ANALIZA INFORMACIJSKIH PRIJETNJI U MOBILNIM UREĐAJIMA I APLIKACIJAMA

Zovkić, Anita

Sveučilište Josipa Jurja Strossmayera u Osijeku
Ekonomski fakultet u Osijeku
Sveučilišni prijediplomski studij Poslovna informatika

Anita Zovkić

ANALIZA INFORMACIJSKIH PRIJETNJI U MOBILNIM UREĐAJIMA I APLIKACIJAMA

Završni rad

Osijek, 2023.

Sveučilište Josipa Jurja Strossmayera u Osijeku
Ekonomski fakultet u Osijeku
Sveučilišni prijediplomski studij Poslovna informatika

Anita Zovkić

ANALIZA INFORMACIJSKIH PRIJETNJI U MOBILNIM UREĐAJIMA I APLIKACIJAMA

Završni rad

Kolegij: Upravljanje informacijskim resursima

JMBAG: 0149228421
e-mail: azovkic@efos.hr

Mentor: doc. dr. sc. Dario Šebalj

Osijek, 2023.

Josip Juraj Strossmayer University of Osijek
Faculty of Economics and Business in Osijek
Undergraduate Study Business informatics

Anita Zovkić

ANALYSIS OF INFORMATION THREATS IN MOBILE DEVICES AND APPLICATIONS

Final paper

Osijek, 2023.

IZJAVA

O AKADEMSKOJ ČESTITOSTI, PRAVU PRIJENOSA INTELEKTUALNOG VLASNIŠTVA, SUGLASNOSTI ZA OBJAVU U INSTITUCIJSKIM REPOZITORIJIMA I ISTOVJETNOSTI DIGITALNE I TISKANE VERZIJE RADA

1. Kojom izjavljujem i svojim potpisom potvrđujem da je završni (navesti vrstu rada: završni / diplomski / specijalistički / doktorski) rad isključivo rezultat osobnoga rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu. Potvrđujem poštivanje nepovredivosti autorstva te točno citiranje radova drugih autora i referiranje na njih.
2. Kojom izjavljujem da je Ekonomski fakultet u Osijeku, bez naknade u vremenski i teritorijalno neograničenom opsegu, nositelj svih prava intelektualnoga vlasništva u odnosu na navedeni rad pod licencom *Creative Commons Imenovanje – Nekomercijalno – Dijeli pod istim uvjetima 3.0 Hrvatska.* 
3. Kojom izjavljujem da sam suglasan/suglasna da se trajno pohrani i objavi moj rad u institucijskom digitalnom repozitoriju Ekonomskoga fakulteta u Osijeku, repozitoriju Sveučilišta Josipa Jurja Strossmayera u Osijeku te javno dostupnom repozitoriju Nacionalne i sveučilišne knjižnice u Zagrebu (u skladu s odredbama Zakona o visokom obrazovanju i znanstvenoj djelatnosti, NN 119/2022).
4. izjavljujem da sam autor/autorica predanog rada i da je sadržaj predane elektroničke datoteke u potpunosti istovjetan sa dovršenom tiskanom verzijom rada predanom u svrhu obrane istog.

Ime i prezime studenta/studentice: Anita Žovkić

JMBAG: 0149228421

OIB: 44715398764

e-mail za kontakt: azovkic@efos.hr.

Naziv studija: Prijediplomski sveučilišni studij Poslovna informatika

Naslov rada: Analiza informacijskih prijetnji u mobilnim uređajima i aplikacijama

Mentor/mentorica rada: doc. dr. sc. Dario Šebalj

U Osijeku, 10. 07. 2023. godine

Potpis Anita Žovkić

Analiza informacijskih prijetnji u mobilnim uređajima i aplikacijama

SAŽETAK

Postizanje informacijske sigurnosti ključan je aspekt svakog informacijskog sustava, a očituje se kroz zaštitu osnovnih elemenata informacijske sigurnosti: povjerljivost, integritet i dostupnost. Napretkom mobilne tehnologije i aplikacija sve više se razvijaju prijetnje te se vrši povreda navedenih elemenata informacijske sigurnosti. Povrede uzrokuju maliciozni napadači koji se javljaju u raznim oblicima poput *malware*-a, hakerskih, fizičkih i APT napada. Rad pruža uvid u pojedinu vrstu informacijske prijetnje te njihov utjecaj na sigurnost sustava. Postoji i mnoštvo vrsta *malware*-a, a neki od najčešćih su virusi, trojanski konji, crvi i *spyware*. O svakoj vrsti napada napisano je nekoliko rečenica ne bi li se dobio sveobuhvatan dojam o rizicima i štetnim posljedicama koje se stvaraju prilikom zaraze uređaja od ovakvih vrsta napada. Budući da je tema rada bazirana na sustave mobilnih uređaja i aplikacija, nakon istraživanja brojne literature, izvršena je analiza malicioznih napada na Android i iOS uređaje. Analizom se došlo do zaključka kako mobilni operativni sustavi pružaju visoku razinu zaštite sustava, ali i njihovih korisnika. U radu se također nalaze mjere zaštite uređaja od malicioznih napada, a provode se u slučaju već nastale zaraze ili prevencije od zlonamjernih napada. Pravilna analiza, identifikacija ranjivosti sustava, ali i pridržavanje i primjena odgovarajućih sigurnosnih mjera smanjuje rizik od potencijalnih napada i omogućuje korisnicima da očuvaju svoju sigurnost i privatnost u mobilnom okruženju.

Ključne riječi: informacijska sigurnost, maliciozni napadi, *malware*, ranjivost sustava, sigurnosne mjere

Analysis of information threats in mobile devices and applications

ABSTRACT

Achieving information security is a key aspect of any information system, and is manifested in the protection of the basic elements of information security: confidentiality, integrity and availability. With the progress of mobile technology and applications, more and more threats are developing, and the aforementioned elements of information security are being breached. Breaches are caused by malicious attackers that come in various forms such as malware, hacking, physical and APT attacks. This final paper provides insight into a particular type of information threat and itsimpact on system security. There are many types of malware, and some of the most common are viruses, Trojan horses, worms and spyware. A few sentences have been written about each type of attack in order to get a comprehensive impression of the risks and harmful consequences that occur when a device is infected by these types of attacks. Since the topic of the work is based on mobile device systems and applications, after researching a lot of literature, an analysis of malicious attacks on Android and iOS devices was performed. The analysis led to the conclusion that mobile operating systems provide a high level of protection for the system, as well as for their users. The final paper also includes measures to protect the device from malicious attacks, which are implemented in case of an existing infection or to prevent malicious attacks. Proper analysis, identification of system vulnerabilities, but also compliance and application of appropriate security measures will reduce the risk of potential attacks and allow users to preserve their security and privacy in the mobile environment.

Keywords: information security, malicious attacks, malware, system vulnerability, security protection

Sadržaj

1. Uvod

S porastom popularnosti korištenja mobilnih uređaja, povećani su i rizici vezani uz sigurnost korištenja samih uređaja te usluga i aplikacija koje nude. Maliciozni napadi u mobilnim uređajima i aplikacijama postali su ozbiljna prijetnja privatnosti i sigurnosti, kako uređajima, tako i njihovim korisnicima. Napadači koriste razne tehnike kako bi iskoristili ranjivost u mobilnim operativnim sustavima te postigli ciljeve vezane uz krađu osobnih i financijskih podataka te preuzeli kontrolu nad uređajima. *Malware*, jedna od zastupljenijih vrsta informacijskih prijetnji, zlоćudni je softver koji uzrokuje povredu informacijskog sustava. Osim ove vrste, u radu su opisani su drugi oblici informacijskih prijetnji, poput hakerskih napada, fizičkih napada, društvenog inženjeringa i APT napada. Obuhvaćene su i metode samih napada koje se svrstavaju u četiri skupine: napadi prekidanjem/presijecanjem, napadi presretanjem, napadi izmjenom i napadi proizvodnjom. Rad detaljno opisuje i pojam informacijske sigurnosti i ističe važnost razumijevanja samog koncepta i primjene odgovarajućih sigurnosnih mjera u borbi protiv zlonamjernih napada informacijske sigurnosti. Pružen je i uvid u elemente informacijske sigurnosti koji se nastoje zaštititi primjenom sigurnosnih politika. Uzimajući u obzir rapidan razvoj tehnologije i kontinuirano povećanje korištenja mobilnih uređaja, analiza malicioznih napada na uređaje i aplikacije postaje od iznimne važnosti. Ona uključuje istraživanje sigurnosnih propusta, prepoznavanje potencijalnih prijetnji i razvoj mjera zaštite mobilnih operativnih sustava. Proučavane su razne vrste *malware*-a uključujući viruse, trojanske konje, crve i *spyware*. Istraženo je na koji način funkcioniraju te koje štetne posljedice uzrokuju. Neprestano se naglašava potreba za pravilnim korištenjem mobilnih usluga u svrhu sprječavanja malicioznih napada, stoga su detaljnije istražene vrste informacijskih prijetnji te analizirani maliciozni napadi na dvije skupine uređaja – Android i iOS. Dani su primjeri zlonamjernih aplikacija koje uzrokuju povredu sigurnosti operativnog sustava. Također, razmotrene su i sigurnosne mjere i tehnike koje se odnose na zaštitu mobilnih operativnih sustava od prijetnji. Korisnici mobilnih uređaja i usluga koje pružaju moraju biti svjesni težine sigurnosnih rizika i na vrijeme poduzimati mjere zaštite. S druge strane, industrija mobilnih uređaja treba nastaviti ulagati u razvoj sigurnosnih mehanizama kako bi svojim korisnicima omogućila sigurno i pozitivno iskustvo korištenja uređaja.

2. Teorijska podloga i prethodna istraživanja

Informacijske prijetnje predstavljaju izrazit problem u današnjem digitalnom svijetu. Budući da su mobilni uređaji postali dio svakodnevnice, a aplikacije primarni oblik interakcije, neminovna je prisutnost sve većeg broja malicioznih napada na sigurnost informacijskog sustav. Glavna zadaća informacijskog sustava je postizanje i održavanje informacijske sigurnosti u okviru integriteta, dostupnosti i povjerljivosti podataka. Istraživanja u ovom području pružaju bolje razumijevanje ranjivosti mobilnih uređaja i aplikacija što uvelike može doprinijeti u stvaranju sigurnijeg mobilnog sustava.

2.1. Informacijska sigurnost

Informacijska sigurnost u mobilnim uređajima i aplikacijama je vrlo važan aspekt čija pojavnost postaje sve češća u digitalnom svijetu. Porastom upotrebe mobilnih uređaja i aplikacija povećava se i broj informacija, ali i osobnih podataka koji se prenose tim kanalima. Stoga, od iznimne važnosti je razumjeti koncept informacijske sigurnosti te primijeniti odgovarajuće mjere zaštite u borbi od potencijalnih informacijskih prijetnji. Informacijska sigurnost podrazumijeva zaštitu informacija/podataka od neovlaštenog pristupa, upotrebe, otkrivanja te naposlijetku uništenja istih. Postoji širok spektar mjera koje se primjenjuju kako bi se osigurali elementi informacijske sigurnosti: povjerljivost, integritet i dostupnost podataka (Whitman i Mattord, 2021). U kontekstu mobilnih uređaja i aplikacija, informacijska sigurnost obuhvaća zaštitu osobnih podataka na samim uređajima te sigurnost aplikacija koje se koriste na istim. Mobilni uređaji često sadrže osjetljive informacije poput bankovnih podataka, lozinki, privatnih fotografija i sl. Napadi u vidu krađe identiteta i zlonamjernih aplikacija ugrožavaju navedene podatke što može stvoriti ozbiljne posljedice za korisnike. Stoga, naglašava se potreba za razvojem i implementacijom sigurnih aplikacija. Gerić i Hutinski (2007) daju preporuke za osiguravanje informacijske sigurnosti u mobilnom okruženju. Jedna od njih je korištenje hibridnog modela pod nazivom model klasifikacije sigurnosnih prijetnji informacijskih sustava (engl. *Information system security threat cube classification*) ili C^3 model koji se ističe po fleksibilnosti i dinamičnosti. Nadalje, Zakon o informacijskoj sigurnosti (NN 79/07) definira zakonski okvir za zaštitu informacija u Republici Hrvatskoj. Za implementaciju sigurnosnih mjera u mobilne uređaje i aplikacije ključno je razumijevanje zakonskih propisa i postupaka upravljanja sigurnošću podataka. Informacijska sigurnost, razumijevanje informacijskih prijetnji i implementacija sigurnosnih protokola ključni su aspekti prilikom zaštite podataka i osiguranja privatnosti podataka.

2.2. Elementi informacijske sigurnosti

Svaki informacijski sustav ima jedan glavni cilj - postizanje informacijske sigurnosti. Postoje tri ključna elementa koja se nastoje zaštititi sigurnosnim politikama: povjerljivost, integritet i dostupnost (Pachghare, 2019). Govoreći o prijetnjama informacijske sigurnosti, naglasak je na narušavanju povjerljivosti informacija, neovlaštenim promjenama i gubitku dostupnosti podacima. Na slici 1 vidljivo je kako su sve tri komponente međusobno povezane te zajedno čine cjelovit sigurnosni okvir za zaštitu informacija.

Slika 1. Elementi informacijske sigurnosti
Izvor: Tyson (2019)

2.2.1. Povjerljivost

Povjerljivost (engl. *Confidentiality)* podrazumijeva zaštitu podataka od neovlaštenog pristupa, korištenja i otkrivanja od strane nepoželjnih osoba. Orijentirana je ka identifikaciji i autentifikaciji korisnika te se primjenjuje na sve vrste podataka: osobne, financijske, poslovne i dr. informacije. Ukoliko se povjerljivim informacijama ne pristupa pravilno, vrlo lako može doći do povrede povjerljivosti. Najčešći oblici prijetnje povjerljivim informacijama su: napadači, lažno predstavljanje, hakiranje, trojanski konji, neovlaštena aktivnost i sl. Upravo zbog navedenih prijetnja, postoji nekoliko metoda zaštite povjerljivosti podataka. Dvije najzastupljenije metode su kontrola pristupa i enkripcija. Kontrola pristupa je metoda kojom se ograničava pristup podacima neovlaštenim osobama, dok ovlaštene osobe imaju određenu razinu pristupa podacima ovisno o aktivnostima i ulogama koje izvršavaju. Enkripcija je kriptografska tehnika koja se koristi u svrhu šifriranja podataka radi osiguranja povjerljivosti

prilikom prijenosa ili pohrane. Podrazumijeva pretvaranje podataka u nečitljiv oblik koji je moguće dešifrirati isključivo pomoću odgovarajućeg ključa (CARNet CERT, 2009:14; Pachghare, 2019:2-5).

2.2.2. Integritet

Glavni cilj integriteta (engl. *Integrity*) je očuvanje cjelovitosti, točnosti i ispravnosti podataka tijekom njihovog prijenosa, obrade i pohrane. Pod tim se podrazumijeva sprječavanje namjernih ili nenamjernih izmjena, brisanja i oštećenja podataka. Integritet podataka ključan je za pouzdanost i povjerenje u informacijske sustave. Kako ne bi došlo do narušavanja integriteta, koji može uzrokovati niz ozbiljnih posljedica poput kršenja privatnosti i financijskih gubitaka, preporuča se korištenje nekih od metoda očuvanja integriteta. Korištenjem kriptografskih funkcija i primjenom pravila pristupa sprječava se neovlašteno mijenjanje i brisanje podataka kao i njihov trajni gubitak (CARNet CERT, 2009:14; Pachghare, 2019:2-5).

2.2.3. Dostupnost

Dostupnost (engl. *Availability*), ujedno i treći element informacijske sigurnosti, osigurava upravo dostupnost podataka ovlaštenim korisnicima onda kada im zatrebaju. Također, podrazumijeva se održavanje pouzdanosti podataka te zaštitu od potencijalnih prijetnji koji mogu ograničiti pristup ili pak onemogućiti pravilno funkcioniranje informacijskih sustava. Poput povjerljivosti i integriteta, i za ovaj aspekt informacijske sigurnosti postoji niz metoda i tehnika u svrhu osiguranja dostupnosti podacima. Mrežna sigurnost obuhvaća niz mjera koje se provode kako bi se osigurala sigurnost mrežnih sustava, a obuhvaća enkripciju podataka i zaštite od napadača zbog kojih dostupnost postaje upitna (npr. DoS[1] napadi, zlonamjerni softveri, nemogućnost obrade podataka) (CARNet CERT, 2009:14; Pachghare, 2019:2-5) .

2.3. Informacijske prijetnje

Prijetnje informacijskoj sigurnosti uključuju širok spektar zlonamjernih aktivnosti usmjerenih na ugrožavanje ranije navedenih povjerljivosti, integriteta i dostupnosti informacijama i podacima. Budući da prijetnje mogu potjecati iz različitih izvora, moguće ih je kategorizirati u četiri skupine: prirodne prijetnje, namjerne prijetnje, nenamjerne prijetnje i oprema. Napredak

[1] DoS *(*engl*. Denial of Service)* – napad uskraćivanja usluga

tehnologije neizbježno povlači za sobom potrebu za implementiranjem sigurnosnih mjera u svrhu zaštite od prijetnji informacijskoj sigurnosti. Zaštita od prijetnji može se provesti kroz upotrebu jakih lozinki, korištenje antivirusnih programa, redovno ažuriranje softvera i drugih sličnih mjera (Pfleeger i sur., 2015; Uskok, 2021).

2.3.1. Izvori informacijskih prijetnji

Prirodne prijetnje imaju izrazit utjecaj na informacijsku sigurnost, unatoč većem fokusu na tehničke i ljudske prijetnje. Neki od primjera ovog izvora prijetnji su (Jouini i sur., 2014; Gudac, 2019).:

- Požari – izazivaju fizičku povredu podatkovnih centara i računalnih sustava. Ukoliko se ne poduzmu adekvatne mjere zaštite, moguć je gubitak podataka, oštećenje sustava i prekid rada sustava.
- Poplave – poplave također uzrokuju štete računalnih sustava. Voda uništava elektroničke uređaje te uzrokuje prekid rada.
- Potresi – loše konstruirana oprema može biti osjetljiva na ovu prirodnu katastrofu. Oštećenje zgrada uzrokovano potresom ima negativan utjecaj na rad računalnih sustava i samu infrastrukturu.
- Oluje i munje – uzrokuju oštećenje električne mreže te elektroničke uređaje, uključujući servere, opremu i računalne sustave. Ova prijetnja najčešće uzrokuje prekide u pristupu internetu, gubitak komunikacije, ali i prekid rada sustava te trajni gubitak podataka

Namjerne prijetnje – najčešći su oblik informacijskih prijetnji. Dijele se na hakerske i fizičke napade, društveni inženjering te *malware* (Jouini i sur., 2014; Gudac, 2019). U sljedećim poglavljima je detaljnije opisana svaka od četiri navedene vrste informacijskih prijetnji.

U **nenamjerne prijetnje** se ubrajaju (Jouini i sur., 2014; Gudac, 2019):

- Ljudske pogreške – greške zaposlenika poput neopreznog rukovanja podacima ili slanja osjetljivih informacija na krivu adresu e-pošte.
- Hardverski kvarovi – obuhvaćaju kvarove računalne opreme (npr. tvrdi disk) koji najčešće dovode do privremenog prekida rada sustava.
- Softverski *bug*-ovi – greške u softveru koje omogućuju neovlašten pristup podacima.
- Tehnički kvarovi – odnose se na poteškoće prilikom napajanja ili mrežnog povezivanja.

Oprema može predstavljati ozbiljnu prijetnju informacijskoj sigurnosti ukoliko nije zaštićena ili se ne upotrebljava na pravilan način. Pod to spadaju (Jouini i sur., 2014; Gudac, 2019):

- Računalni virusi – prijenosna računala, mobilni uređaji, tableti mogu biti zaraženi virusom koji uzrokuje krađu osobnih podataka i preuzima kontrolu nad uređajem.
- Mrežna oprema – mrežni uređaji poput prekidača i usmjerivača ranjivi su na napade, a napadači koriste njihove propuste za preusmjeravanje na zlonamjerne web stranice.
- Prijenosni uređaji – pametni telefoni, tableti i prijenosna računala nerijetko budu izgubljeni ili ukradeni, što omogućava napadačima neovlašten pristup podacima. Ukoliko navedeni uređaji nisu zaštićeni autentifikacijskim metodama (lozinke, biometrija), uređaji mogu biti kompromitirani.
- Fizička sigurnost – oprema poput poslužitelja mora biti smještena u sigurnim prostorijama kako bi se izbjegla krađa uređaja od strane neovlaštene osobe.

Kako bi se smanjio utjecaj navedenih izvora informacijskih prijetnji, preporuča se poduzimanje raznih mjera: sigurna lokacija podatkovnih centara, izrada sigurnosnih kopija podataka, korištenje zaštitnih mjera u slučaju izbijanja požara, upotreba antivirusnih programa te edukacija korisnika o prepoznavanju potencijalnih prijetnji informacijskoj sigurnosti (Jouini i sur., 2014).

2.3.2. Vrste informacijskih prijetnji

Neke od najčešćih vrsta informacijskih prijetnji sigurnosti su:

Malware – maliciozni softver poput virusa, crva, trojanskih konja i ostalih zlonamjernih programa namijenjenih krađi i uništavanju podataka. Obično se infiltriraju u sustav putem zaraženih web stranica, e-pošte i USB uređaja te uzrokuju brisanje i trajno oštećenje podataka. Detaljnije o malicioznim napadima, konkretno na mobilne uređaje i aplikacije je razrađeno u daljnjim poglavljima ovoga rada (Sikorski i Honig, 2012).

Hakerski napadi – predstavljaju ozbiljne prijetnje informacijskoj sigurnosti. Hakeri koriste svoje tehničke vještine kako bi neovlašteno pristupili računalnim sustavima i ukrali osjetljive podatke i onesposobili sustave (Kumar, 2018).

Društveni inženjering – metoda manipulacije ljudskim ponašanjem s ciljem dobivanja osjetljivih informacija poput lozinke, korisnička imena i financijski podaci. Koriste se raznim metodama kako bi postigli određene ciljeve (Salahdine, 2019).

Fizički napadi – metoda napada koja zahtijeva fizički pristup računalnim sustavima i mrežama u svrhu ometanja i narušavanja njihove funkcionalnosti i integriteta, ali i krađe samih uređaja. Informacijske prijetnje također mogu izazvati požari ili prirodne katastrofe koje pripadaju skupini fizičkih rizika od gubitka informacijskih uređaja, pa i cjelokupnog sustava (Zhang, 2021).

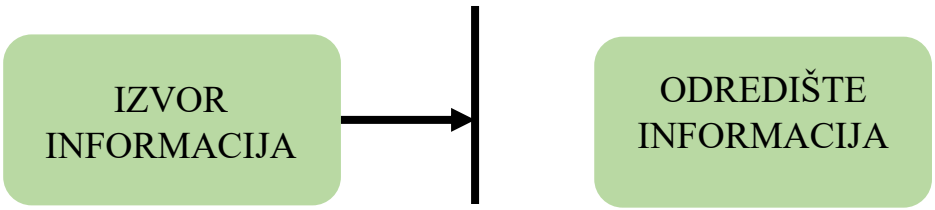
APT *(*engl. *Advanced Persistent Threat)* – sofisticirani, organizirani i dugotrajni napadi koje provode dobro obučene, financirane, organizirane i sposobne skupine ljudi. Vrlo složeni napadi koji zahtijevaju korištenje napredne tehnike u svrhu krađe i pristupa osjetljivim informacijama poput korisničkih podataka i poslovnih tajni (Ahmad, 2019).

2.3.3. Metode napada

Napad se definira kao pokušaj, akcija neovlaštene osobe usmjerena na ugrožavanje i povredu sigurnosti informacijskog sustava (Uskok, 2021).

U nastavku su objašnjene kategorije metoda napada.

Napadi prekidanjem/presijecanjem – metoda prekidanja ili onesposobljenja normalnog funkcioniranja sustava ili usluge između dva korisnika na privremenoj ili trajnoj osnovi. Nerijetko utječu na dostupnost i integritet podataka (Andress, 2014).

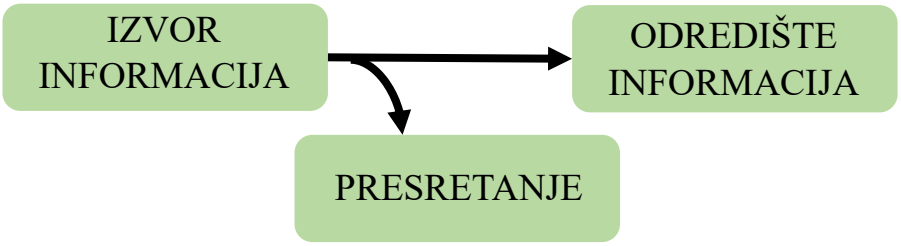


Slika 2. Metoda napada prekidanjem/presijecanjem

Izvor: Izrada autorice prema Uskok (2021)

Slika 2 pruža uvid u prekidanje izvorne informacije do njezinog odredišta od strane napadača. Jednom kada napadač pristupi korisničkoj mreži ima niz mogućnosti koje pospješuju nestabilnost rada sustava: skrivanje identiteta, slanje štetnih podataka aplikacijama, blokiranje prometa mrežnim resursima i dr. (Uskok, 2021).

Napadi presretanjem – primarno se definiraju kao napadi na osjetljivost. Presretanje se javlja u obliku neovlaštenog pristupa podacima, komunikaciji između dvije osobe (npr. telefonski razgovori i SMS poruke) i kopiranja datoteka (Andress, 2014).

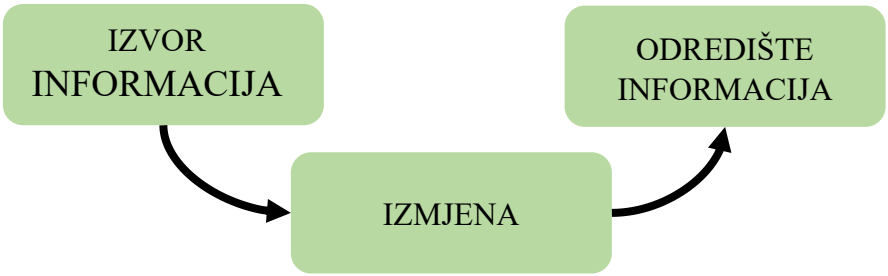


Slika 3. Metoda napada presretanjem

Izvor: Izrada autorice prema Uskok (2021)

Prema slici 3, vidljivo je kako se napadač ubacuje (presreće) u komunikaciju između dva korisnika. Podatke koje je uspio dobiti ovom metodom napada prikuplja u računalu te se lažno predstavlja kao sudionik razgovora ne bi li dobio što više korisnih informacija (Uskok, 2021).

Napadi izmjenom – predstavlja aktivan napad na integritet podataka. Metoda napada izmjenom odnosi se na manipulaciju sadržajem podataka, česta je kod novčanih transakcija. Napadač koristi ranjivost informacijskog sustava kako bi izmjene ostale neprimjetne (Andress, 2014; Uskok, 2021).



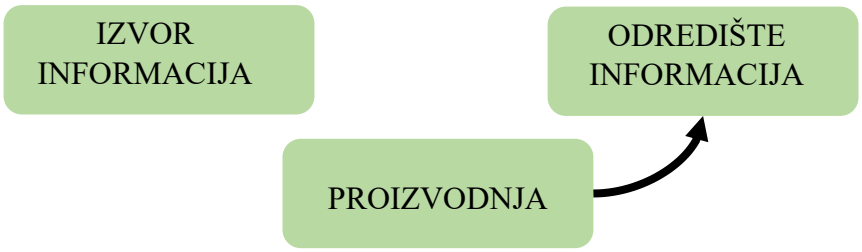
Slika 4. Metoda napada izmjenom

Izvor: Izrada autorice prema Uskok (2021)

Slika 4 prikazuje napadačevu izmjenu informacija bez korisnikova znanja koja se odvija između izvora i odredišta. Često se prilikom ove metode napada dobiju netočne i neispravne informacije koje mogu loše utjecati na poslovanje poduzeća (Uskok, 2021).

Napadi proizvodnjom – metoda napada prilikom kojeg napadač stvara lažne podatke ili poruke te ih ubacuje u sustav ili komunikaciju. Primaran utjecaj ima na integritet, ali i

dostupnost podataka. Primjeri ovog tipa napada su generiranje lažnih transakcija, stvaranje lažnih identiteta i sl. (Andress, 2014).



Slika 5. Metoda napada proizvodnjom

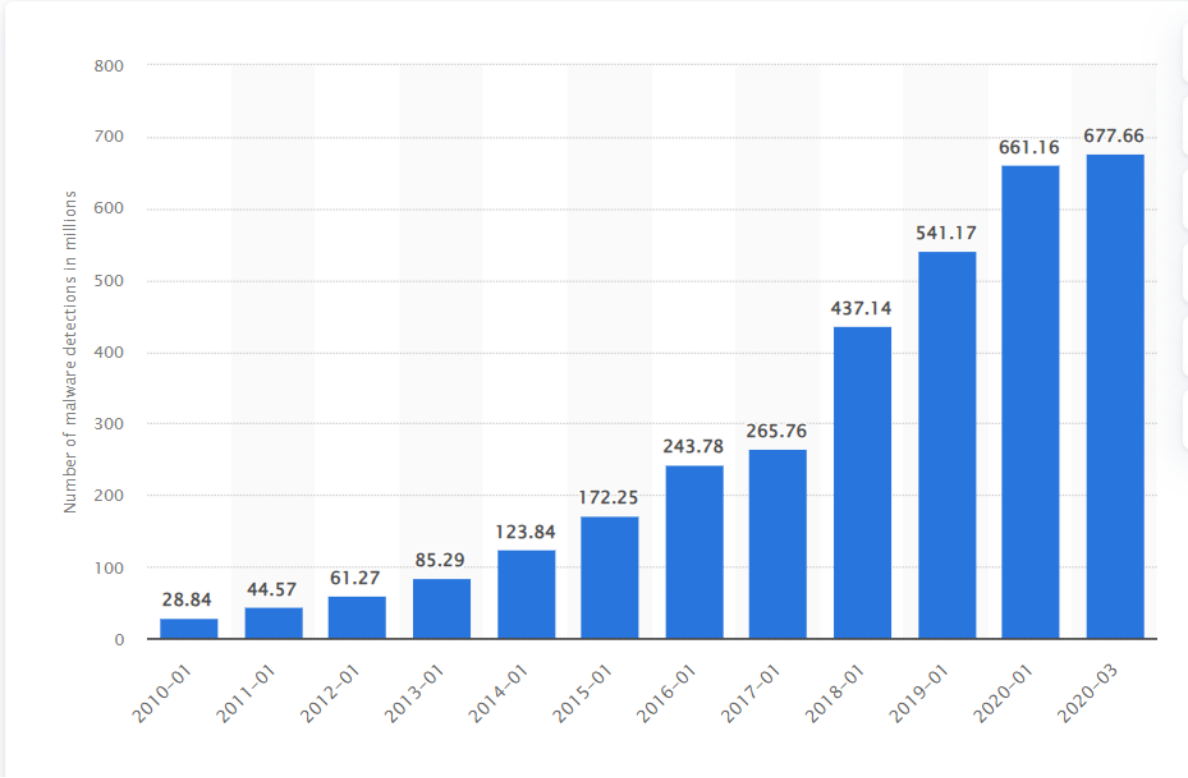
Izvor: Izrada autorice prema Uskok (2021)

Slika 5 prikazuje metodu napada proizvodnjom prilikom kojeg je napadač u ulozi proizvodnje lažnih podataka i takve podatke prenosi do odredišta i nanosi štetu korisniku (Uskok, 2021).

2.4. Maliciozni napadi u mobilnim uređajima i aplikacijama

Maliciozni napadi (engl. *malware*) u mobilnim uređajima i aplikacijama sveprisutna su prijetnja u današnjem digitalnom svijetu. *Malware* može omogućiti napadačima pristup podacima, kontrolu nad uređajem ili izvršavanje štetnih aktivnosti, što korisnike čini žrtvama raznih oblika zloupotrebe. Također, napadi nerijetko mogu uzrokovati narušavanje privatnosti, smanjenje performansi uređaja ili otežano funkcioniranje aplikacija. Kako bi se korisnici mobilnih uređaja zaštitili od malicioznih napada, nužno je poduzeti odgovarajuće sigurnosne mjere poput ažuriranja softvera i instalacije pouzdanih antivirusnih programa. Osim tehničkih oblika zaštite, nije zgorega napomenuti važnost opreznog postupanja s nepoznatim ili sumnjivim porukama i poveznicama. Maliciozni napadi na iOS mobilne uređaje uzrokuju povredu operativnog sustava ili aplikacija dostupnih na navedenim uređajima. Prema mnogim istraživanjima, utvrđeno je da postoje razne aplikacije s lažnim identitetima, aplikacije koje koriste *zero-day* ranjivosti i one koje narušavaju sigurnosna prava App Store-a. *Zero-day* ranjivosti sigurnosni su propusti u softveru koji su nepoznati samom proizvođaču softvera, ali i javnosti. Ova vrsta zlonamjernog napada upućuje na to da javnost i proizvođači softvera nisu obaviješteni o nastanku problema te nemaju niti jedan dan vremena za saniranje štete koja je uzrokovana od strane napadača. Osim *zero-day* ranjivosti, jedan od uobičajenih napada na iOS uređaje je *jailbreaking*, tehnika za prodor u iOS operativni sustav Apple proizvoda. Uređaji na

kojima je izvršen *jailbreaking* postaju osjetljivi na maliciozne napade radi narušavanja značajki nadzora (SMS poruke, pozivi, audio i videozapisi). Zlonamjerne aplikacije jedan su od najčešćih oblika napada i na Android uređaje. Nalaze se u Google Play Store-u, a mogu pripadati raznim skupinama prijetnji poput *spyware*-a i trojanskih konja. Jedan od najprisutnijih *malware*-a u Android uređajima i aplikacijama je *Joker*, otkriven sredinom 2019. g. Vrsta je bankarskog trojanca (dizajniran za krađu financijskih podataka), ali izvršava i druge zlonamjerne radnje poput slanja SMS poruka bez korisnikova znanja, prikazivanja oglasa, pretplata na razne usluge itd. (CARNet CERT, 2010; Qamar i sur., 2019).



Slika 6. Globalna količina novog zlonamjernog softvera 2020

Izvor: Statista (2022)

Podaci prikazani na slici 6 jasno daju do znanja kako je količina zlonamjernih softvera rapidno rasla u periodu od deset godina. Prema podacima vidljivim u grafičkom prikazu, u ožujku 2020. godine je otkriveno 16,5 mil. više *malware*-a negoli u siječnju iste godine.

2.5. Vrste malicioznih napada

Mnoštvo različitih oblika napada ugrožavaju sigurnost mobilnih uređaja i korisničkih podataka. U ovom radu su detaljnije obrađeni sljedeći oblici malicioznih napada: virus, trojanski konj, crv i *spyware*. Zlonamjerni softver se obično širi putem aplikacija koje nisu

preuzete iz pouzdanih izvora, a kako pojedina vrsta *malware*-a utječe na mobilne uređaje i korisnike, opisano je u nadolazećim poglavljima.

2.5.1. Virus

Virusi su zlonamjerni softveri koji ciljaju operacijske sustave mobilnih uređaja i na taj način izazivaju infekciju mobilnih uređaja. Postoje tri osnovne vrste virusa: *boot* sektor virusi, programski i makro virusi. *Boot* sektor virusi kopiraju svoj zlonamjerni kod u glavni *boot* sektor kako bi izvršili napad pri svakom pokretanju računalnog sustava. Makro virusi su oni napisani naprednijim programskim jezikom te imaju mogućnost kopiranja samih sebe. Aktivacija programskih virusa događa se prilikom izvršenja zaraženih datoteka koje završavaju .com ili .exe ekstenzijama. Virusi stvaraju različite vrste problema poput krađe osobnih podataka, oštećenja uređaja te naposlijetku i preuzimanje kontrole nad istim. Na mobilne uređaje se prenose putem zaraženih aplikacija koje korisnici često preuzimaju s nesigurnih izvora, putem web stranica, sumnjivih/zlonamjernih poruka, pa čak i Wi-Fi mreža. Infekcija mobilnog uređaja često rezultira gubitkom podataka, krađom identiteta, slanjem neželjenih poruka što uzrokuje financijske gubitke, ali i narušavanje privatnosti korisnika. Kako bi se izbjegle štete koje virus može uzrokovati, preporuča se opreznije rukovanje aplikacijama u vidu preuzimanja iz pouzdanih izvora (službene trgovine aplikacija). No, u slučaju zaraze mobilnog uređaja virusom, mogu se koristiti antivirusne aplikacije za detekciju i uklanjanje zlonamjernog softvera te se preporuča obnova uređaja na tvorničke postavke (CERT.hr, n.d.a).

2.5.2. Trojanski konj

Budući da su mobilni uređaji ključni dijelovi današnje svakodnevnice, sadrže osjetljive informacije i povezani su s internetom, prisutnost trojanskih konja je postala gotovo neizbježna. Zlonamjerni su softveri koji se vješto predstavljaju kao korisni softveri u obliku privlačnih aplikacija (npr. igrice) ne bi li privukli korisnika i osigurali distribuciju na mobilne uređaje. Trojanski konji imaju niz funkcionalnosti, a šire se preuzimanjem zaraženih/zlonamjernih aplikacija, putem društvenih mreža, SMS poruka i e-mailova. Zbog manjka opreza i korištenja nepogodnih aplikacija, pojava trojanskih konja u mobilnim uređajima može izazvati ozbiljne posljedice po sigurnost korisnika, ali se također mogu koristiti za daljnje širenje malicioznih softvera na druge uređaje ili mreže. Kako bi se izbjegle

navedene štete i saniranje istih, preporuča se korištenje preventivnih mjera (CERT.hr, n.d.b).

2.5.3. Crv

Crv (engl. *Worm*) vrsta je *malware*-a koji se može samostalno replicirati i širiti na druge uređaje bez korisnikovog odobrenja i intervencije. Za razliku od virusa, crv ima mogućnost rasprostiranja bez interakcije korisnika, a prenosi se putem Wi-Fi mreža, Bluetooth veza, e-mailova i zlonamjernih aplikacija. Drugi način širenja ovog zlonamjernog softvera je putem socijalnog inženjeringa. U ovom slučaju, prenošenje crva uključuje interakciju s potencijalnom žrtvom, „maskiraju“ se kao legitimne aplikacije u svrhu privlačenja korisnika. Širenje crva bez interakcije korisnika podrazumijeva iskorištavanje sigurnosnih nedostataka u radu aplikacija koje žrtva svakodnevno koristi te instaliranje vlastite kopije na korisnikov uređaj. Radi prevencije iskorištavanja sigurnosnih nedostataka, potrebno je redovito ažurirati operativni sustav i aplikacije (CERT.hr, n.d.c).

2.5.4. Spyware

U kontekstu mobilnih uređaja i aplikacija, *spyware* može biti izuzetno opasan jer ima pristup brojnim funkcionalnostima uređaja i podacima korisnika. Funkcionira na način da iskorištava zaražene uređaje u komercijalne svrhe, poput *pop-up* reklama, krađe osobnih podataka (uključujući kontakte, poruke, pozive, lozinke, povijest pregledavanja, GPS lokaciju i fotografije). Također, ima mogućnost praćenja korisnikove aktivnosti na društvenim mrežama i drugim aplikacijama. *Spyware* ima izrazit utjecaj na performanse mobilnih uređaja, usporava njihov rad, uzrokuje pregrijavanje te ubrzano pražnjenje baterije. U svrhu sprječavanja navedenog malicioznog softvera, napravljeni su besplatni *anti-spyware* alati za blokiranje ili uklanjanje, poput Ad-Aware SE, Spybot-Search & Destroy *te* Windows Defender (CERT.hr, n.d.d).

2.6. Analiza malicioznih softvera

Za potrebe otkrivanja i identificiranja malicioznih softvera, koriste se dva pristupa: statička i dinamička analiza. Statičkom analizom se ispituju sve aktivnosti u aplikaciji, ali bez izvršavanja iste, što proces same analize čini brzim. Glavni korak prilikom primjene ove analize je provođenje tehnike obrnutog inženjeringa. Ovom tehnikom se dohvaća cijeli kod i

dodatno ispituje sadržaj i struktura same aplikacije. S druge strane, dinamička analiza otkriva zlonamjerni softver pokretanjem malicioznih i benignih (normalnih) aplikacija, u svrhu praćenja i razlikovanja njihova ponašanja. Također, ova analiza zahtijeva i zatvoreno, virtualno okruženje za pokretanje zlonamjernog softvera. Međutim, takvo okruženje i uvjeti nerijetko dovode do nepraktične analize, stoga se statička analiza koristi kao alternativa dinamičke analize (Jusoh i sur., 2021).

U nastavku je prikazana razlika između statičke i dinamičke analize, odnosno njihove prednosti i nedostaci.

Statička analiza	**Dinamička analiza**
PREDNOSTI: Sposobnost otkrivanja zlonamjernog softvera uz pomoć strojnog učenja	Sposobnost otkrivanja zlonamjernog softvera
Primjena tehnike obrnutog inženjeringa, prikladna za mobilne uređaje koji imaju niske specifikacije (npr. memorija)	Sposobnost otkrivanja benignih aplikacija koje se pretvaraju u maliciozne prilikom njihova izvođenja
NEDOSTACI: Nemogućnost otkrivanja normalne aplikacije koja odmah transformira *malware*	Poteškoće u otkrivanju aplikacija koje mogu prikriti zlonamjerno ponašanje
Istraga otkrivanja zlonamjernih softvera se nastavlja kako bi se utvrdile minimalne značajke poput dopuštenja i funkcija poziva	Istraga se nastavlja u svrhu određivanja minimalnih značajki za otkrivanje *malware*-a (npr. memorija)

Tablica 1. Usporedba statičke i dinamičke analize

Izvor: Izrada autorice prema Jusoh i sur. (2021)

3. Metodologija

Problematika kojom se rad bavi su vrste i oblici zlonamjernih napada, uzročno-posljedične veze istih te mehanizmi sigurnosne zaštite. Cilj ovog završnog rada je dati teorijski okvir koncepta informacijske sigurnosti te objasniti vrste malicioznih napada te provesti analizu informacijskih prijetnji mobilnih uređaja i aplikacija.

Pri izradi rada korištena je razna literatura, uključujući knjige, znanstvene i stručne članke iz područja informacijske tehnologije s naglaskom na maliciozne napade u mobilnim uređajima i aplikacijama. Korištene su metode sekundarnog istraživanja u svrhu dobivanja podataka sa službenih internetskih stranica na kojima su objavljeni članci, radovi i tekstovi na odgovarajuću temu rada, a rezultati dobiveni istraživanjem analizirani su deskriptivnom metodom. Također, korištena je i metoda kompilacije pri preuzimanju tuđih rezultata, odnosno pri citiranju i slikovnim prikazima preuzetih iz korištene literature.

4. Opis i rezultati istraživanja

Završni rad se bavi analizom informacijskih prijetnji na mobilne uređaje i aplikacije. Provedeno je istraživanje u svrhu razumijevanja i identificiranja različitih vrsta malicioznih napada koje korisnici mogu doživjeti. Istražen je utjecaj raznih vrsta malicioznih napada (poput virusa, trojanskog konja, crvi i *spyware*-a) na mobilne uređaje.

Nadalje, kao rezultat istraživanja, analizirani su maliciozni napadi na dvije najzastupljenije vrste uređaja: iOS i Android. Napadi poput *zero-day* ranjivosti, *jailbreaking*-a i *Joker*-a uzrokuju ozbiljne posljedice na navedene uređaje, a dani su i konkretni primjeri *malware*-a te njihov zloćudni utjecaj na aplikacije prisutne u Google Play Store-u i App Store-u. Osim vrsta i oblika malicioznih napada, u radu su napisane mjere zaštite od istih te se ističe važnost pravilnog rukovanja uređajima i uslugama koje nudi.

4.1. Analiza malicioznih napada

U nastavku je prikazana analiza malicioznih napada na mobilne uređaje, konkretno Android i iOS uređaje. Navedeni su primjeri *malware*-a na mobilnim uređajima te je istaknut njihov utjecaj na sustav pojedinog uređaja i koje moguće posljedice korištenja malicioznih aplikacija stvaraju. Proučavali su se znanstveni članci i web stranice koje daju uvid u razne vrste napada na Android i iOS uređaje. Također, prikazana je i statistička analiza otkrivanja *malware*-a u Android uređajima.

4.1.1. Maliciozni napadi na iOS uređaje

Prema izvješću McAfee-a, u 2017. g. zabilježeno je 40% napada na iOS uređaje koji su ciljali financijske usluge. U 2019. godini otkrivene su visokorizične ranjivosti u 38% iOS mobilnih aplikacija, a već u prvom kvartalu 2020., navodi se da je broj novih zlonamjernih aplikacija porastao za više od 50% (Mohd Saudi i sur., 2023).

Virus *WireLurker*, otkriven u Kini 2014. g., može se infiltrirati u iOS mobilne uređaje putem USB-a ili preuzimanjem iz nepouzdanih aplikacija. Nakon što zarazi iPhone uređaj, može ukrasti korisničke podatke te preuzeti kontrolu nad samim uređajem. Sljedeći virus čiji se utjecaj analizirao je *Pegasus*. Špijunski softver koji može dobiti pristup kameri, mikrofonu i podacima o lokaciji. Također, ima mogućnost krađe osobnih poruka i lozinka, pa čak i u šifriranim aplikacijama poput WhatsApp-a. Otkriven je 2016., no njegov utjecaj je i dalje

prisutan. Opasan je iz razloga što na vrlo lak način zarazi mobilni uređaj – otvaranjem SMS poruke. Nakon otvaranja poruke, sadržaj je zapravo prazan, no u pozadini preglednika se vrši preuzimanje virusa za instalaciju na mobilni uređaj. Nadalje, 2020. godine otkriven je malware pod nazivom *LightSpy* koji vrši napade na iOS uređaje. Zlonamjerna prijetnja, koja pripada skupini trojanskih napada, distribuirala se putem portala s vijestima poput stranica za ažuriranje aktualnih vijesti o nedavnom virusu Covid-19. *LightSpy* je imao za cilj krađu osobnih podataka, prepoznavanje obližnjih Wi-Fi mreža pa čak i snimanje zaslona. Međutim, jedan od najvećih napada na aplikacije Apple uređaja je zabilježen 2015. g. pod nazivom *XcodeGhost*. Pogađao je niz aplikacija koje potječu iz kineskog App Store-a. *Xcode*, Vrlo poznati alat za razvoj aplikacija, biva napadnut umetanjem zlonamjernog koda i uzrokuje zaraženost velikog broja aplikacija: mbankig aplikacije, aplikacije za trgovanjem dionica, ali i one koje se koriste diljem svijeta poput *WeChat* i *CamScanner*. Još jedan virus, *CoinThief*, može zaraziti iPhone uređaj preuzimanjem aplikacija iz nepouzdanih trgovina. Napada aplikacije za trgovanje bitcoin-om i drugim kripto valutama na način da ih prenosi na račun napadača. Izravno uzrokuje značajan financijski gubitak za korisnika. Drugi virus koji inficira iPhone uređaje širi se preko lažnih ili zlonamjernih aplikacija koje su dostupne izvan App Store-a. *Masque Attack* predstavlja prijetnju za iOS uređaje jer je dizajniran na način da izgleda kao replika pravih aplikacija, a napada one koje mu omogućuju pristup osobnim i privatnim podacima. Unatoč brojnim malicioznim napadima, važno je napomenuti kako Apple redovito poduzima mjere u sprečavanju širenja *malware*-a putem App Store-a. Preuzimanje aplikacija iz pouzdanih izvora, korištenje sigurnosnih značajki poput Face ID i Touch ID, redovno ažuriranje iOS operativnog sustava te provođenje sigurnosnih provjera neke su od mjera koje se preporučaju koristiti radi prevencije zlonamjernih napada (Gui i sur., 2016; Cimitile i sur., 2017; Husainiamer i sur., 2021; Aich, 2021; Phungglan, 2023).

4.1.2. Maliciozni napadi na Android uređaje

Android je vodeći mobilni operativni sustav u svijetu. No, upravo zbog svoje sveprisutnosti postaje ranjiviji na ozbiljne sigurnosne prijetnje poput malicioznih napada. *xHelper* je jedan od malicioznih napada koji zahvaća Android uređaje. Vrlo uporan *malware* pripada skupini trojanskih konja, a karakterizira ga otpornost na bilo koji oblik otkrivanja i brisanja (Brecht, 2020). *HummingBad*, zlonamjerni napad otkriven 2016., trajno instalira *rootkit*[2] na Android

[2] *Rootkit* – zbirka zlonamjernog softvera

uređaje. Čak se prema odluci analitičara procjenjuje da će generirati 300.000 dolara mjesečnog prihoda, a dosegao je više od 85 milijuna preuzimanja. Nadalje, maliciozni napad skupine trojanskih konja, *Triada*, inficira mobilni operativni sustav putem SMS-a i krađe novca žrtvama. Još jedan *malware* koji pripada skupini trojanskih konja je *Hiddad*. Otkriven je 2017. te se koristi za dobivanje pristupa povjerljivim i osobnim podacima. Stručnjaci tvrtke G Data, 2019. g. su otkrili zlonamjerni softver tipa *ransomware* – *GandCrab*, danas najpoznatiji s više od 408 000 verzija. Funkcionira na način da od žrtve traži suradnju u vidu uplate novca u zamjenu za pristup šifriranim podacima. Ukoliko žrtva ne pristane na suradnju, podaci će biti trajno izgubljeni (Cinar i Kara, 2023).

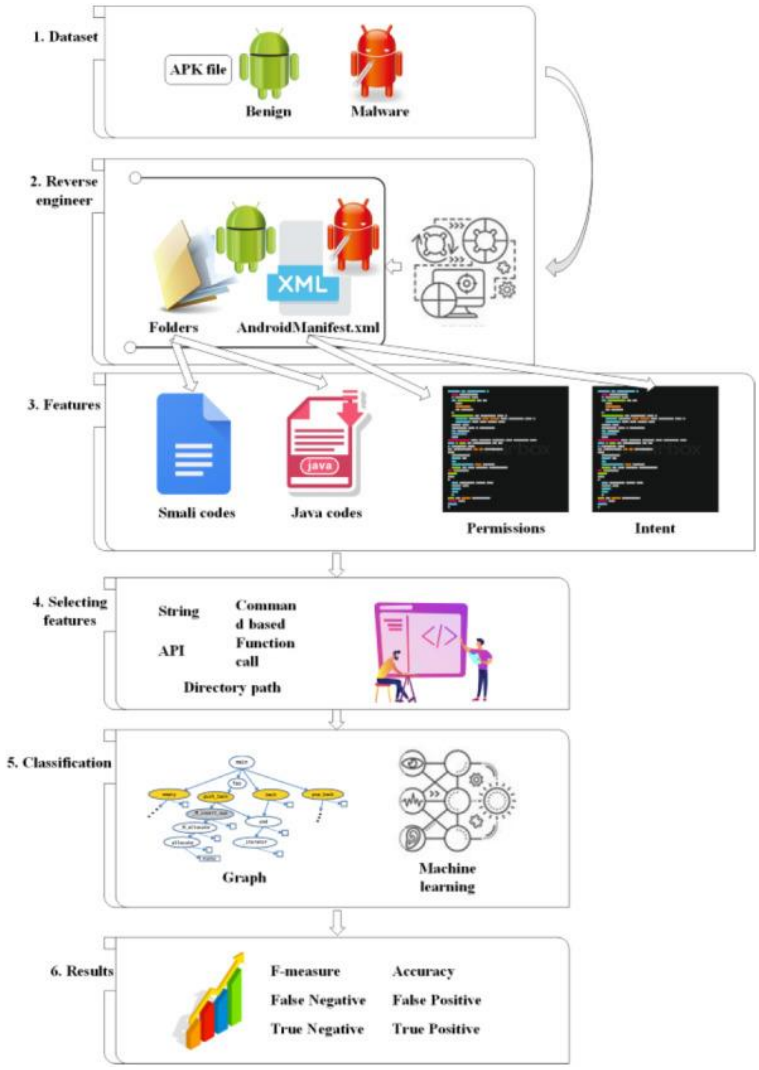
Prema nedavno objavljenim podacima na web stranici pcchip.hr, otkrivene su četiri aplikacije koje je preuzelo više od milijun korisnika: Bluetooth Auto Connect, Bluetooth App sender, Driver: Bluetooth, Wi-Fi, USB i Mobile transfer: smart switch. Aplikacije preusmjeravaju korisnike na sumnjičave stranice koje uzrokuju krađu osjetljivih informacija, ali i generiraju tzv. *pay per view*[3] prihode za operatere. Na istim stranicama, korisnicima se nudi preuzimanje lažnih sigurnosnih alata kako bi, u biti, samostalno instalirali *malware* na svoje uređaje (Mičetić, 2023).

Svi *malware*-i imaju iste i/ili slične ciljeve – krađa osobnih, bankovnih podataka i preuzimanje kontrole nad uređajem. Kako bi se zaštitili osobni podaci i očuvala sigurnost samih uređaja, važno je pridržavati se mjera zaštite: ažuriranje operativnog sustava, pregledavanje dozvole aplikacija, instaliranje sigurnosnog softvera itd. Jedna od sigurnosnih usluga koju Google pruža svojim Android korisnicima je korištenje Google Play Protect usluge. Funkcionira na način da skenira aplikacije dostupne u Google Play Store-u radi sprječavanja preuzimanja zlonamjernih aplikacija koje štete uređajima te samim time i korisnicima istih (Brecht, 2020; Rizqoni i sur., 2020; Bala i sur., 2021).

[3] *Pay per view* – plaćanje po pregledu (pretplatnička usluga)

4.1.3. Statistička analiza malicioznih softvera u Android uređajima

Slika 7 prikazuje statističku analizu malicioznih softvera u Android uređajima, u nekoliko koraka. Prvi korak bilo je prikupljanje benignih i zlonamjernih skupova podataka u Android aplikaciji, svaki s ekstenzijom .apk. Nakon toga, uslijedio je obrnuti inženjering na prikazanim aplikacijama kako bi se dohvatio kod izdvajanjem nekoliko mapa iz jedne .apk datoteke, koja se sastojala od ugniježđenih datoteka s kodovima (Java ili Smali). Nadalje, jedan .apk sadržavao bi otprilike tisuću redaka kodova. Stoga, s ukupno 1000 aplikacija u jednom skupu podataka, stručnjaci za sigurnost morali su pažljivo proučiti milijune linija koda. Završetkom obrnutog inženjeringa provela bi se analiza koja je uključivala značajke. Značajke se sastoje od niza karakteristika aplikacije za otkrivanje zlonamjernog softvera, dok je klasifikacija pristup koji se koristi za razlikovanje zlonamjernog softvera od benigne (normalne) aplikacije (Jusoh i sur., 2021).



Slika 7. Otkrivanje zlonamjernog softvera pomoću statističke analize

Izvor: Jusoh i sur. (2021)

4.2. Zaštita od malicioznih napada

Maliciozni napadi se danas lako mogu prepoznati i na vrijeme poduzeti mjere opreza. Ukoliko postoji sumnja da je mobilni uređaj zaražen, tj. napadnut zlonamjernim softverima, ranjivost se može prepoznati kroz sljedeće stavke: pregrijavanje i sporiji rad uređaja, sumnjivi *pop-up* prozorčići, prisutnost nepoznatih aplikacija i poruka… Zaštita uređaja ne podrazumijeva samo prevenciju od malicioznih napada, već i zaštitu samih korisnika uređaja. Ukoliko dođe do povrede sigurnosti, vrlo često su osobni, osjetljivi podaci meta napadača, a uz njih i njihovi korisnici kao vlasnici svojih podataka. Budući da se mobilni uređaji koriste svakodnevno i mnogima služe kao sredstvo u poslovanju, vrlo je važno poduzeti odgovarajuće mjere zaštite mobilnog operativnog sustava (Bany Muhammad, 2017; Cinar i Kara, 2023):

- Ažuriranje operativnog sustava (Android ili iOS)
- Preuzimanje aplikacija iz pouzdanih izvora (Google Play Store ili App Store)
- Korištenje snažnih lozinki i biometrijskih značajki (prepoznavanje lica, otisak prsta)
- Upotreba pouzdanih antivirusnih programa (*BitDefender*, *Malwarebytes*, *Spybots*)
- Edukacija o sigurnosti mobilnih uređaja.

Osim navedenih savjeta, važna je i svijest korisnika prilikom korištenja raznih usluga i aplikacija koje mobilni uređaju pružaju.

5. Rasprava

Informacijske prijetnje postaju sve više prisutne u mobilnim uređajima i aplikacijama. U prijašnjim poglavljima se pisalo o zastupljenosti malicioznih napada na pojedine uređaje - iOS i Android. Među njima postoje neke sličnosti, ali i različitosti zbog karakteristika i sigurnosnih značajki operativnih sustava. Android uređaji su znatno zastupljeniji i korišteniji na tržištu te imaju otvoreniji (pristupačniji) operativni sustav koji korisnicima omogućuje preuzimanje aplikacija iz različitih izvora. S druge strane, iOS uređaji broje nešto manju zastupljenost te korisnicima ograničavaju instaliranje aplikacija samo preko App Store-a, što uvelike smanjuje rizik od malicioznih napada. Zbog veće otvorenosti i mogućnosti preuzimanja aplikacija iz različitih izvora, Android uređaji postaju lakše dostupni za prodiranje *malware*-a u sustav. Također, zbog zakašnjelih ažuriranja i većih sigurnosnih propusta, Android uređaji su izloženiji napadima. Apple kontrolira svoj sustav te pruža redovite ispravke sigurnosne ranjivosti, no unatoč tome, nije iskorijenjena prisutnost malicioznih napada. Bez obzira na manjkavosti, oba sustava pružaju visoku razinu sigurnosti u borbi protiv malicioznih napada. U konačnici, preferencije korisnika su te koje navedene uređaje i njihov operativi sustav čine prihvatljivijima i privlačnijima za korištenje.

6. Zaključak

Maliciozni napadi na mobilne uređaje i aplikacije javljaju se u različitim oblicima. U radu su detaljnije opisane vrste napada poput virusa, trojanskih konja, crva i *spyware* napada. Svaki od napada uzrokuje posljedice karakteristične za svoj pravac djelovanja, no u suštini su bazirani na krađu osobnih i financijskih podataka, gubitak privatnosti i preuzimanje kontrole nad uređajem. Kako bi se smanjio utjecaj napada, ali i prorijedila njihova pojavnost, rad pruža analizu malicioznih napada na iOS i Android uređaje te metode zaštite od istih. Utvrđeno je kako se većina napada odvija putem preuzimanja aplikacija iz nepouzdanih izvora. Jasno se može zaključiti kako je mobilni sustav Android uređaja osjetljiviji na povrede i napade, što zbog veće otvorenosti sustava i samim time lakšem pristupu nepouzdanim izvorima, ali i zbog činjenice da su Android mobilni uređaji najkorišteniji od svih ponuđenih na tržištu. Dvije najzastupljenije vrste malware-a na Android uređaje koje ovaj rad navodi su *Joker* i *xHelper*. S druge strane, ranjivost iOS sustava nešto je manja u usporedbi s Android sustavima. Apple nudi veću sigurnosnu kontrolu svojih uređaja i nešto redovitija ažuriranja sustava, no bez obzira na ove prednosti, zabilježeni su brojni napadi. *Zero-day* ranjivost i *jailbreaking* najpoznatije su tehnike za prodor napadača u iOS mobilne operativne sustave. Zaključno, analiza malicioznih napada na mobilne uređaje i aplikacije ključna je za razumijevanje njihovih karakteristika, metoda i ciljeva. Postizanje informacijske sigurnosti i osiguravanje korisnicima sigurno iskustvo korištenja uređaja glavni je cilj svih mobilnih operativnih sustava. Konstantno se potiče na poduzimanje mjera sigurnosne zaštite ne bi li se spriječili pokušaji malicioznih napada. Međutim, nove prijetnje ne jenjavaju i iznova pronalaze načine za izbjegavanje sigurnosnih mjera, stoga je važno pratiti negativni trend širenja *malware*-a te uporno istraživati na koje još načine osigurati zaštitu mobilnih uređaja i aplikacija.

Literatura

1. Ahmad, A., Webb, J., Desouza, K. C., Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security*, *86*, 402-418.
2. Aich, R. (2021). *Efficient audit data collection for linux* (Doctoral dissertation, Doctoral dissertation). Stony Brook University. Bao, AC (2023). Is docker secure for web server).
3. Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.
4. Bala, N., Ahmar, A., Li, W., Tovar, F., Battu, A., Bambarkar, P. (2021). DroidEnemy: battling adversarial example attacks for Android malware detection. *Digital communications and networks, 8*, 1040-1047.
5. Bany Muhammad, N. (2017). Malicious softwares threats and risks, Symptoms and impacts. *Review of Business and Technology Research, 14*(2), ISSN 1941-9414.
6. Brecht, D. (2020). xHelper malware: What it is, how it works and how to prevent it | Malware spotlight. INFOSEC. Dostupno na: https://resources.infosecinstitute.com/topic/xhelper-malware-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/ [pristupljeno: 29.06.2023.]
7. CARNet CERT (2009). Sigurnosna politika. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-05-265.pdf [pristupljeno: 22.06.2023.]
8. CARNet CERT (2010). Zero day ranjivosti. Dostupno na: https://www.cert.hr/zero-day-ranjivosti/ncert-pubdoc-2010-01-289/ [pristupljeno: 29.06.2023.]
9. CERT.hr (n.d.a). O virusima. Dostupno na: https://www.cert.hr/virusi/ [pristupljeno: 22.06.2023.]
10. CERT.hr (n.d.b). O trojanskim konjima. Dostupno na: https://www.cert.hr/trojanski_konji/ [pristupljeno: 22.06.2023.]
11. CERT.hr (n.d.c). O crvima. Dostupno na: https://www.cert.hr/crvi/ [pristupljeno: 22.06.2023.]
12. CERT.hr (n.d.d). O adware/spyware softveru. Dostupno na: https://www.cert.hr/adware/ [pristupljeno: 22.06.2023.]

13. Cimitile, A., Martinelli, F., Mercaldo, F. (2017). Machine Learning Meets iOS Malware: Identifying Malicious Applications on Apple Environment. In *ICISSP* (pp. 487-492).
14. Cinar, A. C., Kara, T. B. (2023). The current state and future of mobile security in the light of the recent mobile security threat reports. *Multimedia Tools and Applications*, 1-13.
15. Gerić, S., Hutinski, Ž. (2007). Information system security threats classifications. *Journal of Information and organizational sciences*, *31*(1), 51-61.
16. Gudac, N. (2019). Sigurnosni aspekt informacijskih sustava [Završni rad]. Veleučilište u Karlovcu.
17. Gui, X., Liu, J., Chi, M., Li, C., Lei, Z. (2016). Analysis of malware application based on massive network traffic. *China Communications*, *13*(8), 209-221.
18. Husainiamer, M. A., Saudi, M. M., Ahmad, A., Syafiq, A. S. M. (2021). Mobile Malware Classification for iOS Inspired by Phylogenetics. *International Journal of Advanced Computer Science and Applications*, *12*(8).
19. Jouini, M., Rabai, L. B. A., Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489-496.
20. Jusoh, R., Firdaus, A., Anwar, S., Osman, M. Z., Darmawan, M. F., Ab Razak, M. F. (2021). Malware detection using static analysis in Android: a review of FeCO (features, classification, and obfuscation). *PeerJ. Computer science*, *7*, e522. Dostupno na: https://doi.org/10.7717/peerj-cs.522 [pristupljeno: 11.07.2023.]
21. Kumar, S., Agarwal, D. (2018). Hacking attacks, methods, techniques and their protection measures. *International Journal of Advance Research in Computer Science and Management*, *4*(4), 2253-2257.
22. Mičetić, E. (2023). Pronađena je grupa od četiri maliciozne aplikacije na Google Play Storeu! Dostupno na: https://pcchip.hr/softver/sigurnost/pronadena-je-grupa-od-cetiri-maliciozne-aplikacije-na-google-play-storeu-preuzelo-ih-je-vise-od-milijun-korisnika/ [pristupljeno: 10.07.2023.]
23. Mohd Saudi, M., Husainiamer, M. A., Ahmad, A., Idris, M. Y. I. (2023). iOS mobile malware analysis: a state-of-the-art. *Journal of Computer Virology and Hacking Techniques*, 1-30.
24. Pachghare, V. K. (2019). *Cryptography and information security*. PHI Learning Pvt. Ltd.

25. Pfleeger, S. L., Pfleeger, C. P., Margulies, J. (2015). *Security in Computing, Fifth Edition*. Pearson.
26. Phungglan, J. (2023). Most common viruses on iPhone. Dostupno na: https://macpaw.com/how-to/most-common-iphone-viruses [pristupljeno: 10.07.2023.]
27. Qamar, A., Karim, A., Chang, V. (2019). Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems*, *97*, 887-909.
28. Rizqony, Y. I., Akbi, D. R., Setiawan, F. D. S. (2020). Analisis Karakteristik Malware Joker Berdasarkan Fitur Menggunakan Metode Statik Pada Platform Android. *J. Repos*, *2*(10), 1368-1379.
29. Salahdine, F., Kaabouch, N. (2019). Social engineering attacks: A survey. *Future internet*, *11*(4), 89.
30. Sikorski, M., Honig, A. (2012). *Practical malware analysis: the hands-on guide to dissecting malicious software*. No starch press.
31. Statista (2022). *Cumulative detections of newly-developed malware applications worldwide from 2015 to March 2020*. Dostupno na: https://www.statista.com/statistics/680953/global-malware-volume/ [pristupljeno: 11.07.2023.]
32. Tyson, J. (2019). *The CIA Triad*. Dostupno na: https://blog.jamestyson.co.uk/the-cia-and-dad-triads [pristupljeno: 11.07.2023.]
33. Uskok, I. K. (2021). Izvori i oblici prijetnji sustavu sigurnosnih informacija [Završni rad]. Veleučilište s pravom javnosti Baltazar Zaprešić.
34. Whitman, M. E., Mattord, H. J. (2021*). Principles of information security.* Cengage learning.
35. Zakon o informacijskoj sigurnosti (NN 79/07). Dostupno na: https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti [pristupljeno: 20.06.2023.]
36. Zhang, H., Liu, B., Wu, H. (2021). Smart grid cyber-physical attack and defense: A review. *IEEE Access*, *9*, 29641-29659.

Popis slika i tablica