SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 6475

METODE I ALATI ZA ISTRAŽIVANJE NAPADA DRUŠTVENIM INŽENJERSTVOM NA INTERNETU

Mirna Veršić

Zagreb, Siječanj 2020

SADRŽAJ

1.Uvod

Sve većim razvojem i napretkom tehnologije računala su postala sastavni dio ljudskih života. Danas je postalo veoma teško zamisliti život bez osobnih računala, tableta i pametnih telefona. Raznorazni uređaji integrirani su u sve aspekte ljudskog društva, od poslovnog do privatnog. Društvene mreže postale su standard online društvenog života. Prema podatcima objavljenima u prosincu 2019. godine, jednu od najpopularnijih društvenih mreža Facebook, na mjesečnoj bazi koristi 2,5 milijardi korisnika [1]. Za usporedbu, procjenjuje se da je na Zemlji u travnju 2019. godine živjelo oko 7,7 milijardi ljudi [2], što znači da je u prosijeku svaki treći čovjek barem jednom mjesečno pristupio Facebooku.

Iako je Internet mjesto na kojem se korisnici osjećaju sigurno, on je također i mjesto koje sadrži i čuva puno osobnih i drugih podataka koje bi pojedinci mogli iskoristiti u vlastite, često ilegalne, svrhe. Jedan takav primjer bila bi krađa identiteta. Krađa identiteta može se manifestirati na nekoliko različitih načina. Primjerice, napadač bi mogao osobne podatke žrtve iskoristiti za prijavu za traženje studentskih zajmova, otvaranje bankovnih računa ili izdavanje kreditnih kartica u žrtvino ime. Ova vrsta krađe identiteta naziva se financijskom krađom identiteta [3]. Nadalje, napadač može žrtvine privatne podatke iskoristiti u drugim ilegalnim djelima čime krivicu za počinjenje kaznenog djela svaljuje na žrtvu. Primjer ovakve krađe identiteta bilo bi davanje žrtvinih informacija u trenutku dobivanja kazne za brzu vožnju. Ova vrsta krađe naziva se krađom identiteta s kažnjivim namjerama [3]. Napadač također može iskoristiti žrtvine osobne podatke pri pretplaćivanju na raznorazne pretplate poput pretplate na dodatne televizijske programe. Ova vrsta krađe identiteta naziva se krađom identiteta radi osobne korisnosti [3]. Najraniji računalni napadi pojavljuju se u 1980-im, a do danas se razvila čitava lepeza računalnih napada [4]. Napadi koji najčešće pogađaju obične korisnike internetskih usluga uglavnom spadaju u kategoriju phishing napada [5]. Jedan takav napad dogodio se u Hrvatskoj u kolovozu 2019. godine, a na materijalima dobivenim iz tog napada pokušati će biti provedena analizu phishing napada počinjenog elektroničkom poštom.

Za uspješnu provedbu analize elektroničke pošte nužno je poznavati osnovne mehanizme prijenosa elektroničke pošte od pošiljatelja do primatelja, kao i osnovne protokole koji se pri tome koriste, te strukture zaglavlja elektroničke pošte. Ovi pojmovi opisani su u drugom poglavlju. U trećem poglavlju opisani su načini prikupljanja osobnih podataka preko javnih izvora, te phishing i spear phishing napadi koji počivaju na iskorištavanju javno dostupnih osobnih podataka. Načini prikupljanja osobnih podataka iz javno dostupnih izvora su također opisani u ovom poglavlju, kao i metodete filtriranja spam poruka. Kao potpoglavlje ovog poglavlja opisani su detalji gore

spomenutog phishing slučaja u Hrvatskoj. U četvrtom poglavlju opisane su tehnike koje se koriste pri forenzici elektroničke pošte, dok peto poglavlje opisuje instalaciju i osnovne upute za korištenje alata Maltego koji se koristi u forenzici elektroničke pošte. U šestom poglavlju opisano je korištenje alata Maltego nad phishing slučajem opisanim u trećem poglavlju.

2. Mehanizmi slanja elektroničke pošte

Prethodno opisani slučaj Internet prijevare koristio je elektroničku poštu kao sredstvo za komunikaciju između počinitelja i žrtve. Elektronička pošta sadrži niz korisnih informacija koje su skrivene od običnog korisnika, a ekstrapolacijom i istraživanjem tih podataka bavi se grana forenzike pod nazivom forenzika elektroničke pošte [46]. Za uspješno razumijevanje podataka koje skriva elektronička pošta nužno je najprije poznavati mehanizme razmjene elektroničke pošte i protokole koji se pri tome koriste. U potpoglavlju 2.1 opisani su protokoli elektroničke pošte. Potpoglavlje 2.2 opisuje mehanizme razmjene elektroničke pošte, dok potpoglavlje 2.3 opisuje strukturu zaglavlja elektroničke pošte. Potpoglavlja 2.4 i 2.5 opisuju proširenja elektroničkih poruka za multimediju i sigurnost.

2.1. Protokoli elektroničke pošte

Pri razmjeni elektroničke pošte od pošiljatelja do primatelja potrebno je osigurati da tu poštu ne primi nitko drugi osim osobe kojoj je namijenjena . U tu svrhu se pri slanju elektroničke pošte koristi nekoliko protokola [6]:

- POP3 – *Post Office Protocol version 3*
- SMTP – *Simple Mail Transfer Protocol*
- IMAP – *Internet Message Access Protocol.*
- MAPI – *Messaging Application Programming Interface*
- EAS – *Exchange ActiveSync*
- ...

Svaki od ovih protokola se brine za određeni aspekt slanja elektroničke pošte. POP3 protokol i IMAP protokol koriste se za dohvaćanje elektroničke pošte sa servera elektroničke pošte, dok se SMTP protokol koristi za prijenos elektroničke pošte [7].

2.1.1. POP3 i IMAP protokoli

I POP3 i IMAP protokol koriste se za dohvaćanje elektroničke pošte sa udaljenog servera. POP3 protokol funkcionira na način da se spoji na udaljeni server, pokupi sve poruke sa servera i prebaci ih na lokalno računalo, te ih potom obriše sa servera [7]. Ovaj način rada ima svoje prednosti, ali i mane. Zbog

brisanja svih poruka sa udaljenog servera i spremanja tih poruka lokalno, manja je opterećenost udaljenog servera. No, ukoliko se POP3 protokol koristi za dohvaćanje elektroničke pošte na više uređaja, može doći do konflikata. Naime, ukoliko se jedan uređaj spoji na server, prebaci poštu lokalno i obriše poštu sa servera, drugi uređaj neće pronaći nikakvu novu poštu na serveru kada se spoji. Zato se korištenje POP3 protokola za dohvaćanje elektroničke pošte sa udaljenog servera preporuča isključivo kada se samo jedan uređaj spaja na udaljeni server. POP3 protokol svoj posao obavlja koristeći dva osnovna priključka (porta) [7]:

- Priključak (port) 110 – Standardni priključak. Koristi se za nekriptirani prijenos podataka.
- Priključak (port) 995 – Priključak se koristi za enkriptirani prijenos podataka. POP3 i IMAP protokol koriste TLS protokol za enkripciju [8]. TLS (*Transport Layer Security*) je protokol koji enkriptira komunikacijski kanal pri slanju e-poruke, a najčešće se implementira u transportnom sloju. [9].

IMAP protokol stvorio je Mark Crispin 1986. godine kao pokušaj poboljšanja POP protokola koji se do tada koristio [10]. Cilj IMAP protokola je podrška za višestruko pristupanje poštanskom sandučiću na udaljenom serveru [10]. Za razliku od POP3 protokola, IMAP protokol ne obavlja brisanje elektroničke pošte sa udaljenog servera u trenutku spremanje elektroničke pošte na lokalno računalo. Na taj način, kada se drugi uređaj spoji na server, elektronička pošta će još uvijek biti tamo i uređaj će ju moći preuzeti. Brisanje elektroničke pošte sa servera prepušteno je korisniku. Zbog ovakvog načina rada, IMAP protokol omogućava spremanje privremenih lokalnih kopija poruka u obliku privremenog cachea. Spremanjem kopija poruka IMAP protokol omogućava korisniku pregledavanje sadržaja poruka bez prethodnog spajanja na Internet, dok u isto vrijeme sve poruke ostaju na udaljenom serveru [11]. IMAP protokol koristi dva priključka (porta) [5]:

- Priključak (port) 143 – Standardni priključak. Koristi se za nekriptirani prijenos podataka.
- Priključak (port) 993 – Priključak se koristi za enkriptirani prijenos podataka. IMAP protokol koristi TLS protokol za enkripciju [8].

2.1.2. SMTP protokol

SMTP je komunikacijski protokol koji služi za razmjenu elektroničke pošte [7]. Za razliku od IMAP i POP3 protokola koji služe za dohvaćanje elektroničke pošte sa udaljenog servera, SMTP protokol služi za slanje pošte na udaljeni server. SMTP protokol je prvotno razvijen 1982. g., a posljednju reviziju dobio je 2008. g. kada je nastao tzv. *Extended SMTP* [12].

Najveći nedostatak SMTP protokola je njegova nemogućnost da se njime prenese poruka koja sadrži bilo koje druge znakove osim znakova sadržanih u ASCII kodu [13]. SMTP protokolom ne može se prenijeti poruka koja sadrži posebne znakove pojedinih jezika poput kineskog, hrvatskog ili ruskog jezika. Također, SMTP protokol ne pruža mogućnost prijenosa multimedijskih datoteka poput slika, videa i zvuka [13]. Upravo zbog ovih nedostataka SMTP protokola postoje proširenja SMTP protokola koja su opisana u potpoglavlju 2.1.3.

Izvorno je SMTP protokol koristio priključak 25 za slušanje, te mnogi klijenti elektroničke pošte i danas dopuštaju njegovo korištenje, ali prema posljednjoj reviziji standardno se koristi priključak 587 za slušanje [7]. Također se koristio i priključak 465, ali je on zastario [7]. SMTP protokol dopušta korištenje proizvoljnih priključaka za slušanje kada je riječ o internoj pošti unutar jedne organizacije. U tom slučaju svi klijenti elektroničke pošte moraju biti podešeni tako da koriste proizvoljno odbran priključak [51]. Proizvoljno odabrani priključci ne mogu se koristiti za razmjenu pošte sa klijentima izvan organizacije zato što pri slanju elektroničke pošte, pošiljateljev klijent ne može znati na kojem priključku sluša primateljev klijent, te će pretpostaviti da se radi o priključku 25 [51].

2.1.3. Ostali protokoli

SMTP, POP3 i IMAP protokoli su standardizirani protokoli koji se koriste pri razmijeni elektroničke pošte. Osim njih, postoji i niz drugih protokola koji se koriste u specifične svrhe.

Neki od takvih protokola su MAPI i EAS protokoli. I MAPI i EAS protokoli su protokoli koji se koriste pri komunikaciji sa Microsoft Exchange Serverom [6][15]. Microsoft Exchange Server je server za elektroničku poštu razvijen od strane Microsofta. Koristi se uz druge Microsoftove proizvode poput Microsoft Outlooka koji služi kao desktop ili web inačica klijenta elektroničke pošte.

MAPI je klijentski protokol koji služi za pristup korisnika poštanskom sandučiću preko Outlooka ili nekog drugog desktop MAPI klijenta [6]. Prema pretpostavljenim postavkama Outlook klijenta, MAPI pristup je unaprijed omogućen. Osim MAPI-ja kao klijentskog protokola, postoji i protokol MAPI over HTTP [14]. MAPI over HTTP je transportni protokol koji služi za povećanje stabilnosti i pouzdanosti veze između Outlooka kao klijenta elektroničke pošte i Microsoft Exchange Servera kao servera elektroničke pošte [14]. Veću stabilnost veze između Outlooka i Microsoft Exchange Servera protokol MAPI over HTTP ostvaruje izgradnjom transportnog sloja koristeći HTTP kao model [14].

EAS je Microsoftov sinkronizacijski protokol koji služi za sinkronizaciju podataka sa Microsoft Exchange Servera i podataka na korisničkim uređajima poput tableta ili pametnog telefona [15]. Temeljna razlika između MAPI i EAS

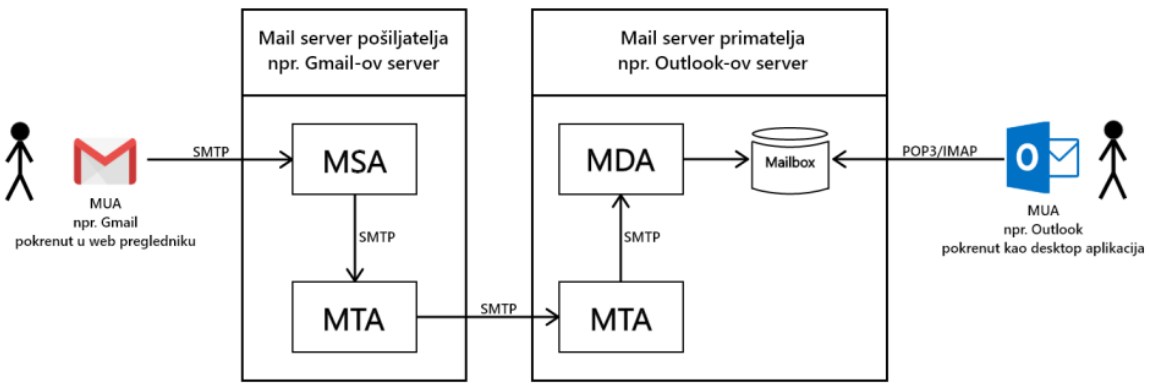
protokola je u uređajima za koje su namijenjeni. MAPI protokol je namijenjen desktop inačicama klijenata elektroničke pošte, dok je EAS namijenjen mobilnim uređajima [16]. Iako je moguće sinkronizirati Outlook preko EAS protokola, to se ne preporuča zato što se u tu svrhu koristi MAPI protokol. Osnovna zamisao EAS protokola je dati korisniku mogućnost pristupa podatcima na Microsoft Exchange Serveru, omogućiti lokalno spremanje tih podataka, te korisniku pružiti mogućnost pregledavanja tih podataka bez potrebe spajanja na mrežu [15].

IMAP i MAPI protokoli nude slične funkcionalnosti, ali osnovna razlika između ova dva protokola je u njihovoj primjenjivosti na različite platforme. MAPI protokol je Microsoftov protokol koji je ponajprije namijenjen za korištenje uz ostale Microsoftove proizvode poput Microsoft Outlooka, dok je IMAP standardizirani protokol primjenjiv na svim platformama [17].

Razlika između IMAP protokola i EAS protokola slična je razlici između EAS i MAPI protokola. IMAP protokol koristi se uz desktop inačice web klijenata, dok je EAS protokol namijenjen mobilnim uređajima [18]. Pri prebacivanju poruka IMAP protokolom, IMAP protokol će prebaciti sve poruke pronađene u sandučiću, dok EAS protokol neće prebaciti sve poruke, nego će prebaciti poruke unatrag zadnjih par tjedana. Na taj način štedi se na memorijskom prostoru koji je često znatno manji na mobilnim uređajima nego na stolnim računalima.

2.2. Razmjena elektroničke pošte

Razmjena elektroničke pošte odvija se u nekoliko koraka. Grafički prikaz slanja elektroničke pošte od pošiljatelja do primatelja prikazan je na slici 2.1.



Slika 2.1: Razmjena elektroničke pošte.

Za slanje i primanje elektroničke pošte korisnici koriste desktop ili web klijente elektroničke pošte. Neki od poznatijih desktop klijenata elektroničke pošte su Outlook i Thunderbird, dok su najčešće korišteni web klijenti elektroničke pošte Gmail, Hotmail i drugi. Skupni naziv za klijente elektroničke pošte je korisnički agent elektroničke pošte (*MUA – mail user agent).* MUA najprije poštu šalje na korisnički agent za slanje elektroničke pošte (*MSA – mail submission agent)* koristeći SMTP protokol [19].

MSA je program koji se vrti na serveru elektroničke pošte. MSA prima elektroničku poruku od MUA, pretražuje poruku u potrazi za pogreškama i prosljeđuje poruku MTA agentu također koristeći SMTP protokol [19]. Prvi agent za prijenos elektroničke pošte (*MTA - Mail transfer agent)* uvijek se nalazi na istom serveru kao i MSA agent. MTA agent zadužen je za dohvaćanje domene primatelja pošte. Kako bi mogao dohvatiti domenu, MTA šalje poruku na DNS (*Domain name system*) uređaj. [19]

DNS uređaj je zadužen za pretvaranje domene primatelja u IP – adresu [20]. Osim toga, DNS može dohvaćati nadležni DNS uređaj ili pretvarati IP – adresu u domenu. No, MTA ne zna MAC – adresu DNS uređaja, te kako bi ju saznao najprije mora poslati *Broadband* ARP upit. ARP upit je vrsta upita u komunikacijskim mrežama koja na temelju poznate IP adrese dohvaća MAC adresu uređaja. Nakon što je dohvaćena MAC adresa DNS uređaja, od njega se zahtijeva da ukoliko mu je poznata, vrati IP adresu tražene domene ili da upit proslijedi nekom nadležnom DNS uređaju koji će možda posjedovati tu informaciju [6].

Nakon što MTA dohvati domenu primatelja pošte, MTA se spaja na server za razmjenu pošte koristeći SMTP protokol. Ukoliko je trenutni MTA ujedno i krajnji MTA primatelja, MTA prosljeđuje poruku na agenta za prihvat elektroničke pošte (*MDA – Mail delivery agent*), inače MTA šalje poruku na sljedeći MTA u nizu [19].

Nakon što je MDA agent primio elektroničku poruku, on je spremljena u poštanski sandučić primatelja. Jednom kada je poruka spremljena u poštanski sandučić primatelja, korisnik ju može otvoriti koristeći MUA agenta. Primateljski MUA agent pristupa poštanskom sandučiću koristeći IMAP ili POP3 protokol [19].

2.3. Struktura elektroničkih poruka

Svaka e-poruka, osim osnovnih dijelova vidljivih korisniku, sadrži i niz drugih korisnih informacija sakrivenih od korisnika. Te informacije nalaze se u zaglavlju elektroničke poruke. Zaglavlju elektroničke poruke otvorene preko Gmail web klijenta može se pristupiti tako da se na izbornoj traci elektroničke

poruke odabere opcija *More,* a potom u padajućem izborniku opcija *Show original,* dok se zaglavlju elektroničke poruke otvorene preko Yahoo web klijenta može pristupiti tako da se na alatnoj traci odabere ikona u obliku tri točke, te se potom odabere opcija *View Raw Message* [21][22]. Zaglavlju elektroničke pošte pri korištenju desktop inačice Microsoft Outlooka može se pristupiti tako da se najprije dva puta klikne na poruku čije se zaglavlje želi prikazati [23]. Na taj način se željena poruka otvara u zasebnom prozoru. U novom prozoru pritiskom na tipku File otvara se novi izbornik u kojem se zatim treba odabrati opcija Properties. Ovom opcijom otvara se još jedan novi prozor koji sadrži zaglavlje elektroničke pošte u polju pod nazivom Internet headers [23]. Primjer zaglavlja elektroničke poruke dan je u privitku 1. U ovom potpoglavlju biti će objašnjeno značenje pojedinih polja u zaglavlju elektroničke pošte, kao i struktura zaglavlja elektroničke pošte, dok će analiza zaglavlja biti objašnjena u šestom poglavlju.

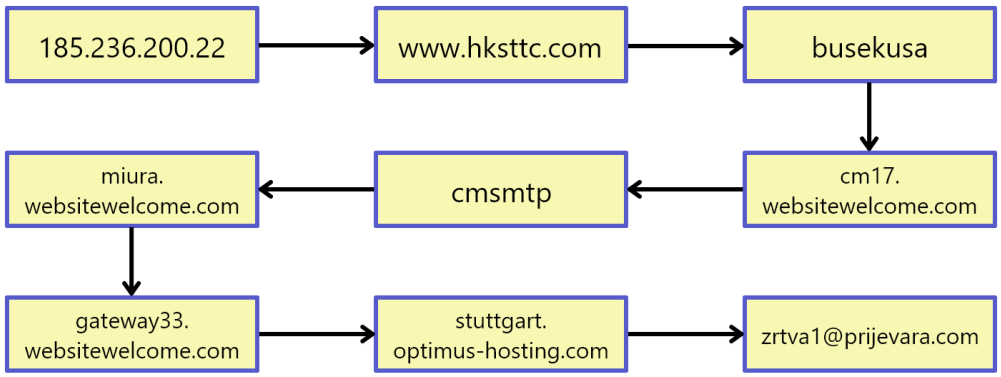
Zaglavlja e-poruka najlakše je čitati odozdola prema gore zato što su tim redoslijedom dodavane informacije u zaglavlje. Najdonje dijelove e-poruke generirao je klijent elektroničke pošte pošiljatelja, a svaki sljedeći dio iznad generirali su MTA agenti kroz koje je e-poruka prošla na putu do primatelja [24]. Najgornji dio zaglavlja generirao je klijent elektroničke pošte primatelja. Najdonja polja zaglavlja koja počinju sa oznakom "X-..." nazivaju se X-zaglavljima e-poruke. X – zaglavlja su nestandardizirana zaglavlja generirana na temelju sadržaja same poruke, a mogu biti generirana u bilo kojoj fazi slanja [25]. Najčešće korištena X – zaglavlja vezana su uz testiranje poruka na spam. X – zaglavlja sadrže informacije potrebne da se poruka dostavi u mapu za spam, umjesto u korisnikovu mapu dolaznih poruka. Svatko može pisati svoja X – zaglavlja, čime se smanjuje njihov kredibilitet [55]. Proučavanje vrijednosti pojedinih polja X – zaglavlja korisno je u svrhu razumijevanja načina filtriranja spam poruka, ali nije vjerodostojan izvor informacija jer ih svatko može napisati. Značenje pojedinih polja X – zaglavlja i načini testiranja poruke na spam biti će detaljnije objašnjeni u poglavlju 3.

Opis strukture zaglavlja e-poruke započeti će opisom polja od *Date* do *Reply – To.* Ova polja su označena brojem {1} u privitku 1. Polja *Date* do *Reply - To* sadrže osnovne informacije o pošiljatelju i primatelju. Polje *Date* sadrži vrijeme slanja e-poruke. Vrijeme se zapisuje u obliku timestampea po UTC (*Coordinated Universal Time*) vremenu, a zadnji broj označava za koliko je trenutno vrijeme ispred ili iza UTC vremena. U primjeru u privitku 1 zadnji broj je -5 što znači da trenutno vrijeme pošiljatelja kasni 5 sati za UTC vremenom.

Sljedećih par polja sadrži redom informacije o temi e-poruke, imenu i e-adresi pošiljatelja, te e-adresi primatelja. Polje *Reply – To* sadrži informaciju o e-adresi na koju će pristizati odgovor koji primatelj vrati pošiljatelju. Ta adresa može se razlikovati od e-adrese pošiljatelja. Zanimljivo je za uočiti da se korisniku prikazuje samo e-adresa koja se nalazi u polju *From*, a ne i e-adresa koja se nalazi u polju *Reply – To.* Ukoliko korisnik želi vidjeti obje adrese,

odnosno želi potvrditi da se njegov odgovor na poruku prosljeđuje na prikazanu pošiljateljevu adresu, korisnik treba otvoriti zaglavlje e-poruke i usporediti vrijednosti polja *From* i *Reply – To*.

Sljedeći niz informacija u strukturi zaglavalja e-poruke je popis svih MTA agenata kroz koje je e-poruka prošla na putu od pošiljatelja do primatelja. Ova polja označena su brojem {2} na privitku 1. Kako bi se uspješno rekonstruirao put e-poruke kroz MTA agente, ovaj dio zaglavlja potrebno je čitati odozdola prema gore. Zadnji odlomak koji započinje sa tekstom "*Recieved: from ...*" ujedno je i prva stanica kroz koju je e-poruka prošla na svom putu od pošiljatelja do primatelja. Prikaz svih MTA agenata kroz koje je prošla poruka prikazana u primjeru 1 dan je na slici 2.2.



Slika 2.2: IP adrese i MTA agenti kroz koje je prošla e-poruka.

Svaki MTA agent kroz koji poruka prođe na putu od pošiljatelja do primatelja u zaglavlje e-poruke dodaje informacije o tome od koga je primio poruku i gdje će je proslijediti. Također, MTA dodaje i informacije o protokolu koji je korišten pri prijenosu, kao i e-adresu krajnjeg korisnika kojem se poruka prosljeđuje. Prvi "*Recieved: from ...*" odlomak sadrži IP – adresu pošiljatelja i MUA na koji se pošiljatelj spojio. Iz dijela odlomka u kojem piše "*... with HTTP*" može se zaključiti da je korisnik pristupio svom poštanskom sandučiću koristeći web-klijent.

Osim informacija o MTA agentima kroz koje je e-poruka prošla na putu od pošiljatelja do primatelja, neki MTA agenti provjeravaju i sadržaj same e-poruke. Rezultat provjere sadržaja e-poruke su već ranije spomenuta X-zaglavlja e-poruke koja će biti opisana u poglavlju 3.

2.4. Proširenje elektroničkih poruka za multimediju

U svrhu proširenja osnovnih spospobnosti elektroničke pošte, Bell Communications je 1991. g. uveo MIME (*Multipurpose Internet Mail Extension*) protokol [26]. Ograničenja SMTP protokola i e-poruka prethodno su opisani u poglavlju 2.1.2. MIME protokol omogućuje prijenos ne-ASCII znakova i multimedijskih datoteka preko SMTP protokola [26].

MIME protkol radi na način da sve ne-ASCII znakove kodira koristeći ASCII zapis [26]. Takav kodirani ASCII zapis šalje se od pošiljatelja do primatelja koristeći SMTP protokol. Na primateljevoj strani MIME protokol dekodira kodirani ASCII zapis, te primatelj dobiva izvorni zapis. Koristeći MIME protokol korisnici mogu, osim običnog znakovnog teksta, razmjenjivati i poruke koje sadrže posebne znakove njihovog jezika, kao i slike, video uratke, zvuk i ostalo [26].

Podatci o MIME protokolu i vrsti provedenog kodiranja dodaju se u zaglavlje e-poruke. Postoji pet polja koja se dodaju u zaglavlje e-poruke [26]:

1. MIME Version – polje koje sadrži podatak o korištenoj verziji MIME protokola.
2. Content Type – polje koje sadrži podatak o tipu podataka koji se prenosi. To može biti običan tekst, zvukovna ili slikovna datoteka i drugo.
3. Content Transfer Encoding – polje koje sadrži podatak o načinu kodiranja poruke.
4. Content Id – polje koje sadrži jedinstveni identifikator poruke.
5. Content description – polje koje sadrži informaciju o tome da li je sadržaj poruke slika, video ili zvuk.

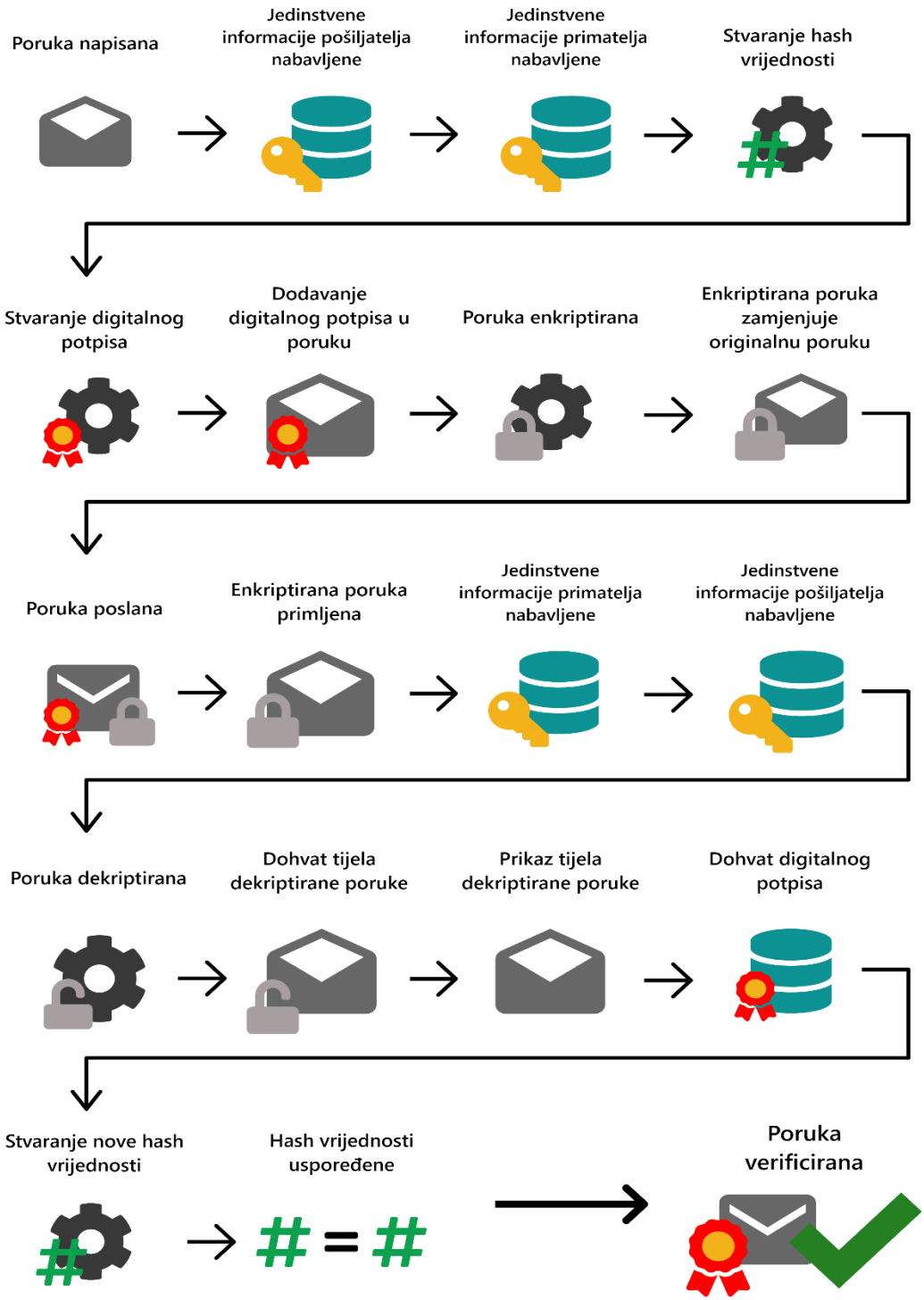
Ova polja označena su brojem {4} u privitku 1.

2.5 Proširenje elektroničkih poruka za sigurnost

Jedna od, možda i najvećih mana SMTP protokola je njegova nemogućnost autentifikacije pošiljatelja [27]. Autentifikacija je postupak kojim se jednoznačno potvrđuje identitet pošiljatelja [27]. Na taj način primatelj može biti siguran da je poruka uistinu i došla od pošiljatelja. U svrhu povećanja sigurnosti SMTP protokola razvijen je S/MIME (*Secure/Multipurpose Internet Mail Extensions)* protokol. S/MIME protokol pruža dvije osnovne usluge [27]:

1. Digitalno potpisivanje elektroničkih poruka
2. Enkripcija poruka.

Digitalno potpisivanje i enkripcija elektroničkih poruka često se koriste zajedno. Digitalni potpis osigurava identitet pošiljatelja, dok se enkripcijom čuva sadržaj same poruke [27]. Prikaz postupka stvaranja digitalnog potpisa, enkripcije, potvrđivanja potpisa i dekripcije dan je na slici 2.3, a sami postupci biti će opisani u narednim poglavljima.



Slika 2.3: Stvaranje digitalnog potpisa, enkripcija, potvrđivanje potpisa i dekripcija.

2.5.1 Digitalno potpisivanje elektroničkih poruka

Digitalno potpisivanje elektroničkih poruka je postupak sličan stvarnom potpisivanju legalnih dokumenata. Pri tome se koristi metoda privatnog i javnog ključa [27]. Svaki korisnik posjeduje privatan i javni ključ. Javni ključ je dostupan svima, dok je privatan ključ poznat samo vlasniku. Javni i privatni ključevi generiraju se matematičkim funkcijama koje jamče da se na temelju poznatog javnog ključa korisnika ne može generirati njegov privatan ključ [28].

Jednom potpisana poruka jamči pošiljateljev identitet te ga pravno obvezuje, isto kao i pri potpisivanju legalnih dokumenata [27]. Prema Pravilniku o pružanju i korištenju usluga povjerenja udaljeni kvalificirani elektronički potpis je kvalificirani potpis koji se koristi pod isključivom kontrolom potpisnika [30]. Potpisnik daje svoju suglasnost pružatelju usluga kojom prihvaća uvjete potpisivanja u kojima se korisnika ne mora pitati za potvrdu potpisa pri slanju svake e-poruke [30]. Ova obveza u praksi znači da se pri potpisivanju poruke potpisniku ne moraju predočiti podatci prije potpisivanja, ali da se potpisnik ne može pozvati na nemogućnost uvida u podatke prije potpisivanja zbog suglasnosti koju je prethodno dao pružatelju usluga [30].

Digitalni potpis elektroničke poruke nudi korisniku mehanizme kojima se potvrđuje da je poruku poslala osoba koja tvrdi da ju je poslala, odnosno da poruka nije lažirana. Digitalnim potpisom nije moguće u potpunosti spriječiti lažiranje e-poruke, ali je to znatno otežano u odnosu na SMTP protokol koji ne pruža nikakve sigurnosne mehanizme. Ova funkcija digitalnog potpisa zove se autentifikacija pošiljatelja. Digitalni potpis također pravno obvezuje pošiljatelja zato što digitalno potpisanu e-poruku u pravilu nije moguće opovrgnuti kao lažiranu [27]. Opovrgavanje digitalnog potpisa moguće je jedino ukoliko potpisnik digitalnog potpise može dokazati da oštećena strana nije poduzela ili je pogrešno poduzela radnje vezane za validaciju elektroničkog potpisa [29]. Ova funkcija digitalnog potpisa zove se neporecivost. Posljednja uloga digitalnog potpisa je osiguravanje primatelju da je prispjela poruka uistinu i ona poruka koja je poslana, te da poruka nije mijenjana na putu od pošiljatelja do primatelja. Ova funkcija zove se čuvanje integriteta podataka.

Digitalno potpisivanje i verifikacija prispjele elektroničke pošte odvijaju se u nekoliko koraka. Koraci obavljanja digitalnog potpisa i enkripcije poruke prikazani su na slici 2.3 Nakon što pošiljatelj napiše poruku i pritisne tipku za slanje, S/MIME protokol poziva hash funkciju koja generira hash na temelju napisane poruke [31]. Hash funkcije su matematičke funkcije koje iz proizvoljno dugačkog niza znakova generiraju niz točno određene duljine [31]. Svojstvo hash funkcija je da će svaki hash generiran nad istim nizom biti jednak, te da je vjerojatnost generiranja iste hash vrijednosti za dva različita niza znakova veoma malena, ali ne i nemoguća. Dobra hash funkcija daje jako različite hash vrijednosti čak i za vrlo slične nizove. Generirana hash vrijednost

se zatim enkriptira koristeći pošiljateljev privatni ključ čime nastaje digitalni potpis. Digitalni potpis dodaje se u tijelo poruke. Poruka se zatim šalje primatelju. Primatelj najprije dohvaća poruku, a zatim digitalni potpis pošiljatelja i njegov javni ključ. Javnim ključem pošiljatelja primatelj dekriptira hashiranu vrijednost digitalnog potpisa. Primatelj zatim generira novu hash vrijednost na temelju prispjele poruke, te ju uspoređuje sa prispjelom dekriptiranom hash vrijednosti. Pri tome se mora koristiti ista matematička funkcija korištena za stvaranje hash vrijednosti na strani pošiljatelja, jer inače hash vrijednosti neće odgovarati. Ukoliko odgovaraju, poruka je uspješno verificirana [27].

2.5.2 Enkripcija elektroničkih poruka

Enkripcija elektroničkih poruka je postupak zaštite elektroničkih poruka kojim se štiti sam sadržaj poruke [27]. Za razliku od digitalnog potpisa kojim se jamčio identitet osoba koje razmjenjuju poruke, kao i da sadržaj poruke nije mijenjan, enkripcijom se štiti sadržaj kako bi se osiguralo da poruku pročita samo primatelj. Enkripcija je postupak zaštite sadržaja poruke na način da se poruka pretvara iz formata razumljivog ljudima u niz znakova i riječi koje nemaju smisla osobama koje ne znaju pretvoriti enkriptirani tekst poruke u originalni tekst [32]. Samo osoba kojoj je poruka namijenjena zna kako vratiti poruku u izvorni oblik. Na taj način, čak i ako bi netko presreo poruku na putu od pošiljatelja do primatelja ne bi mogao odgonetnuti što piše u njoj. Ova usluga enkripcije elektroničkih poruka naziva se povjerljivost.

Osnovna razlika između digitalnog potpisa i enkripcije je u informacijama koje ove dvije usluge koriste za stvaranje digitalnog potpisa, odnosno za enkripciju poruke. Postupak stvaranja digitalnog potpisa koristi informacije o pošiljatelju zato što je njegova glavna svrha potvrđivanje identiteta pošiljatelj, dok postupak enkripcije koristi informacije o primatelju kako bi samo primatelj mogao dešifrirati tu poruku [27]. Za oba postupka koristi se metoda javnog i privatnog ključa. Pri stvaranju digitalnog potpisa za enkripciju stvorenog hasha koristi se privatni ključ pošiljatelja, dok se za dekripciju koristi pošiljateljev javni ključ. Ukoliko se poruka može dekriptirati pošiljateljevim javnim ključem, može se zaključiti da je ona uistinu i enkriptirana pošiljateljevim privatnim ključem, odnosno potvrđuje se identitet pošiljatelja. Pri enkripciji pošiljatelj enkriptira poruku javnim ključem primatelja. Na taj način poruku može dekriptirati samo primatelj poruke, zato što samo on zna privatan ključ potreban za dekripciju.

Enkripcija i dekripcija napisane poruke odvijaju se u nekoliko koraka. Postupci enkripcije, dekripcije i stvaranja digitalnog potpisa prikazani su na slici 2.3. Ukoliko se koristi metoda digitalnog potpisivanja e-poruke, poruka se najprije potpiše na način opisan u potpoglavlju 2.5.1. Poruka se zatim enkriptira koristeći primateljev javni ključ. Enkriptirana poruka šalje se primatelju. Nakon

što poruka dođe do primatelja, primatelj dekriptira prvi sloj poruke koristeći svoj privatni ključ, a zatim dekriptira drugi sloj poruke koristeći pošiljateljev javni ključ [28]. Primatelju se potom prikazuje izvorna poruka [27]. Na primateljevoj strani zatim se generira nova hash vrijednost na temelju prispjelog sadržaja poruke te se uspoređuje sa prispjelom dekriptiranom hash vrijednosti. Ukoliko odgovaraju, poruka je uspješno validirana. Digitalnim potpisivanjem potvrđen je identitet pošiljatelja, dok je enkripcijom poruke zaštićen sadržaj poruke.

3. Phishing napadi

Phishing je vrsta društvenog napada s ciljem krađe privatnih podataka poput korisničkog imena, lozinke, bankovnih računa i drugo [33]. Phishing počiva na ideji lažnog predstavljanja i zadobivanja povjerenja ciljane osobe. Termin phishing pojavio se sredinom 1990-ih godina, a korijen riječi phish dolazi od engleske riječi fish što znači riba [34]. Slično kao i pri pecanju, napadač baci mamac (pošalje e-poruku u kojoj se lažno predstavlja) i čeka da vidi hoće li žrtva zagristi. Napadač potom najčešće djeluje na način da preko lažirane e-poruke od žrtve traži da otvori zlonamjernu poveznicu [35]. Ukoliko žrtva zagrize i otvori zlonamjernu poveznicu, biti će preusmjerena na lažiranu Internet stranicu koja nalikuje originalnoj stranici i od žrtve će se tražiti unos osjetljivih podataka poput korisničkog imena i lozinke. Pribavljanjem tih informacija napadaču se otvara put za daljnje iskorištavanje drugih podataka žrtve ili organizacije u kojoj žrtva radi.

Otvaranje zlonamjerne poveznice može rezultirati i preuzimanjem zlonamjernog programa na računalo žrtve [34]. Zlonamjerni program zatim dohvaća osjetljive podatke žrtve i prosljeđuje ih napadaču. Jedan od specifičnih phishing napada je lažno predstavljanje kao osoba od povjerenja unutar neke organizacije. Nakon početne uspostave komunikacije, napadač nastavlja komunikaciju sa ciljanom osobom preko e-poruke nudeći im usluge iz područja koje bi ih moglo zanimati, te od njih traži žurnu akciju. Napadač se često predstavlja kao nadležna osoba tvrtke u kojoj ciljana osoba radi, te od nje traži da hitno prebaci veće svote novca na neki račun. Primjer ovakvog phishing napada dogodio se 2018. godine u Đakovu [36]. Pročelnik za financije grada Đakova je u srpnju 2018. godine dobio zahtjev od tadašnjeg gradonačelnika grada Đakova za hitnom uplatom sredstava na račun gospodinu Johnu Smithu. Pročelnik nije primijetio da je zahtjev došao sa domene e-adrese koja uopće ne pripada gradu Đakovu, te je isplatio 50 tisuća eura na račun gospodina Johna Smitha. Kako se kasnije ispostavilo cijela elektronička poruka bila je lažirana, te je pročelnik postao žrtvom phishing napada.

Jedan od medijski najpopraćenijih phishing napada dogodio se 2016. godine za vrijeme predsjedničke kampanje Hillary Clinton. Član njene kampanje, John Podesta primio je u ožujku 2016. godine elektroničku poruku u kojoj mu tehnička potpora njegovog web klijenta Gmaila javlja kako se netko upravo pokušao prijaviti u njegov poštanski sandučić, ali kako je taj pokušaj spriječen [37]. Od Podeste se zatim tražilo da žurno promijeni lozinku svog poštanskog sandučića, te mu je u tu svrhu priložena poveznica koju treba otvoriti kako bi promijenio svoju lozinku. John Podesta nije primijetio netipičnu domenu googlemail.com s koje mu je poruka poslana, kao ni URI za promjenu lozinke koji uopće ne sliči drugim Gmail URI-evima, te je postao još jedna u

nizu phishing žrtava. Pristup njegovom poštanskom sandučiću napadači su iskoristili u listopadu iste godine kada su u medije procurile interne poruke Johna Podeste.

3.1. Tehnike phishing napada

Prvi phishing napadi pojavili su se početkom 1990-ih godina što phishing napade čini jednim od najstarijih računalnih napada na svijetu [38]. Zbog njihovog dugog postajanja postoje različite inačice i tipovi phishing napada, ali ono što ih sve povezuje je lažno predstavljanje [39]. Bilo da se napadač predstavlja kao banka koja od korisnika traži unos podataka bankovne kartice ili kao nadležne osoba tvrtke u kojoj pojedinac radi, od pojedinca se uvijek traži neka akcija koja otkriva njegove privatne podatke.

Najčešće se od korisnika traži jedna od sljedećih dviju vrsta akcija: prva akcija žrtvi nudi poveznicu na lažiranu internetsku stranicu koja izgleda identično kao i originalna stranica, ali je URI stranice izmijenjen [34]. Od žrtve se potom traži da unese svoje korisničke podatke ili podatke svoje bankovne kartice. Cilj druge akcije je skidanje zlonamjernog programa na ciljano računalo [34]. Zlonamjerni programi se često predstavljaju kao legitimni dokumenti koji se šalju žrtvi. Jedan takav dokument mogao bi biti životopis osobe koja se želi zaposliti u ciljanoj firmi. Napadač pošalje žrtvi svoj životopis u obliku kompresirane datoteke koja sadrži zlonamjerni program. U trenutku raspakiravanja datoteke, zlonamjerni program se smješta žrtvi na računalo, te od tamo prikuplja osjetljive informacije žrtve. Ukoliko napadač blokira pristup pojedinim dijelovima računala žrtve i za povrat kontrole nad računalom traži otkupninu, phishing napad može prerasti u ransomware napad.

Ransomware je vrsta računalnog napada kojim napadač stječe pristup osobnim podatcima žrtve, poput privatnih slika i dokumenata, te ih enkriptira tako da postaju nečitljivi žrtvi [40]. Od žrtve se potom traži da se napadaču isplati određena svota novca, a nakon isplate napadač bi trebao vratiti pristup podatcima žrtvi. Naravno, ne postoji nikakva garancija da će se napadač držati svog dijela dogovora, te se može dogoditi da bez obzira na isplatu žrtva i dalje ostane bez svojih privatnih podataka.

Također postoje i ucjenjivački phishing napadi koji počivaju na ucjenjivanju žrtve. Najčešće se radi o elektroničkim porukama u kojima napadač tvrdi da posjeduje ili eksplicitne slike i video uratke žrtve ili da posjeduje žrtvine korisničke podatke poput korisničkog imena i lozinke [41]. Od žrtve se zatim traži da napadaču isplati određenu svotu novca na račun jer će u suprotnom napadač proslijediti informacije koje posjeduje u javnost. Ucjenjivačke e-poruke su najčešće lažirane, te napadači ne posjeduju informacije koje tvrde da posjeduju. Ova vrsta napada temelji se na masovnom odašiljanju lažirane poruke u nade da će makar i malen broj ljudi zagristi.

Osim po akcijama koje se traže od žrtve, phishing napadi se mogu razlikovati i po profilima ciljanih žrtava. Neke od vrsta phishing napada obzirom na profil ciljane žrtve su [39]:

- E-mail phishing napadi – Žrtve se izabiru nasumično. Bilo tko može biti odabran.
- Spear phishing napadi – Žrtve se izabiru unutar organizacije koju se napada, a to mogu biti i viši i niži službenici organizacije.
- Whale phishing napadi – Žrtve su visokopozicionirani članovi organizacije.
- i drugi.

E-mail phishing napadi ne traže od napadača prethodno prikupljanje i proučavanje osobnih podataka o ciljanoj osobi kako bi se prijevara dogodila [33]. Napadač jednostavno pošalje na tisuće, pa čak i stotine tisuća e-poruka koje sadrže zlonamjerne poveznice [33]. Najčešće se radi o lažnom predstavljanju organizacija koje od korisnika zahtijevaju brzo reagiranje, primjerice od korisnika se traži žurno mijenjanje lozinke zbog neautorizirane prijave u korisnički poštanski sandučić. Iako je ovu vrstu napada puno lakše za uočiti od spear phishing napada, dovoljno je da samo malen broj korisnika nasjedne na prijevaru da bi napadač uprihodio velike svote novca.

Pri spear phishing napadu, prije samog početka komunikacije između počinitelja i ciljane osobe, počinitelj mora prikupiti podatke o ciljanoj osobi i smisliti kakva usluga bi mogla zainteresirati tu osobu [34]. Počinitelj prikupljanje podataka vrši pretražujući javno dostupne podatke ciljane osobe. Društvene mreže, poput Facebooka, Instagrama i Twittera su jedan takav izvor informacija. LinkedIn, kao poslovna društvena mreža, također može biti izvor prikupljanja informacija. Ukoliko korisnik nije pažljiv pri postavljanju postavki privatnosti, njegovi osobni podatci mogu biti javno dostupni svima. Temeljitom pripremom napadač se može uspješno predstaviti kao odgovorna osoba organizacije s kojom je žrtva već prethodno poslovala ili kao nadležna osoba u organizaciji u kojoj žrtva radi. Napadač potom od žrtve traži ili žurnu uplatu sredstava na neki račun ili promjenu podataka bankovnog računa na koji se vrše uplate [34].

Whale phishing napadi su veoma slični spear phishing napadima, ali mete su im visokopozicionirani članovi neke tvrtke [34]. Najčešće se radi o članovima upravnog odbora tvrtke koji ne sudjeluju aktivno u radu tvrtke. Kako ove osobe nisu aktivni zaposlenici tvrtke, one često nemaju službenu e-adresu tvrtke, nego za komunikaciju koriste privatne e-adrese. Velike tvrtke vrlo često uvode dodatne mjere zaštite za e-adrese svojih zaposlenika poput dvostupanjske verifikacije, ali članovi upravnog odbora koji nemaju e-adresu tvrtke često nisu obuhvaćeni tim mjerama zaštite. U praksi ljudi često koriste iste korisničke podatke za pristup raznim sustavima. Napadači mogu tu činjenicu iskoristiti na način da pokušaju nabaviti korisničke podatke ciljane osobe preko nekog+

drugog, manje sigurnog sustava, te potom ukradene korisničke podatke iskoriste za pristup ciljanom sustavu [34].

3.2. Tehnike prevencije phishing napada

Prevencija phishing napada nije lak zadatak. Ne postoji neki univerzalan program koji može pružiti zaštitu od phishing napada. Kako phishing napadi vrlo često počivaju na masovnom odašiljanju lažiranih e-poruka, kao mjera zaštite protiv phishing napada mogu se koristiti spam filteri. Više o spamu i spam filterima biti će rečeno u potpoglavlju 3.3. Uporabom programa za detekciju spam poruka korisnike se štiti od masovno odašiljanih lažiranih poruka, ali phishing napade koji ciljaju točno određene osobe nije lako za uočiti. Metode koje se preporučaju za prevenciju phishing napada su edukacija zaposlenika o phishingu i vrstama phishing napada, te uvođenje dvostupanjske verifikacije [33]. U razgovoru sa jednim zaposlenikom tvrtke Croatia osiguranje otkriveno je da tvrtka svake godine provode edukaciju o phishingu i drugim računalnim napadima. Nažalost, edukacija zaposlenika o phishing napadima vrlo često nema željeni učinak [42]. Uobičajeni način edukacije zaposlenika o phishingu uključuje niz predavanja u kojima se zaposlenika upoznaje sa ovom vrstom računalnog napada [42]. Provedeno ispitivanje pokazuje da je razlika u postotku zaposlenika educiranih na ovaj način koji otvore phishing poveznicu i zaposlenika koji nisu prošli edukaciju vrlo malena, odnosno da edukacija nije polučila željene rezultate [42].

Osim edukacije zaposlenika, tvrtke bi trebale implementirati i metode zaštite od phishing napada poput uvođenja dvostupanjske verifikacije ili uvođenja jedne odgovorne osobe koja ima pravo mijenjati podatke o bankovnim računima organizacija s kojima tvrtka posluje. Dvostupanjska verifikacija je postupak prijave u sustav koji od korisnika traži, osim korisničkog imena i lozinke, još jedan podatak koji potvrđuje identitet korisnika [43]. Najčešće se kao drugi korak verifikacije koriste SMS poruke koje korisnik primi na svoj telefon pri pokušaju prijave u sustav. SMS poruka sadrži nasumično generirani tekst koji korisnik mora unijeti u zatraženo polje kako bi dovršio prijavu u sustav. Ovakvim načinom zaštite sustav se štiti čak i ako dođe do gubitka korisničkih podataka zato što napadač ne može pristupiti sustavu bez mobilnog telefona korisnika.

3.3 Tehnike detekcije spam poruka

X – zaglavlja su nestandardizirani dijelovi zaglavlja elektroničke pošte, a mogu nastati u bilo kojoj fazi slanja e-poruke [25]. X – zaglavlja e-poruke označena su brojem {3} na privitku 1. Dio polja X – zaglavlja vezan je uz detekciju spam

poruka, a spam dijelove prikazane na privitku 1 generirao je MTA agent stuttgart.optimus-hosting.com. Kako su X - zaglavlja ne standardizirana, različiti davatelji usluge elektroničke pošte generiraju različita X – zaglavlja. Spam polja X – zaglavlja analiziranih u nastavku biti će objašnjena na primjeru Microsoft Outlooka [44]. Kako bi program mogao ustvrditi da li je riječ o spam poruci ili ne, mora provjeriti sadržaj same poruke. Poruka se provjerava na način da se provede niz heurističkih testova nad njenim sadržajem, a rezultat svakog testa je procjena vjerojatnosti poruke na spam. Primjer jednog takvog testa bi bila klasifikacija e-poruke Bayesovim naivnim klasifikatorom [45]. Naivni Bayesov klasifikator čita poruku u potrazi za specifičnim riječima ili izrazima poput oznake cijene, sniženja ili čak imena neke slavne osobe. Svaki put kada pronađe traženu riječ povećava brojač za tu riječ. Po završetku čitanja poruke, naivni Bayesov klasifikator klasificira poruku koristeći Bayesovu formulu. Naivnom Bayesovom klasifikatoru često se dodaju proširenja koja u obzir uzimaju i font i boju slova, kao i broj poveznica u poruci. Po završetku svih testova, na temelju izračunatih procjena za pojedini test računa se ukupna procjena vjerojatnosti poruke na spam. Ukoliko je procjena iznad granične vrijednosti, poruka se označava kao spam, inače se poruka označava kao legitimna poruka. Osjetljivost testova na spam može se podijeliti u četiri kategorije spama ovisno o graničnoj vrijednosti procjene [44]:

1. Siguran spam – vjerojatnost procjene mora biti preko 300 da bi poruka bila spam.
2. Agresivan spam – vjerojatnost procjene mora biti između 50 i 300 da bi poruka bila spam.
3. Umjeren spam – vjerojatnost procjene mora biti između 100 i 300 da bi poruka bila spam.
4. Opušteni spam – vjerojatnost procjene mora biti između 150 i 300 da bi poruka bila spam.

Vjerojatnostima spama odgovaraju polja X-Spam-Score, X-Spam-Status i X-Spam-Bar u X – zaglavlju e-poruke. Polje X-Spam-Status sadrži informaciju o tome da li je poruka kategorizirana kao spam ili nije. Polje X-Spam-Score sadrži informaciju o rezultatu testova poruke na spam, dok polje X-Spam-Bar sadrži ili jedan znak "-", ili više znakova "+". Znak "-" u polju X-Spam-Bar označava poruku koja nije kategorizirana kao spam, dok količina znakova "+" označava koliko je jako poruka kategorizirana kao spam. Više znakova "+" označava veću vjerojatnost da je poruka spam.

Osim polja o spamu, X – zaglavlja nude i niz drugih informacija o pošiljatelju.

Značenje nekih od polja u X – zaglavlju e – poruke:

- Polje X – AntiAbuse: Primary Hostname sadrži domenu primarnog MTA agenta koji je dodao X – zaglavlje u zaglavlje e-poruke.

- Polje X – AntiAbuse: Original Domain sadrži domenu primatelja e-poruke.
- Polje X – AntiAbuse: Sender Address Domain sadrži domenu pošiljatelja e-poruke.
- Polje X – Source: IP sadrži IP adresu pošiljatelja.
- Polje X – Source: Sender sadrži adresu pošiljatelja.
- Polje X – Source: Auth sadrži informaciju o MTA agentu koji je proveo autentifikaciju korisnika.

Iz primjera sa privitka 1, može se uočiti da su pojedina polja, poput IP adrese pošiljatelja i e- adrese pošiljatelja prazna. Pri slanju e – poruka, moguće je zaštiti vlastite podatke i zabraniti MTA agentu da ih ubacuje u X – zaglavlja e – poruke. Nažalost, ova opcija znatno otežava postupak analize zaglavlja e – poruke zato što smanjuje količinu dostupnih informacija u zaglavljima e-poruka.

3.3. Slučaj phishing napada u Hrvatskoj u kolovozu 2019. godine

Krajem kolovoza 2019. godine došla sam u doticaj sa jednim slučajem internet prijevare korištenjem spear phishing tehnike. Početkom kolovoza iste godine vlasnik tvrtke primio je e-poruku od osobe koja se predstavila kao direktor tvrtke s kojom je tvrtka žrtva već prethodno uspješno poslovala. Domena adrese s koje je osoba poslala poruku odgovarala je domeni adresa prethodno primljenih poruka. Osoba se predstavila, ali nije pružila dodatne informacije o tome zašto im se upravo ona javlja, niti zašto u komunikaciji ne sudjeluju osobe koje su sudjelovale u prethodnim razgovorima. Napadač nije izazvao nikakvu sumnju kod tvrtke žrtve, te je ubrzo s njima dogovorio narudžbu robe iz Kine. Prije isporuke robe zahtijevao je od tvrtke žrtve uplatu cijelog iznosa troška, što je tvrtka žrtva i napravila. Kako je vrijeme prolazilo, napadač je uvjeravao tvrtku žrtvu kako će roba uskoro stići, ali kako kasni zbog raznoraznih razloga. Tvrtka žrtva i dalje nije ništa posumnjala, te je s napadačem sklopila još jedan ugovor. Ovaj put im je napadač nudio istu narudžbu ali po nižoj cijeni, te je također zahtijevao uplatu unaprijed. Tek nakon druge uplate i još par tjedana čekanja tvrtka žrtva je posumnjala u napadačevu vjerodostojnost. Tvrtka žrtva i napadač su ostali još neko vrijeme u kontaktu nakon što je tvrtka žrtva posumnjala da je prevarena, ali iz te komunikacije nisu uspjeli izvući nikakvu korist.

4. Postupci analize elektroničke pošte

Forenzika e-pošte grana je računalne forenzike koja se bavi analizom i istragom zločina počinjenih koristeći e-poruke. Osim mehanizama prijenosa e-poruka, nužno je poznavati na koje se sve načine može doći do dodatnih informacija o sudionicima e-razgovora, te koji se alati pri tome koriste. U praksi se pri istrazi e-poruka koriste sljedeće tehnike i alati [46]:

1. Analiza zaglavlja e-poruke
2. Analiza servera
3. Analiza mrežnih uređaja
4. Analiza klijenata e-poruke
5. Analiza priloženih privitaka
6. Analiza korištenjem whois naredbe
7. Analiza korištenjem nslookup naredbe.

4.1 Analiza zaglavlja e-poruke

Ukoliko se sumnja u legitimnost primljene elektroničke poruke ili ukoliko je počinjen računalni napad putem e-poruke, prvi korak u analizi elektroničke pošte je analiza zaglavlja e-poruka. Zaglavlje e-poruke sadrži mnoštvo informacija o pošiljatelju, te o putu kojim je e-poruka prošla od pošiljatelja do primatelja. Pri prolasku poruke od pošiljatelja do primatelja, e-poruka prolazi kroz niz MTA uređaja pri čemu svaki MTA uređaj dodaje vlastite informacije o tome od kojeg MTA uređaja je primio poruku, na koji MTA uređaj će poruku proslijediti, kada ja primio poruku, ID poruke koju je primio, itd. Sve te informacije spremaju se u zaglavlje e-poruke, a korisniku se ne prikazuju osim ako tako eksplicitno ne zatraži [7]. Analizom zaglavlja e-poruka mogu se otkriti informacije poput IP adrese pošiljatelja, Reply – To adrese pošiljatelja ili korištenog klijenta elektroničke pošte. Zaglavlja elektroničke pošte detaljno su opisana u poglavlju 2.

4.2 Analiza servera

Analiza servera provodi se nad serverima zaduženim za dostavu e-poruke [46][47]. Primjeri tih servera mogu biti proxy serveri ili interni serveri neke organizacije. Proxy serveri su serveri koji se koriste pri spajanju na Internet

kako bi se korisniku omogućilo sigurno i anonimno korištenje Interneta. Organizacije koje koriste interne servere najčešće sadrže server na koji pristižu sve poruke poslane na domenu organizacije, a korisnici svoje poruke dobavljaju spajanjem na server. Ukoliko su elektroničke poruke obrisane od strane pošiljatelja ili primatelja, te ih nije moguće povratiti, analiza servera dohvaća kopije poslanih e-poruka sa servera. Osnovno ograničenje u analizi poruka servera je u tome što se poruke na serveru nalaze ograničenu količinu vremena, a potom se brišu [46][47].

4.3 Analiza mrežnih uređaja

Ponekad se ne može provesti analizu servera zato što vlasnici servera ne pristaju na davanje pristupa podatcima servera [46][47]. U tom slučaju koristi se analiza mrežnih uređaja. Pri analizi mrežnih uređaja, istražitelj pokušava pristupiti zapisima spremljenim na usmjerivače i komutatore kroz koje je poruka prošla na putu od pošiljatelja do primatelja [46][47]. Ukoliko se ovi podatci pribave, moguće je utvrditi da li je poruka stvarno prošla kroz MTA agente navedene u njenom zaglavlju. Ako je promijenjen zapis puta kroz koji je poruka prošla od pošiljatelja do primatelja, analizom mrežnih uređaja to se lako otkriva. Naime, ako u zaglavlju e-poruke stoji da je poruka prošla kroz navedeni MTA uređaj, a u zapisima preuzetim sa MTA uređaja ne postoji zapis o toj poruci, onda poruka nije prošla kroz taj MTA uređaj. Također, treba uzeti u obzir da je poruka možda obrisana iz zapisa, te provjeriti i tu mogućnost. Pristup podatcima na mrežnim uređajima u pravilu je znatno zahtjevniji od pristupa podatcima na serveru, te se koristi samo kada primarni izvori informacija, poput analize zaglavlja i analize servera, nisu dostatni [46][47]. Također, vrlo je vjerojatno da se barem dio MTA uređaja neće nalaziti unutar iste države, što znači da će se istražitelj trebati koordinirati sa osobama nadležnim za te uređaje u drugim državama i od njih tražiti pristup. Naravno, ne postoji nikakva garancija da će istražitelj dobiti traženi pristup.

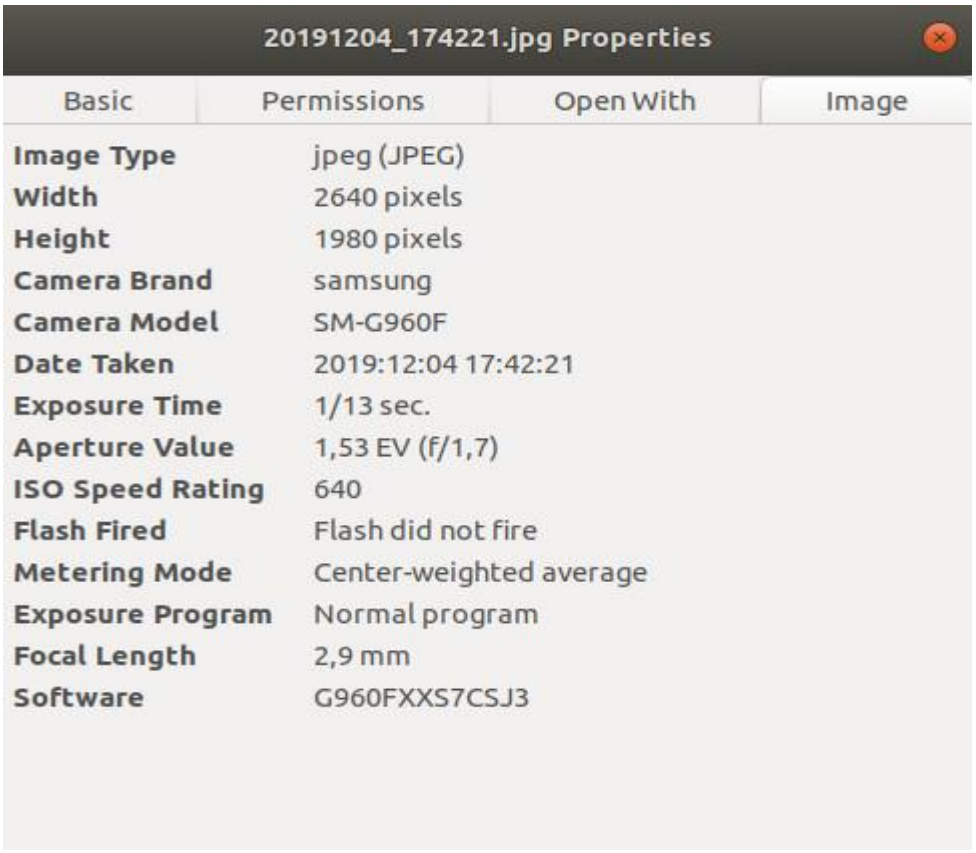
4.4 Analiza klijenata e-poruke

Analiza klijenata e-poruke podrazumijeva analizu informacija koje je u zaglavlje e-poruke umetnuo korišteni klijent elektroničke pošte [46][47]. Ti podatci su označeni brojem 1 na privitku 1, a prethodno su opisani u poglavlju 2. Analizom klijenta e-poruke može se ustvrditi da li je poruka uistinu poslana sa tog klijenta, kao i da li je poslana u vrijeme zapisano u zaglavlju e-poruke. Naime, pri slanju e-poruke, svaki klijent poruci dodjeljuje jedinstveni ID kako bi se ona lako mogla kasnije referencirati preko tog ID-a. ID poruke se najčešće sastoji od vremenske oznake koja označava vrijeme slanja e-poruke i od domene

pošiljatelja. Ukoliko je poruka mijenjana, promijeniti će se i njen ID, te vremenska oznaka više neće odgovarati [46][47].

4.5 Analiza priloženih privitaka

Ukoliko su u porukama razmijenjeni privitci, vrlo često se koristi tehnika analize poslanih privitaka [46]. Mehanizmi slanja privitaka elektroničkom poštom opisani su u poglavlju 2. Mnoge datoteke sadrže korisne informacije o osobi koja ih je stvorila, datumu stvaranja datoteke, datumu posljednje izmjene i drugo. Ti podatci se nazivaju metapodatcima datoteke, a njihov primjer dan je na slici 4.1.



Slika 4.1. Primjer metapodataka slike

Metapodatcima slike na operacijskom sustavu Ubuntu 18.04, može se pristupiti tako da se pritisne desnom tipkom miša na sliku, te se u padajućem izborniku odabere opcija Properties. Zatim se otvara novi prozor, te se na izbornoj traci odabere opcija Image. Drugi način pregleda metadata podataka datoteke, je korištenjem naredbe exif u Terminalu. Korisnik se treba pozicionirati u direktorij u kojem je spremljena datoteka čije metapodatke želi pregledati, te potom treba iskoristiti naredbu exif kojoj se kao argument predaje ime datoteke. Iz primjera sa slike 4.1. može se iščitati da se radi o slici zapisanoj u jpeg

formatu (polje Image Type), da je korištena kamera marke Samsung (polje Camera brand), da pri slikanju slike nije korištena bljeskalica (polje Flash Fired), da je slika slikana 04.12.2019. godine u 17:42:21 i drugi. Ukoliko se ova opcija ne isključi manualno u postavkama pametnog telefona, pri snimanju fotografije u metapodatke slike zapisuju se i podatci o geografskoj dužini i širini lokacije na kojoj je slika snimljena. U korist mnogim korisnicima društvenih mreža ide činjenica da se pri slanju slika društvenim mrežama briše većina metapodataka slike kako bi se smanjila veličina slike koju treba poslati. No, ukoliko se slika šalje elektroničkom poštom, njezini metapodatci ostaju netaknuti.

4.6 Analiza korištenjem whois i nslookup naredbe

U tehnike analize elektroničke pošte spadaju i tehnike analize registriranih domena sa kojih su poruke poslane. U tu svrhu može se koristiti alat Maltego čija je instalacija i uporaba opisana u poglavljima 5 i 6, ali mogu se koristiti i naredbe poput whois. Whois naredba pretražuje referentne baze podatka u potrazi za traženom domenom, te korisniku vraća ispis svih podataka o toj domeni. Whois naredba može nabaviti i ime vlasnika tražene domene ukoliko vlasnik ne zaštiti svoje privatne podatke. Whois naredba poziva se na način da se nakon ključne riječi whois napiše ime domene koju se želi pretražiti. Ukoliko se žele uključiti dodatne opcije pretraživanja one se navode prije imena domene, a prefiksiraju se znakom -. Više o dodatnim opcijama pretraživanja može se saznat čitajući upute o naredbi whois. Upute se mogu otvoriti tako da se najprije upiše ključna riječ man, a zatim ime naredbe. Primjer ispisa whois naredbe za domenu facebook.com dan je na slici 4.2.

```
Domain Name: FACEBOOK.COM
   Registry Domain ID: 2320948_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrarsafe.com
   Registrar URL: http://www.registrarsafe.com/
   Updated Date: 2020-01-15T16:52:39Z
   Creation Date: 1997-03-29T05:00:00Z
   Registry Expiry Date: 2028-03-30T04:00:00Z
   Registrar: RegistrarSafe, LLC
   Registrar IANA ID: 3237
   Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
   Registrar Abuse Contact Phone: +1-650-308-7004
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: A.NS.FACEBOOK.COM
   Name Server: B.NS.FACEBOOK.COM
   Name Server: C.NS.FACEBOOK.COM
   Name Server: D.NS.FACEBOOK.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

Slika 4.2: Primjer ispisa whois naredbe.

Osim podataka o vlasniku domene, whois naredba vraća i podatke o akreditiranom tijelu koje je izdalo tu domenu (polje Registrar), datumu stvaranja domene (Creation Date), datumu posljednje izmjene domene (Updated Date) i druge.

Uz whois naredbu najčešće se koristi i nslookup naredba. Za razliku od whois naredbe koja pristupa bazi podataka domena i od tamo vraća podatke o vlasniku domene, nslookup naredba pristupa svom nadležnom DNS uređaju, te od njega traži IP i MAC adresu za zadanu domenu. Princip rada DNS uređaja također je opisan u poglavlju 2. Nslookup naredba može se koristiti i za reverznu DNS potragu. Pri reverznoj DNS potrazi nslookup naredbi se kao argument predaje IP ili MAC adresa računala, te se od računala zahtjeva domena u simboličnom zapisu.

5. Instalacija i korištenje alata Maltego

Prethodno opisani mehanizmi slanja e-poruka i strukture zaglavlja e-poruka nužno je poznavati pri ekstrapolaciji i obradi dostupnih informacija u postupcima forenzike e-poruka. Alat koji je korišten u provedbi forenzike e-poruke u sklopu ovog završnog rada zove se Maltego, a njegova instalacija i upute za osnovno korištenje opisani su u narednim poglavljima.

5.1. Instalacija Maltego alata

U ovom primjeru Maltego alat će se instalirati na Linux operacijski sustav inačice Ubuntu 18.04.3 LTS. Maltego alat može se instalirati i na druge operacijske sustave, uključujući i Windows, a na operacijskom sustavu Kali Linux uključen je u osnovne programe operacijskog sustava, te ga ne treba posebno instaliravati [48]. Za potrebe instalacije potrebno je poznavati ili lozinku korisnika trenutne sesije ili lozinku root korisnika kako bi se mogle koristiti shell naredbe poput naredbe apt ili apt-get koje služe za dohvaćanje i instalaciju programa na Ubuntu operacijskim sustavima.

Koraci pri instalaciji Maltego alata:

1. Otvoriti stranicu https://www.paterva.com/ i na navigacijskoj traci odabrati opciju Downloads.
2. Odabrati operacijski sustav na koji se želi instalirati Maltego. U ovom primjeru odabran je operacijski sustav Linux i vrsta datoteke sa ekstenzijom .deb. Nakon što odabira operacijskog sustava i vrste datoteke, potrebno je kliknuti na gumb *Download.*
3. Po završetku preuzimanja datoteke na računalo, koristeći Terminal pozicionirati se u direktorij u kojem se nalazi preuzeta datoteka. Najčešće je to direktorij pod nazivom Downloads koji se nalazi unutar Home direktorija. Pozicionirati se može naredbom: cd ~/Downloads

4. Sljedeći korak je instalacija Maltego alata. Instalaciju se može napraviti koristeći naredbu:

```
sudo dpkg -i MaltegoCE.v4.2.8.12786.deb
```

Ukoliko korisnički račun nije dodan u grupu sudoers, dpkg naredba može se iskoristiti tako da korisnik najprije postane root korisnik, a zatim unese naredbu, no za to se mora poznavati lozinka root korisnika [49]. Jednostavniji način je dodavanje korisnika u grupu sudoers i zatim korištenje željene naredbe. Nakon

unosa naredbe, Terminal će zatražiti lozinku korisnika trenutne sesije.

Napomena: oblik gornje naredbe ovisi o trenutno stabilnoj verziji Maltego alata i može se mijenjati. Kako ne bi došlo do problema, najbolje je nakon što se u terminal upiše naredba sudo dpkg – i upisati prvih par slova preuzete datoteke i nakon toga pritisnuti tipku Tab na tipkovnici.

5. Nakon što je uspješno izvršen 4. korak, Maltego bi trebao biti instaliran na računalu. Alat se može pokrenuti odabirom opcije Activities u gornjem lijevom kutu ekrana i upisivanjem ključne riječi Maltego u tražilicu koja se nalazi na sredini ekrana.

Pri pokretanju Maltego alata, program će tražiti korisničko ime i lozinku. Ukoliko prije toga nije obavljena registracija, potrebno je otići na stranicu https://www.paterva.com/ i obaviti registraiciju.

Koraci pri registraciji u Paterva sustav:

1. Otvoriti stranicu https://www.paterva.com/ i na navigacijskoj traci kursorom miša prijeći preko opcije Community. Na padajućem izborniku odabrati opciju Register(Free).
2. Popuniti polja potrebna za registraciju i poslati zahtjev za registracijom.
3. Na danu e-adresu upisanu pri registraciji biti će poslan link za potvrdu registracije. Nakon klika na poveznicu, registracija će biti uspješno obavljena.

Nakon uspješne registracije u Paterva sustav, potrebno je unijeti odabrano korisničko ime i lozinku u Maltego i nastaviti sa daljnjim podešavanjem alata.

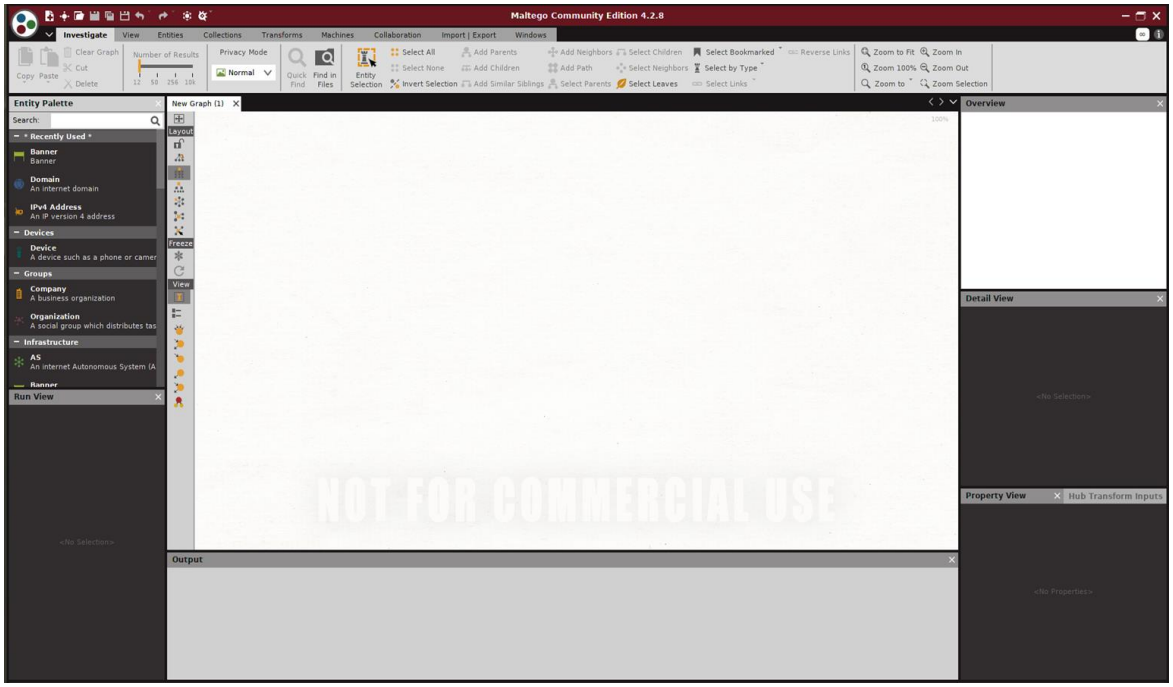
U sljedećem koraku postoji mogućnost odabira vrste instalacije Maltego alata. Moguće vrste su:

- Desktop inačica
  - Maltego Classic
  - Maltego XL
  - Maltego CE
- Server inačica
  - CTAS
  - ITDS
  - Comms.

U ovom primjeru odabran je Maltego CE zato što je besplatan za uporabu. Po završetku postavljanja alata otvoriti će se prazan prozor u kojem je moguće započeti stvaranje novog grafa.

5.2. Korištenje Maltego alata

Pri pokretanju Maltego alata uvijek se najprije otvori početna stranica. Ako u gornjem lijevom kutu odaberete opciju New, otvoriti će vam se novi prazan graf [50]. Prikaz sučelja alata Maltega dan je na slici 5.1.

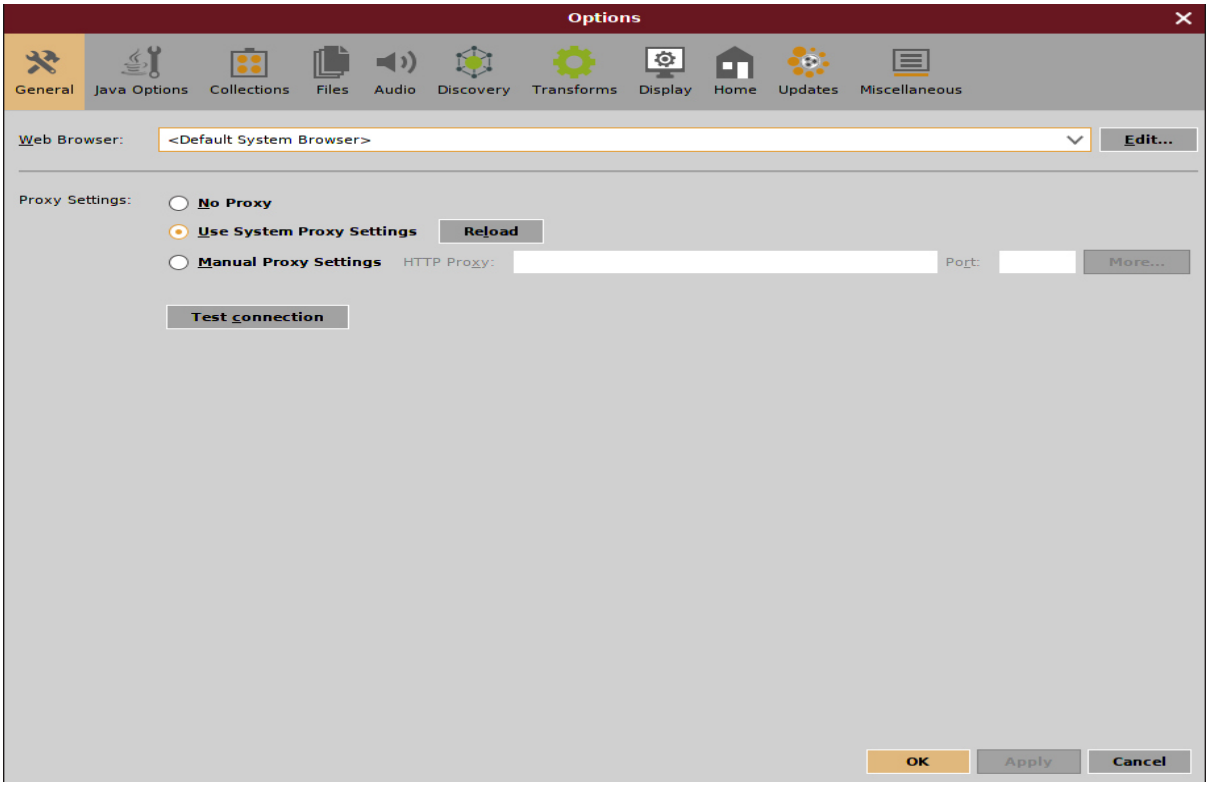


Slika 5.1: Početni prozor Maltega.

U gornjem lijevom kutu prozora nalazi se ikona sa logom Maltega. Lijevim klikom na logo otvara se padajući izbornik koji nudi opcije za stvaranje novog grafa, spremanje postojećeg grafa, uvoz i izvoz postavki alata, ispis grafa, pregled postojećih alata i podešavanje postavki [50].

Lijevim klikom na opciju Tools, otvara se padajući izbornik koji nudi nekoliko različitih opcija. Ovdje bih samo spomenula opciju Open Example Graph koja nudi mogućnost otvaranja primjera grafa koji pokazuje i spaja osnovne elemente Maltego alata, te opciju Open Logs Folder koja otvara direktorij u kojem se nalaze datoteke u koje se spremaju povratne poruke koje alat generira za vrijeme rada. Ovakve poruke su bitne kako bi se moglo ustanoviti zašto nešto ne radi i koje pogreške se događaju pri izvođenju [50].

Posljedjna opcija, Options služi za postavljanje osnovne konfiguracije Maltega. Lijevim klikom na tu opciju otvara se prozor kao na slici 5.2. [50].



Slika 5.2: Options prozor.

Pod opcijom Genral mogu se postaviti neka općenita svojstva Maltega poput internet preglednika u kojem će Maltego otvarati poveznice, te hoće li pri tome koristiti proxy server ili ne.

Od ostalih opcija zanimljive su opcije postavljanja Jave u kojima možete odabrati verziju Jave koju želite koristiti.

Desno od Applications Menu gumba nalaze se redom gumbi za :

- stvaranje novog grafa
- dijeljenje grafa
- otvaranje postojećeg grafa
- spremanje grafa
- poništavanje posljednje promjene
- ponovno vraćanje poništene promjene
- Transform hub
- Run Machine.

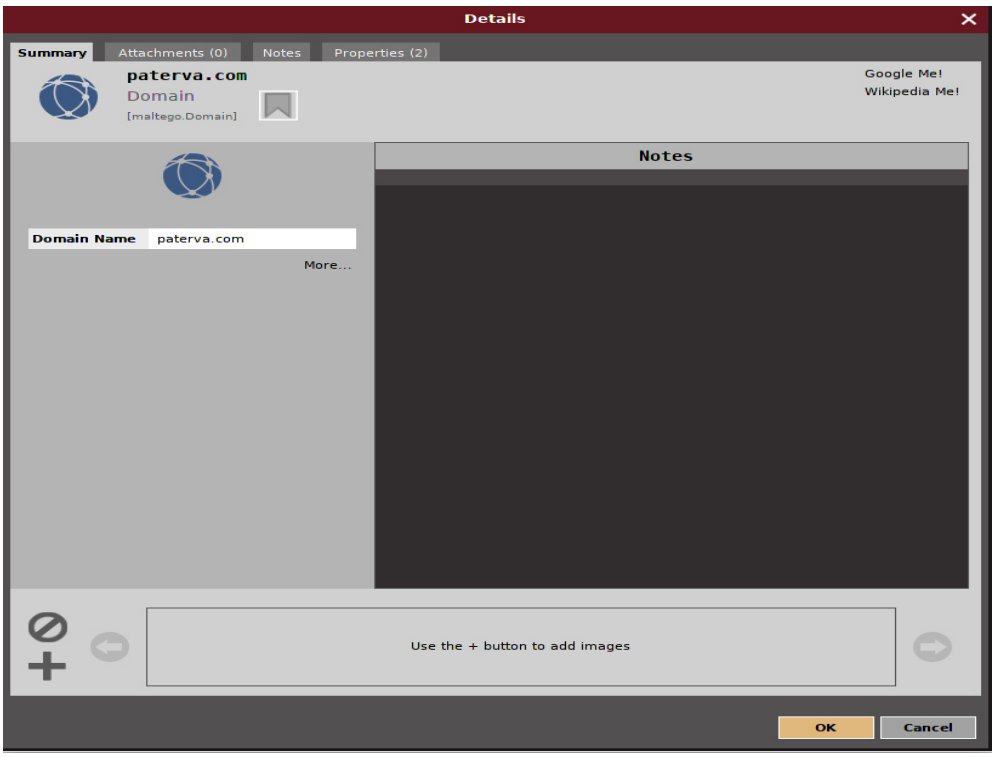
Ispod ove trake nalazi se alatna traka koja sadrži gumbe za uređivanje samog grafa. Ispod alatne trake, u lijevom dijelu ekrana nalazi se Entity Palette ili paleta entiteta. Ona sadrži predefinirane entitete koji se mogu koristiti pri izradi grafova. Entiteti su podijeljeni u nekoliko skupina [50]:

- uređaji (devices)

- grupe (groups)
- infrastruktura (infrastructure)
- lokacija (location)
- malware
- penetracijsko testiranje (penetration testing)
- osobno (personal)
- društvene mreže (social networks)

od kojih se najčešće koriste entiteti grupa Infrastruktura i Osobno. Također je moguće stvoriti vlastite entitete odabirom opcije Entities na alatnoj traci, te potom opcije New Entity Type. Entiteti se na graf mogu dodavati tako da se na paleti entiteta odabere entitet koji želite stvoriti, te ga se lijevim klikom odvuče na graf [50].

Dvostrukim klikom na stvoreni entitet otvara se prozor Details koji nudi mogućnosti podešavanja parametara tog entiteta. Taj je prozor prikazan na slici 5.3. U ovom primjeru stvoren je entitet domene. Unutar prozora Details pod karticom Summary može se mijenjati ime domene, mogu se dodavati bilješke o entitetu, te se mogu dodavati slike vezane uz odabrani entitet. U gornjem desnom kutu prozora nalaze se opcije Google Me! i Wikipedia me!. Klikom na svaku od tih opcija otvoriti će se internet preglednik sa rezultatima pretraživanja imena odabrane domene, odnosno wikipedia članak sa rezultatima pretrage [50].



Slika 5.3: Details prozor.

Odabirom kartice Attachments otvara se mogućnost dodavanja datoteka koje su vezane uz odabrani entitet, dok se odabirom kartice Notes otvara mogućnost dodavanja bilješki [50].

Ukoliko postoji bilješka za neki entitet, na grafu će se, pored ikone entiteta prikazati žuta ikonica papira kao na slici 5.4. Dvostrukim klikom na ikonu, prikazati će se oblačić sa bilješkom o tom entitetu.

Slika 5.4: Entitet i pripadajuća bilješka.

Desnim klikom na entitet otvara se prozor pod nazivom Run transformations koji nudi mogućnosti pokretanja različitih transformacija nad odabranim entitetom. Taj prozor prikazan je na slici 5.4. Transformacije su grupirane po sličnosti i svojstvima, a prikaz svih transformacija jedne grupe može se vidjeti tako da se lijevim klikom odabere neka grupa transformacija. Kliknete li zatim na strelicu koja se nalazi pored neke transformacije, ta će se transformacija i izvršiti [50].

Slika 5.5: Run Transformations prozor.

Osim izvršavanja transformacije, moguće je podešavati postavke transformacija i dodavanje transformacija u grupu Favourites. Lijevim klikom na dvostruku strelicu koja se nalazi pored određene grupe transformacija izvršava se opcija Run All, koja će izvršiti sve transformacije te grupe. Na dnu prozora Run transformations nalaze se gumbi za rad s entitetom. Gumbi omogućavaju redom [50]:

- kopiranje entiteta na novi graf
- brisanje entiteta
- promijenu tipa entiteta
- spajanje entiteta
- kopiranje entiteta
- izrezivanje entiteta
- pridjeljivanje datoteke entitetu
- slanje entiteta na danu URL adresu
- izvršavanje akcija Google Me! I Wikipedia Me!
- brisanje i ponovno učitavanje slika.

Ako se želi označiti više entieta odjednom, to se može učiniti držanjem tipke Shift i lijevim klikanjem na entitete koje želite označiti. Sve označene entitete može se skupa pomicati po grafu tako da se lijevim klikom klikne na entitet te ga se povuče u smjeru gdje ga se želi staviti [18].

Desno od palete entiteta nalazi se stupac u kojem se mogu odabrati različite načini prikaza grafa. Neke od vrsta prikaza grafa su [18]:

- prikaz bloka
- hijerarhijski prikaz
- kružni prikaz
- organski prikaz
- interaktivni organski prikaz.

Također je moguće promijeniti veličinu pojedinih entiteta. Neke od mogućnosti su:

- Ball Size by Diverse Descent – Veličina entiteta ovisi o broju nadolazećih veza u krug. Više veza znači veći entitet, ali ne vrednuju se podjednako veze koje imaju zajedničkog djeda i one koje nemaju. One koje nemaju se vrednuju više.
- Ball Size by Links (all) – Veličina entiteta ovisi o broju ulaznih i izlaznih veza. Više veza znači veći entitet.
- Ball Size by Links (incoming) – Veličina entiteta ovisi o broju ulaznih veza.

- *Ball Size by Links (outgoing)* – Veličina entiteta ovisi o broju izlaznih veza.
- *Ball Size by Rank* – Veličina entiteta ovisi o broju svih ulaznih i izlaznih veza, kao i o broju ulaznih i izlaznih veza susjednih čvorova.
- *Ball Size by Weight* –Veličina entiteta ovisi o njegovoj težini. Neke transformacije pridjeljuju težinu čvorovima, koja se onda koristi u ovom prikazu.

Gumb List View prikazuje graf u obliku liste, dok ga gumb Graph View vraća u oblik grafa [50].

6. Analiza zaglavlja elektroničkih poruka korištenjem alata Maltego

Poznavanjem strukture zaglavlja elektroničke poruke i pomnim čitanjem zaglavlja priloženog u privitku 1, iz zaglavlja elektroničke pošte izvučene su sljedeće informacije:

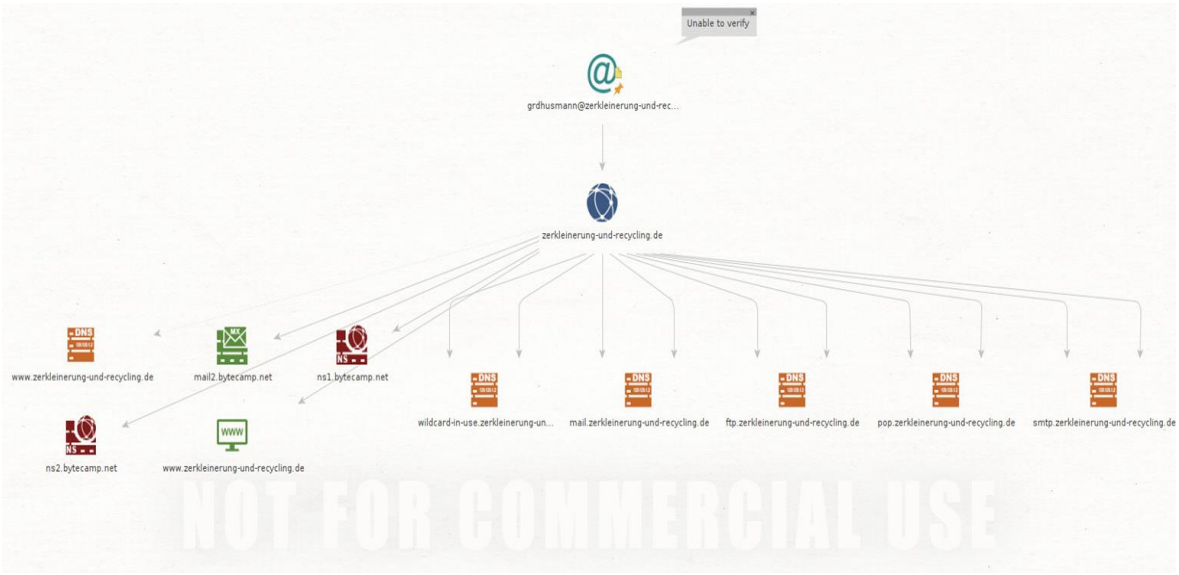
From	grdhusmann(@)zerkleinerung-und-recycling.de
Reply - To	president(@)cottinusa.com
Datum	Thu, 1 Aug 2019 04:09:20 -0500
User - Agent	SquirrelMail/1.5.2
Message-ID	0a5a5786780a580bd74b37463c04321b.squirrel(@)www.hksttc.com
MTA agenti kroz koje je poruka prošla	1. www.hksttc.com 2. busekusa 3. miura.websitewelcome.com 4. cm17.websitewelcome.com 5. gateway33.websitewelcome.com 6. stuttgart.optimus-hosting.com
IP adresa pošiljatelja	185.236.200.22
X-AntiAbuse: Sender Address Domain	zerkleinerung-und-recycling.de
X-Spam-Status	No, score=1.0
X-Spam-Score	10
X-Spam-Bar	+

Tablica 6.1: Prikaz informacija iz zaglavlja e-poruke. Napomena: u zapisu e-adresa, znak @ okružen je oblim zagradama kako ne bi predstavljao poveznicu. Stvarne e-adrese nemaju oble zagrade oko znaka @.

Zaglavlja elektroničke pošte pišu se odozdola prema gore, te ih se tim redom treba i analizirati. Najdonji dijelovi zaglavlja koji nisu dio X-zaglavlja poruke, sadrže informacije o pošiljatelju i primatelju. Prva stvar koju je moguće zapaziti pri analizi zaglavlja elektroničke poruke danoj u privitku 1, je da se adresa From razlikuje od adrese Reply-To, odnosno da pošiljatelj poruke šalje sa adrese grdhusmann(@)zerkleinerung-und-recycling.de, a prima ih na adresu president(@)cottinusa.com. Stvarne e-adrese nemaju oble zagrade oko znaka @. Ovdje i u daljnjem tekstu su korištene oble zagrade kako bi se spriječila interpretacija e-adrese kao poveznice. Adrese elektroničke pošte mogu se analizirati korištenjem Maltego alata tako da se u izborniku Entity Palette odabere entity Email Address. Nad stvorenim objektom e-adrese može se provesti niz transformacija koje pokušavaju pribaviti informacije o vlasniku te e-adrese. Maltego informacije pribavlja pretražujući javno dostupne informacije poput informacija na Internetu, te javno dostupnih servera. Maltego također može pretraživati i privatne izvore podataka uz nadoknadu, te može pretraživati i korisnikove lokalne podatke [53]. Primjerice, pri potvrđivanju da e-adresa postoji, Maltego koristi transformaciju *Verify email address exists.* Maltego najprije pronalazi nadležnog poslužitelja za tu e-adresu, te potom uspostavlja komunikaciju s njim [52]. Kao test, Maltego najprije od poslužitelja zatraži nepostojeću e-adresu [52]. Ukoliko poslužitelj ne vrati poruku o pogrešci, Maltego zaključuje da test nije prošao i vraća vrijednost Inconclusive. Inače, Maltego nastavlja s komunikacijom tražeći stvarnu e-adresu te vraća dobiveni rezultat [52]. Transformacije korištene nad ovim objektom su:

- *To Domain* – ova transformacija vraća domenu na kojoj je registrirana e-adresa. Transformacija će pretražiti Internet u potrazi za domenama sa sličnim nazivima, te će vratiti sve što je pronašla.
- *To Person* – ova transformacija vraća ime osobe kojoj e-adresa pripada.
- *Verify email address exists* – ova transformacija potvrđuje da e-adresa postoji.

Rezultati provedbe transformacija nad e-adresom grdhusmann(@)zerkleinerung-und-recycling.de dani su na slici 6.1.



Slika 6.1: Graf dobiven iz e-adrese grdhusmann(@)zerkleinerung-und-recycling.de

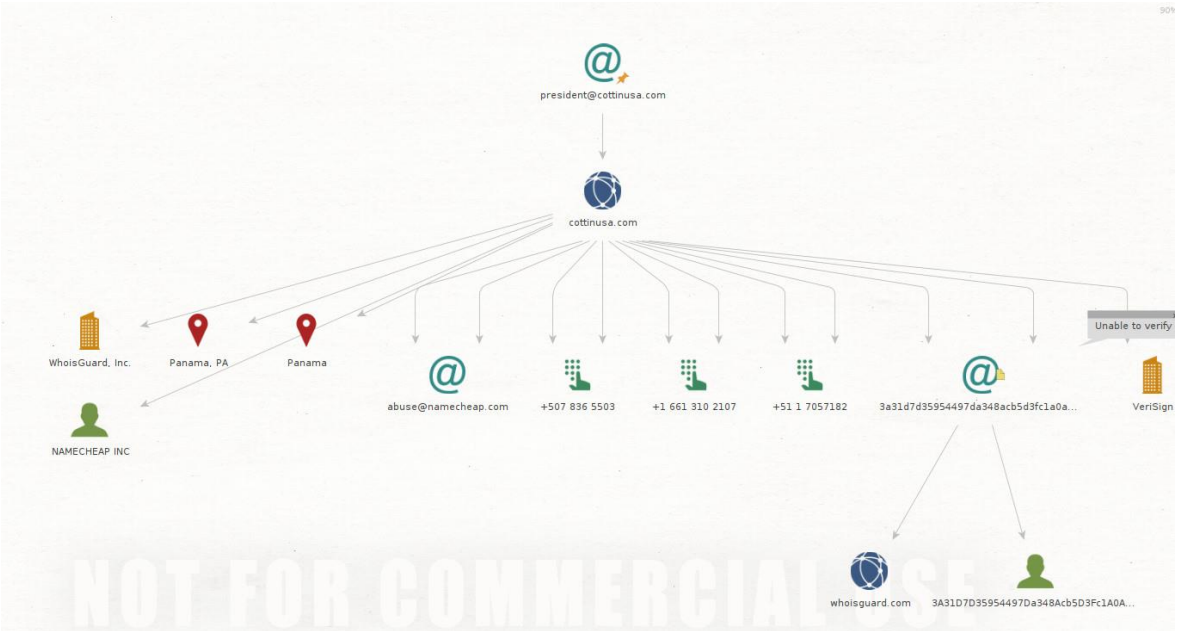
Transformacija *To Domain* vratila je kao rezultat domenu e-adrese zerkleinerung-und-recycling.de. Transformacija *To Person* nije uspjela pronaći podatke o imenu vlasnika adrese, a transformacija *Verify email address exists* uspjela je potvrditi da je domena valjana, ali nije mogla potvrditi valjanost ove adrese. Nakon analize adrese elektroničke pošte, analizira se pronađena domena vezana uz tu e-adresu. Nad domenom se može provesti nekoliko skupina transformacija:

- *DNS from Domain* – vraća informacije o DNS uređajima zaduženim za tu domenu
- *Domain Owner Detail* – vraća informacije o vlasniku domene
- *Email Address From Domain* – dohvaća adrese elektroničke pošte povezane sa tom domenom
- *Files and Documents From Domain* – dohvaća datoteke povezane sa tom domenom.

Najzanimljivija transformacija pri provedbi istrage elektroničke pošte je transformacija *Domain Owner Detail* koja pokušava pronaći informacije o vlasniku domene. Kao što je ranije spomenuto, podatci o vlasniku domene mogu se sakriti, što je u ovom primjeru i bio slučaj. Transformacija *Domain Owner Detail* nije vratila nikakve informacije. Transformacija *Email Address From Domain* može biti korisna ukoliko se uspiju pronaći druge e-adrese registrirane na tu domenu. U ovom slučaju i ta transformacija nije pronašla nikakve informacije. Transformacijom *DNS from Domain* vraćaju se DNS uređaji zaduženi za tu domenu. Oni se mogu vidjeti na slici kao objekti na kojima piše DNS. Podatci o DNS uređajima neke domene nemaju preveliku informacijsku

vrijednost. Ova transformacija također pronalazi i web stranice povezane sa traženom domenom. U ovom primjeru, transformacija *DNS from Domain* vratila je poveznicu na internetsku stranicu www.zerkleinerung-und-recycling.de. Internetska stranica je stvarna stranica tvrtke zerkleinerung-und-recycling, što nije iznenađuje obzirom da je domena pošiljateljeve adrese prethodno proglašena valjanom. Ovom posljednjom transformacijom iscrpljene su sve opcije u istraživanju e-adrese grdhusmann(@)zerkleinerung-und-recycling.de, te se istraga nastavlja istraživanjem e-adrese navedene u polju Reply-To.

Elektronička adresa navedena u polju Reply-To je president@cottinusa.com. U analizi ove e-adrese poduzeti su koraci identični koracima poduzetim u analizi e-adrese grdhusmann(@)zerkleinerung-und-recycling.de. Najprije je stvoren objekt Email Adress koji predstavlja e-adresu president(@)cottinusa.com, a zatim su nad tim objektom provedene transformacije. Iz e-adrese otkrivena je samo domena kojoj pripada ta e-adresa, te nije bilo moguće potvrditi valjanost te e-adrese. U sljedećem koraku nad pronađenom domenom provedene su iste transformacije kao i pri analizi e-adrese grdhusmann(@)zerkleinerung-und-recycling.de. Rezultat ovih transformacija dan je na slici 6.2.



Slika 6.2: Graf dobiven iz e-adrese president@cottinusa.com

Transformacije *Domain Owner Detail* vratile su informacije o akreditirajućem tijelu koje je izdalo tu domenu, NAMECHEAP INC, o lokaciji te tvrtke, te niz telefonskih brojeva koji nisu povezani sa samim vlasnikom domene, nego sa

tvrtkom NAMECHEAP INC.

Uz Maltego alat korištena je i naredba whois za analizu gore navedenih domena. Whois naredba nije pronašla nikakve nove informacije vezano uz domenu zerkleinerung-und-recycling.de, ali je pronašla informacije o vremenu nastanka domene cottinusa.com. Napadač je domenu zakupio u ožujku 2019. g., samo pet mjeseci prije napada.

Kao posljednji korak u analizi dostupnih podataka iz zaglavlja elektroničke pošte, obavljena je analiza IP adrese pošiljatelja što je prikazano na slici 6.3.

Slika 6.3: Graf dobiven iz IP adrese 185.236.200.22

Iako podatak o IP adresi napadača najčešće nema veliku informacijsku vrijednost, pomoću IP adrese korisnika može se odrediti u kojem se gradu osoba nalazila u trenutku slanja poruke. Maltego alat povezao je IP adresu sa Los Angelesom, gradom u SAD-u. Podatak o lokaciji može se dodatno potvrditi činjenicom da vrijeme pošiljatelja poruke prikazano u polju Date u privitku 1 kasni 5 sati za UCT vremenom, što upućuje na SAD. Na temelju ova dva podatka može se nagađati da se napadač u trenutku napada nalazio u SAD-u, ali to ne mora biti slučaj zato što se svi podatci vezani uz zaglavlja elektroničke pošte mogu lažirati.

Pretragom domena pošiljatelja i pošiljateljeve IP adrese, iscrpljeni su svi izvori informacija dostupni u ovom zaglavlju elektroničke pošte. Kao posljednji izvor informacija ostali su podatci o MTA agentima kroz koje je poruka prošla na putu od pošiljatelja do primatelja, no pristup tim podatcima zahtjeva koordinaciju sa nadležnim mrežnim administratorima. Ukoliko bi se provodio i ovaj dio istrage trebalo bi stupiti u kontakt sa nadležnim mrežnim administratorima, te od njih zatražiti pristup mrežnim uređajima i zapisima o traženim e-porukama. Ovaj dio analize e-poruka nije proveden u sklopu ove istrage.

7. Zaključak

Računalna forenzika je kompleksna grana forenzike koja se bavi istraživanjem računalnih napada. Phishing napadi i drugi napadi počinjeni elektroničkom poštom, samo su mali dio svih računalnih napada koji postoje. Pri analizi phishing napada od pojedinca se zahtjeva dubinsko znanje o različitim aspektima računalnih napada, od tehničkog do društvenog aspekta. Provođenje računalne forenzike nad elektroničkom poštom od istražitelja ponajprije zahtjeva da u potpunosti razumije mehanizme prijenosa elektroničke poruke, dijelove zaglavlja i njihov značaj, kao i dostupne tehnike i alate koji se koriste pri forenzici elektroničke pošte. Iz ovih razloga, veći dio ovog rada bazirao se na prikupljanju znanja potrebnih za razumijevanje napada počinjenih elektroničkom poštom.

Analizom zaglavlja elektroničke pošte dobivenih iz e-poruka prethodno opisanog phishing slučaja u Hrvatskoj, može se zaključiti da iako zaglavlja elektroničke pošte obiluju mnoštvom informacija, većina tih informacija i nije od neke koristi. One informacije koje jesu korisne najčešće su vrlo oskudne ili čak skrivene od strane napadača. Informacije poput IP adrese pošiljatelja nemaju veliku informacijsku vrijednost zbog dinamičkog načina dodjeljivanja IP adresa. Pomoću nečije IP adrese može se samo odrediti područje na kojem se osoba nalazila u trenutku slanja poruke, ali ne i točna lokacija. Također, IP adrese moguće ja lažirati korištenjem posebnih metoda kojima se umjesto korisnikove trenutne IP adrese prikazuje neka druga IP adresa. Na taj način čak ni podatak o lokaciji korisnika nije pouzdan, zato što se zamjenska IP adresa mogla nalaziti bilo gdje na svijetu. Pri analizi zaglavlja elektroničke pošte puno su zanimljivije informacije o domeni pošiljatelja. Pretraživanjem tih domena koristeći alate poput naredbi whois i nslookup ili alata Maltego može se otkriti niz korisnih informacija o napadaču. No, SMTP protokol dopušta postavljanje bilo koje adrese kao adrese pošiljatelja, te se na taj način može lažirati i sama e-adresa ili domena e-adrese [54]. Također, informacije o vlasniku neke domene i drugi detalji mogu se sakriti od strane vlasnika domene što znatno otežava istragu.

Istraga provedena u ovom radu nije uspjela pronaći dodatne informacije koje bi upućivale na identitet napadača. Iz zaglavlja e-poruka izvučene su informacije o e-adresi napadača i o e-adresi na koju je napadač primao odgovore. Ova prva e-adresa sadrži domenu stvarne tvrtke s kojom je tvrtka žrtva prethodno poslovala, koristeći Maltego alat nije bilo moguće potvrditi njenu ispravnost, dok se o ovoj drugoj e-adresi, kao ni o njenoj domeni ne zna mnogo. Jedino što je otkriveno je da je ta domena registrirana u ožujku 2019. godine, a da je nadležno tijelo kod kojeg je domena registrirana NAMECHEAP INC. Podatci o napadaču bili su oskudni, te su svi tragovi vodili u slijepe ulice.

Na kraju, nužno je napomenuti da phishing napade nije moguće u potpunosti spriječiti, ali pravilnom i pravovremenom edukacijom zaposlenika može se smanjiti vjerojatnost od phishing napada. Uvođenjem dvostruke verifikacije posao napadača znatno se otežava. Također, valja pripaziti na podatke objavljene na profilima na društvenim mrežama. Bit društvenih mreža je dijeljenje privatnog sadržaja poput slika i videa s putovanja, ali informacije poput adrese elektroničke pošte, broja mobitela, mjesta stanovanja i druge trebaju biti zaštićene i dostupne samo vlasniku profila.

Literatura

[1] *Facebook Reports Fourth Quarter and Full Year 2019 Results,* Menlo Park Calfironia siječanj 2020 [pristupljeno 02.02.2020.]

[2] United Nations Department of Economic and Social Affairs, *World population 2019* [pristupljeno 02.02.2020.]

[3] 5 Kinds of ID Theft Using a Social Security Number, https://www.lifelock.com/learn-identity-theft-resources-kinds-of-id-theft-using-social-security-number.html [pristupljeno 10.02.2020.]

[4] The history of cyber attacks – a timeline, https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm [pristupljeno 04.02.2020.]

[5] Common Types of Cybersecurity Attacks, https://www.rapid7.com/fundamentals/types-of-attacks/ [pristupljeno 04.02.2020.]

[6] Understanding Email protocols (POP, Imap, MAPI, EAS, Exhange), https://www.contactgenie.info/understanding-email-protocols-pop-imap-mapi-eas/ [pristupljeno 10.02.2020.]

[7] Email Protocols – POP3, SMTP, and IMAP Tutorial https://www.siteground.com/tutorials/email/protocols-pop3-smtp-imap/ [pristupljeno 24.01.2020.]

[8] SSL, TLS, and STARTTLS, https://www.fastmail.com/help/technical/ssltlsstarttls.html [pristupljeno 10.02.2020.]

[9] What Is Transport Layer Security (TLS)?, https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/ [pristupljeno 10.02.2020.]

[10] IMAP (Internet Message Access Protocol), https://www.tech-faq.com/imap.html [pristupljeno 05.02.2020.]

[11] The IMAP advantage, https://www.macworld.com/article/1051268/julymobilemac.html [pristupljeno 10.02.2020.]

[12] History of SMTP, www.circleid.com/posts/history_of_smtp/ [pristupljeno 10.02.2020.]

[13] Multipurpose Internet Mail Extension (MIME) Protocol, https://www.geeksforgeeks.org/multipurpose-internet-mail-extension-mime-protocol/ [pristupljeno 02.02.2020.]

[14] MAPI over HTTP in Exhange Server, https://docs.microsoft.com/en-us/exchange/clients/mapi-over-http/mapi-over-http?view=exchserver-2019 [pristupljeno 24.01.2020.]

[15] Exchange ActiveSync, https://docs.microsoft.com/en-us/exchange/clients/exchange-activesync/exchange-activesync?view=exchserver-2019 [pristupljeno 24.01.2020.]

[16] Overview of EAS vs. MAPI/EWS vs. IMAP, https://portal.smartertools.com/kb/a2731/overview-of-eas-vs_-mapi-ews-vs_-imap.aspx [pristupljeno 10.02.2020.]

[17] Difference between IMAP and MAPI protocol, http://www.differencebetween.info/difference-between-imap-and-mapi-protocol [pristupljeno 05.02.2020.]

[18] Exchange ActiveSync (EAS) vs IMAP Overview, https://account.negox.com/knowledgebase/372/Exchange-ActiveSync-EAS-vs-IMAP-Overview.html [pristupljeno 05.02.2020.]

[19] Mail Terminology, https://afreshcloud.com/sysadmin/mail-terminology-mta-mua-msa-mda-smtp-dkim-spf-dmarc [pristupljeno 24.01.2020.]

[20] What Is DNS | How DNS Works, https://www.cloudflare.com/learning/dns/what-is-dns/ [pristupljeno 10.02.2020.]

[21] A Guide to Viewing Full Email Headers in Gmail, https://www.lifewire.com/how-to-see-full-email-headers-in-gmail-1171960 [pristupljeno 02.02.2020.]

[22] How to Show Headers in Yahoo Mail, https://www.lifewire.com/see-headers-of-message-yahoo-1174546 [pristupljeno 02.02.2020.]

[23] How to View Full Message Headers in Outlook 2019/2016, https://www.technipages.com/outlook-view-message-headers [pristupljeno 10.02.2020.]

[24] What all the stuff in email headers means – and how to sniff out spoofing, https://arstechnica.com/information-technology/2019/08/ars-forensic-files-how-to-parse-through-e-mail-headers-and-spot-obfuscation/ [pristupljeno 24.01.2020.]

[25] How to Analyze Spam Email Headers, https://www.vircom.com/blog/how-to-analyze-spam-email-headers/ [pristupljeno 10.02.2020.]

[26] Multipurpose Internet Mail Extension (MIME) Protocol, https://www.geeksforgeeks.org/multipurpose-internet-mail-extension-mime-protocol/ [pristupljeno 10.02.2020.]

[27] Understanding S/MIME, https://docs.microsoft.com/en-us/previous-versions/tn-archive/aa995740(v=exchg.65) [pristupljeno 02.02.2020.]

[28] Public Key Cryptography and Digital Signatures, https://medium.com/coinmonks/a-laymans-explanation-of-public-key-cryptography-and-digital-signatures-1090d4bd072e [pristupljeno 10.02.2020.]

[29] Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, https://narodne-novine.nn.hr/clanci/sluzbeni/2017_06_62_1430.html [pristupljeno 10.02.2020.]

[30] Pravilnik o pružanju i korištenju usluga povjerenja, https://narodne-novine.nn.hr/clanci/sluzbeni/2019_06_60_1150.html [pristupljeno 10.02.2020.]

[31] Cryptography Hash functions, https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm [pristupljeno 10.02.2020.]

[32] What is Encryption | Types of Encryption, https://www.cloudflare.com/learning/ssl/what-is-encryption/ [pristupljeno 10.02.2020.]

[33] Phishing Attacks, https://www.imperva.com/learn/application-security/phishing-attack-scam/, [pristupljeno 24.01.2020.]

[34] What is phishig? How this cyber attack works and how to prevent it, https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html [pristupljeno 02.02.2020.]

[35] What is a Phishing attack?, https://www.cloudflare.com/learning/security/threats/phishing-attack/ [pristupljeno 10.02.2020.]

[36] Ne budite uhljeb iz Đakova, nemojte popušiti ove mailove, https://www.index.hr/vijesti/clanak/ne-budite-uhljeb-iz-djakova-nemojte-popusiti-ove-mailove/2025204.aspx [pristupljeno 02.02.2020.]

[37] The phishing email that hacked the account of John Podesta, https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/ [pristupljeno 02.02.2020.]

[38] History of Phishing, https://cofense.com/history-of-phishing/ [pristupljeno 10.02.2020.]

[39] The 5 most common types of phishing attacks, https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack [pristupljeno 10.02.2020.]

[40] What is ransomware and how to help prevent ransomware attacks, https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html [pristupljeno 10.02.2020.]

[41] I got a phishing email that tried to blackmail me – what should I do?, https://www.theguardian.com/technology/askjack/2019/jan/17/phishing-email-blackmail-sextortion-webcam [pristupljeno 10.02.2020.]

[42] Why Most Cyber Security Training Fails and What We Can Do About it, https://www.youtube.com/watch?v=3L3IrAN30a4 [pristupljeno 10.02.2020.]

[43] What is Two – Factor Authentication (2FA)?, https://authy.com/what-is-2fa/ [pristupljeno 10.02.2020.]

[44] What Is X – Spam – Status In Message Headers, https://kb.intermedia.net/article/1680 [pristupljeno 10.02.2020.]

[45] What Is Bayesian Spam Filtering?, https://www.lifewire.com/bayesian-spam filtering-1164096 [pristupljeno 10.02.2020.]

[46] Email Forensics: Investigation Techniques, https://articles.forensicfocus.com/2019/02/15/email-forensics-investigation-techniques/ [pristupljeno 24.01.2020.]

[47] M. Tariq Banday, *Techniques and Tools for Forensic Investigation of e-mail,* International Journal of Network Security & Its Applications studeni 2011 [pristupljeno 02.02.2020.]

[48] Kali Linux Tool Listing, https://tools.kali.org/tools-listing [pristupljeno 10.02.2020.]

[49] File '/etc/sudoers': Why do I need to use the sudo command if I am in the sudo group?, https://askubuntu.com/questions/977756/file-etc-sudoers-why-do-i need-to-use-the-sudo-command-if-i-am-in-the-sudo-g [pristupljeno 10.02.2020]

[50] Maltego Getting Started, https://docs.maltego.com/support/solutions/folders/15000003603/page/1?url_locale= [pristupljeno 24.01.2020.]

[51] Does all SMTP communication happen over 25?, https://stackoverflow.com/questions/664758/does-all-smtp-communication-happen-over-25 [pristupljeno 15.02.2020.]

[52] To Email Address [using Search Engine], https://docs.maltego.com/support/solutions/articles/15000019035-to-email-address-using-search-engine- [pristupljeno 15.02.2020.]

[53] Data at your fingeprints, https://www.maltego.com/transform-hub/ [pristupljeno 15.02.2020.]

[54] Faking email domain names, https://security.stackexchange.com/questions/107971/faking-email-domain-names [pristupljeno 15.02.2020.]

[55] What is X-header, https://www.symantec.com/connect/forums/what-x-header [pristupljeno 15.02.2020.]

Metode i alati za istraživanje napada društvenim inženjerstvom na internetu

Sažetak

Krajem kolovoza 2019. godine autorici ovog završnog rada prezentiran je slučaj spear phishing napada, te je tražena provedba računalne forenzike nad tim slučajem. Ovaj završni rad objedinjuje svo znanje stečeno pri provedbi računalne forenzike, kao i same rezultate analize napada. Napad se dogodio putem elektroničke poruke, te je napadač iza sebe ostavio niz zaglavlja elektroničke pošte. Svako zaglavlje e-poruke sadrži korisne informacije koje se mogu iskoristiti u analizi phishing napada. Prije provedbe analize bilo je potrebno prikupiti znanje o strukturi zaglavlja elektroničke pošte, kao i o mehanizmima prijenosa elektroničke pošte i protokolima koji se pri tome koriste. Zatim je bilo potrebno proučiti dostupne alate i metode analize e-poruka, te potom odabrati alate i metode koje će biti korišteni. U ovom završnom radu koristio se alat Maltego uz naredbe whois i nslookup. Odabirom alata i metoda analize završila je faza učenja o phishing napadima, te je započela faza provedbe analize opisanog napada. Sama analiza nije polučila velike rezultate zbog opreznosti napadača i oskudnosti dostupnih informacija.

Ključne riječi: Elektronička pošta, protokoli elektroničke pošte, phishing, spear phishing, zaglavlja elektroničke pošte.

Methods and tools for investigation of social engineering attacks on the internet

Abstract

At the end of the August 2019. the author of this final paper was presented with a case of spear phishing attack and was asked to perform computer forensics on it. This final paper combines knowledge gained during the computer forensics as well as the results obtained from the analysis. The attack occured via email leaving behind a series of email headers. Each email header contains valuable information that might be used in the analysis of this phishing attack. Before the analysis of the case it was needed to gain knowledge about email header structure as well as email transport mechanisms and used protocols. After acquiring this knowledge, it was necessary to gain knowledge of the tools and methods available to perform email analysis and to choose which tools and methods will be used. This final paper used Maltego tool along with whois and nslookup command. With the selection of tools and methods for analysis, the phase of learning about phishing attacks ended, and the phase of

carrying out the analysis of the described attack began. The analysis itself did not produce great results because of the cautiousness of the attackers and the scarcity of information available.

Key words: Email, email protocols, phishing, spear phishing, e-mail headers.

Privitak 1.
Primjer zaglavlja elektroničke poruke

```
Return-Path: <grdhusmann@zerkleinerung-und-recycling.de>
Delivered-To: zrtva1@prijevara.com
Received: from stuttgart.optimus-hosting.com                                    {2}
by stuttgart.optimus-hosting.com with LMTP
id kHF6FWysQl1nNRkAFnQO9A
(envelope-from <grdhusmann@zerkleinerung-und-recycling.de>)
for <zrtva1@prijevara.com>; Thu, 01 Aug 2019 11:10:04 +0200
Return-path: <grdhusmann@zerkleinerung-und-recycling.de>
Envelope-to: zrtva1@prijevara.com
Delivery-date: Thu, 01 Aug 2019 11:10:04 +0200
Received: from gateway33.websitewelcome.com ([192.185.146.21]:21119)
by stuttgart.optimus-hosting.com with esmtps (TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384:256)
(Exim 4.92)
(envelope-from <grdhusmann@zerkleinerung-und-recycling.de>)
id 1ht762-006vpd-VH
for zrtva1@prijevara.com; Thu, 01 Aug 2019 11:10:04 +0200
Received: from cm17.websitewelcome.com (cm17.websitewelcome.com [100.42.49.20])
by gateway33.websitewelcome.com (Postfix) with ESMTP id D4EEC51842
for <zrtva1@prijevara.com>; Thu,  1 Aug 2019 04:09:20 -0500 (CDT)
Received: from miura.websitewelcome.com ([192.185.83.207])
by cmsmtp with SMTP
id t75MhlbCJ90ont75MhcjZQ; Thu, 01 Aug 2019 04:09:20 -0500
X-Authority-Reason: nr=8
Received: from busekusa by miura.websitewelcome.com with local (Exim 4.92)
(envelope-from <grdhusmann@zerkleinerung-und-recycling.de>)
id 1ht75M-000j5Q-BP
for zrtva1@prijevara.com; Thu, 01 Aug 2019 04:09:20 -0500
Received: from 185.236.200.22 ([185.236.200.22])                  Prvi MTA u nizu
      (SquirrelMail authenticated user enquiry@busekusa.com)
      by www.hksttc.com with HTTP;
      Thu, 1 Aug 2019 04:09:20 -0500
Message-ID: <0a5a5786780a580bd74b37463c04321b.squirrel@www.hksttc.com>
Date: Thu, 1 Aug 2019 04:09:20 -0500                                            {1}
Subject: Hello
From: "Gerhard Husmann" <grdhusmann@zerkleinerung-und-recycling.de>
To: zrtva1@prijevara.com
Reply-To: "Gerhard Husmann" <president@cottinusa.com>
User-Agent: SquirrelMail/1.5.2 [SVN]
```

MIME-Version: 1.0 {4}
Content-Type: text/plain;charset=iso-8859-1
Content-Transfer-Encoding: 8bit

X-AntiAbuse: This header was added to track abuse, please include it with any abuse report {3}
X-AntiAbuse: Primary Hostname - miura.websitewelcome.com
X-AntiAbuse: Original Domain - prijevara.com
X-AntiAbuse: Originator/Caller UID/GID - [5804 32003] / [47 12]
X-AntiAbuse: Sender Address Domain - zerkleinerung-und-recycling.de
X-BWhitelist: no
X-Source-IP:
X-Source-L: No
X-Exim-ID: 1ht75M-000j5Q-BP
X-Source:
X-Source-Args:
X-Source-Dir: :/base/3rdparty/squirrelmail/src
X-Source-Sender:
X-Source-Auth: busekusa
X-Email-Count: 23
X-Source-Cap: YnVzZWt1c2E7b3NhaG9uO21pdXJhLndlYnNpdGV3ZWxjb21lLmNvbQ==
X-Local-Domain: no
X-Spam-Status: No, score=1.0
X-Spam-Score: 10
X-Spam-Bar: +
X-Ham-Report: Spam detection software, running on the system "stuttgart.optimus-hosting.com",
 has NOT identified this incoming email as spam. The original
 message has been attached to this so you can view it or label
 similar future email. If you have any questions, see
 root\@localhost for details.
 Content preview: Hello, Can we chat on email for a moment please? I have an
   obligation that I would like you to complete ASAP. Gerhard Husmann CEO/Managing
   Director Maschinen- und Landmaschinenfabrik Husmann GmbH Gerhard-Husmann-Straße
   2, 49762 Lathen, Germany.
 Content analysis details: (1.0 points, 5.0 required)
  pts rule name   description
 ---- ---------------------- --
 -0.0 SPF_HELO_PASS   SPF: HELO matches SPF record
  1.0 KAM_LAZY_DOMAIN_SECURITY Sending domain does not have any
                              anti-forgery methods
X-Spam-Flag: NO
X-BitdefenderWKS-SpamStamp: Build: [Engines: 2.15.9.1247, Stamp: 3],
 Multi: [Enabled, t: (0.000003,0.002110)], BW: [Enabled, t:
 (0.000006)], RTDA: [Enabled, t: (1.047828), Hit: No, Details: v2.7.48;
 Id: 17.1i631ps.1dh8j5qjn.ag4q], total: 0(775)
X-BitdefenderWKS-Spam: No - 0