5.2.6 Voice phishing

Voice phishing or "vising" is a form of social engineering. It is a fake phone call designed to obtain sensitive information such as login credentials. For example, an attacker may call pretending to be a support agent or a representative of your company. New hires are often vulnerable to these types of scams, but they can happen to anyone - and are becoming more common.

2 THREE LEVELS OF PROTECTION AGAINST CYBER ATTACKS

In the previous research on Internet security and data protection, it is known that an antivirus program alone is not enough, but the question arises as to what organizations should actually do to improve their

[52] https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~types-of-phishing-attacks– access date 27.12.2022.

protection. In order to get the most value from security solutions, organizations must focus on the main sources of risk, i.e. the three levels of protection.[53]

2.1 Protecting users from malicious content with XDR: From PC to email

Content protection assumes timely detection of malicious content, automatic correlation of events and contextualization of detection - from endpoint computers to email traffic. Instead of individual detections, we are talking about a new improved technology - XDR (Extended Detection and Response) - which provides an effective response to today's modern threats. XDR brings automation and thus facilitates data analysis. When a threat is suspected, the user can easily access the historical event list and find out what led to the alert. At the same time, the need to search log records from different sources is eliminated, time is saved and real insight into the risks arising from individual detection (or combination of detections) of malicious content is obtained. Although XDR solutions were until recently reserved only for organizations with "deeper pockets", today, XDR is equally accessible to small and medium-sized enterprises. Instead of relying on classic anti-virus, with XDR, companies will combine multiple products into a single tool and significantly reduce risks. Such a solution is easy to manage and automatically eliminates the required analysis time. XDR greatly facilitates the analysis of threats in e-mail traffic, on the entire network, in the cloud infrastructure and, of course, on the users' endpoint computers themselves.

2.2 Identity management

With the growth of the number of publicly available access points to the organization (VPN, SSL VPN, RDP...), but also with the increasing number of as-a-service web applications, the opportunities for attackers to enter the organization also increase. Identity theft is therefore one of the main lines of attack for gaining unauthorized access to the IT system. The need for remote access during the COVID pandemic has increased the attack surface of many organizations. At the same time, the attacker's job is made easier if passwords are used without additional checks or factors (eg certificate, one time password, etc.). The situation is made easier by not using managed identities to access all business applications.

Identity management solutions bring multi-factor authentication and single sign-on (SSO). They ask users to rely as little as possible on passwords. Applications should be accessible from anywhere, which was especially evident during the pandemic. Their use should be safe for the organization. Likewise, administrators need to see who accessed which application and when. Solutions for multi-factor authentication reduce the role of passwords and therefore unauthorized access to accounts and computers.[54]

2.3 Educating employees about cyber threats

The last level of organization's defense against attack is the employee. Namely, in many cases it all comes down to whether or not the employee will click on the link or on the attachment sent in the e-mail. Being educated about attacks, especially those delivered via email, is key to making an organization resilient to breaches and intrusions. Large organizations have traditionally solved such problems with systematic employee education about security threats. However, traditional SAT (Security Awareness Training) initiatives

[53] https://mreza.bug.hr/kako-se-zastititi-od-cyber-napada-u-tri-tocke/- access date 29.12.2022.

[54] https://pcpress.rs/tri-nivoa-zastite-od-cyber-napada/- access date 29.12.2022.

require sufficient money and time, which are limited resources. Attackers know this well and take advantage of it

CONCLUSION

In this paper, we have shown in detail what cybercrime is, what are the most common types of cybercrime. In the first part of the work, a table with the number of cyber attacks in the world was presented, and we saw that we as a country are in 86th place in terms of the number of attacks that take place on computer networks and user data. The problems caused by cyber attacks and the types of viruses that hackers use to access data and extort money in order to return the same data to the owner are shown. Also shown is one of the strongest types of virus attack, a ransomware virus that leads to total destruction of user data and locking of all files. The three levels of protection against cyber attacks are also explained. All three levels are explained in detail and it was concluded that only one level of protection is not quite enough for complete security, but that a combination of protection is needed. And finally, the most important thing is to raise the awareness of both employees and other users of the Internet and digital devices, because no one is completely protected.

LITERATURE

Books:

1) Mary Aiken (2017) - The Cyber Effect
2) Monnappa KA (2019) - Protection against malicious programs (Malware analysis)
3) Eric Cole (2021) - Online danger how to protect yourself and loved ones from the evil side of the Internet
4) Bruce Schneier (2019) - DATA AND GOLIATH: The Invisible War to Collect Your Data and Control Your Life
5) Alexey Kleymenov, Amr Thabet (2019) - Mastering Malware Analysis
6) dr. Erdal Ozkaya (2019) - Cybersecurity: The Beginner's Guide
7) Victor Marak (2015) - Windows Malware Analysis Essentials

Websites:

- https://seon.io
- https://virusi.hr
- https://www.cisco.com/c/en/us/products/security/adware-vs-spyware.html
- https://www.imperva.com
- https://usa.kaspersky.com/resource-center/definitions/scareware
- https://mreza.bug.hr
- https://pcpress.rs