Krađa identiteta kao metoda napada prema mobilnom terminalnom uređaju

Arapović, Ivan

Undergraduate thesis / Završni rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:445022

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository







SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Ivan Arapović

KRAĐA IDENTITETA KAO METODA NAPADA PREMA MOBILNOM TERMINALNOM UREĐAJU

ZAVRŠNI RAD

Zagreb, 2019.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

KRAĐA IDENTITETA KAO METODA NAPADA PREMA MOBILNOM TERMINALNOM UREĐAJU

IDENTITY THEFT AS AN ATTACK METHOD TOWARDS MOBILE TERMINAL DEVICE

Mentor: dr. sc. Siniša Husnjak

Student: Ivan Arapović

JMBAG: 0135236224

Zagreb, rujan 2019.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 1. travnja 2019.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Terminalni uređaji**

ZAVRŠNI ZADATAK br. 5095

Pristupnik: **Ivan Arapović (0135238421)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Krađa identiteta kao metoda napada prema mobilnom terminalnom uređaju**

Opis zadatka:

Prikazati razvoj i korištenje mobilnih terminalnih uređaja. Identificirati zlonamjerne prijetnje usmjerene mobilnim terminalnim uređajima. Razlikovati mehanizme i svojstva napada krađe identiteta. Dati primjere i značajke aktualnih napada krađe identiteta. Ispitati alate i načine zaštite i prevencije od napada krađe identiteta.

Mentor:

dr. sc. Siniša Husnjak

Predsjednik povjerenstva za završni ispit:

SAŽETAK

Mobilni terminalni uređaji danas su sveprisutni i mnogo poslovnih ili privatnih aktivnosti obavlja se pomoću tih uređaja i upravo preko njih korisnici sve češće postaju metom napada. Uporabom aplikacija, usluga i ostalih mogućnosti, korisnik je izložen brojnim napadima, među kojima su najčešći oni krađe identiteta. Krađa identiteta označava neovlašteni pristup i otuđivanje osobnih podataka poslovnih ili privatnih korisnika mobilnih terminalnih uređaja. Korisnika se navodi da sam preda željene podatke te se zbog toga napadačima rijetko može ući u trag. Zbog izloženosti napadima koji rezultiraju većim financijskim gubicima, prijetnjama, gubicima ugleda ili gubicima vrijednih podataka, nužno je korisnike informirati i obrazovati o uobičajenim kategorijama prijetnji. Također je bitna i zaštita od napada, gdje se nudi mnoštvo alata i softverska rješenja za povećanje sigurnosti uređaja. Cilj ovog rada je izrada konciznog i preglednog uvida u zlonamjerne napade krađom identiteta usmjerene mobilnim uređajima, načine na koje se odvijaju i načine na koje se mogu spriječiti.

KLJUČNE RIJEČI: krađa identiteta; zlonamjerni napad; zaštita; mobilni uređaj

ABSTRACT

Mobile terminal devices are ubiquitous today, many business and private activities are being done with the help of these devices and, through them, users are increasingly becoming the targets of an attack. By using applications, services, and other features, the user is exposed to numerous attacks, most often identity thefts. Identity theft is an unauthorized access to and stealing of personal data that belong to business or private users of mobile terminal devices. The user is lured to provide the desired information himself/herself, so the attackers can rarely be traced. Due to the exposure to attacks that result in greater financial losses, threats, loss of reputation or valuable information, it is important for users to be informed and educated about the common threat categories. Prevention from the attack is also important and there is a plethora of tools and software solutions offered to increase the security of the device. The aim of this paper is to produce a concise and clear insight into malicious attacks on identity theft targeted towards mobile devices, the ways in which it takes place, and into the ways in which identity theft can be prevented.

KEYWORDS: identity theft; malicious attack; protection; mobile devices

SADRŽAJ

1. Uvod 1
2. Razvoj i korištenje mobilnih terminalnih uređaja 3
2.1. Razvoj funkcionalnosti mobilnih mreža 3
2.1.1. Generacije mobilnih mreža (1G – 4G) 4
2.1.2. Peta generacija mobilnih mreža (5G) 6
2.2. Razvoj mobilnih terminalnih uređaja 6
2.3. Korištenje mobilnih terminalnih uređaja 8
3. Zlonamjerne prijetnje usmjerene mobilnim terminalnim uređajima 10
3.1. Trend sigurnosnih nedostataka 11
3.2. Izvori i vrste napada 12
3.3. Svrha i žrtve napada 13
4. Mehanizmi i svojstva napada krađom identiteta 14
4.1. Vrste napada krađom identiteta 15
4.2. Proces stvaranja mehanizama za napad krađom identiteta 18
4.2.1. Stvaranje lažne e-pošte 18
4.2.2. Stvaranje lažne *web* lokacije 24
4.2.3. Stvaranje lažne aplikacije na Android sustavu 30
5. Primjeri i značajke aktualnih napada krađom identiteta 33
5.1. Operacija Phish Phry 33
5.2. Walter Stephan 33
5.3. Target / FMS prijevara 33
5.4. Napad na ukrajinsku elektroenergetsku mrežu 34
5.5. Prijevara tijekom Svjetskog nogometnog prvenstva 2018. 34
6. Alati i načini zaštite i prevencije 35
6.1. Postojeća rješenja 35
6.1.1. Anti-botnet rješenja 35
6.1.2. Alat Lookout 37
6.2. Novija rješenja 38
7. Zaključak 41
Literatura 42
Popis kratica 45
Popis slika 46

Popis grafikona 47
Popis tablica 48

1. Uvod

Napadi krađom identiteta usmjereni mobilnim uređajima najčešći su današnji zlonamjerni napadi. Prelaskom na sve veće, gotovo pa neizostavno korištenje mobilnih terminalnih uređaja, unatoč svim prednostima, zlonamjerni napadi predstavljaju nedostatak. Uspješni napadi krađom identiteta podrazumijevaju samovoljno, ali i nesvjesno odavanje osobnih podataka (npr. broja kreditne kartice) napadačima. Načini i vrste napada su raznoliki, a u najvišem postotku odnose se na poruke e-pošte ili ostale najpopularnije oblike komunikacije, te uglavnom sadrže zlonamjerne poveznice. Zbog osjetljivosti podataka, bez obzira na to o kojoj vrsti podataka se radi, njihovoj vrijednosti ili zaštiti privatnosti, korisnici posežu za informiranjem o načinima sprječavanja napada. Nadalje, jedan od ciljeva je i zaštititi mrežu i sami sustav nad kojim bi, eventualnim preuzimanjem kontrole, napadač napravio štetu.

Cilj rada je prikazati važnost i učestalost korištenja mobilnih terminalnih uređaja, opisati mehanizme i svojstva napada krađom identiteta prema tim uređajima, a onda i korisnicima te približiti načine zaštite i informiranja o istima. Rad je podijeljen u sedam cjelina:

1. Uvod
2. Razvoj i korištenje mobilnih terminalnih uređaja
3. Zlonamjerne prijetnje usmjerene mobilnim terminalnim uređajima
4. Mehanizmi i svojstva napada krađom identiteta
5. Primjeri i značajke aktualnih napada
6. Alati i načini zaštite i prevencije

U drugom poglavlju je riječ o razvoju mobilnih generacija usporedno s generacijama mobilne mreže, te podjela rasta funkcionalnosti mobilnih uređaja kroz faze razvoja. Opisuju se i navode razlozi zbog kojih je došlo do ubrzanog rasta, kao i pružene mogućnosti i usluge koje su svojom pojavom postepeno zamjenjivale stolna računala.

Treće poglavlje sadrži statističke podatke o broju napada, opisuje izvore, vrste, razloge i ciljeve napada, što podrazumijeva razmišljanja sa stajališta napadača i ona od strane korisnika, odnosno, žrtve.

Četvrto poglavlje donosi detaljan opis stvaranja mehanizama za napad krađom identiteta usmjerenog mobilnim uređajima te se prikazuju najčešći oblici napada, odnosno, napadi koji se odvijaju e-poštom, putem lažne stranice ili lažne aplikacije.

U petom poglavlju navedeni su i istraženi neki od najvećih napada ove vrste kako bi se korisnik više osvijestio o mogućim ishodima u slučaju napada. Navedene su i materijalne štete, načini krađe identiteta i iskorištavanje ukradenih resursa.

Šesto poglavlje iznosi rješenja koja se nude na tržištu, kao i neke ideje koje su u razvoju. Poglavlje odgovara na pitanja kako se zaštititi u određenoj situaciji, bavi se alatima za sigurnost i softverskim rješenjima koja bi korisniku mogla olakšati zaštitu svojih uređaja, a samim time i podataka.

2. Razvoj i korištenje mobilnih terminalnih uređaja

Mobilni terminalni uređaji, kao i sama tehnologija kojoj pripadaju, bilježe veliku brzinu razvoja od samoga nastanka do danas. Nije ih jednostavno kategorizirati zbog raznovrsnosti njihovih tehničkih specifikacija, računalne snage, veličine ili rezolucije zaslona, operativnih sustava i slično. Za tematiku ovoga završnog rada, navedeno ne stvara značajniji problem jer se napadi krađom identiteta usmjereni mobilnim uređajima (engl. *mobile phishing*) odvijaju s jednakom mogućnošću kod svake vrste mobilnog terminalnog uređaja budući da se napad odvija softverskim putem. U mobilne terminalne uređaje mogu se ubrojiti:

- mobilni uređaji (engl. *feature phones)*
- pametni mobilni uređaji (engl. *smartphones*)
- tablet uređaji
- phablet uređaji
- pametni satovi
- ostalo (pametne naočale, pametni prsten itd.)

Kako bi se uvelo u problematiku, potrebno je upoznati se s razvojem i korištenjem navedenih uređaja da bi se kasnije shvatili razlozi i učestalost napada krađom identiteta usmjerenih prema mobilnom uređaju.

2.1. Razvoj funkcionalnosti mobilnih mreža

Za razvoj svih komponenti mobilnih terminalnih uređaja bilo je potrebno osigurati i temelj za njihovo korištenje, a to su poboljšanja mobilnih mreža čije su generacijske karakteristike navedene u tablici 1.

Tablica 1. Usporedba mobilnih mreža od prve do pete generacije, [1]

Tehnologija	1G	2G	3G	4G	5G
Početak korištenja	1970. - 1980.	1990. - 2004.	2004. – 2010.	Trenutno se koristi	Predviđeni početak korištenja: do 2020.
Tehnologija	Analogna	Digitalna	CDMA 2000, UMTS, EDGE	Wi-Max, Wi-Fi, LTE	WWWW (*Worldwide wireless web*)
Primarna usluga	Analogni telefonski pozivi	Digitalni telefonski pozivi i poruke	Telefonski pozivi, poruke i mobilni podaci	All-IP Service (uključujući glasovne poruke)	Visoka brzina, kapacitet i pružanje prijenosa velike količine podataka
Širina pojasa	2 kbit/s	64 kbit/s	2 kbit/s	1 kbit/s	Više od 1 kbit/s
Ključna razlika	Mobilnost	Sigurnost	Bolje iskustvo korištenja interneta	Brži širokopojasni internet, niža latencija	Bolja pokrivenost i nema ispuštenih poziva, niža latencija, bolje performanse
Nedostatak	Loša spektralna učinkovitost, veliki sigurnosni nedostaci	Ograničene brzine prijenosa podataka teško podržavaju potražnju	Stvarna izvedba ne odgovara tipu, neuspjeh WAP-a za pristup internetu	Korištenje baterije je veće, potreban složeniji i skuplji hardver	Još nije ispitano

Iz tablice generacija mobilnih mreža vidljiv je veoma brz napredak u svakom navedenom segmentu, a u idućim potpoglavljima bit će opisane detaljnije karakteristike istih.

2.1.1. Generacije mobilnih mreža (1G – 4G)

Mobilni uređaji prve generacije korišteni su za glasovne usluge i temeljeni su na tehnologiji nazvanoj AMPS (engl. *Advanced Mobile Phone System*). AMPS sustav je frekventno moduliran te se koristi frekvencijski višestruki pristup FDMA (engl. *Frequency-*

division Multiple Access) s kapacitetom kanala od 30 KHz i frekvencijskim pojasom od 824 – 894 MHz, [1]. Njegove osnovne značajke su brzina od 2,4 kbit/s, korištenje analognog signala, loša kvaliteta glasa, malo trajanje baterije, ograničeni kapacitet, loša pouzdanost, nedovoljna sigurnost i vrlo niska razina učinkovitosti spektra, [1].

Druga generacija mobilnih mreža (2G) temelji se na GSM-u (engl. *Global System for Mobile* Communications). Koristi digitalne signali za prijenos glasa. Glavni fokus ove tehnologije su digitalni signali i osiguravanje usluga za isporuku tekstualnih i slikovnih poruka pri maloj brzini. Koristi širinu pojasa od 30 do 200 KHz, [1]. Glavne značajke 2G su brzine prijenosa podataka do 64 kbit/s, korištenje digitalnih signala, omogućavanje usluga kao što su tekstualne, slikovne i multimedijske poruke, bolja kvaliteta, veći kapacitet i potreba za dobrom mrežnom pokrivenosti, [1].

Uz 2G, 2.5G sustav koristi paketnu komutiranu domenu i komutiranu domenu te pruža brzine do 144 kbit/s. GSM tehnologija kontinuirano se poboljšavala kako bi pružila bolje usluge koje su dovele do razvoja napredne tehnologije između 2G i 3G. Glavne značajke 2.5G su slanje / primanje poruka e-pošte i pretraživanje interneta, [1].

Treća generacija mobilnih mreža (3G) nudi veću brzinu podataka. Koristi širokopojasnu bežičnu mrežu. Djeluje na rasponu od 2100MHz i ima propusnost od 15 - 20MHz koja se koristi za brzi internetski servis i video razgovore, [1]. Ključne značajke 3G sustava su: veća brzina prijenosa podataka, mogućnost video poziva, poboljšana sigurnost, veći broj korisnika i pokrivenost, podrška za mobilne aplikacije, podrška za multimedijske poruke, praćenje lokacije i karte, bolje pregledavanje web stranica, itd, [2].

Četvrta generacija mobilnih mreža (4G) nudi brzinu preuzimanja od 100 mbit/s. LTE (engl. *Long Term Evolution*) smatra se 4G tehnologijom. Razvijen je kako bi zadovoljio zahtjevima korisnika i budućim aplikacijama poput bežičnog širokopojasnog pristupa, usluga multimedijskih poruka, video razgovora, mobilne TV, visokokvalitetnog sadržaja, digitalnog video emitiranja, itd., [1]. Neke od značajki ove generacije su: mnogo veća brzina prijenosa podataka do 1Gbit/s, povećana sigurnost i mobilnost, smanjena kašnjenja za kritične aplikacije, govor preko LTE mreže VoLTE (koriste se IP paketi za prijenos glasa). Nedostaci sustava su skupi hardver i infrastruktura te spektar (u većini zemalja preskup), potrebni su vrhunski mobilni uređaji kompatibilni s 4G tehnologijom te široka implementacija i nadogradnja zahtijevaju mnogo vremena, [2].

2.1.2. Peta generacija mobilnih mreža (5G)

5G omogućuje ne samo povezivanje ljudi, već upravljanje strojevima, objektima i uređajima. To podrazumijeva višestruke brzine prijenosa podataka, ultra nisku latenciju, masivan kapacitet i ujednačenije korisničko iskustvo. Također, očekuje se i veliki napredak te implementacija u korištenju unutar okvira internet stvari te industrijskih pogona. Glavne značajke 5G-a su:

- Visoka podržanost WWWW-a (engl. *Wireless World Wide Web*)
- Velika brzina, veliki kapacitet
- Veliko emitiranje podataka u Gbit/s
- Brži prijenos podataka od prethodne generacije
- Velika memorija telefona, brzina biranja, bolja kvaliteta u audio / videozapisu, [1].

2.2. Razvoj mobilnih terminalnih uređaja

Usporedno s razvojem mrežnih mogućnosti, neophodan je bio i razvoj mobilnih terminalnih uređaja. Tehničke specifikacije, veličina zaslona uređaja, inačice operativnog sustava te općenite mogućnosti mobilnih terminalnih uređaja mijenjale su se i, s vremenom, proširile. Kako je područje istraživanja veoma opširno, ovaj sažetak razvoja usmjeren je na generacije mobilnih mreža te faze razvoja pametnih mobilnih uređaja. Razvoj mobilnih terminalnih uređaja može se podijeliti i u tri faze, ovisno o namijenjenim korisnicima istih.

U prvoj fazi nalaze se mobilni terminalni uređaji namijenjeni poslovnim korisnicima, nedostupni širem tržištu zbog jako visokih cijena. Stoga su funkcionalnosti i aplikacije osmišljene da zadovolje zahtjeve tražene od strane poslovnih korisnika. Prva faza započela je pojavom IBM-ovog prvog pametnog mobilnog uređaja naziva *The Simon* koji je imao mogućnosti govornih usluga, prijenosa podataka, telefaksa i dlanovnika (engl. *PDA – Personal Digital Assistant*), [3].

Druga faza svoj početak bilježi pojavom *iPhone* mobilnog uređaja koji je potaknuo proizvođače da određenom subvencijom kupnje uređaja zadrže broj svojih korisnika, a da se na taj način tržište otvori i za privatne korisnike, što je zapravo i glavno obilježje ove faze.

Treća faza donosi izjednačenje odnosa privatnih i poslovnih korisnika u broju uređaja te u dostupnosti na tržištu. Osim toga, glavna značajka ovog razdoblja je poboljšanje

korisničkog sučelja (engl. *User interface – UI*) i operativnog sustava. Operativni sustav i njegova nadogradnja označavaju početak ove faze. Nakon toga se bilježi rast proizvođača i uspjeh istih, te razvoj brojnih sustava kao što su iOS, Android, Blackberry OS, Windows, [3].

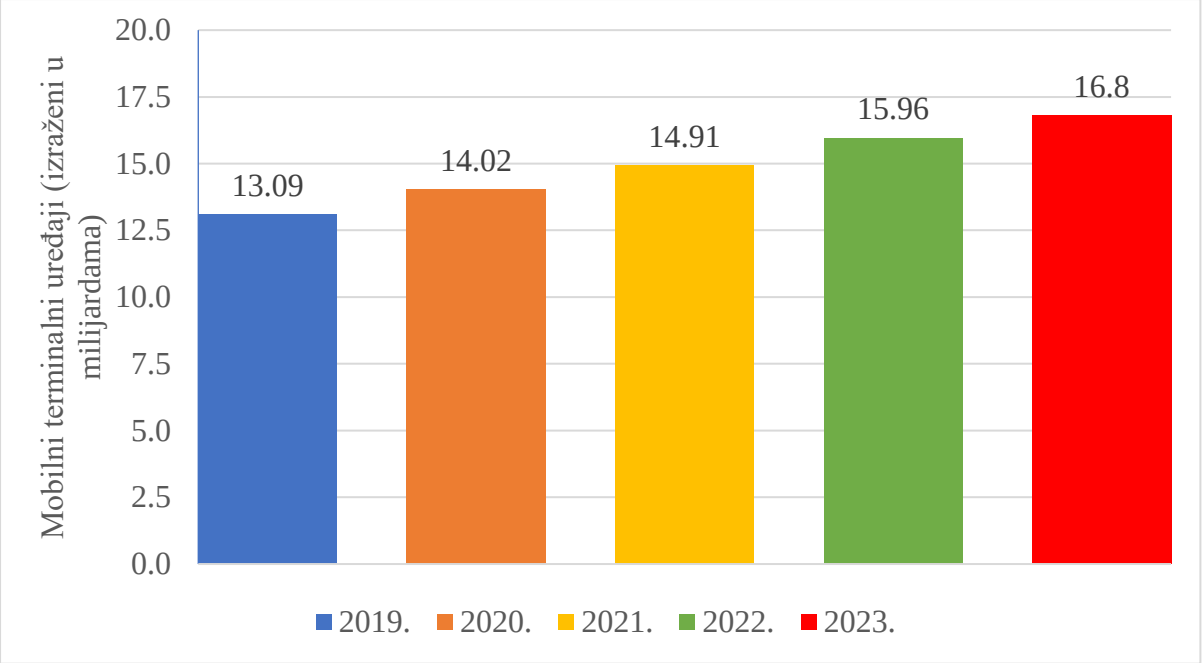
Zbog velike mogućnosti primjene, različitosti izvedbi te pristupa mrežama i aplikacijama, mobilni terminalni uređaji velik su dio korisnikove svakodnevice. Primjerice, tu su komunikacija korisnika, arhiviranje dokumenata, fotografija i datoteka na *cloud* servere ili, pak, redovno plaćanje računa putem aplikacije banke. Ovo su samo neke od mnoštva mogućnosti koje su prisutne, a kada se uzmu u obzir zastupljenost i korištenje mobilnih terminalnih uređaja te vrijednost podataka koji se nalaze zapisani u uređaju ili koji se unose putem aplikacija, pojava zlonamjernih napada krađom identiteta usmjerenih mobilnom uređaju ne iznenađuje.

2.3. Korištenje mobilnih terminalnih uređaja

Mobilni terminalni uređaj utjecao je na gotovo sve aspekte ljudskog života. Značajna područja gdje se očituju utjecaji mobilnih terminalnih uređaja su poslovni, obrazovni, zdravstveni i društveni život. Mobilna tehnologija uvelike utječe i na promjenu kulturnih normi i ponašanje pojedinaca. Kao kod svakog razvoja neke tehnologije, i ovdje postoje pozitivni i negativni utjecaji. Zbog niza mogućnosti, uređaji pružaju korisnicima korištenje istih u dobre ili u zlonamjerne svrhe. Kada se govori o poduzetništvu, korištenje ove tehnologije otvorilo je brojne mogućnosti kao što su razvoj mobilnih aplikacija i pružatelja usluga putem interneta, sve u cilju stjecanja konkurentnih prednosti, [4].

Pozitivni utjecaji su, osim rasta poslovanja širokopojasnih internetskih usluga, razvoj proizvođača mobilnih terminalnih usluga zbog njihove velike prodaje, te osiguravanje sredstava za daljnji razvoj. Pozitivan je primjer i rast konkurentnosti aplikacija gdje većina operativnih sustava ima svoje „tržište“ i gdje su korisnicima omogućili preuzimanje korisnih aplikacija za razne potrebe, bile one besplatne ili uz cijenu. Velik pomak ostvaren je i u području marketinga koji je, radi jednostavnosti i učinkovitosti, podignut na višu razinu, [4].

Nadalje, uređaji podržavaju određene tehnologije koje pomažu korisniku u svakodnevnom životu. Primjerice, tu je primjena kućnog sustava zdravstvene skrbi baziran na IoT-u (engl. *Internet of things*), zaštita osobne imovine video nadzorom, funkcionalnost pametne kuće kao što je udaljeno upravljanje, racionalno iskorištavanje električne energije i slično, [5]. Negativni utjecaji, s druge strane, ovise o načinu korištenja mobilnih uređaja. Količina podataka spremljena na mobilnim uređajima je ogromna te korisnici većinom nisu upoznati s osobnim podacima spremljenima u njihovim mobilnim uređajima. Gubitak ili krađa uređaja vlasnika dovodi do velike opasnosti zbog mogućnosti krađe identiteta, gubitka financijskih sredstava, narušavanja ugleda te bilo kojeg drugog oblika manipuliranja podacima od strane zlonamjernog napadača. Manipuliranje podatcima predstavlja značajnu opasnost i na poslovnom području, budući da se podaci spremljeni u uređaj karakteriziraju kao uvelike osjetljivi, [4].



Grafikon 1. Broj korisnika mobilnih terminalnih uređaja u milijardama u 2019. godini i predviđanje broja do 2023. godine, Izvor: [6]

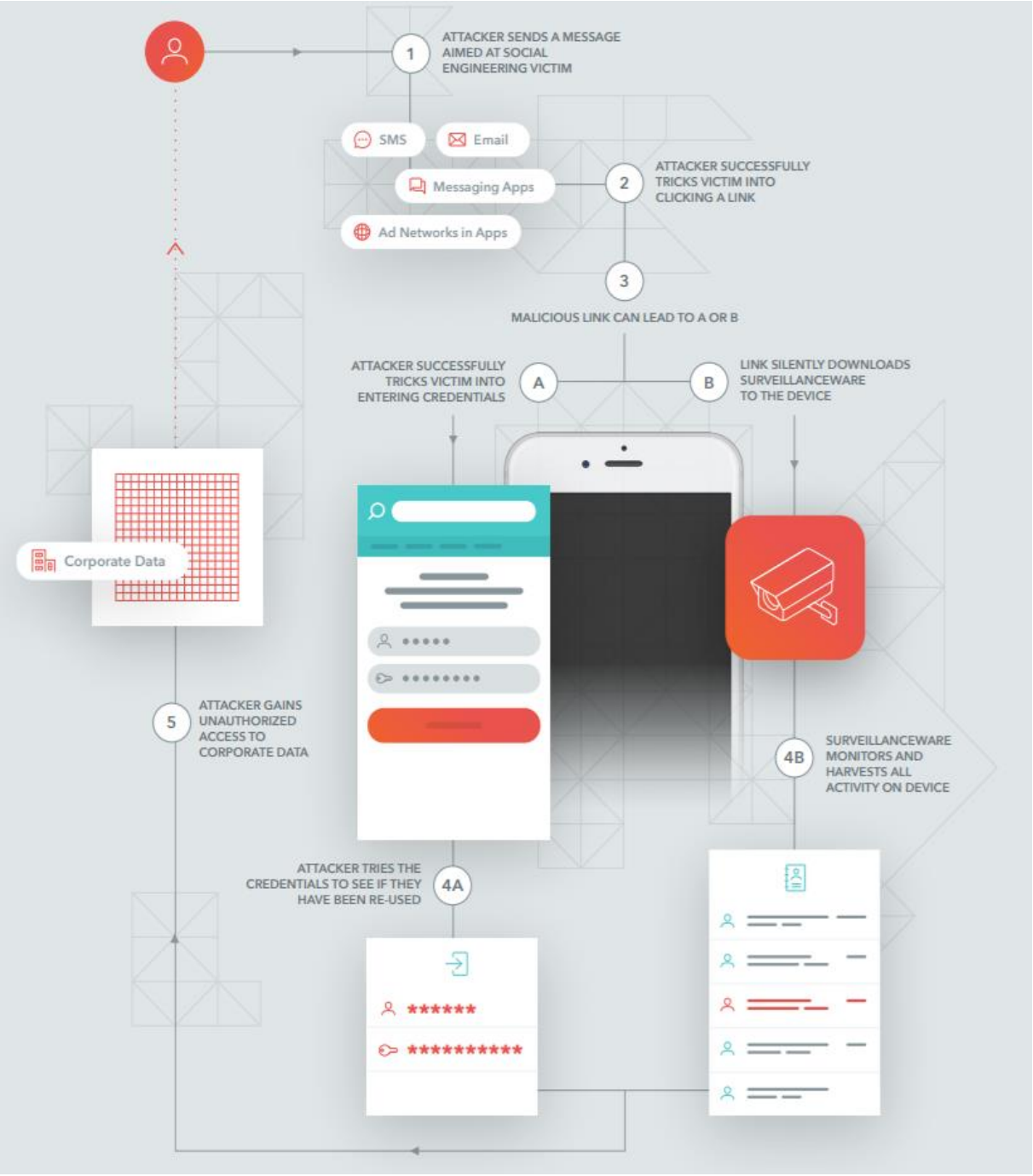
Na grafikonu 1, vidljivo je da je već odavno premašen broj populacije u vidu korištenja mobilnih terminalnih uređaja. U slijedeće četiri godine predviđa se rast broja korisnika čak do 16,8 milijardi.

Razvoj mobilnih uređaja također je transformirao poduzeća, doslovno mijenjajući način na koji se posao odvija. Poduzeća aktivno traže načine promicanja produktivnosti i fleksibilnosti zaposlenika, a da pritom osjetljive podatke, informacije o zaposlenicima i klijentima te mrežu održe sigurnima. Administratori u takvim okruženjima žele omogućiti zaposlenicima slobodno pregledavanje sadržaja na internetu putem mobilnih uređaja uz korištenje blokiranja za neželjene internetske sadržaje. Također, često se formiraju posebni sigurnosni odjeli koji izdaju upozorenja na mobilnim uređajima zaposlenika.

Jedno od čestih rješenja unutar okruženja poduzeća je BYOD (engl. *Bring Your Own Device*). On predstavlja praksu dopuštanja zaposlenicima organizacije da koriste vlastite osobne uređaje u poslovne svrhe. Statistički podaci pokazuju da je u 2017. godini 59% organizacija dopustilo je zaposlenicima da koriste vlastite uređaje za potrebe rada, a sljedeće godine 13% više. To je samo pokazatelj da se BYOD praksa pokazala veoma učinkovitom, [7].

3. Zlonamjerne prijetnje usmjerene mobilnim terminalnim uređajima

Zbog broja uređaja te zbog razloga korištenja i adaptiranja mobilnih terminalnih uređaja u svrhu svega u čemu su primjenjivi, jasna je značajnost podataka koji se pohranjuju na uređaju. Stoga je potrebno osigurati maksimalnu sigurnost istih te spriječiti zlonamjerne prijetnje i napade usmjerene prema mobilnom uređaju. Dijagram toka zlonamjernog napada usmjerenog mobilnom uređaju prikazan je na slici 1.



Slika 1. Dijagram toka zlonamjernog napada usmjerenog mobilnom uređaju, [8].

Na slici je vidljiv proces zlonamjernog napada gdje napadač prvotno šalje poruku žrtvi koristeći različite načine (SMS, E-mail poruke i sl.) te, ukoliko uspješno navede žrtvu na pristupanje poslanoj poveznici, vodi do dvije različite opcije. U jednoj žrtvu navodi na unošenje podataka za prijavu te ih potom „prisvaja“ i pristupa sustavu kojeg je žrtva dio, dok u drugom odlaskom na poveznicu žrtvi se na uređaj pozadinski preuzima nadzorni sustav koji napadaču služi kao sustav za nadzor i prikupljanje aktivnosti koje se odvijaju na uređaju.

3.1. Trend sigurnosnih nedostataka

Osim zlonamjerne strane, bitno je spomenuti i same korisnike te nedovoljnu informiranost ili neodgovorno upravljanje uređajem. Statistike iz [9] navode sljedeće:

- Više od 82% korisnika Android operativnog sustava tijekom ispitivanja koristili su verziju stariju od dvije godine.
- Mjesec dana nakon dostupnosti ažuriranja, samo 55% korisnika Apple iOS-a je obavilo nadogradnju sustava na inačicu iOS 11.
- 35% komunikacije odaslane putem mobilnih terminalnih uređaja nije kodirano, što znači da je čak jedna trećina prenesenih podataka bila izložena opasnosti.
- Svaki mobilni uređaj u prosjeku se dnevno se spoji na 160 jedinstvenih IP adresa.
- 45% korisnika ne koristi lozinku, PIN ili uzorak za zaključavanje na svojim uređajima.
- 82% Android uređaja je bilo podložno najmanje 25 „ranjivosti“ u operativnom sustavu.
- Poslovne aplikacije su tri puta više izložene curenju podataka o korisničkoj prijavi od onih prosječnih, što znači da izlažu opasnosti poslovne i osobne podatke.
- Aplikacije društvenih mreža u prosjeku tri puta više izlažu opasnosti podatke za prijavu.
- 24.7% mobilnih aplikacija sadrže barem jedan visokorizični nedostatak
- Polovica aplikacija s pet do deset milijuna preuzimanja sadrže sigurnosne nedostatke, [9].

Pametni telefoni su krajnje točke telekomunikacijske mreže i interneta, što znači da su povezani i s internetskim i s telekomunikacijskim mrežama.

Kako je već navedeno, imaju brojne mogućnosti i prenosivi su. Sadrže različite operativne sustave (Microsoft Windows, iOS i Android itd.). To potencijalnom napadaču omogućuje širok spektar različitih zlonamjernih programa za prebacivanje s interneta na telekomunikacijske mreže. Ovaj zlonamjerni softver predstavlja prijetnju te tzv. *malware* koji se prenosi putem interneta ili drugih mreža.

3.2. Izvori i vrste napada

Postoje različiti izvori napada krađom identiteta usmjerenih mobilnim terminalnim uređajima. Ovi napadi ne utječu samo na njih, već i na telekomunikacijske mreže.

Glavni izvor napada predstavlja Internet. Najčešća vrsta napada je širenje zlonamjernog softvera i zlonamjerni napad zbog postojanja bežičnih internetskih (*Wi-Fi*) veza koje su omogućene, a njihov broj raste iz dana u dan u domovima i tvrtkama. Pametni uređaji imaju ugrađenu Wi-Fi podršku, a veza često nije ispravno osigurana. Taj propust se iskorištava zloupotrebom i napadom na mrežu na koju je uređaj spojen, [10].

Nadalje, moguća je krađa osobnih podataka. Primjerice, spremljene zaporke, PIN kodovi itd. Nezakonito oduzeti zaštićeni podaci mogu biti preuzeti pomoću uređaja od strane napadača koji se „skriva“ koristeći pristupnu točku koju koristi korisnik. Napadač se može služiti i slanjem zlonamjernih poruka e-pošte pomoću nezaštićenih WiFi veza.

U poslovnom okruženju, zlonamjerni član tvrtke može otuđiti osjetljive podatke iz tvrtke i kasnije ih zloupotrebljavati, [10].

Postoji i mogućnost prijenosa virusa s osobnog računala na mobilni uređaj prilikom njihovog korištenja i to zbog sinkronizacije ili prijenosa podataka. Moguće je i da je računalo zaraženo virusom i tijekom prijenosa podataka ili tijekom sinkronizacije podataka. U tom slučaju može se zaraziti osobni uređaj ili uređaj poduzeća, te u konačnici i cijela mreža. Uzroci zaraze datoteka mogu biti različiti. Tu je prijenos podataka, sinkronizacija podataka, instalacija softvera putem osobnog računala i dopuštanje instalacije nepotvrđenih aplikacija.

Pametni mobilni uređaji koriste i različite veze za prijenos podataka, a, uz internet, postoje i bežični uređaji kratkog dometa veze. Riječ je o infracrvenoj i Bluetooth tehnologiji koje se također mogu koristiti za širenje zlonamjernog softvera i druge napade. Primjerice, prvi otkriveni crv u povijesti bio je *Cabir* koji se pojavio kod korisnika operativnog sustava Symbian. On je, koristeći *Bluetooth* tehnologiju, prepoznavao druge uređaje s istim načinom

rada te se širio automatski i na njih. Kod infracrvene tehnologije, koja predstavlja vezu veoma kratkoga dometa, javlja se problem gdje korisnik, upravo zbog opsega dometa, vjeruje da je povezan na uređaj od povjerenja, te da će zaprimiti podatke samo iz pouzdanih izvora. No, slučaj nije uvijek takav, te se i na ovaj način uređaj može zaraziti zlonamjernim softverom, [10].

Druge opasnosti, koje su predmet ovoga rada, krađa identiteta i lažiranje, predstavljaju mogućnost da putem kompromitiranog uređaja, napadač može koristiti identitet uređaja za bilo koju aktivnost u ime legitimnog korisnika.

Postoji i udaljeno prisluškivanje gdje se pomoću kompromitiranog uređaja može snimiti bilo koji telefonski razgovor koji napadač može i zadržati.

3.3. Svrha i žrtve napada

Uz povećanje korištenja pametnih telefona, sigurnosni problemi se, također, povećavaju. Tijekom napada na uređaj, napadač može otuđiti ili oštetiti različitu imovinu kao što su osobni podaci (osjetljivi podaci kao što su osobni dokumenti, osobne bilješke, kalendar, popis zadataka itd.), korisničku internetsku vezu, kontakte, posjetnice, videozapise ili multimediju.

Moguće prijetnje prema korisničkim uređajima mogu biti zlonamjernog koda koji uređaj može uništiti, prekinuti mu standardne funkcije i na taj način dati napadaču pristup informacijama i podacima pohranjenim u uređaju. Potrebno je i provjeravati poveznice na *web* stranice, e-poštu ili tekstualnu poruku koja potiče na neopreznosti kako bi korisnici otkrili lozinke, financijske podatke ili druge privatne podatke. Sve navedeno uvijek je u interesu zlonamjernoj strani te se eventualni sigurnosni nedostaci maksimalno iskorištavaju, [10].

Razlozi koji mobilne uređaje čine zanimljivim strani napadača su brojni. Primjerice, osim navedenog rasta samog broja uređaja, zanimljiva je i stalna povezanost s Internetom koja, ukoliko je zlonamjerni napad takve vrste, omogućuje napadaču nadzor te kontrolu nad uređajem što zlonamjerni napad čini vremenski neovisnim (osim u slučaju da žrtva otkrije te se pobrine o prekidu istoga).

4. Mehanizmi i svojstva napada krađom identiteta

Krađa identiteta (engl. *mobile phishing*) predstavlja praksu slanja lažnih komunikacija koje dolaze iz vjerodostojnog izvora. Obično se obavlja putem e-pošte. Cilj mu je otuđiti osjetljive podatke kao što su podaci o kreditnoj kartici i podaci za prijavu ili instalirati zlonamjerni softver na žrtvinom uređaju. Krađa identiteta uobičajena je vrsta *cyber* napada te počinje s lažnom e-poštom ili drugom vrstom komunikacije osmišljenom kako bi privukla žrtvu. Poruka je napravljena da izgleda kao da dolazi od pouzdanog pošiljatelja. Ako žrtvu obmanjuje, on ili ona se nagovaraju na pružanje povjerljivih informacija, često na *web* lokaciji s prijevarama. Ponekad se zlonamjerni softver, također, preuzima na ciljni uređaj.

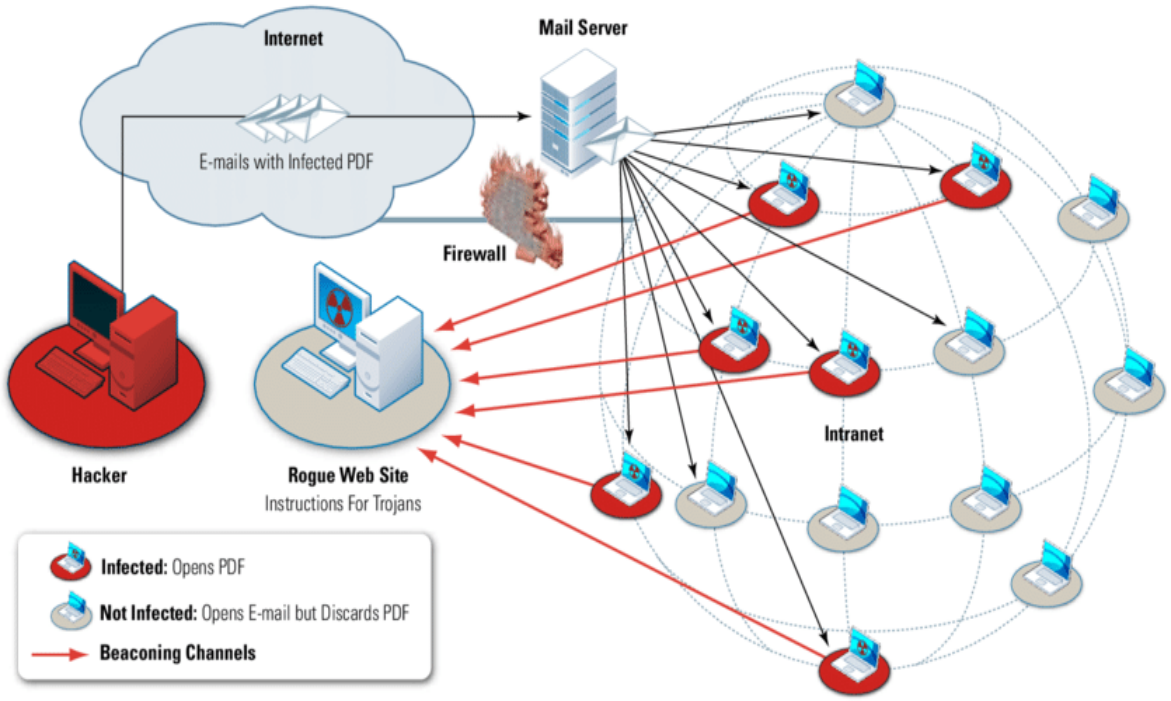
Ponekad su napadači zadovoljni dobivanjem podataka o kreditnoj kartici žrtve ili drugih osobnih podataka radi financijske dobiti. U drugim slučajevima, *phishing* e-poruke šalju se radi dobivanja podataka za prijavu zaposlenika ili drugih detalja za korištenje u naprednom napadu na određenu tvrtku. Napadi *cyber* kriminala kao što su napredne trajne prijetnje i *ransomware* često počinju s *phishingom*. Ovi napadi spadaju u kategoriju *web* baziranih prijetnji, [11].

Pokušaji krađe identiteta najčešće počinju s porukom e-pošte koja pokušava dobiti osjetljive informacije putem interakcije s korisnikom, kao što je pristupanje zlonamjernoj vezi ili preuzimanje zaraženog privitka. Kroz manipulaciju linkovima, e-pošta se može prikazati s vezama koje lažno prikrivaju legitimne URL-ove, a manipulirane veze mogu sadržavati suptilne pogreške ili korištenje poddomene. Prijevare krađe identiteta mogu koristiti krivotvorenje *web* lokacije koja koristi naredbe JavaScripta kako bi URL *web* lokacije izgledao legitimno. Koristeći tajno preusmjeravanje, napadači mogu pokvariti legitimne *web* lokacije sa zlonamjernim skočnim dijaloškim okvirima koji preusmjeravaju korisnike na *web* mjesto za krađu identiteta. Zaraženi privitci, kao što su *.exe* datoteke, datoteke sustava Microsoft Office i PDF dokumenti, mogu instalirati *ransomware* ili drugi zlonamjerni softver. Prijevara putem krađe identiteta može uključivati i telefonske pozive, tekstualne poruke i alate društvenih medija kako bi se žrtve navele na pružanje osjetljivih informacija.

4.1. Vrste napada krađom identiteta

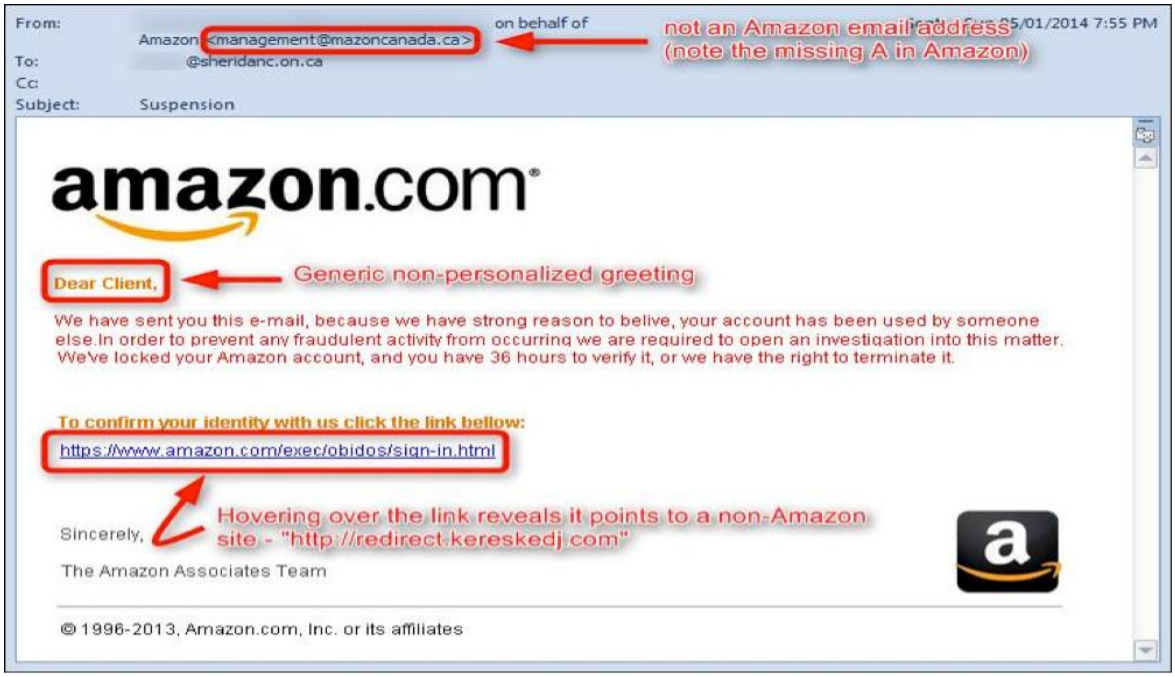
Neke vrste *phishing* prijevare koriste više ciljanih metoda za napad na određene pojedince ili organizacije:

1) ***Spear phishing*** - poruke e-pošte za krađu identiteta neće izgledati slučajno kao općenitiji pokušaji krađe identiteta. Napadači će često prikupljati informacije o svojim ciljevima kako bi ispunili e-poštu s autentičnijim kontekstom. Neki napadači čak otimaju poslovnu e-poštu i stvaraju vrlo prilagođene poruke. Na slici 2 prikazan je proces širenja zaražene pdf datoteke od zlonamjerne strane (engl. *hacker*) u intranet mrežu putem *mail* poslužitelja.



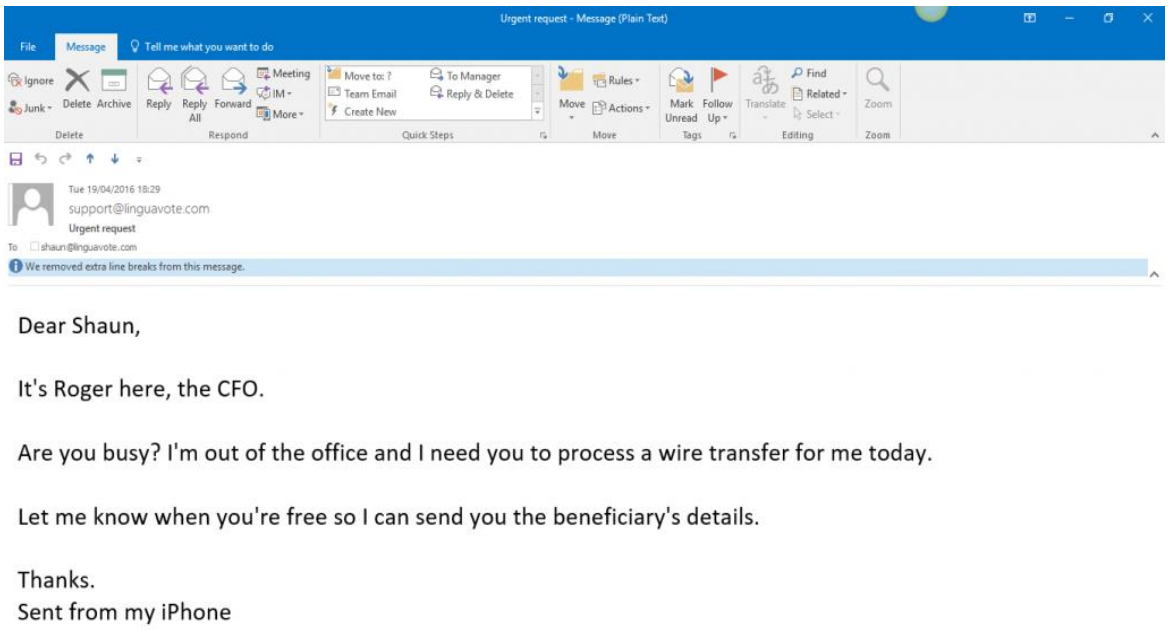
Slika 2. Opis *spear phishing* napada, [12]

2) ***Clone phishing*** - napadači mogu pregledati legitimne, prethodno isporučene poruke e-pošte, izraditi gotovo identičnu kopiju ili klonirati, a zatim promijeniti privitak ili vezu u nešto zlonamjerno. Slika 3 prikazuje otkrivene neuobičajenosti lažne e-pošte dobivene na adresu žrtve, kao što su, primjerice, sumnjiva domena adrese odredišta te pogrešna e-mail adresa koja oponaša onu službenu.



Slika 3. Primjer napada *clone phishingom*, [13]

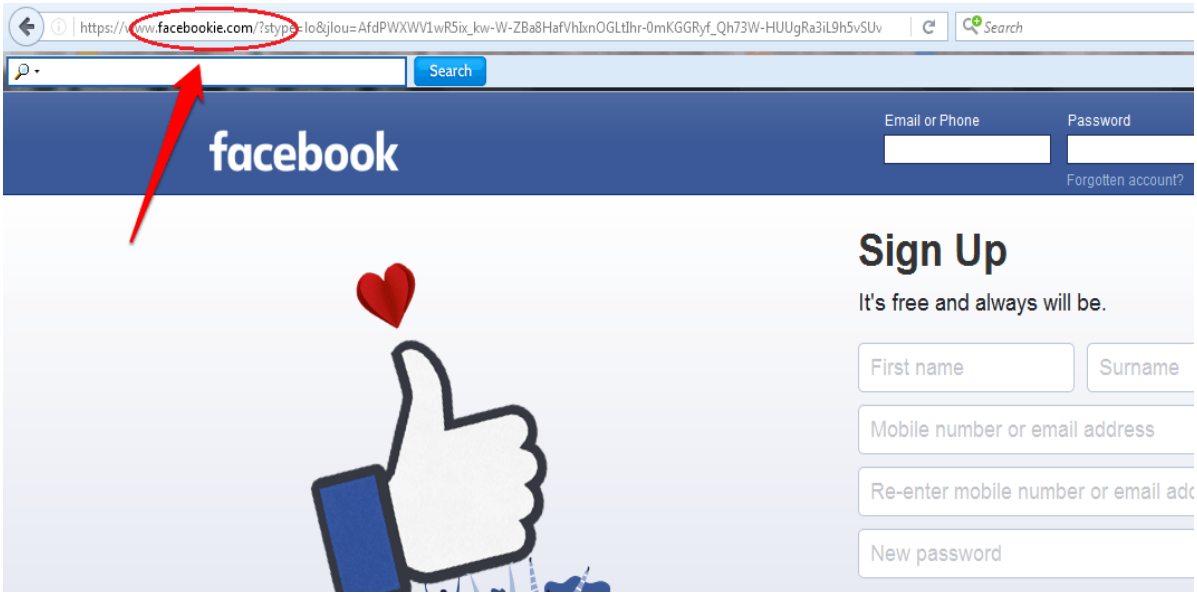
3) ***Whaling*** **-** posebno cilja osobe visokog profila i/ili više rukovoditelje u nekoj tvrtki. Sadržaj pokušaja *whalinga* često će se predstavljati kao pravna komunikacija ili drugi visoki izvršni posao, [14]. U primjeru ispod, na slici 4, prikazan je upravo primjer lažnog predstavljanja gdje se napadač predstavlja kao dio poduzeća čijeg je žrtva dio.



Slika 4. Prikaz *whaling* napada, [15]

4) ***Krivotvorenje* web *lokacije (engl.* website forgery*)***

Na slici 5 uočljivo je kako je napadač lažirao standardnu internetsku domenu društvene mreže Facebook s dva dodatna slova na kraju („facebookie“) kako bi se ostvario cilj da žrtva nesvjesno unese svoje podatke za prijavu ne provjeravajući vjerodostojnost poveznice.



Slika 5. Primjer krivotvorenja web-lokacije, [16]

Navedene ciljane metode napada moguće je uočiti uz dovoljno pozornosti te se, ovisno od napadača, mogu razlikovati u kvaliteti i izdvojenom trudu prilikom istih.

4.2. Proces stvaranja mehanizama za napad krađom identiteta

Ovo potpoglavlje opisuje proces stvaranja pokušaja krađe identiteta te će, u edukacijske svrhe, prikazati navedeno u oblicima koji su najčešći, a to su:

- krađa identiteta slanjem lažne e-pošte
- krađa identiteta stvaranjem i slanjem lažne, ali što vjerodostojnije web-lokacije
- krađa identiteta stvaranjem i preuzimanjem lažne aplikacije putem Android sustava

4.2.1. Stvaranje lažne e-pošte

Napadi na e-pošte (engl. *e-mail phishing*) veoma su uvjerljivi i unikatni za svaku situaciju. Proces stvaranja uspješne kampanje *phishing* e-pošte je veoma metodičan, a velik dio vremena i napora ulaže se već u razdoblju planiranja napada.

Za početak, bitno je naznačiti da je e-pošta dobro zaštićena višeslojnim sigurnosnim pristupom, što ovaj proces čini još težim i kompleksnijim budući da u svakom sloju postoji mogućnost da sigurnosni sustav odbaci i uništi odaslanu poštu. Na slojevima se tako može naići na filtre neželjene e-pošte, neželjenu poštu programa *Outlook*, antivirusne programe, filtriranje izlaznih datoteka, sustave za sprječavanje nedozvoljenog „upada“, *web proxy* poslužitelje i slično.

Proces zaobilaska navedenih funkcionalnosti na sigurnosnim sustavima je složen. Potrebno je krenuti od nabrajanja *e-mail* adresa, odnosno, određivanja kome se točno treba poslati e-pošta. Postoji niz izvora koji rade analizu i prikupljaju podatke. Takvi programi obično sadrže opciju da rezultat bude vidljiv i u formatu baze podataka. Skripte koje su integrirane u programe ovakve prirode imaju mogućnost pretraživanja različitih tražilica te njihovo sakupljanje. Na slici 6 prikazan je upravo ispis rezultata prikupljanja adresa u CSV datoteci baze podataka pomoću programa naziva *Jigsaw*, [17].

```
$ ./jigsaw.rb -i 215043 -r google -d google.com -u username -p password
Found 1047 records in the Sales department.
Found 666 records in the Marketing department.
Found 870 records in the Finance & Administration department.
Found 249 records in the Human Resources department.
Found 150 records in the Support department.
Found 1282 records in the Engineering & Research department.
Found 354 records in the Operations department.
Found 1171 records in the IT & IS department.
Found 300 records in the Other department.
Generating the final google.csv report
Wrote 6079 records to google.csv
```

Slika 6. Nabrajanje e-mail adresa, [17]

Nadalje, korisno je poznavati antivirusne programe, što uvelike može pomoći u stvaranju uspješnog napada. Pri tome se koristi DNS (engl. *Domain Name System*) koji pomaže u određivanju postojećeg antivirusnog programa. Potrebno je instalirati antivirusni program u virtualnom stroju (engl. *Virtual Machine Manager*) prije slanja e-pošte za krađu identiteta. Preporučuje se instalacija točne verzije antivirusnog programa kod žrtve, iako to nije uvijek moguće. Također, potrebno je instalirati nekoliko besplatnih antivirusnih programa (npr. AVG, Security Essentials) jer je prvotno bitno zaobići antivirusni program u virtualnom računalu napadača kako bi se povećala mogućnost zaobilaženja onoga kod žrtve.

Za filtriranje postavljenih ograničenja potrebno je odabrati korisni tok. Postoje dvije opcije, „reverse_http“ koji je svjestan postojanja *web proxyja* ili „reverse_tcp_all_ports“ toka koji zavaravaju tok podataka na strani žrtve. Bitan modul „reverse_tcp_all_ports“ toka je obrnuti TCP (engl. *Transmission Call Protocol*) koji radi sa stavkama označenim kao „allports“. Ovaj rukovatelj „osluškuje“ na jednom TCP *portu*, a operativni sustav preusmjerava sve dolazne veze na sve *portove* upravo na navedeni port za „osluškivanje“. Ovaj proces podrazumijeva korištenje IP tablica ili drugog filtra paketa kako bi ispravno obavljao zadanu funkciju, [17].

```
iptables -t nat -A PREROUTING -p tcp --dport 1:65534 -j REDIRECT --to-ports 443
```

Slika 7. Primjer naredbe “iptables”, [17]

Slika 7 prikazuje kako naredba *iptables* izgleda na Linux operativnom sustavu. Naredba iz primjera svaki *port* usmjerava na 443/tcp gdje rukovatelj sluša i spreman je dohvatiti ljuske porta. Ono što se omogućuje ovim procesom je premještanje SSH-a (engl.

Secure Shell), odnosno, mrežnog protokola za uspostavu sigurnog komunikacijskog signala na *port* 65535 tako da se i dalje ostavlja mogućnost daljinskog prijavljivanja, ali da to ne utječe na proces *phishinga*.

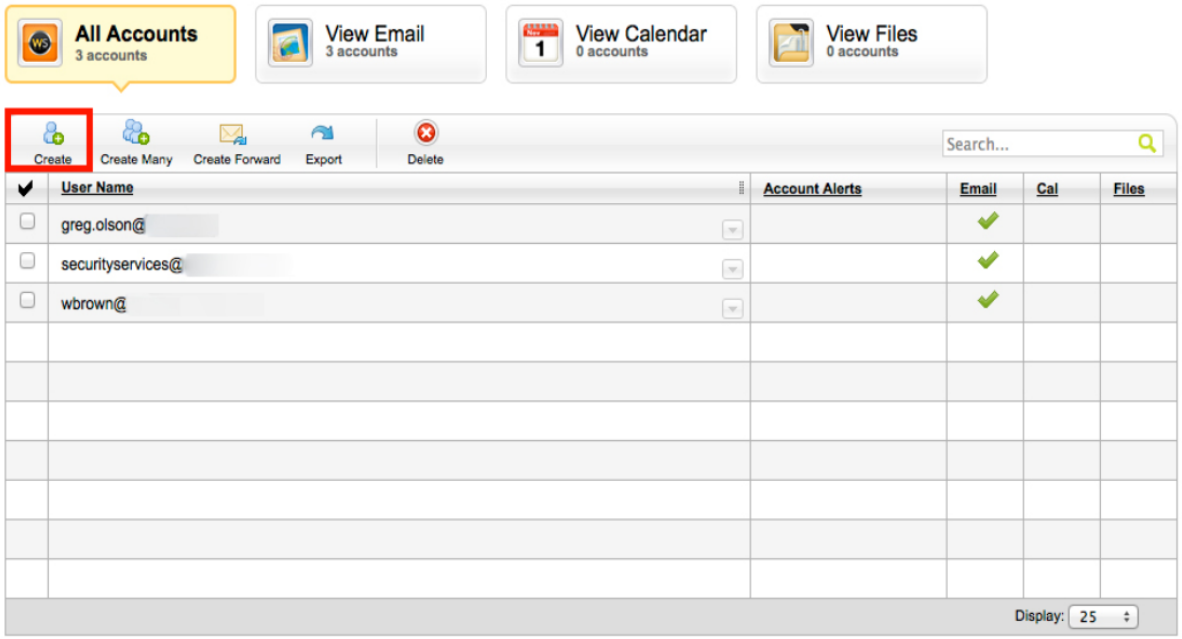
Reverse_https je još jedna velika prednost jer uspostavlja i šifrira povratni kanal na *metasploit* (korišteni alat za proboj sustava u primjeru) poslužitelj i otežava sustavima za sprječavanje upada u tunelu da otkriju zlonamjerni promet. Ne samo da oblaže sadržaj, već je i svjestan *proxyja*, što znači da će iskoristiti sve postavke na programu internetskog pretraživača. *Rev_https* izgleda veoma slično generičkom HTTPS-ovom (*HyperText Transfer Protocol Secure*) prometu, što znači da je veoma težak za detektiranje u odsustvu SSL-a (*Secure Sockets Layer*), [18].

Odabir sadržaja *phishinga* e-pošte je zapravo najjednostavniji dio procesa. Prema broju napada, tj. klikova na zlonamjerne veze, uočljivo je da žrtve često nasjedaju na takvu vrstu prijevare. Primjerice, žrtvama vjerodostojno zvuči i izgleda sadržaj e-pošte koji dolazi od člana poduzeća (npr. iz informatičkog odjela) koji moli zaposlenike da preuzmu i instaliraju određene stavke te ih se povezuje s internetskim adresama koje su, u ovom primjeru, izrađene pomoću programa SET koji služi za veoma brzo kloniranje *web* lokacije odabrane od napadača.

Mnoga poduzeća koriste *web-proxy* poslužitelje koji blokiraju krajnje korisnike od posjeta određenim *web* lokacijama. Također, oni mogu imati i antivirusni mehanizam za proces skeniranja koji razotkriva zlonamjerni promet s *web* lokacija. Postoji i mogućnost restrikcije krajnjim korisnicima da uopće preuzimaju izvršne datoteke (s ekstenzijom *.exe*). No, kupnjom SSL certifikata za *web* lokaciju s koje dolazi napad, moguće je zaobići navedena ograničenja.

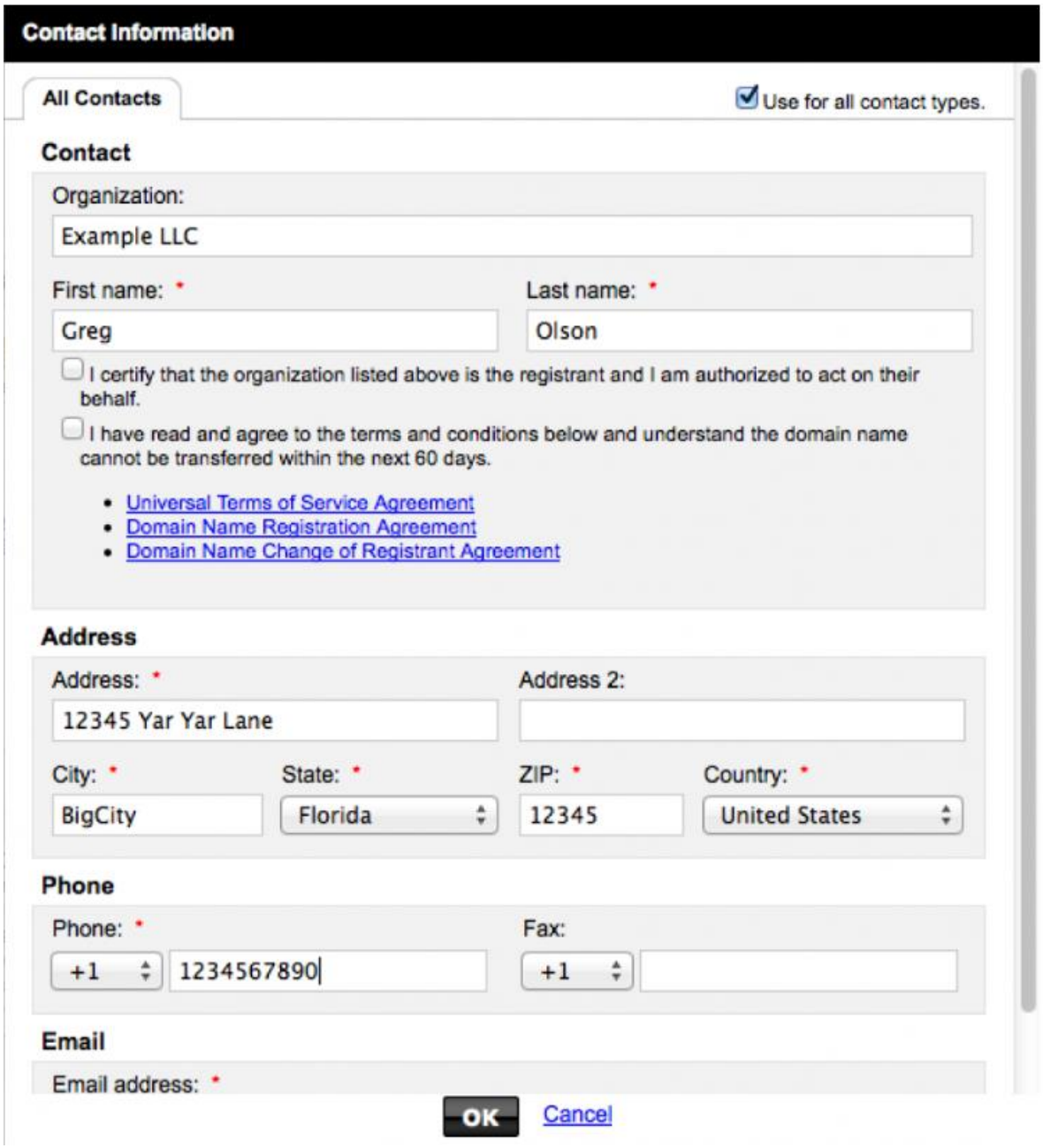
Kod slanja e-pošte postoje razne opcije. Kod primjera koji se u ovom slučaju prati, tu se podrazumijeva kupljena domena putem *web* lokacije *GoDaddy* gdje se prijavom na vlastiti račun i odabirom simbola [+] kod kategorije „e-pošta“ klikom na gumb za pokretanje otvara upravljačka ploča. Nakon otvaranja, odabire se gumb "Stvori" kako bi brzo stvorili račun e-pošte, kao što je prikazano na slici 8. Prednost kod stvaranja računa e-pošte navedenog davatelja usluge *hostinga* je ta da automatski postavlja MX (*Mail exchanger record*), odnosno zapis za specifikaciju *mail* poslužitelja. To je korisno jer se kod mnogih pristupa obavlja obrnuto DNS pretraživanje domene s kojeg je primljena e-pošta. Ukoliko domene nema, mnogi će pristupnici odmah ispustiti poruku te iz tog razloga poruka koja bi

eventualno omogućila krađu identiteta putem e-pošte nikada ne bi dospjela u korisničku pristiglu poštu, [17].



Slika 8. Brzo stvaranje e-pošte, [17]

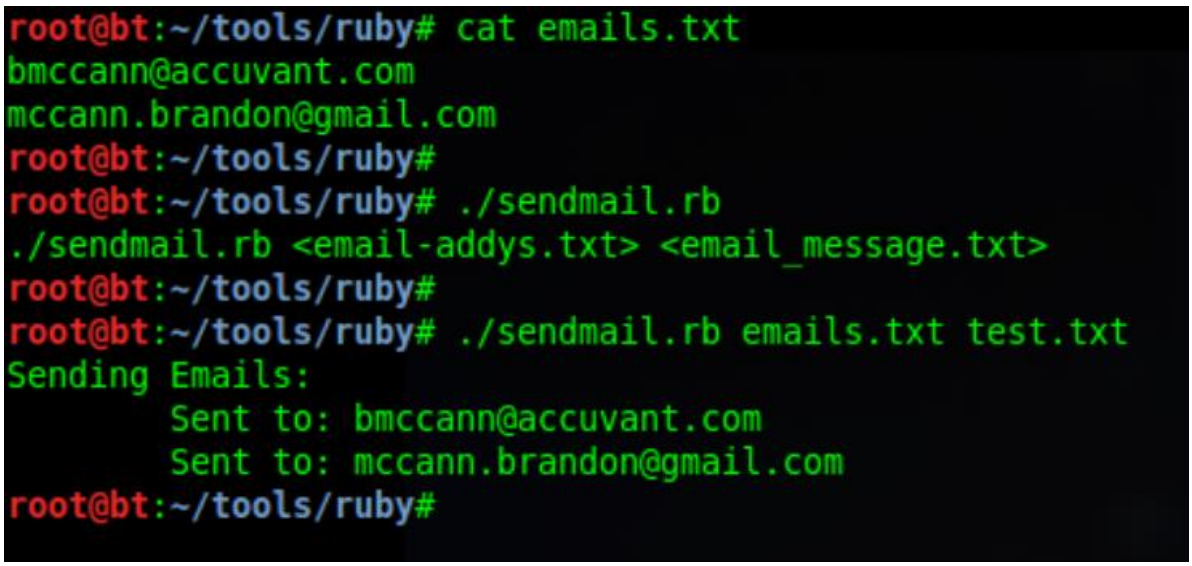
Dalje se može naići i na još jedan sloj sigurnosti, a to je SMTP (*Simple Mail Transfer Protocol*). On vrši pretragu naziva *Whois*, koja je usredotočena na domenu s koje se šalje e-pošta, sve u cilju osiguravanja ispravnosti i podudarnosti, [19]. Zaobilazak ovoga pretraživanja može pružiti navedeni *hosting GoDaddy* gdje se može urediti „*Whois* informacija“ da se ispravno podudara s onom koja se traži. Primjerice, za oponašanje domene *example.com*, izvršava se *Whois* pretraživanje te se provjerava podudarnost. *GoDaddy* sučelje za brzo mijenjanje „*Whois* informacija“ za kupljeno ime domene prikazano je na slici 9.



Slika 9. Sučelje *hostinga GoDaddy* za kupljenu domenu, [17]

Nakon konfiguriranja računa e-pošte, u ovom primjeru povezuje se klijent e-pošte *Thunderbird* za primanje i slanje pošiljki. Kod slanja poruka e-pošte postoje i neke dodatne pogodnosti kod slanja poruke e-pošte iz skripte. U primjeru je napisana skripta „sendmail.rb“, čija je zadaća popisivanje adresa e-pošte, uključujući poruku koja se šalje ciljanim korisnicima. Skripta „sendmail.rb“ pruža mogućnost praćenja pojedinog korisnika kada se poruke e-pošte šalju iz skripte. Prije slanja e-pošte, ona kodira adresu e-pošte korisnika i dodaje je na kraj URL-a za phishing e-pošte.

Na primjer, ukoliko je želja napadača da korisnik klikne na „http://example.com“, sendmail.rb će izmijeniti URL u poruci e-pošte tako da postane nešto kao „http://example.com/index.php?dXNIckBleGFtcGxlLmn===“. Kada korisnik klikne na navedeni link za phishing, dobiva se jedinstveni unos u pristupne bilješke koji kasnije prikazuje zahtjev koji se daljnjim postupkom dekodira, te se na osnovu toga određuje adresa e-pošte tog korisnika. Na slici 10 prikazan je pojednostavljeni primjer slanja skripte dvjema korisnicima, [17].



Slika 10. Prikaz skripte za slanje „sendmail.rb“ skripte dvama korisnicima, [17]

Važno je napomenuti kako je prikazani primjer [17] jedan od mnogih te da, zbog specifičnosti svake situacije, ovaj proces neće uvijek funkcionirati.

4.2.2. Stvaranje lažne *web* lokacije

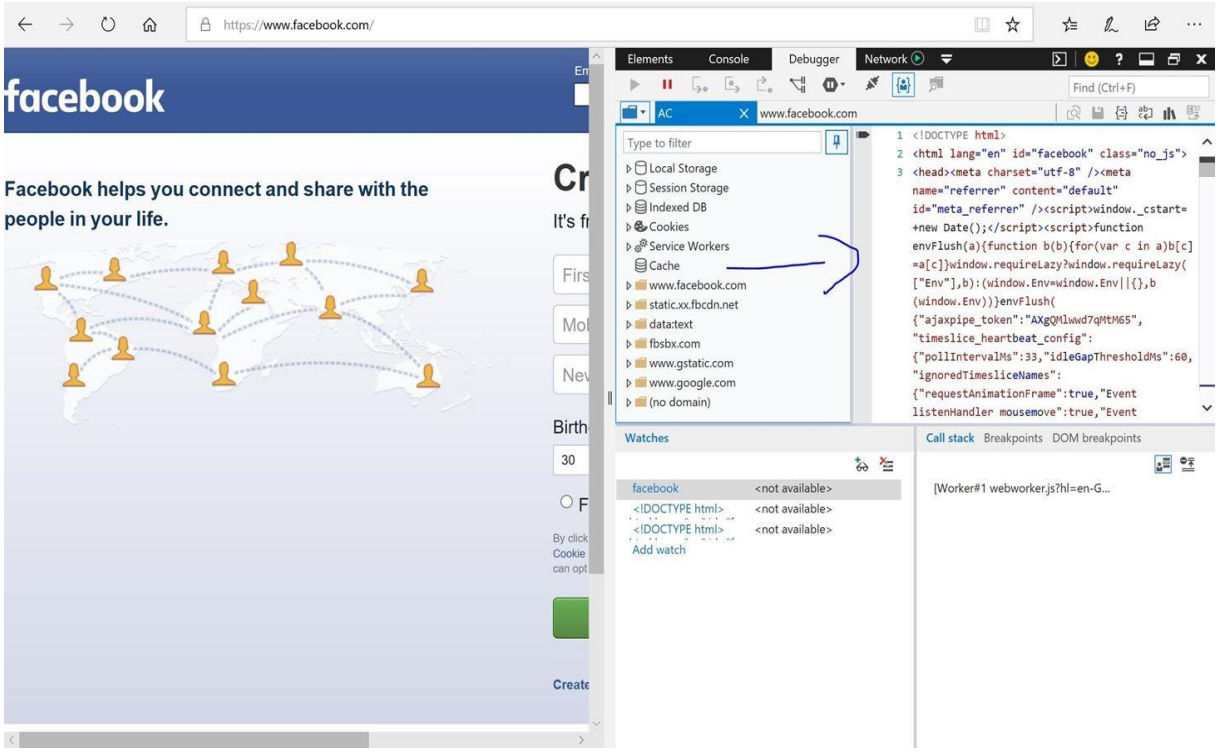
Stvaranje ovakvih *web* lokacija poprilično je kompleksan proces. Naročito u novije vrijeme gdje se od strane *hostinga* sve češće uklanjaju ovakve stranice prilikom detekcije istih.

Za početak, potrebno je preuzeti HTML indeks web-lokacije. U ovom primjeru će se koristiti primjer stvaranja što vjerodostojnije kopije stranice društvene mreže Facebook, čiji je originalni izgled prikazan na slici 11.



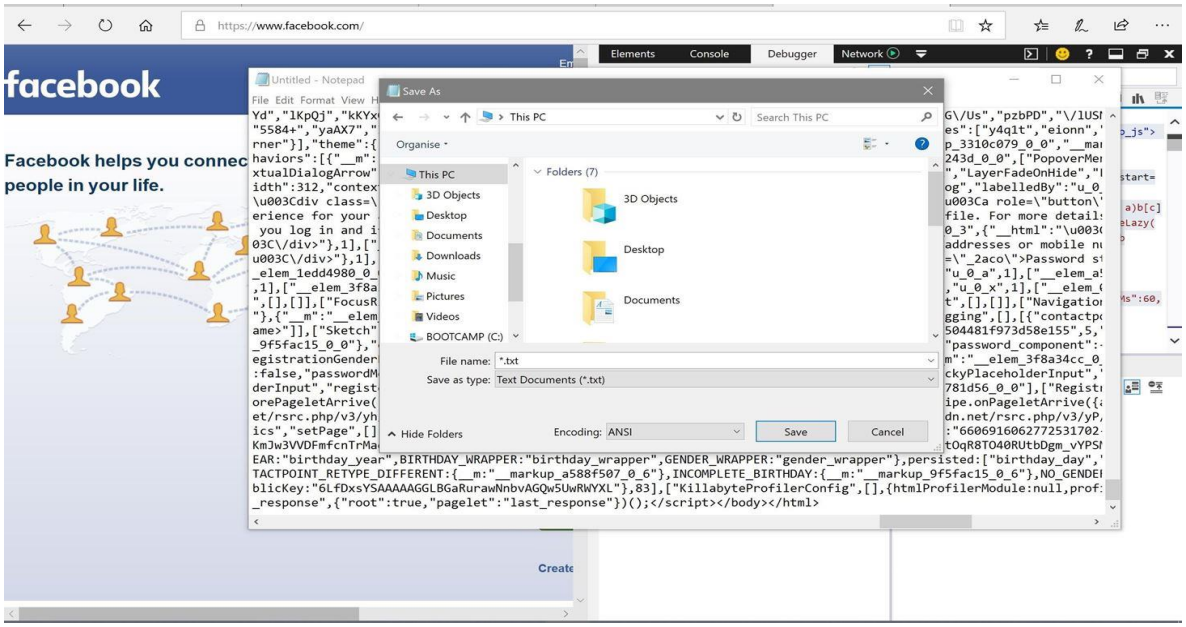
Slika 11. Izvorni izgled *web* stranice Facebooka, [20]

Za preuzimanje HTML indeksa, obično je potrebno samo desnim likom na web lokaciju u izborniku izabrati „Prikaži izvor“, što je opisano na slici 12.



Slika 12. Prikaz izvora *web* lokacije, [21]

Kako bi odabrali i preuzeli izvor *web* lokacije sa slike iznad, potrebno je kopirati i zalijepiti kompletan tekst u tekstni dokument. Prikaz dobivenog rezultata ovog postupka opisan je slikom 13.



Slika 13. Prikaz sadržaja izvora u tekstnom dokumentu, [21]

Prema izborniku sa slike iznad, potrebno je izabrati „Spremi kao“ i postaviti opciju „Sve datoteke“ te promijeniti kodiranje u način *Unicode*. Nakon toga, dokument je potrebno nazvati kao „index.html“.

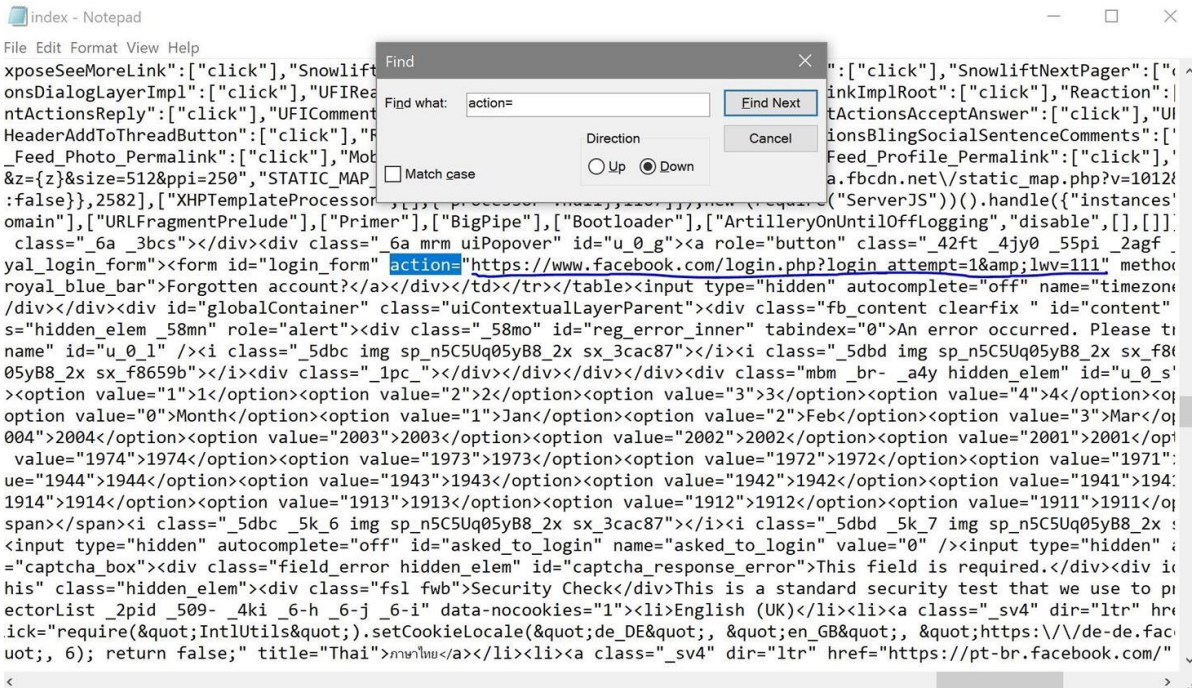
Nadalje, potrebno je stvoriti PHP datoteku za prikupljanje lozinki. Ona predstavlja alat koji prikuplja lozinku žrtve te se, i bez znanja programiranja, lako može naći gotova PHP datoteka s željenom funkcijom. Primjer gotove skripte iz ovog slučaja prikazan je na slici 14.

```
<?php
header ('Location: facebook.com');
$handle = fopen("log.txt", "a");
foreach($_POST as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n\n\n\n");
fclose($handle);
exit;
?>
```

Slika 14. PHP skripta za prikupljanje korisničkih lozinki, [21]

Kao i u prethodnom odjeljku, ovu se datoteku pohranjuje kao „Sve datoteke“ te se odabire „post.php“ i za kodiranje se postavlja *Unicode*.

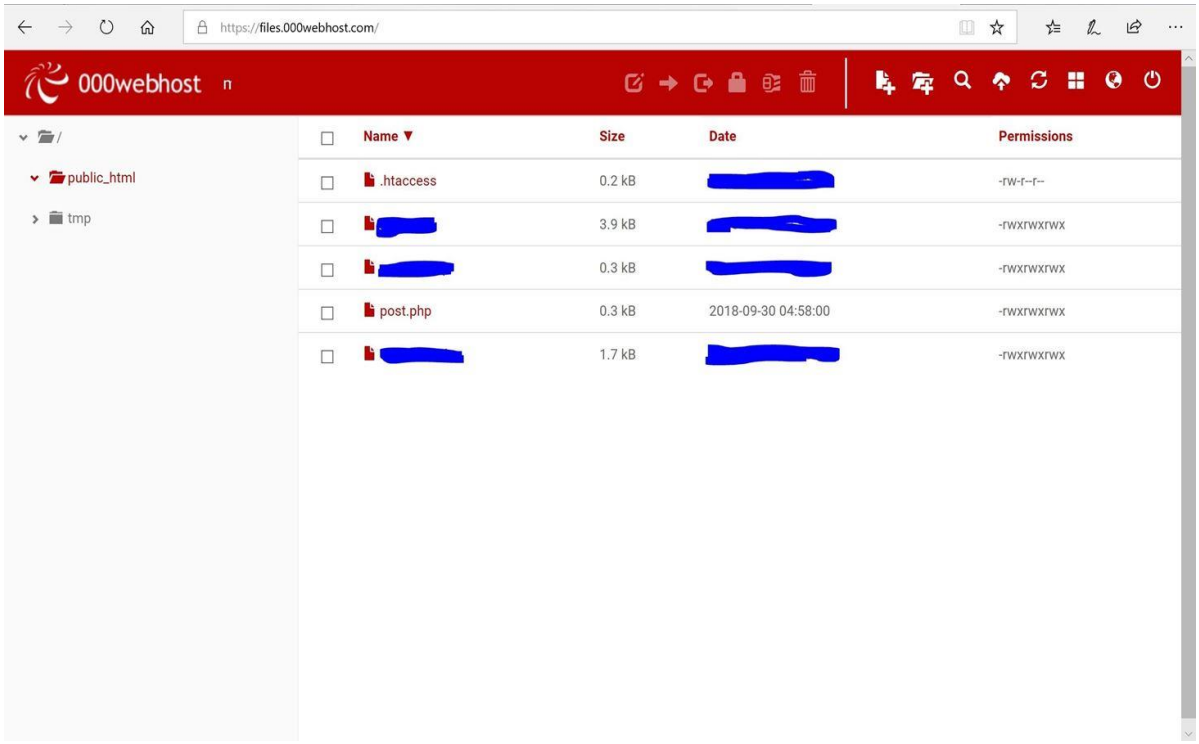
Idući korak ovoga procesa je promjena datoteke HTML stranice kako bi se unutar nje uključila i spremljena PHP datoteka. Potrebno ju je ugraditi kako bi obavljala svoju već navedenu funkciju. Za to je potrebno pronaći način slanja lozinke, tj. proučiti procesiranje *web* lokacije kada dolazi do pokušaja prijave korisnika. U ovom primjeru, potrebno je pomoću opcije traženja u dokumentu upisati „= action“ u polje za pisanje, a to je prikazano na slici 15, [21].



Slika 15. Opcija traženja potrebnog teksta u dokumentu, [21]

Podcrtani dio na slici iznad potrebno je zamijeniti s tekstom „post.php“. Važno je napomenuti da kod drugačijih tipova stranica koje imaju različit zapis od navedenog, postoji alat „Inspect elements“ pomoću kojega pronalazimo slično rješenje.

Daljnji postupak, koji zahtijeva otvaranje PHP datoteke za pohranu korisničke lozinke, je aktiviranje lažne stranice te omogućavanje korisnicima pristup istoj. Kao i u prethodnom primjeru, može se uzeti besplatna ili kupljena usluga *hostinga* i pohrane lozinki. U ovom primjeru korišten je *000webhost* čije je sučelje prikazano na slici 16.



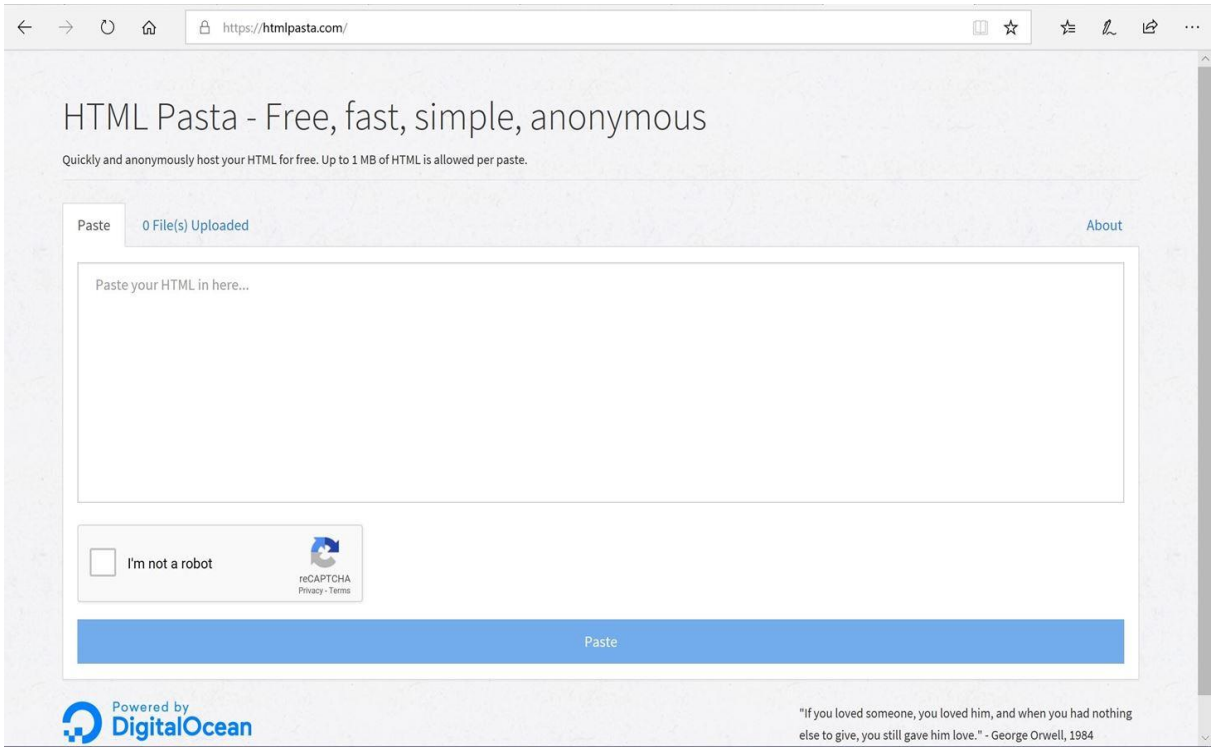
Slika 16. Prikaz sučelja *000webhost*-a, [21]

Naredni korak u procesu je učitati datoteku pomoću upravljača datotekama te izmijeniti dopuštenja. Na slici iznad već je učitana PHP datoteka i to u glavnu mapu FTP (*File Transfer Protocol*) poslužitelja. Nadalje, potrebno je promijeniti dopuštenje na „777“, što označava svako pojedinačno dopuštenje, te se, kada sustav zatraži označavanje okvira za dozvole, označava svaka dozvola, [22].

U sljedećem koraku se često nailazi na zabrane pokretanja ovakvih tipova stranica u veoma kratkom roku. No, potrebno je pronaći pravo rješenje *hostinga*.

Nadalje, prije pokretanja stranice, potrebno je iz konfigurirane skripte „post.php“ ponovno pronaći obrazac za prijavu unutar „index.html-a“ i zamijeniti „post.php“ sa stranicom koja je kreirana (npr., „http://yourwebsiteforyourphpupload/post.php“). Ako je sve ispravno zalijepljeno, odlaskom na ovaj URL, stranica bi trebala preusmjeravati na „facebook.com“ stranicu.

Hosting stvarne stranice provjerava se odlaskom na „htmlpasta.com“ gdje se javlja prikaz kao na slici 17.



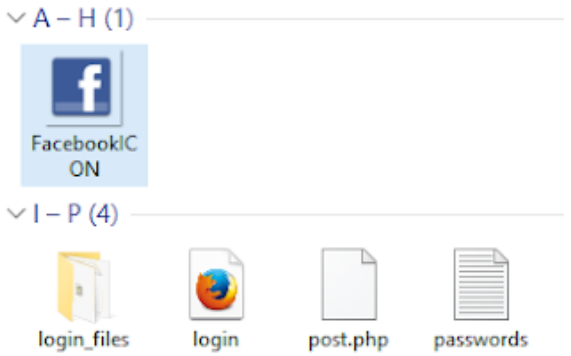
Slika 17. Prikaz sučelja *web* lokacije „htmlpasta.com“, [21]

U slobodni prostor za upisivanje na slici iznad, potrebno je kopirati datoteku „index.html“ te se nakon toga dobije veza za *web* lokaciju kreiranu za *phishing*. Proces je time i službeno završen te se eventualna provjera je li korisnik „nasjeo“ na lažnu stranicu i upisao korisničke podatke za prijavu provjerava na FTP poslužitelju gdje je smještena „post.php“ datoteka. Unutar nje trebao bi se pojaviti novi dokument naziva „log.txt“ gdje su smješteni navedeni podaci za prijavu.

4.2.3. Stvaranje lažne aplikacije na Android sustavu

U ovom primjeru također će se raditi o Facebook *phishing* metodi, ali ovoga puta će biti objašnjeno stvaranje aplikacije za nju. Rezultat je isti, a to su korisnički podaci za prijavu. Aplikacija u ovom slučaju, također, izgleda kao prava aplikacija Facebooka, s identičnim ikonama, što onemogućuje korisnicima prepoznavanje izvornosti. Zanimljivo je istaknuti kako su neke od glavnih komponenti stvaranja, kao što su gotovi kodovi ili pokretačke datoteke javno i lako dostupne.

Za početak stvaranja lažne aplikacije, potrebno je napraviti phishing Facebook stranicu za prijavu, kao *web* preglednik Androida i *host* na *web*. U ovom primjeru, datoteka koja je javna i dostupna, te čini temelj ove aplikacije, priložena je pod nazivom „fb phishing.zip“ te sadrži četiri datoteke i ikonu navedene aplikacije. Taj sadržaj prikazan je na slici 18.



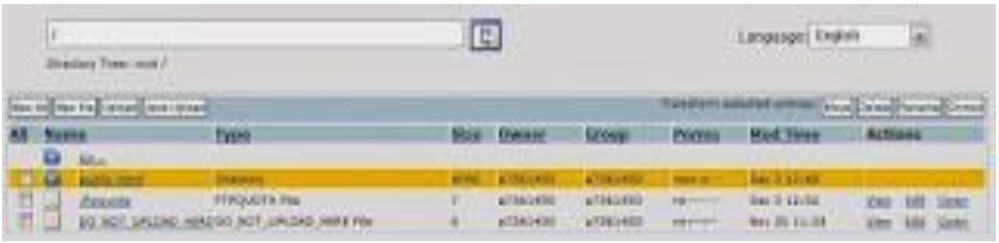
Slika 18. Prikaz sadržaja datoteke „fb phishing.zip“, [22]

U preuzetoj datoteci dostupna je i prilagođena verzija Facebook *phishing* stranice za mobilni preglednik, što znači da će se pomoću nje automatski preusmjeravati na stvarnu Facebook stranicu te će se, nakon pokušaja prijave, javljati greška uz natpis „Vaša lozinka je netočna“. Nakon toga, potrebno je učitati četiri datoteke na *hosting web* lokacije i preuzeti URL lažne stranice. Odlaskom na neki od besplatnih *web hostinga* (u primjeru je naveden „http://www.000webhost.com/888372.html“), potrebno je ispuniti tražene informacije te se registrirati. Nakon toga i potvrđivanja računa putem e-pošte, potrebno se prijaviti na upravljačku ploču na adresi „http://panel.000webhost.com/“.



Slika 19. Upravljač datoteka na stranici *000webhost*, [23]

Odlaskom i prijavom na upravljač datoteka prikazan na slici 19, potrebno je kliknuti na „Public_html“, što je prikazano na slici 20.



Slika 20. Potrebna datoteka „Public_html“, [22]

Nadalje, potrebno je prenijeti četiri datoteke iz početno preuzete mape naziva „login_files“, „login.html“, „post.php“ i „andpasswords.txt“. Nakon učitavanja navedenih stavki, potrebno je kliknuti na datoteku „login.html“, te će se tim postupkom otvoriti lažna, *phishing* stranica i pojaviti URL iste.

Drugi dio postupka je stvaranje Android aplikacije pomoću bilo kojeg besplatnog ili kupljenog alata. U ovom primjeru korišten je alat sa stranice „www.appsgeyser.com“. U prvom koraku potrebno je zalijepiti adresu stranice pomoću koje je planirana krađa identiteta. Taj postupak prikazan je na slici 21.



Slika 21. Stvaranje lažne mobilne aplikacije, [22]

Aplikaciju je potrebno nazvati „Facebook“ ili nešto povezano s tim kako bi izgledalo što vjerodostojnije. Nakon postavljanja priložene ikone i opisa aplikacije, proces stvaranja je dovršen, te je, za kraj, potrebno da korisnik preuzme i instalira aplikaciju na svoj uređaj i pokuša se prijaviti, [22].

Upoznavši se s mogućim oblicima prijetnje usmjerene mobilnim uređajima, u sljedećim poglavljima razmatrat će se primjeri te načini sprječavanja istih pomoću različitih alata. Vidljivo je kako su mehanizmi napada raznovrsni te se zbog toga konstantno traže nova rješenja koja bi povećala sigurnost i zaštitila korisničke uređaje.

5. Primjeri i značajke aktualnih napada krađom identiteta

Zbog zabilježenog rasta napada krađom identiteta, važno je nabrojati neke od napada koji su obilježili povijest kako bi se okvirno utvrdilo koje koristi napadači postižu i na koje načine. Neki od značajnijih napada u nedavnoj prošlosti bili su:

5.1. Operacija *Phish Phry*

FBI (engl. *Federal Bureau of Investigation*) prije deset godina otkrio je organiziranu skupinu kriminalaca koja je zavarala mnoge klijente banaka, odnosno, korisnike kreditnih kartica, oduzimajući im financijska sredstva na protuzakonit način u iznosu od 1.5 milijun dolara, prebacujući novce na račune koje su posjedovali. Kako bi nastavili borbu sa ovakvim prijevarama, FBI se ponajviše oslonio na službe zakona, poduzeća, sveučilišta i građane širom svijeta, [24]. Sam napad započeo je tako što su klijenti primili poruku e-pošte sadržaja sličnom onom službenom i koji je koristio lažne financijske web-lokacije. Žrtve su pristupanjem stranicama i unošenjem osobnih podataka i brojeva kartica napadačima omogućile pristup podacima, što je rezultiralo najvećim međunarodnim slučajem phishinga koji je ikada proveden. Slučaj je završio s više od stotinu optuženih, a više od polovice napadača bilo je locirano izvan teritorija Sjedinjenih Američkih Država, [25].

5.2. Walter Stephan

Walter Stephan je ime austrijskog izvršnog direktora zrakoplovstva koji, po statistikama, drži neslavan rekord u najvećoj izgubljenoj svoti novca - zbog e-mail phishinga izgubio je čak 47 milijuna dolara. Budući da je bio odgovoran za poznate zrakoplovne tvrtke, napadači su iskoristili njegovu poziciju, te su zatražili navedeni iznos novca za tzv. „projekt za nabavu“. Pretpostavlja se da su napadači slučajno pogodili točnu adresu e-pošte Waltera Stephana, stvorili lažnu kopiju i kontaktirali zaposlenika koji se bavio financijskim transakcijama. Nasjevši na prijevaru, povjerio je e-poštu i poslao iznos koji su napadači tražili. Ovaj slučaj potaknuo je ostala poduzeća da na dodatne načine potvrđuju komunikaciju koja se odvija putem e-pošte, [25].

5.3. Target / FMS prijevara

Povreda podataka u Targetu 2013. godine izravno je utjecala na 110 milijuna korisnika, od čega je 41 milijun povreda podataka bilo putem maloprodajnih računa. Nakon testiranja napada i detaljne analize, napadači su instalirali i poslali pet verzija *malwarea* na

veći dio POS uređaja. *Malware* se prerušio u svrhu oponašanja elementa koji se koristi u uređaju za upravljanje podatkovnim centrom. Zlonamjerni softver skupljao je podatke više od mjesec dana i poslao ih na različita odredišta u Sjedinjenim Američkim Državama. Taj potez okarakteriziran je pokušajem prikrivanja kompromitiranih podataka kao da su dio redovnog poslovnog prometa. Nakon toga, podaci su poslani u Moskvu, a kad se sve otkrilo, ukradeni podaci su već bili poslani i uklonjeni, [26].

5.4. Napad na ukrajinsku elektroenergetsku mrežu

Ovaj događaj se opisuje kao napad na fizičke strojeve putem zlonamjernog *firmwarea.* Za svoj proboj, napad je koristio najprije *phishing,* te je zapamćen kao prvi korisnik zlonamjernog softvera koji je korišten u svrhu istovremenog onemogućavanja više web lokacija. Napad je došao iz smjera Rusije, a napadači su imali potpun pristup podacima svakog postrojenja elektrane dosta vremena prije samog napada. Upravo zbog duljine vremena pristupa, bili su spremni nadjačati bilo koji način obrane te su imali kontrolu nad svim što se nalazilo u elektranama – od hladnjaka do aerodromskih komunikacijskih tornjeva. Uzrok napada bila je nesmotrena greška zaposlenika koji je nasjeo na *phishing* napad, [25].

5.5. Prijevara tijekom Svjetskog nogometnog prvenstva 2018.

Najaktualnija prijevara bila tijekom navedenog natjecanja u Rusiji, točnije, u Moskvi. Zbog velikog interesa za natjecanje, napadači su odlučili iskoristiti prednosti koje im je nudila situacija, a to je pomama za ulaznicama na utakmice prvenstva te za smještajem osoba. Napadači su vršili prijevare putem e-pošte. Slali su velik broj poruka i sve navedeno su garantirali tijekom događaja. Između ostalog, u slučaju se navodi da su napadači ciljali korisnike putem portala *Booking.com*. Poruke su se slale putem društvenih mreža ili se radilo o SMS-u, a vjerodostojnost su im davali podaci o korisnicima, koji su uključivali i potpune osobne podatke koje su napadači ukrali iz nesigurnih hotelskih sustava. To je sve potaknulo na korištenje protokola za slanje sigurnih podataka te se javnost osvijestila o važnosti osjetljivih informacija, [25].

6. Alati i načini zaštite i prevencije

Nakon osvještavanja o razlozima napada i na koje se sve različite načine može doći do napada krađom identiteta, bitno je i saznato više o mogućim načinima zaštite podataka kako bi se korisnici uspješno obranili od eventualnog napada.

6.1. Postojeća rješenja

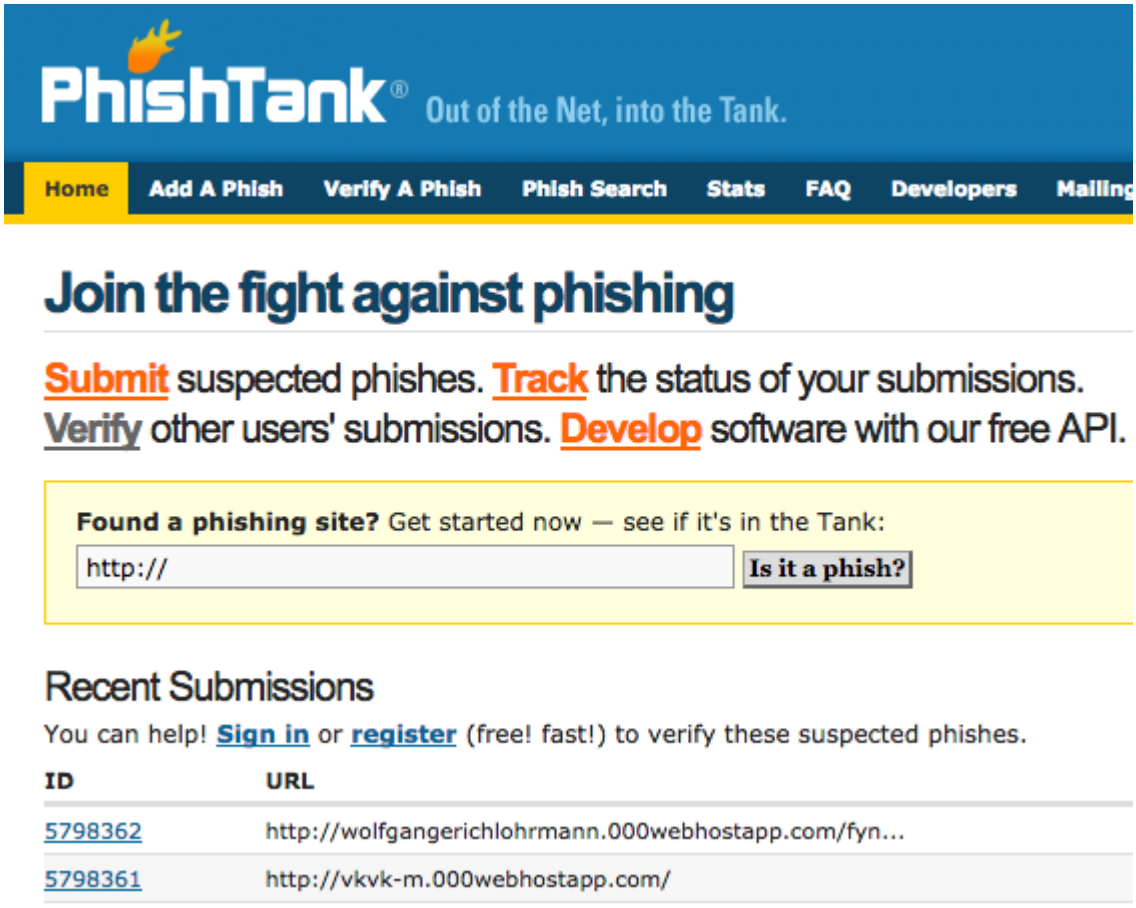
U ovome dijelu će se govoriti o već postojećim rješenjima koje preporučuje Anti-botnet sustav te o alatu Lookout. Oba alata podržavaju i omogućuju razne funkcionalnosti s ciljem zaštite od zlonamjernih napada krađe identiteta usmjerene mobilnim uređajima.

6.1.1. Anti-botnet rješenja

Anti-botnet predstavlja servis za smanjenje broja zaraženih računala, tableta i mobilnih uređaja, te pruža pomoć pri čišćenju uređaja od zlonamjernih programa, [27]. Pružatelj ovoga servisa je CARnet. Anti-botnet navodi neke od korisnih alata za provjeru zlonamjernih web lokacija i pruža korisne savjete. Neki od savjeta korisnicima su:

- instalacija antivirusne zaštite s uključenim filterima za zaštitu protiv neželjenih poruka na mobilni terminalni uređaj
- apel da se ne otvaraju prilozi i poveznice e-pošte koja dolazi od nepoznatih osoba
- poziv na opreznost u slučaju dobivanja zahtjeva za ažuriranjem podataka putem interneta
- pri posjeti *web* dućana, stranice banke ili ostalih stranica koje obrađuju osobne podatke, potrebno je pripaziti koristi li se sigurni protokol „https“ koji je prepoznatljiv po simbolu zaključanog lokota na početku adrese *web* stranice
- potrebno je biti veoma oprezan kada se preuzima program s neprovjerenih stranica
- preporučuje se korištenje dobrih lozinki i česta promjena istih
- redovno ažuriranje sustava će također povećati sigurnost korisnika, [27].

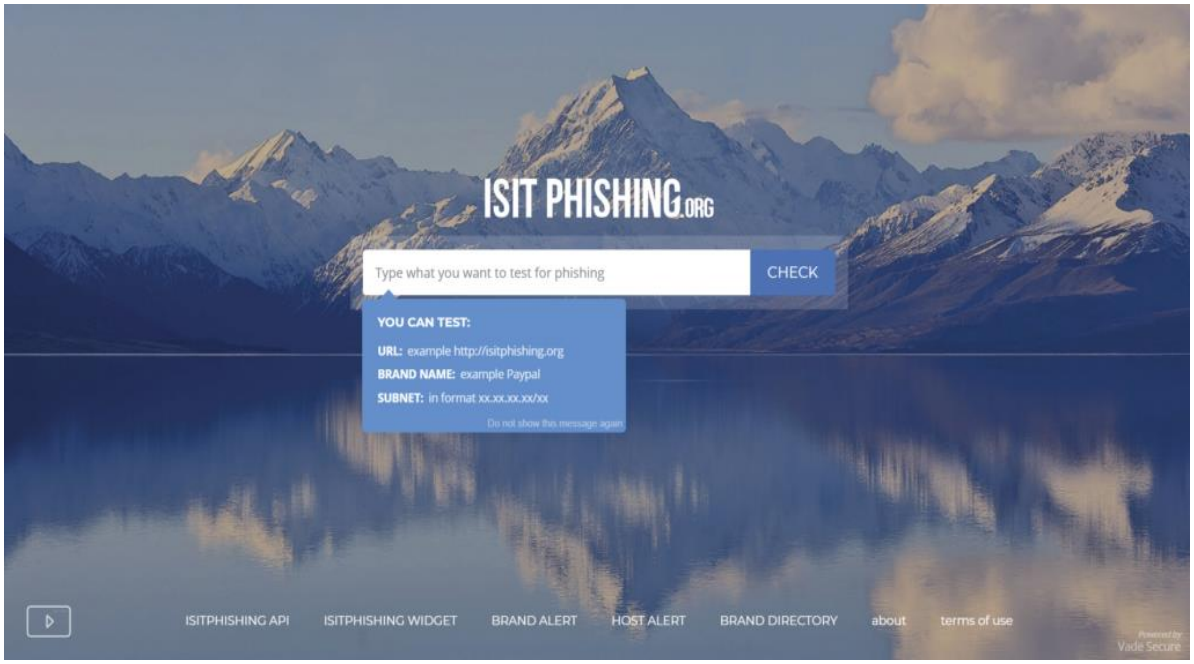
Od korisnih alata, preporuka je u slučaju sumnje koristiti provjerene stranice za otkrivanje *phishinga*. Anti-botnet navodi dva rješenja – *Phishtank* i *isitPhishing*. Prvi, prikazan na slici 22, služi kao baza podataka koja bilježi podatke o otkrivenim *phishing* stranicama, te besplatno nudi primjenu istih podataka na korisničke aplikacije.



Slika 22. Izgled Phishtank rješenja za *phishing* napade, [28]

Drugi se pak ponajviše fokusira na e-poštu i nudi besplatnu uslugu s ciljem borbe protiv krađe identiteta. E-pošta, kao jedini komunikacijski alat koji je besplatan, univerzalan je, neovisan i služben. U slučaju zlonamjernog napada, u e-pošti je sadržana lažna *web* lokacija koja ima namjeru korisniku otuđiti vrlo vrijedne i povjerljive informacije.

Ovaj sustav radi na principu heurističke tehnologije i strojnog učenja i učinkovit je kod pojave skraćenih dinamičkih veza. Istraživanje *web* stranica jedinstvena je tehnologija koja se odvija u roku od 1,8 sekundi od trenutka klika. Korisnici su zaštićeni i tvrtke su upozorene tijekom i nakon valova *phishinga*, [29]. Na slici 23 prikazan je izgled ovoga alata koji funkcionira na način da korisnik upiše URL, ime tvrtke ili podmrežu koju želi testirati i pričeka rezultate.



Slika 23. Prikaz alata *isitPhishing*, [30]

Trendovi rješenja mijenjaju se usporedno s poboljšanjem uspjeha i povećanjem broja zlonamjernih napada. Alata je mnogo, a rješenja također. Problem predstavlja unikatnost situacija. Stoga je potrebno pratiti savjete za zaštitu mobilnog terminalnog uređaja, instalirati dodatke za preglednike, antivirusne programe i učiniti ostale potrebne korake, te tako maksimalno zaštititi osobne ili poslovne podatke.

6.1.2. Alat Lookout

Zaštita od krađe identiteta i sadržaja „Lookout“ je alat koji blokira svaki pokušaj povezivanja na zlonamjerne i *phishing* URL-ove na mrežnoj razini kada se mobilni uređaj ili korisnik pokušava povezati na iste. Ono što je bitno drugačije kod ovog pristupa jest to da se ne pregledava sadržaj zlonamjerne poruke. Mnoge društvene platforme za razmjenu poruka koje se koriste na mobilnim uređajima kao što su SMS, WhatsApp, Facebook Messenger i e-pošta su vrlo osjetljive u smislu privatnosti korisnika. Prilikom samog pregledavanja URL-a u vrijeme pokušaja pojedinca ili uređaja da se poveže, Lookout osigurava zaštitu privatnosti korisnika. Pregledom URL-ova na razini mreže, on je u stanju zaštititi korisnike od povezivanja s zlonamjernim ili phishing URL-ovima s bilo koje e-pošte, tekstualne poruke, društvenih poruka ili poruka s bilo koje druge aplikacije, [31].

6.2. Novija rješenja

In-line i *out-of-band cloud* proizvodi za sprečavanje krađe identiteta koji se nalaze između poslužitelja e-pošte i interneta standardna su rješenja koja skeniraju zaglavlja e-pošte, privitke, tijelo ili neku njihovu kombinaciju. Analizu ovakvih proizvoda obavlja je tvrtka Zimperium, [32].

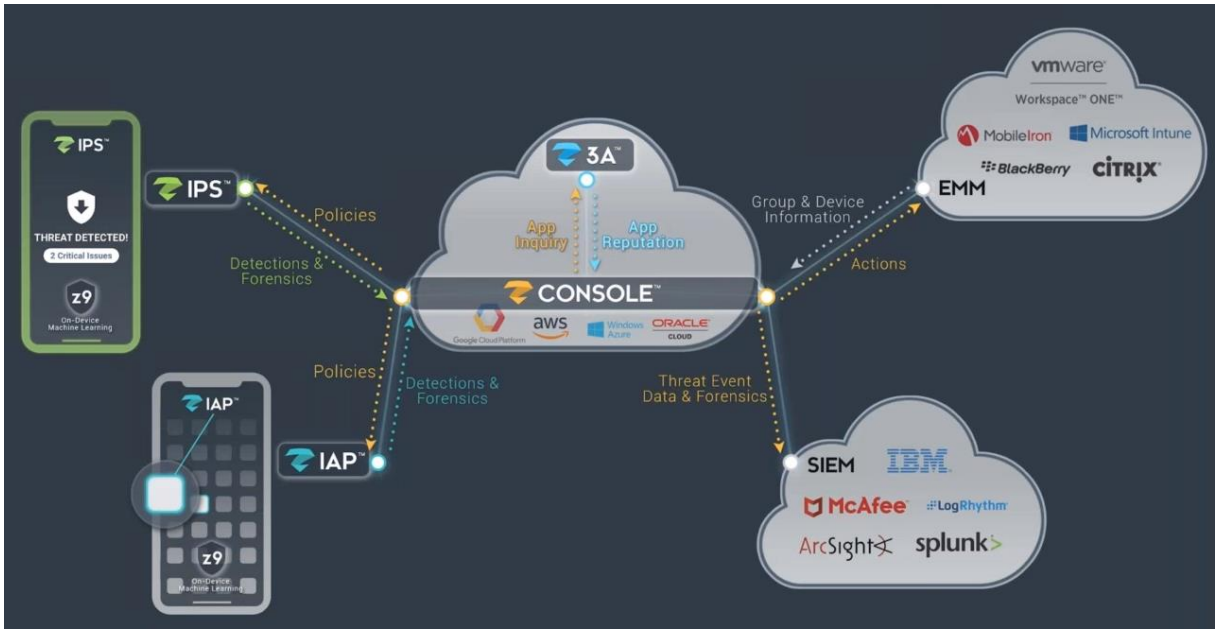
Oni su analizirali razvoj i implementaciju krajnjih točaka, te alate i dodatke koji se pokreću na njima i dizajnirani su za izoliranje aplikacija i URL-ova u e-pošti. Također, od tradicionalnih rješenja pratili su skeniranje softverskih privitaka u e-pošti i provjeravali prisutnost zlonamjernog softvera. Nadalje, od postojećih rješenja podrazumijevala se zaštita domene koja je bila osiguravajući standard za e-poštu, odnosno, upućivala je na to da e-pošta ne može biti lažna. Posljednji dio tradicionalnih rješenja bio je trening zaposlenika ili korisnika bez čije se nesvjesnosti i neznanja napad u većini slučajeva ne bi ni dogodio. Njih je bilo potrebno dodatno educirati, čemu se posebno davao značaj.

Ideja novoga rješenja obuhvaćala je pružanje sigurnosti e-pošte korisnicima, *backend* između interneta i poslužitelja pošte, djelotvorne reakcije inteligencije na prijetnju i izvještavanje. Postojao bi zaseban tim stručnjaka koji bi analizirao korisničke komunikacije uz mnoštvo analize.

Nadalje, u poslovnom okruženju najveći problem bilo je vrijeme zaposlenika koje provedu povezani na mreže izvan tvrtke, a to je iznosilo 90% vremena. Spajajući se na druge mreže, korisnikov uređaj postaje veoma ranjiv. Također, današnji mobilni terminalni uređaj prosječno sadrži 90 aplikacija. MDM (engl. *Mobile Device Management*) može spriječiti neka štetna djelovanja od strane zlonamjernih aplikacija, ali ne uvijek i „curenje“ podataka. Analize navode kako je 90% prijevara započelo napadom krađe identiteta, a 61% zlonamjernih poruka e-pošte otvoreno je na mobilnom terminalnom uređaju, [32].

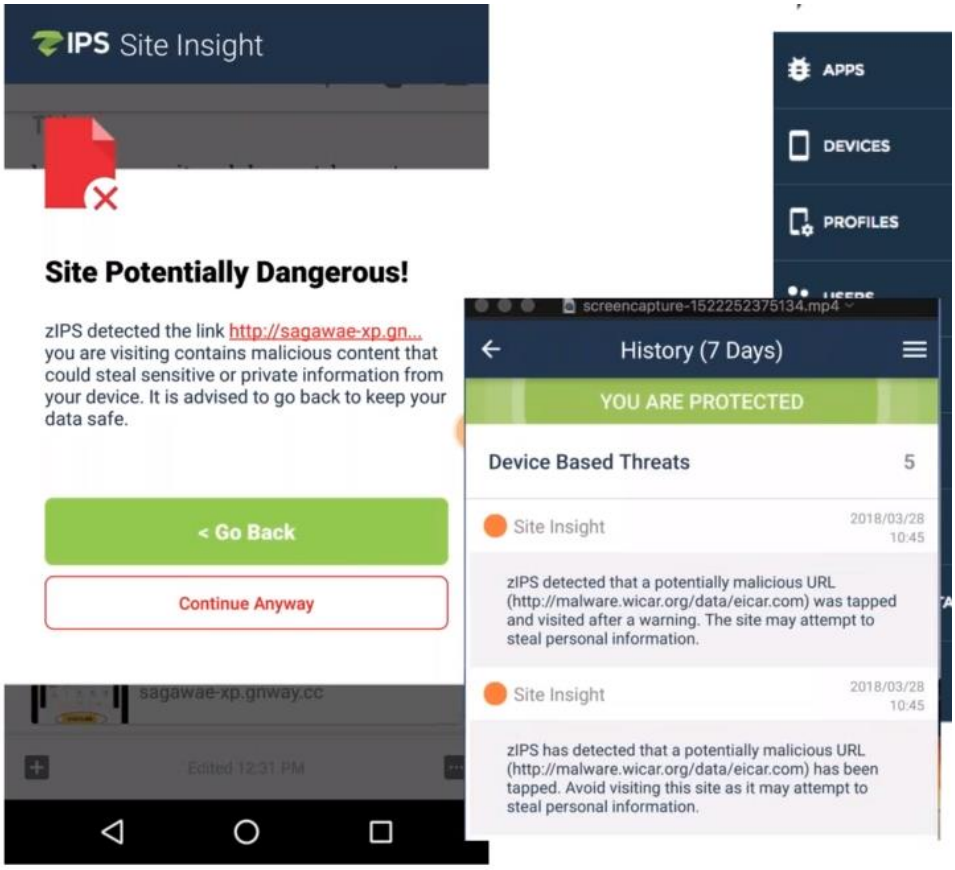
Stoga je tvrtka Zimperium izgradila proizvod koji ima mehanizam koji koristi strojno učenje kako bi osigurao zaštitu na uređaju u stvarnom vremenu protiv poznatih i nepoznatih prijetnji. Shvatili su da korisnici moraju detektirati prijetnju na uređaju jer devet od deset napada danas započinje napadom na mrežu. Ideja je da je pogonski softvare "z9" jezgra cijeloga pogona. Postoje dvije opcije za korištenje: „z9“ je integriran na uređaj ili predstavlja aplikaciju za preuzimanje (aplikacija štiti i sesije korisnika). Nakon toga, obje dolaze u

glavnu konzolu jer je detekcija na uređaju, a ne na *cloud* sustavu kao ranije, što je prikazano na slici 24.



Slika 24. Zimperium „z9“ softver – način rada, [32].

Na uređaju se aktivno traži bilo koja komunikacijska aplikacija. Skenira se svaki URL i odlučuje se je li *phishing* napad. Ako jest, korisnik uređaja se upozorava, a prizor upozorenja vidljiv je na slici 25.



Slika 25. Upozorenje korisniku „z9“ softvera, [32]

Ključna rješenja ovoga sustava bila bi zaustavljanje primarnog izvora napada, poboljšanje odgovornosti i performansi sigurnosnih timova te se usmjeriti prema boljim rezultatima.

7. Zaključak

Kako se broj terminalnih uređaja povećava, tako se povećava i broj pokušaja i vrsta krađe identiteta, odnosno mobile phishinga. Zaključak je taj da su krajnji korisnici oni koji najviše osjećaju posljedice borbe između prevaranata i proizvođača raznoraznih zaštita i prevencija koje naposljetku služe kako bi spriječili krađu podataka i informacija.

Budući da danas postoji velik broj osobnih podataka zapisanih u digitalnom obliku, potrebno je pojačati zaštitu, što mnogi poslovni korisnici (poput banaka, platnih servisa, društvenih mreža itd.) i čine. Poželjno je i poznavati načine i izvore napada koji su često korišteni baš zbog lakšeg formiranja „obrane“ sustava i uređaja od mobile phishinga.

Također, stupanj informatičke pismenosti i informatičkog obrazovanja predstavlja presudan faktor u prevenciji krađe identiteta. Postoje razne edukacijske inicijative usmjerene prema tom cilju. Ono što nije bilo zastupljeno prije dvadesetak godina je uplitanje vladinih organizacija u prevenciju ili zaštitu od krađe podataka/identiteta. U današnje vrijeme, kao što je vidljivo iz primjera Europske Unije, radi se na tome da se ne zaštite samo podatci i prava privatnih lica, nego i da se zaštite velike tvrtke i poslovi kojima može biti načinjena velika šteta u slučaju krađe podataka bitnih za poslovanje ili financijsko stanje neke tvrtke.

Spomenuti mobile phishing ima za sada prepoznatljive karakteristike koje su navedene u ovom radu te ga je moguće prepoznati ovisno o kvaliteti izrade (bilo da se radi o aplikaciji, lažnoj web lokaciji ili poveznici) od strane napadača ili o educiranosti žrtve te zaštiti postavljenoj na sami uređaj. Jedan od glavnih koraka napada mobile phishingom je slanje poveznice te nasjedanje žrtve da pristupi istoj te tako otvori mogućnost zlonamjernoj strani da nadzire sustav uređaja ili se okoristi neovlašteno preuzimajući podatke. Činjenica je da svi korisnici posjeduju vrijedne podatke na svojim uređajima, što ovu vrstu napada čini još pogodnijom za zlonamjernu stranu jer sam napad ne mora nužno biti ciljan. Stoga, svako eventualno nasjedanje žrtve na lažnu poveznicu napadačima može predstavljati uspjeh.

Literatura

[1] Vora LJ. Evolution of mobile generation technology: 1G to 5G and review of upcoming wireless technology 5G. International Journal of Modern Trends in Engineering and Research (IJMTER). 2015;10(2): 285.

[2] Rfpage portal. Preuzeto sa: https://www.rfpage.com/evolution-of-wireless-technologies-1g-to-5g-in-mobile-communication/ [Pristupljeno: kolovoz 2019.]

[3] Sarwar M, Soomro TR. Impact of Smartphones on Society. European Journal of Scientific Research. 2013;98(2):216-226.

[4] Mišić V. Istraživanje sigurnosnih aspekata primjene vlastitih uređaja u korporativnom okruženju. Diplomski rad. Sveučilište u Zagrebu. Fakultet prometnih znanosti. Zagreb. 2019.

[5] Ray P. A Survey on Internet of Things Architectures. Journal of King Saud University – Computer and Information Sciences. 2018;30:291–319. Preuzeto sa sustava Merlin [Pristupljeno: studeni 2018.]

[6] Statista portal. Preuzeto sa: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/ [Pristupljeno: svibanj 2019.]

[7] Nowsecure portal. Preuzeto sa: https://www.nowsecure.com/resource/infographic-surprising-stats-exposing-mobile-data-dangers/ [Pristupljeno: svibanj 2019.]

[8] Lookout: Phishing and content protection. Preuzeto sa: https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Phishing-and-Content-Protection-DS-UK.pdf [Pristupljeno: kolovoz 2019.]

[9] Waheed Muzammil A, Khan Z. Project report for information security course. Linkopings universitet Sweden. 2019. Preuzeto sa: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.298.2585&rep=rep1&type=pdf [Pristupljeno: svibanj 2019.]

[10] Staffbase portal. Preuzeto sa: https://staffbase.com/blog/six-advantages-byod-bring-your-own-device/ [Pristupljeno: lipanj 2019.]

[11] Cisco. Preuzeto sa: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html [Pristupljeno: svibanj 2019.]

[12] Researchgate portal. Preuzeto sa: https://www.researchgate.net/profile/Karen_Goertzel/publication/233569977/figure/fig1/AS:669414374522888@1536612232409/Spear-phishing-attack.png [Pristupljeno: svibanj 2019.]

[13] Infosec institute. Preuzeto sa: https://mk0resourcesinfm536w.kinstacdn.com/wp-content/uploads/1-30-768x389.png [Pristupljeno: svibanj 2019.]

[14] Forcepoint: What is phishing attack?. Preuzeto sa: https://www.forcepoint.com/cyber-edu/phishing-attack [Pristupljeno: svibanj 2019.]

[15] Perspective risk portal. Preuzeto sa: https://www.perspectiverisk.com/wp-content/uploads/2016/07/Blog1-Pic1-1024x545.png [Pristupljeno: svibanj 2019.]

[16] Merabheja portal. Preuzeto sa: https://merabheja.com/wp-content/uploads/2016/06/2phishing.png [Pristupljeno: svibanj 2019.]

[17] Pentestgeek portal: How do I phish?. Preuzeto sa: https://www.pentestgeek.com/phishing/how-do-i-phish-advanced-email-phishing-tactics [Pristupljeno: svibanj 2019.]

[18] Symantec portal. Preuzeto sa: https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=28589 [Pristupljeno: svibanj 2019.]

[19] Whois portal. Preuzeto sa: https://manage.whois.com/kb/node/365 [Pristupljeno: svibanj 2019.]

[20] Coder Glass portal. Preuzeto sa: https://www.coderglass.com/social/images/facebook-style-homepage.JPG [Pristupljeno: svibanj 2019.]

[21] Null-byte forum. Preuzeto sa: https://null-byte.wonderhowto.com/forum/complete-guide-creating-and-hosting-phishing-page-for-beginners-0187744/ [Pristupljeno: svibanj 2019.]

[22] Xplace portal. Preuzeto sa: https://www.xplace.com/article/3447 [Pristupljeno: svibanj 2019.]

[23] 000webhost forum. Preuzeto sa: https://www.000webhost.com/forum/t/how-to-unzip-files-using-unzipper/51626 [Pristupljeno: kolovoz 2019.]

[24] FBI: Operation Phish Phry. Preuzeto sa: https://archives.fbi.gov/archives/news/stories/2009/october/phishphry_100709 [Pristupljeno: svibanj 2019.]

[25] Phishprotection portal. Preuzeto sa: https://www.phishprotection.com/blog/the-top-5-phishing-scams-in-history-what-you-need-to-know/ [Pristupljeno: svibanj 2019.]

[26] Carleton.edu portal. Preuzeto sa: https://people.carleton.edu/~carrolla/story.html [Pristupljeno: svibanj 2019.]

[27] AntiBotnet – Nacionalni centar podrške. Preuzeto sa: http://www.antibot.hr/ [Pristupljeno: svibanj 2019.]

[28] The Windows club: Phishtank will help you verify or report Phishing websites. Preuzeto sa: https://www.thewindowsclub.com/phishtank-report-phishing-attempts [Pristupljeno: svibanj 2019.]

[29] Isitphishing servis. Preuzeto sa: https://isitphishing.org/ [Pristupljeno: svibanj 2019.]

[30] Infologo: Isitphishing original features. Preuzeto sa: https://infologo.ch/wp-content/uploads/2018/12/isitphishing-org-features-1024x503.png [Pristupljeno: svibanj 2019.]

[31] Lookout: Mobile phishing: Myths and facts facing every modern enterprise today. Preuzeto sa: https://www.lookout.com/info/lookout-mobile-phishing-lp [Pristupljeno: lipanj 2019]

[32] Gigaom webinar. Preuzeto sa: https://gigaom.com/webinar/enterprise-phishing-attacks-and-the-need-to-defend-mobile-endpoints/?source=Zimperium [Pristupljeno: svibanj 2019.]

Popis kratica

CSV (Comma-Separated Values) tekstualna datoteka s uporabom zareza za razdvajanje vrijednosti

DNS (Domain Name System) protokol za davanje imena mrežnim adresama

FTP (File Transfer Protocol) protokol za prijenos podataka

HTTP (HyperText Transfer Protocol) protokol za prijenos informacija na webu

IoT (Internet of Things) Internet stvari

MDM (Mobile Device Management) upravljanje mobilnim uređajem

PDF (Portable Document Format) prenosivi format dokumenta

PHP (Hypertext Preprocessor) programski jezik za web stranice

POS (Point of Sale) sustav za transakciju financijskih sredstava

TCP (Transmission Call Protocol) protokol za kontrolu prijenosa podataka

UI (User Interface) korisničko sučelje

UMTS (Universal Mobile Communications System) tehnologija treće generacije mobilnih mreža

URL (Uniform Resource Locator) ujednačeni lokator sadržaja

ZIP (File format) format datoteke

SEG (Secure email gateway) sigurni pristupnik e-pošti

AMPS (Advanced Mobile Phone System) napredni sustav mobilnih telefona

FDMA (Frequency-division Multiple Access) višestruki pristup s podjelom frekvencije

WWWW (Wireless World Wide Web) bežični internet

Popis slika

Slika 1. Dijagram toka zlonamjernog napada usmjerenog mobilnom uređaju

Slika 2. Opis spear phishing napada

Slika 3. Primjer napada clone phishingom

Slika 4. Prikaz whaling napada

Slika 5. Primjer krivotvorenja web-lokacije

Slika 6. Nabrajanje e-mail adresa

Slika 7. Primjer naredbe “iptables”

Slika 8. Brzo stvaranje e-pošte

Slika 9. Sučelje *hostinga* „GoDaddy“ za kupljenu domenu

Slika 10. Prikaz skripte za slanje „sendmail.rb“ skripte dvjema korisnicima

Slika 11. Izvorni izgled web stranice Facebook-a

Slika 12. Prikaz izvora web lokacije

Slika 13. Prikaz sadržaja izvora u tekstnom dokumentu

Slika 14. PHP skripta za prikupljanje korisničkih lozinki

Slika 15. Opcija traženja potrebnog teksta u dokumentu

Slika 16. Prikaz sučelja 000webhost-a

Slika 17. Prikaz sučelja web lokacije „htmlpasta.com“

Slika 18. Prikaz sadržaja datoteke „fb phishing.zip“

Slika 19. Upravljač datoteka na stranici 000webhost

Slika 20. Potrebna datoteka „Public_html“

Slika 21. Stvaranje lažne mobilne aplikacije

Slika 22. Izgled Phishtank rješenja za *phishing* napade

Slika 23. Prikaz alata isitPhishing,

Slika 24. Zimperium „z9“ softver – način rada

Slika 25. Upozorenje korisniku „z9“ softvera

Popis grafikona

Grafikon 1. Broj korisnika mobilnih terminalnih uređaja u milijardama u 2019. godini i predviđanje broja do 2023. godine

Popis tablica

Tablica 1. Usporedba mobilnih mreža od prve do pete generacije

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **Krađa identiteta kao metoda napada prema mobilnom terminalnom uređ**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 4.9.2019.

Student/ica:

Ivan Arapović
(potpis)