Karakteristike zlonamjernog softvera kao sigurnosne prijetnje mobilnim uređajima

Prgomet, Mario

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Mario Prgomet

KARAKTERISTIKE ZLONAMJERNOG SOFTVERA KAO SIGURNOSNE PRIJETNJE MOBILNIM UREĐAJIMA

ZAVRŠNI RAD

Zagreb, 2017.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

KARAKTERISTIKE ZLONAMJERNOG SOFTVERA KAO SIGURNOSNE PRIJETNJE MOBILNIM UREĐAJIMA

CHARACTERISTICS OF MALWARE AS A SECURITY THREAT TO MOBILE DEVICES

Mentor: dr. sc. Siniša Husnjak

Student: Mario Prgomet
JMBAG: 0135237354

Zagreb, rujan 2017.

SAŽETAK

Zlonamjerni ili zloćudni softver programski je specijalizirano napravljen kod čija je svrha infiltracija u računalne sustave bez korisnikova pristanka. Najčešće čine štetu korisniku. Današnji su mobilni terminalni uređaji dostupni, sveprisutni, jednostavno se koriste i česta su meta zlonamjernog softvera koji mogu biti ozbiljna sigurnosna prijetnja. Brzo širenje i sve veća dostupnost tehnologija koja se koristi u svijetu mobilnih uređaja i komunikacija, povećava se mogućnost napada pa korisnici postaju meta hakera. Uz povećanje broja korisnika mobilnih uređaja povećava se uporaba usluga vezanih uz e-mail poštu, audio i video komunikaciju, internetsko bankarstvo itd. Sve te aplikacije podrazumijevaju stalnu povezanost sustava s mrežom, što povećava mogućnosti napada. Izazov je to za identifikaciju te kategorizaciju prijetnje kako bi se uspješno zaštitili uređaji i ublažila moguća šteta za krajnje korisnike. Kibernetički kriminal prati tehnološku evoluciju te konstantnim razvojem novih oblika napada i tehnika omogućava prodiranje i u složenije sustave. Tako se čine značajne štete, a pritom počinitelji često ne budu otkriveni. Kako bi se napadi prevenirali, krajnje je korisnike nužno stalno informirati o zlonamjernom softveru, opasnostima kojim je izložen korisnik i o mogućnostima zaštite.

KLJUČNE RIJEČI: zlonamjerni softver; mobilni uređaji; sigurnost; zaštita

SUMMARY

Malicious software is a specialized software program designed to infiltrate computer systems without user consent. Most commonly they are harming the user. Today’s mobile terminal devices are available, omnipresent, easy to use and are often a target of malicious software that can be a serious security threat. The rapid spread and the increasing availability of technology that is used in the world of mobile devices and communications, the possibility to be attacked is increased so users become a target for hackers. With the increasing number of users of mobile devices, their usage of e-mail, audio and video communications, Internet banking etc., is also increasing. All of these applications imply permanent network connectivity, which increases attack capabilities. It is the challenge for identification and threat categorization to successfully protect devices and mitigating possible damage for end users. A cybercrime accompanies technological evolution and the constant development of the new forms of attacks and techniques allows penetration into more complex systems. This is how significant damages are made, while perpetrators are not often disclosed. In order to prevent attacks, end users need to be constantly informed about the malicious software, the dangers to which the users is exposed and the possibilities of protection.

KEY WORDS: malware; mobile devices; security; protection

Sadržaj

1. Uvod

Razvoj tehnologije i informatičkih uređaja doveo je do naglog porasta korištenja mobilnih terminalnih uređaja. Mobilni terminalni uređaji napredovali su do razine osobnih računala s mnogobrojnim funkcijama i velikom količinom sadržanih podataka o samim korisnicima. Nove mogućnosti daju veću slobodu korištenja uređaja, a samim time pružaju veći horizont zlonamjernim aktivnostima. Upravo zlonamjerne aktivnosti korisnicima terminalnih uređaja predstavljaju veliku prijetnju te korisnici postaju žrtve, a da toga uopće nisu svjesni.

Obradom ove teme pruža se uvid u korištenje terminalnih uređaja i kakve su navike korisnika po tom pitanju te se konkretno obrađuju različitosti zlonamjernih prijetnji koje prijete korisnicima terminalnih uređaja.

Naslov završnog rada je *Karakteristike zlonamjernog softvera kao sigurnosne prijetnje mobilnim uređajima*, a cilj je detaljnije objasniti prijetnje mobilnim uređajima i principe njihove zaštite. Rad je podijeljen u šest cjelina:

1. Uvod
2. Korištenje terminalnih uređaja
3. Zlonamjerne prijetnje terminalnim uređajima
4. Tipovi i karakteristike zlonamjernog softvera terminalnih uređaja
5. Mogućnosti zaštite terminalnih uređaja
6. Zaključak

Poglavlje *Korištenje terminalnih uređaja* definira raznovrsnu prisutnost terminalnih uređaja i principe njihova korištenja u svakodnevnom životu koje su omogućene od strane usluga koje podržavaju.

Treće poglavlje govori o zlonamjernim prijetnjama s kojima se terminalni uređaji, a i korisnici susreću prilikom njihova korištenja te kroz koje se sve načine prijetnje ostvaruju.

U četvrtome poglavlju konkretno su spomenuti primjeri zlonamjernih prijetnji te je svaka prijetnja detaljnije objašnjena.

Peto poglavlje obrađuje važnu ulogu raznih mogućnosti zaštite terminalnih uređaja u svrhu sprječavanja pozitivnog ishoda zlonamjernih prijetnji.

2. Korištenje terminalnih uređaja

Od prve pojave na tržištu, sedamdesetih godina 20. stoljeća, mobilni se telekomunikacijski, a potom i terminalni uređaji, smatraju značajnijim izumima u povijesti čovječanstva. Zbog veličine i težine prvi su telekomunikacijski uređaji izgledali nezgrapno, bili su skupu i napajali su se iz neefikasnih i nezgrapnih baterija. U to vrijeme im je svrha bila da omoguće prijenos govora na veće udaljenosti bez korištenja fiksne linije. Međutim, tijekom godina napredak je tehnologije omogućio da mobilni uređaji postanu manji, praktičniji pa će u cijelom svijetu postati i najčešće korišteni elektronički uređaji.

U novije vrijeme, paralelno s pojavom Interneta, mobilni uređaji prerastaju u terminalne uređaje. S vremenom Internet preuzima važnu ulogu u čovjekovu privatnom i poslovnom životu, a mobilni terminalni uređaji doživljavaju preporod. Od komunikacijskih uređaja, čija je svrha uspostava poziva i prijenos govora na daljinu, prateći razvoj tehnologije i potrebe ljudi, oni prerastaju u informacijske uređaje. Moderni terminalni uređaji u pravilu su povezani s Internetom i obavljaju gotovo sve funkcije kao i stolna računala, ali s jednom značajnom karakteristikom - uklapanja u čovjekov ubrzani ritam života i svakodnevne aktivnosti, [1].

2.1. Raznolikost terminalnih uređaja

Sukladno istraživanjima i razvoju mobilnih terminalnih uređaja kroz godine, raznolikost koju obuhvaćaju dosta je opsežna i teško ih je sve precizno kategorizirati. Predstavljaju uređaje koji imaju veliku mogućnost primjene zbog raznih i različitih načina izvedbi. Razne vrste terminalnih uređaja prema [2] predstavljaju:

- mobilni terminalni uređaji
- ugrađeni terminalni uređaji
- nosivi terminalni uređaji
- računala (stolna, prijenosna, tablet)
- igraće konzole
- ostali terminalni uređaji

Glavna okosnica mobilnih terminalnih uređaja upravo su bili tradicionalni terminalni mobilni uređaji. U sve naprednijem tehnološkom svijetu, pojava pametnih mobilnih uređaja odnosno *smarthphonea* predstavila je veliki korak u ovome području. Pametni telefoni su poprimili karakteristike slične računalima (napredne hardverske i softverske mogućnosti), ali u znatno manjim dimenzijama, dovoljno malim da ih možemo nositi u džepovima. Proširili su mogućnosti koje su nam dolazile u sklopu tradicionalnih mobilnih terminalnih uređaja (od glasovnih poziva, tekstualnih i glasovnih poruka do pretraživanja Interneta, slanja e-mail poruka, online trgovine itd.), imaju vlastiti operativni sustav i podržane aplikacije te su omogućili korisnicima stalan pristup Internetu, a značajna karakteristika im je bio zaslon osjetljiv na dodir i različite rezolucije ekrana.

Ugrađeni terminalni uređaji predstavljaju uređaje specifične namjene koji su ukomponirani kao komponenta nekog većega proizvoda i ostvaruju svoju zadanu funkciju. Primjer ugrađenih uređaja bili bi uređaji ugrađeni u automobilima, plovilima itd. (navigacijski uređaj/sustav, sustav dijagnostike i upozorenja, napredni sustav senzora zračnih jastuka itd.).

Nosivi terminalni uređaji (engl. *wearables*) je skup elektroničkih elemenata koji se povezuju u jednu cjelinu, uglavnom s pametnim telefonima, putem internetske veze ili *Bluetooth* tehnologije te je opremljena senzorima koji pomažu korisnicima u raznim aktivnostima ili poslovnoj organizaciji. Kao što sam naziv govori, nosivi uređaj je naprava koju nosite na sebi. Primjeri ovakvih uređaja su: fitnes narukvice, pametni satovi, nakit i odjeća, [3].

Osobna računala dijelimo na stolna i prijenosna računala. Stolno računalo vezano je za jednu lokaciju i stacionarno je, kao i komponente koje ga sačinjavaju, dok prijenosna računala (*notebook* ili *laptop*) imaju mogućnost promjene lokacije i manjih su dimenzija nego stolna računala s jednakim karakteristikama, međutim ovise o trajanju baterije koja im omogućuje mobilnost. Daljnjim razvojem stvorena su *netbook* računala i tablet uređaji. *Netbook* računala su slična prijenosnim računalima, ali manjih su dimenzija i skromnijih performansi. Tablet uređaji su kombinacija računala i mobilnog uređaja koji imaju zaslon osjetljiv na dodir. Prijenosni su uređaji, slični laptopu, ali pružaju drugačije iskustvo korisniku. Pokreću aplikacije koje su dizajnirane posebno za te uređaje te dolaze u raznim veličinama.

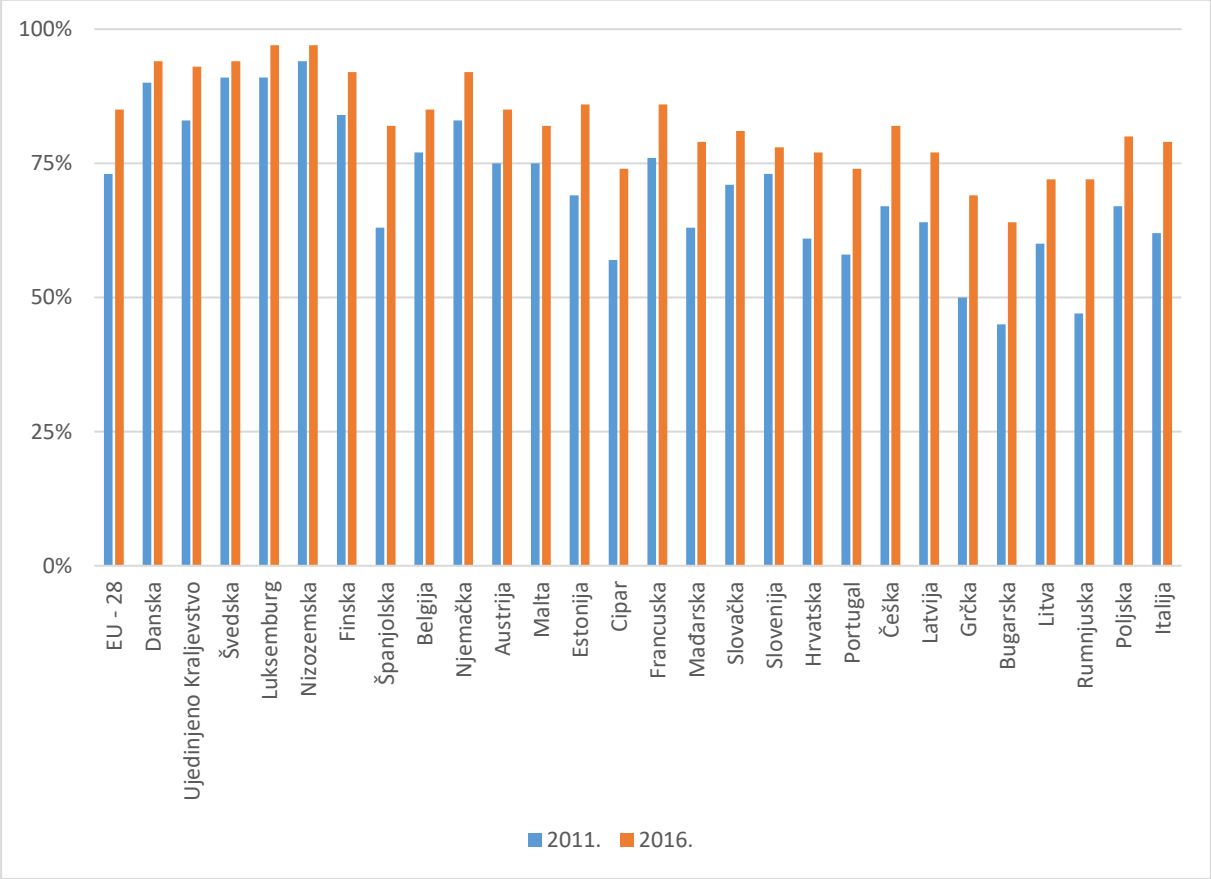
Igraće konzole su vrsta terminalnih uređaja namijenjenih za igranje zabavnih igara te omogućuju spajanje na Internet. Također postoje i mobilne igraće konzole, koje su manji mobilni terminalni uređaji sa svim komponentama za mogućnost igranja zabavnih igara, [2].

2.2. Trendovi korištenja

Mogućnošću većega izbora mobilnih terminalnih uređaja i njihovim napretkom, potreba ljudi za upotrebom istih se mijenjala i u konstantnom je porastu. Kroz godine su se mijenjale potrebe ljudi te su se terminalni uređaji prilagođavali upravo prema korisnicima. Danas je apsolutno sigurno da je terminalnim uređajima prijeko potreban pristup Internetu. Mobilni terminalni uređaji imaju ulogu olakšavanja života korisnika odnosno uklapanje u njihove svakodnevne aktivnosti te su od iznimne je važnosti u životu ljudi.

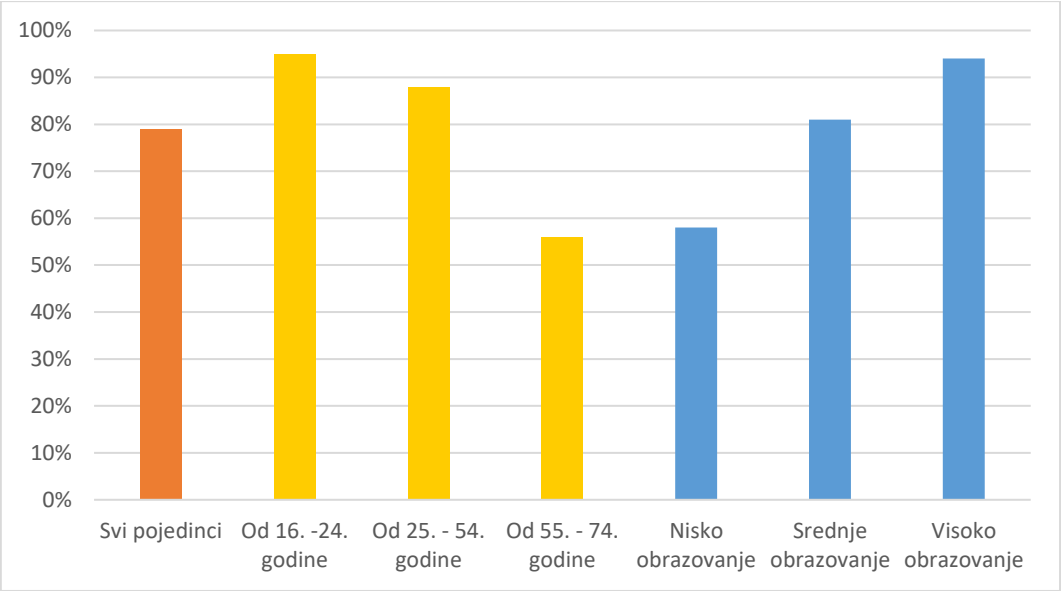
U današnje vrijeme mobilni uređaji dio su svakodnevnog života, korisni u poslovnim funkcijama kao radno sredstvo te u slobodno vrijeme. Valja napomenuti kako su mobilni uređaji postali prvenstveno alati za osnovne informacije i potrebe kao što su informacije o vremenu, postavljanje budilice i snimanje fotografija čime su zamijenili tradicionalne predmete poput satova i budilica, a to ilustrira koliko su nam mobilni uređaji značajni, [4].

Kao što je ranije spomenuta uloga Interneta, podaci koji govore o udjelu pojedinaca koji putem mobilnih uređaja pristupaju Internetu u zadnjih nekoliko godina doživio je značajan rast. Na grafikonu 1, konkretno je prikazan rast koji se odnosi na Europsku Uniju i njezinih 28 članica koje su bile obuhvaćene istraživanjem od strane Eurostata. U razdoblju od pet godina, mobilni uređaji pokazali su kao važno sredstvo prilikom pristupanja Internetu, a u idućim godinama koje dolaze očekuje se i dalje rast ovakvoga trenda, [5].



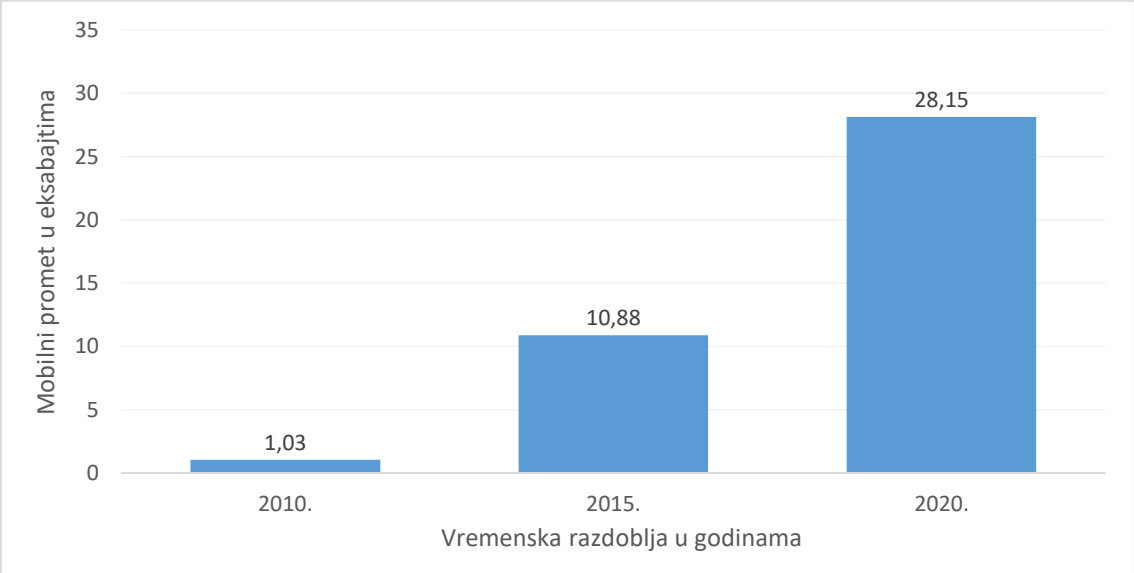
Grafikon 1. Pojedinci koji su koristili prijenosna računala ili mobilne uređaje za pristup Internetu 2011. i 2016. godine (% pojedinaca u dobi od 16 do 74 godine)
Izvor: [5]

Na trend korištenja mobilnih terminalnih uređaja, utjecaj ima i dobna skupine korisnika te razina formalnog obrazovanja, što je prikazano na grafikonu 2. Ukupan postotak ljudi koji koristi mobilne uređaje, prema podacima koji su bazirani na Europsku Uniju, doseže skoro 80 posto stanovništva. Najaktivniji, što se dobne skupine tiče, su korisnici između 16. i 24. godine. Takav podatak može se povezati i s razinom edukacije jer u tu dobnu skupinu spadaju tinejdžeri i studenti koji zbog svojih obrazovnih potreba upravo najviše koriste Internet. Niža edukacija, kao i što se više ide prema starijoj životnoj dobi, pokazuje manji interes i samim time manji prosjek prilikom korištenja Interneta putem mobilnih uređaja, [5].



Grafikon 2. Postotak pojedinaca koji su u prosjeku koristili Internet barem jednom tjedno, po dobnoj skupini i razini formalnog obrazovanja u 2016. godini
Izvor: [5]

Podatkovni promet koji mobilni terminalni uređaji ostvare prilikom spajanja na Internet, mobilni promet, kao i ostale karakteristike, poprimio je trend rasta. Prema [6], početkom 2017. godine, mobilni promet zauzimao je 50 posto ukupnog internetskog prometa. Primjerice, u Europi je tijekom 2010. godine izmjeren mobilni promet od 1,03 eksabajta te se predviđa značajan rast istoga godišnjeg prometa do vrijednosti oko 28,15 eksabajta u 2020. godini. Taj znakoviti skok prikazan je u grafikonu 3, [7]. Predviđa da će globalni mobilni mjesečni podatkovni promet porasti s vrijednosti od sedam eksabajta (koliko je izmjereno 2016. godine) na 49 eksabajta koliko se očekuje 2021. godine, [8].



Grafikon 3. Godišnji mobilni promet u Europi od 2010. do 2020. godine
Izvor: [7]

Sukladno rastu cjelokupnog prometa vezanog uz mobilne terminalne uređaje, rasti će i broj mobilnih uređaja kojima se koriste korisnici. Razlozi generiranja tolikog prometa leže u aplikacijama instaliranim na mobilnim uređajima, ali i različitim omogućenim uslugama za koje su mobilni terminalni predviđeni. U sljedećem odlomku, obradit će se neke usluge koje su omogućene terminalnim uređajima.

2.3. Usluge omogućene terminalnim uređajima

Velikom raznovrsnošću terminalnih uređaja, gotovo svi su pronašli svoju svrhu i implementirani su u čovjekov svakodnevni život. Danas, zahvaljujući tehnologiji, gotovo svi imaju jednake mogućnosti, ali se razlikuju po osobnim karakteristikama i veličini u kojima ih nalazimo na globalnom tržištu.

Danas su velika „pošast“ pametni mobilni terminalni uređaji. Oni sa svojim mogućnostima, koje su proširene u velikom pogledu naspram klasičnih mobilnih terminalnih uređaja, imaju vlastiti operativni sustav, sadržavaju velik broj razno raznih aplikacija i omogućuju prijenos podataka. Zbog pristupačne veličine većina ljudi ih nosi u svojim džepovima. Pametni telefoni se koriste za pristupanje društvenim mrežama (npr. Facebook), korištenje kamere u svrhu stvaranja fotografija i videa, razni načini komunikacijskih tehnologija, koriste NFC (engl. *Near Field Communication*) tehnologiju za beskontaktno plaćanje, razne usluge m-bankarstva, pohrana kontakata, razni korisnički računi koji su međusobno povezani na sam uređaj i razne druge opcije. Prethodno navedenim pruža se velika mogućnost korisniku za korištenjem raznovrsnih usluga, ali i time što se sve to nalazi na jednome uređaju predstavlja primamljivu metu trećim stranama ili hakerima da se domognu nečijih podataka i na taj način ugroze i kompromitiraju korisnika.

U današnje vrijeme terminalni uređaji postali su stvarnost oko nas. Postoje naznake da će okvirno kroz nekoliko desetaka godina IoT (engl. *Internet of Things*) biti implementiran u svako kućanstvo, a samim time biti i povezano na mrežu i omogućit će upravljanje raznim stvarima putem jednog mobilnog terminalnog uređaja. Osim toga, svjedoci smo ugrađivanja terminalnih uređaja u automobile, plovila i sl., ali nismo svjesni kakve nam to prijetnje može predstavljati. Kada realno sagledamo sliku u kojem smjeru se tehnologija razvija i da se nalazi svuda oko nas postavlja se pitanje sigurnosti korisnika.

3. Zlonamjerne prijetnje terminalnim uređajima

Sukladno razvoju tehnologije, svake godine bilježi se porast broja napada na korisnike terminalnih uređaja. Načini i oblici prijetnji sve su brojniji i bilježe kontinuiran rast, čija je svrha što veći broj zaraženih uređaja i teže otkrivanje, a samim time i uklanjanje. Korisnici olako shvaćaju terminalne uređaje i ne pridaju veliku pozornost opasnostima koje ih mogu zadesiti, s obzirom na to da se unutar terminalnih uređaja nalaze velike količine osobnih podataka koje mogu biti lako zloupotrijebljene.

3.1. Identificiranje prijetnji

Identificiranje prijetnji, važan je korak koji je iznimno bitan u cilju uklanjanja prijetnji te mora biti proveden da bi se donijela ispravna odluka o daljnjim koracima. Identificiraju se prijetnje koje mogu utjecati na uređaj, njegov sustav i ugroziti resurse. Za klasificiranje prijetnji, prema [9] mogu se koristiti dva temeljna pristupa:

- STRIDE – pristup temeljen na cilju kod kojega se razmatraju ciljevi napadača
- kategorizirani popisi prijetnji – kod ovoga pristupa započinje se od popisa učestalih prijetnji svrstanih u mrežnu, domaćinsku i aplikacijsku kategoriju

3.1.2. STRIDE

STRIDE je klasifikacijska shema za karakteriziranje poznatih prijetnji prema vrsti iskorištavanja za koju se koriste ili prema motivaciji napadača. STRIDE predstavlja akronim sastavljen od prvih slova svake od šest kategorija prijetnji prema [9]:

- ***S****poofing identity* – pretvaranje identiteta
- ***T****ampering* – uplitanje
- ***R****epudiation* – odbijanje
- ***I****nformation disclosure* – povreda informacija
- ***D****enial of Service* – uskraćivanje usluga
- ***E****levation of privilege* – podizanje prava

Pretvaranje identiteta (engl. *Spoofing identity*) je pokušaj pristupa sustavu pomoću lažnog identiteta. To je ključan rizik za aplikacije koje imaju mnogo korisnika, a osiguravaju jedan kontekst izvođenja na aplikacijskoj razini i razini baze podataka.

Uplitanje (engl. *Tampering*) znači neovlaštena promjena podataka. Postoji mogućnost da korisnici promijene primljene podatke te ih tako izmijenjene vrate natrag. Aplikacija ne bi smjela korisniku slati podatke koji se mogu dobiti samo unutar nje same. Isto tako, aplikacija bi trebala pažljivo provjeriti podatke primljene od korisnika te provjeriti njihovu valjanost i primjenjivost prije njihovog korištenja ili pohranjivanja.

Odbijanje (engl. *Repudiation*) karakterizira kada korisnik može osporiti transakcije s nedovoljnim revizijama i pohranama aktivnosti. Stoga je potrebno razmotriti zahtijeva li aplikacija neodbijajuće nadzore poput zapisa o web pristupu ili zapisa o pristupu i korištenju sustava.

Povreda informacija (engl. *Information disclosure*) predstavlja neželjeno čitanje privatnih podataka. Aplikacija mora uključivati strogi nadzor kako bi spriječila mijenjanje i zlouporabu korisničkih identifikacijskih oznaka, posebice ako koristi jedan kontekst za izvođenje cijele aplikacije. Jednako tako, valja imati na umu da internetski preglednici mogu biti izvori „curenja“ informacija, stoga je potrebno količinu informacija pohranjenu web preglednikom svesti na najmanju moguću.

Uskraćivanje usluga (engl. *Denial of Service*) je djelovanje onemogućavanjem usluge. Kako bi se pokušalo izbjeći ovu vrstu napada potrebno je korištenje skupih resursa omogućiti isključivo autentificiranim i autoriziranim korisnicima, a onemogućiti anonimnim korisnicima. Za aplikacije za koje ovo nije moguće postići, potrebno je svaki njezin aspekt najviše pojednostaviti kako bi se spriječili jednostavniji DoS napadi.

Podizanje prava (engl. *Elevation of privilege*) predstavlja se kao način kada korisnik s manjim pravima preuzima identitet privilegiranijeg korisnika. Potrebno je sve akcije ograditi pomoću autorizacijske matrice, kako bi se osiguralo da samo korisnik s dopuštenim pravima može pristupiti privilegiranoj funkcionalnosti.

3.1.2. Kategorizacija prijetnji

Unutar ovoga pristupa, prema [9] potrebno je izvršavanje sljedeća tri zadataka:

- identificirati mrežne prijetnje (engl. *network threats*) – zadatak za mrežne dizajnere i administratore. Najznačajnije mrežne prijetnje koje treba razmotriti u fazi dizajna uključuju:
    - korištenje sigurnosnih mehanizama koji se oslanjaju na IP (engl. *Internet Protocol*) adresu pošiljatelja (relativno je jednostavno poslati IP pakete s lažnom IP adresom izvora)
    - prosljeđivanje identifikatora sjednice ili kolačića (engl. *cookies*) preko nešifriranih mrežnih kanala (što može dovesti do krađe IP sjednice)
    - prosljeđivanje tekstualnih akreditacijskih uvjerenja ili ostalih osjetljivih podataka preko nešifriranog komunikacijskog kanala (što može omogućiti napadaču da nadzire mrežu, dobije podatke o logiranju i ostale osjetljive podatke)
- identificirati domaćinske prijetnje (engl. *host threats*) – koristi se pristup podjele konfiguracije u odvojene kategorije. Glavne ranjivosti koje ovdje treba uzeti u obzir su:
    - održavanje „nezakrpanih“ (engl. *unpatched*) poslužitelja koji mogu biti izloženi zlonamjernim programima
    - korištenje vrata (engl. *ports*), protokola i usluga koje nisu nužne
    - dozvoljavanje anonimnog neovlaštenog pristupa
    - korištenje slabe politike zaporki i računa
- identificirati aplikacijske prijetnje (engl. *application threats*) – razmatraju se svi aspekti sigurnosnog profila aplikacije. Naglasak je na aplikacijskim prijetnjama, prijetnjama svojstvenim za pojedine tehnologije i prijetnjama koda. Neke od glavnih ranjivosti koje ovdje treba razmotriti su:

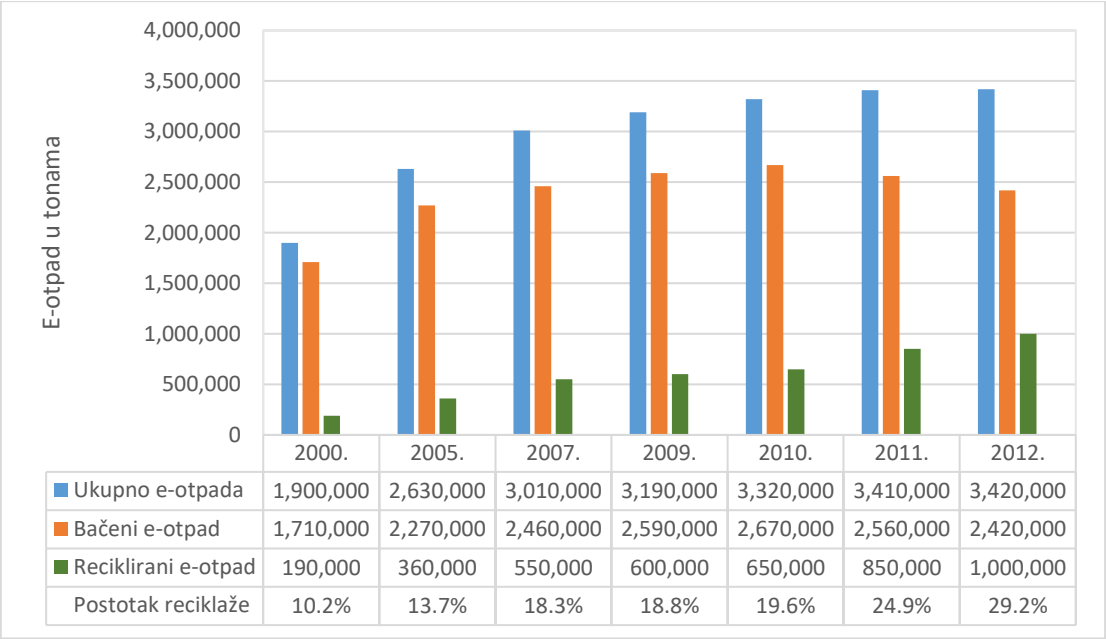
- korištenje slabe provjere valjanosti ulaznih podataka, koja vodi do više vrsta napada (napad umetanjem SQL koda, napad prepunjenjem spremnika)
- prijenos autentikacijskih uvjerenja ili kolačića preko nekriptiranih mrežnih poveznica, što može dovesti do krađe podataka
- korištenje slabe politike zaporki i računa što može dovesti do neovlaštenih pristupa
- pohranjivanje konfiguracijskih tajni u otvorenom, nešifriranom tekstu
- korištenje nesigurnog rukovanja iznimkama, koje može dovesti DoS napada te otkrivanja detalja o sustavu koji mogu biti korisni napadaču
- korištenje slabe i nedovoljnog šifriranja te nedovoljna zaštita kriptirajućih ključeva

3.2. Fizički zasnovane prijetnje

Fizički zasnovane prijetnje predstavljaju načine koji prijete korisnicima putem gubitka ili krađe mobilnih uređaja. Prva navedena prijetnja izrazito je interesantna napadačima zbog relativno malih dimenzija uređaja i to što se uvijek nalaze uz korisnika, [10].

Krađe predstavljaju namjerne napade na pojedinca ili sustave koji imaju pristup osjetljivim podacima te mogu uzrokovati puno veće štete od same krađe uređaja. Kradljivci uređaja uglavnom žele zaraditi novac na uređaja ili ako uspiju otkriti korisničke podatke, upravo će im oni donijeti još veću profitabilnost. Gubitak uređaja predstavlja nepažljivost od strane korisnika i moguće je nehotično otkrivanje korisničkih podataka, [11]. Jedna od solucija da se zaštite podaci na ukradenom uređaju je korištenje zaključavanja uređaja pomoću lozinki ili uzoraka na ekranu, čime će se onemogućiti pristup uređaju, a samim time i korisničkim podacima i svemu što se nalazi na uređaju.

Druga prijetnja su napadi na uređaje namijenjenih recikliranju, [10]. Statistika reciklaže, prema [12], zabilježila je značajan rast u promatranom razdoblju od 2000. godine do 2012. godine, kao što prikazuje grafikon 4. U slučaju neispravnog rukovanja uređajima za recikliranje i neovlaštenog pristupa određenim dijelovima uređaja moguće je dobiti podatke određenim akcijama, a da korisnici toga nisu svjesni.



	2000.	2005.	2007.	2009.	2010.	2011.	2012.
Ukupno e-otpada	1,900,000	2,630,000	3,010,000	3,190,000	3,320,000	3,410,000	3,420,000
Bačeni e-otpad	1,710,000	2,270,000	2,460,000	2,590,000	2,670,000	2,560,000	2,420,000
Reciklirani e-otpad	190,000	360,000	550,000	600,000	650,000	850,000	1,000,000
Postotak reciklaže	10.2%	13.7%	18.3%	18.8%	19.6%	24.9%	29.2%

Grafikon 4. Udio e-otpada i njegove reciklaže u razdoblju od 2000. godine do 2012. godine
Izvor: [12]

3.3. Aplikacijski zasnovane prijetnje

U aplikacijski zasnovane prijetnje spada zlonamjerni softver odnosno tzv. *malware*. Zlonamjerni softver predstavlja zajednički naziv za softver koji je izrađen s namjenom u kojoj se specifično cilja na oštećenja sustava i uređaja, [13]. Detaljnijom obradom raznih vrsta zlonamjernog softvera doprinijet će pobližem pojašnjenju njihove uloge. Različite vrste koje su u daljnjem tekstu obrađene su: virus, crv i trojanski napad.

Sljedeći oblici zlonamjernih aplikacija se prema [14] mogu protumačiti kao vrste zlonamjernog softvera:

- *spyware* – neovlašteno praćenje korisničkih aktivnosti te prosljeđivanje informacija i podataka trećoj strani
- *rootkit* – prikrivanje aktivnosti modifikacijom sustava
- *keylogger* – neovlašteno očitavanje i bilježenje unosa s tipkovnice uređaja

3.3.1. Virus

Virus je samoumnažajući program kojemu je glavni cilj promijeniti način rada uređaja, bez znanja i dopuštenja korisnika. Pokrenuti virus nastoji inficirati određene datoteke u svrhu širenja i na ostale uređaje koji su povezani u mreži. Inficiranje datoteke je proces u kojem virus nastoji uklopiti programski kod unutar legitimne datoteke na disku. Prilikom otvaranja legitimne datoteke, neprimjetno će se aktivirati i sam virus koji je ranije pokrenut prilikom učitavanja inficirane datoteke u memoriji uređaja. Moć virusa može varirati, od jednostavnih poruka na zaslonu uređaja do brisanja podataka ili onesposobljavanja mreže, [13].

3.3.2. Crv

U početku su napravljeni u znanstvene svrhe da bi se kasnije iskoristili u svrhu ilegalnih aktivnost. Kao i virusi imaju sposobnost samoumnažanja, ali im za širenje nisu potrebni drugi izvršni programi i ostali materijali, već se šire sami. Najčešće su oblikovani tako da iskorištavaju nedostatke u sigurnosti pri prijenosu podataka pa se koriste resursima mreže kako bi napravili kopije koje potom odašilju dalje bez ikakve intervencije zbog kojeg blokiraju ostali promet i djeluju na cjelokupnu mrežu. Razlikuju se od virusa zbog toga što virusi napadaju samo jedan uređaj. Povezuje ga se s napadima na poslovne mreže, a uzrokuje velike troškove održavanja mreža, [13].

3.3.3. Trojanski napad

Trojanski napadi su vrste zlonamjernog programa koji su maskirani kao legitimni programi ili je njihov programski kod ugrađen unutar legitimnih programa. Bezopasnim izgledom zavaravaju korisnika, no kada se pokrenu opasnost im je velika. Ime su preuzeli iz grčke mitologije točnije iz legende o Troji. Prema [13] dijelimo ih na dva osnovna tip:

- legitimni programi u kojemu se nalazi zloćudan programski kod kojeg je haker ubacio i on se izvršava za vrijeme uporabe programa
- poseban program koji odaje dojam da služi nečemu korisnom u svrhu zavaravanja korisnika

Trojanski napadi se kao takvi ne mogu izvršavati samostalno, nego to ovisi o postupcima korisnika koji koristi zaraženi terminalni uređaj. Neke od šteta nanesenih od strane ovoga virusa su: omogućuju udaljeni pristup uređaju, šalju podatke, uništavaju datoteke i resurse uređaja te ostalo.

3.4. Web zasnovane prijetnje

Web zasnovane prijetnje, prema [10], dijele se u nekoliko kategorija:

- iskorištavanje web preglednika
- automatsko preuzimanje aplikacija
- *phishing* napadi

Iskorištavanje web preglednika može biti provedeno pomoću ranjivosti koje se nalaze unutar samog web preglednika ili pomoću specijaliziranih softvera koji se pokreću putem web preglednika, poput Adobe Flash Playera. Uz ovo, korisnik može pokrenuti aplikaciju koja može instalirati zlonamjerni softver ili obavljati druge radnje, bez korisnikova znanja.

Automatsko preuzimanje aplikacija se događa prilikom posjeta korisnika određenoj web stranici ili putem određene aplikacije. Preuzimanjem aplikacije mogu se pojaviti određeni zahtjevi koje korisnik mora poduzeti kako bi otvorio aplikaciju (primjerice traže se određene dozvole na uređaju). U drugim slučajevima također je moguće da se ti zahtjevi pokrenu automatski, bez korisnikova odobrenja.

Phishing napadi ili drugačije nazvani, napadi vezani uz krađu identiteta korisnika predstavljaju fenomen u kojem napadači prikupljaju korisničke vjerodajnice (kao što su lozinke i brojevi kreditnih kartica) putem lažnih aplikacija ili poruka (SMS, e-mail poruke) koje se čine kao da su prave. Krađa identiteta predstavlja protuzakonit način izdvajanja povjerljivih podataka s uređaja, kao što su broj bankovnih računa i kartica, lozinke za mrežne transakcije, korisnička imena i zaporke društvenih mreža itd. Zlonamjerni *phishing* program posebno je dizajniran za uređaje na kojima izvode napade i pokušavaju dobiti pristup ograničenim informacijama na uređaju, [15].

4. Tipovi i karakteristike zlonamjernog softvera terminalnih uređaja

U ovome poglavlju obraditi će se nekoliko značajnijih tipova zlonamjernog softvera koji su obilježili prethodna razdoblja u svijetu terminalnih uređaja.

4.1. Zeus

Od raznih vrsta zlonamjernog softvera prvi navedeni, Zeus, predstavlja jedan primjer poznatijeg bankarskog trojanskog napada, koji je unutar informatičkih krugova poznatiji kao *crimeware*. Ovakva vrsta trojanskog napada krade podatke zaraženih uređaja putem web preglednika i zaštićenih memorija za pohranu podataka. Jednom zaraženo računalo, automatski šalje ukradene podatke prema *bot* upravitelju i omogućuje mu kontroliranje servera, gdje su sami podaci pohranjeni, [16].

Zeus se, prema podacima, u kriminalnom podzemlju prodaje kao alat okvirne vrijednosti između 3000 do 4000 USD. Zbog relativno visoke cijene, smatra se da je jedan od tipova zlonamjernog softvera koji je najčešće korišten od strane kriminalnih skupina specijaliziranih za financijske prevare. Postepenim razvojem kroz godine, evoluirao je do zavidne granice te je razvio čitav niz sposobnosti krađa informacija prema [16]:

- krade podatke podnesene u HTTP formi
- krade podatke certifikata javnog ključa infrastrukture i korisničke podatke koji su pohranjeni u zaštićenim podatkovnim spremnicima
- krade FTP i POP korisničke vjerodajnice
- modificira HTML ciljanih stranica u svrhu krađe informacija
- preusmjerava žrtve s traženih web stranica prema onima koje napadač kontrolira
- pretražuje i preuzima podatke sa zaraženog uređaja
- izvršava transakcije bez znanja korisnika zaraženog uređaja

Posljednje verzije Zeusa prodavane su privatno, a sam autor nadogradio ga ih je s tim da je postigao velike duljine zapisanog računalnog koda koristeći sustav licenciranja baziranih na hardveru. Jednom kada se pokrene, dobije se kod sa specifičnog računala, zatim se od strane autora dodjeljuje ključ za korištenje na samo tom računalu. Godine 2010. bio je prvi put da su se sigurnosni stručnjaci u svijetu susreli sa zlonamjernim softverom koji ima ovakvu razinu kontrole.

Zeus provodi izvlačenje ukradenih podataka i daljinsko upravljanje pomoću kriptiranih HTTP zahtjeva za naredbe i kontrolu web servera. Dok je primarna funkcija ovoga zlonamjernog softvera raditi razne financijske prijevare, njegova karakteristika krađe informacija predstavlja prijetnju svim poduzećima. Kriminalne skupine ili njihovi pojedinci obično traže podatke od interesa za izravno dobivanje novca u njihovoj protuvrijednosti ili te iste podatke preprodaju drugim zainteresiranim stranama.

Nekoliko od ovih navedenih zadataka mogu se izvesti na zahtjev putem HTTP baziranog upravljačkog panela i usmjeravanjem na određeno odabrano zaraženo računalo. Slučajevi koji se temelje na zahtjevu mogu biti izvedeni preko specijalnih komandnih datoteka koje mogu biti izvršavane na odabranom sustavu. Ovakve komandne datoteke mogu biti iskorištene u svrhu snimanja zaslona zaraženog sustava ili uređaja i u svrhu ažuriranja, [16].

4.1.1. Polimorfna enkripcija

Autori ovoga virusa, razvijaju nove verzije i koje se završetkom izrade puštaju u beta testiranja da shvate njegovo ponašanje i eventualno isprave nedostatke koje su uočili. Verzija 1.4, uključivala je komponente dvaju ključa koji je sam virus učinila još tajnijim i sveobuhvatnijim. Prema [16], komponente su:

1. Web injektiranje u Internet preglednik
2. Polimorfna enkripcija: Verzija 1.4 omogućila je trojanskom napadu da ponovno kriptira samoga sebe svaki put kada zarazi novi uređaj te na bazi toga svaka nova zaraza će biti jedinstvena (sadržavat će kod koji ranije nije bio korišten). Ova verzija također je omogućila da imena datoteka budu nasumično generirane, a svaka zaraza će sadržavati drugačiji datotečni naziv. Slijedom ovih koraka antivirusni programi imaju jako težak zadatak identificiranja Zeusa na žrtvinim uređajima.

Zeus uključuje sposobnosti da pripomogne automatiziranoj prijevari vezanoj uz financije. U Sjedinjenim Američkim Državama, najpoznatiji je primjer s ACH, elektroničkom mrežom za financijske transakcije. Ova mreža je korištena za online plaćanje računa, plaćanje izravnih depozita od poslodavca i prenošenje novca s jednog korisničkog računa na drugi. Zeus u ovakvoj akciji ima za cilj iskoristiti ACH za prenošenje novca na korisničke račune kriminalaca, [16].

4.1.2. Savjeti za vlastitu zaštitu

Za zaštitu od ove vrste zlonamjernog softvera predlaže se da poslovni korisnici i tvrtke općenito te oni koji uređaje koriste u privatne svrhe, online bankarske transakcije i razne financijske transakcije obavljaju na izoliranim radnim stanicama koje se ne koriste za opće Internetske aktivnosti, kao što su pregledavanje web preglednika i čitanje e-mail pošte što može povećati rizik da će uređaj biti zaražen.

Tvrtke mogu uzeti u obzir korištenje alternativnog operativnog sustava za radne stanice s kojima se pristupa osjetljivim podatcima ili financijskim računima. Potrebno je održavati ažuriranja antivirusnih programa, operativnih sustava i softvera. Također se navodi da se ne otvara sumnjiva e-mail pošta s raznim privitcima ili linkovima od strane nepoznatih ljudi, pa čak i u slučaju da ih da ih poznajemo, potrebno je provjeriti s njima jesu li vam prethodno poslali nešto vezano za otvaranje dodanog privitka. Osim toga, ključna je svijest korisnika i zaposlenika. Konkretno, zaposlenici koji koriste sučelja s klijentima trebaju biti svjesni ovih vrsta prijetnji kojima će se pomoći zaštiti potencijalne žrtve, [16].

4.2. CryptoLocker

Sredinom rujna 2013. godine, uočena je nova obitelj zlonamjernog softvera vezana za *ransomware* pod nazivom CryptoLocker. *Ransomware* kao zlonamjerni softver u proteklih nekoliko godina stvarao je naročite probleme te korisnicima trošio vrijeme i novac. *Ransomware* ima ulogu sprečavanja da žrtva koristi uređaj na normalan način (pa će im tako na primjer zaključati zaslon) i koristiti utjecaj socijalnog inženjeringa kako bi uvjerio žrtve da nepoštivanje uputa autora zlonamjernog programa dovodi do posljedica u stvarnom svijetu. Te posljedice, kao što su suočavanja s uhićenjima i zatvorske kazne, prikazane su kao rezultat ilegalnog skidanja određenih sadržaja putem Interneta. *Ransomware* u stvari predstavlja oblik otkupnine, a žrtve mogu ignorirati zahtjeve i koristiti sigurnosne softvere za otključavanje sustava i uklanjanje zlonamjernog programa koji im prijeti. CryptoLocker mijenja dinamiku ovakve vrste zlonamjernog softvera načinom agresivnog šifriranja datoteka na žrtvinom uređaju i vraćanje kontrole na sustavom tek nakon što se tražena otkupnina plati.

Rane verzije CryptoLockera distribuiraju se putem e-pošte s neželjenim sadržajem koji ciljaju na ljude iz poslovnog svijeta. Mamac je često bio „pritužba potrošača“ protiv primatelja e-pošte ili njegove poslovne organizacije. Priloženo tim porukama bila je ZIP datoteka unutar koje se nalazi zlonamjerni program. CryptoLocker skriva svoju prisutnost od žrtava dok ne uspije kontaktirati naredbenog i kontrolnog poslužitelja te šifrirati datoteke na povezanim diskovima. Prije tih radnji, zlonamjerni softver osigurava da i dalje radi na zaraženim uređajima i da se pojavljuje tijekom ponovno pokretanja. Kada se prvo izvodi, zlonamjerni softver stvara kopiju samoga sebe u jedno od direktorija vezanim uz aplikacije i zatim briše izvornu izvršnu datoteku.

Umjesto korištenja prilagođene kriptografske implementacije, koja je prisutna kod drugih obitelji zlonamjernog softvera, CryptoLocker koristi snažnu certificiranu enkripciju treće strane koju nudi Microsoftov CryptoAPI. Korištenjem implementacije zvuka i praćenjem najboljih praksi u informatičkom svijetu vezanom za enkripciju, autori zlonamjernog softvera stvorili su robustan program kojeg je teško zaobići, pritom koristeći posebne algoritme za stvaranje ključeva i šifriranje podataka. Proces enkripcije započinje nakon što je CryptoLocker uspostavio svoju prisutnost na sustavu i uspješno je lociran, povezan te komunicira s poslužiteljem koji je pod kontrolom napadača. Zatim se odabire mjesto u sustavu na koju će se taj proces primijeniti, obično su to lokalni diskovi, ali također mogu biti i eksterni uređaji koji se spajaju na glavni uređaj te se datoteke na tom mjestu trenutno zaključavaju dok se otkupnina ne plati. Valja napomenuti kako se nisu u početku zaključavale sve vrste datoteke, kao na primjer PDF, ali su kasnijom nadogradnjom programa bile i one obuhvaćene kao i velika većina ostalih. Svaka se datoteka šifrira jedinstvenim ključem koji ima naziv AES. Šifrirani ključ ima malu količina metapodataka i sadržaj datoteke zapisuju na disk zamjenjujući originalnu datoteku. Šifrirane datoteke mogu se vratiti pomoću drugog privatnog ključa (RSA) koji se isključivo nalazi na strani sudionika u prijetnji. Nakon završetka procesa šifriranja datoteka, CryptoLocker periodički je programiran da nadomješta sustav s novim datotekama koje su namijenjene šifriranju. Zlonamjerni softver ne otkriva svoju prisutnost žrtvi sve dok se ciljane datoteke ne šifriraju. Nakon

što se žrtvu upozna da je uređaj zaražen pojavljuje se zaslon koji sadrži upute i sat odbrojavanja kao što je prikazano na slici 1, [17].

Slika 1. Zaslon predstavljen žrtvama CryptoLockera, [17]

4.2.1. Plaćanje otkupnine

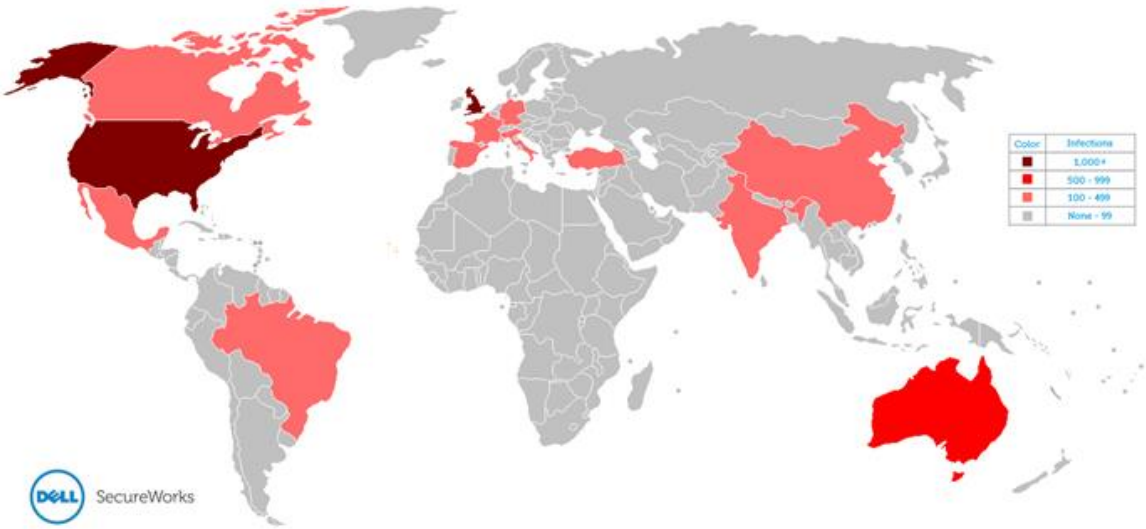
Vrijednost otkupnine varirala je u ranim počecima od kad se zlonamjerni softver pojavio na tržištu, međutim nakon nekoliko tjedana cijena se stabilizirala na iznosu od 300 USD ili 2 Bitcoina. Autori prijetnje nudili su različite načine plaćanja žrtvama. Metode koje su bile ponuđene spadaju u anonimne metode plaćanja, koje su okarakterizirane nemogućnošću praćenja podrijetla novca i konačnog odredišta plaćanja. Na zaslonu se pojavljuje izbornik kojim se korisniku omogućuje odabir između sljedećih metoda plaćanja: cashU, Ukash, Paysafecard, Bitcoin i Green Dot MoneyPak. Na slici 2, prikazan je zaslon odabira metode plaćanja putem Bitcoina, iako postoji padajući izbornik na kojem se može izabrati bilo koja od prethodno navedenih metoda. Raznolikost opcija plaćanja i izbora valute, sugeriraju da su autori CryptoLockera očekivali da će postati globalna prijetnja, [17].

Bitcoin predstavlja kriptovalutu, odnosno to je digitalni novac koji se može slati putem Interneta te se temelji na kriptografskom protokolu koji je neovisan o središnjim bankovnim ustanovama. Bitcoin se može prenijeti putem računala ili pametnog telefona bez posredničke financijske institucije. Vrijednost otkupnine u ovoj valuti iznosila je dva (2) Bitcoina, što je bilo u protuvrijednosti 300 USD, premda je tržišna vrijednost Bitcoina doživjela izniman rast u to vrijeme, vrijednost otkupnine se smanjivala sve do vrijednosti od 0,3 Bitcoina, [18].

Slika 2. Opcija plaćanja pomoću usluge Bitcoin, [17]

4.2.2. Žrtve

Na temelju svog dizajna, metoda implementacije i empirijskih promatranja njegove distribucije, čini se da CryptoLocker cilja engleske govornike, posebno one koji se nalaze u Sjedinjenim Američkim Državama. Infekcije su se pojavile u financijskim i javnim ustanovama, međutim nije zabilježeno da je ciljano na neku određenu granu industrije. Napadi su se također proširili i na privatne korisnike. Sigurnosni stručnjaci procjenjuju da je 200 000 do 250 000 sustava zaraženo na globalnoj razini tijekom prvih 100 dana prijetnje CryptoLockerom, a slika 3, predstavlja njegovu globalnu distribuciju u prosincu 2013. godine, [17].



Slika 3. Globalna distribucija CryptoLocker infekcije tijekom prosinca 2013. godine, [17]

4.3. Citadel

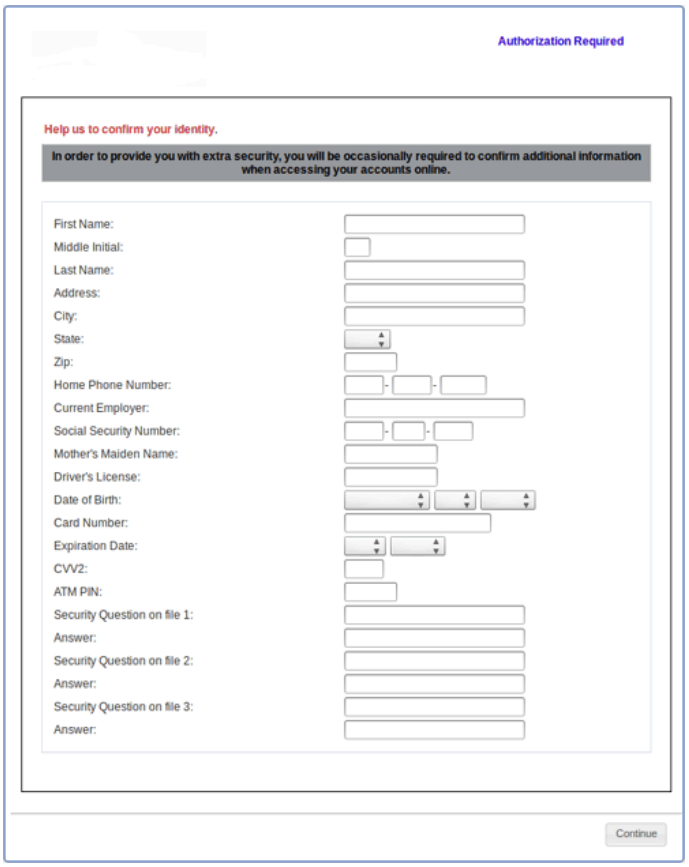
U listopadu 2012. godine pojavio se istaknuti zlonamjerni softver u bankarskom području, pod nazivom Citadel. Od početka pojavljivanja, ažuriranje ovog softvera i njegove nove inačice omogućile su nekoliko novih značajki, za koje se tvrdi da poboljšavaju i performanse i upotrebljivost, [19].

4.3.1. Značajke

Kao jedna od značajnih karakteristika predstavljena je nova verzija kriptografije. Napravljene su dodatne izmjene u kriptografskim algoritmima koji se koriste za šifriranje mrežnih komunikacija, datoteka i podataka pohranjenih u registrima. Podaci koji su šifrirani pomoću modificiranog kriptografskog algoritma, obuhvaćaju konfiguracijske datoteke, log datoteke koje služe kao privremena pohrana za ukradene podatke te konfiguraciju i podatke stanja koji su pohranjeni unutar registara. Dodana je i opcija koja omogućuje operaciju dodatnog šifriranja.

Sposobnost stvaranja web injektiranja koji može mijenjati HTML ciljane web stranice jedan je od najmoćnijih alata dostupan korisnicima Citadela i sličnih bankarskih vrsta zlonamjernog softvera. Ova opcija u Citadelu dodana je da *botnet* može stvarati nova web injektiranja na zaraženim sustavima bez potrebe za stvaranjem i ažuriranjem cijele postojeće konfiguracijske datoteke. Upravo ta značajka pruža fleksibilnost napadaču da lako izbacuje nova web injektiranja na sve zaražene sustave, sustave unutar određenog područja na primjer jedne države ili cilja na samo jednog korisnika. Zlonamjerni softver posjeduje zasebni modul koji služi za krađu HTTP *cookiesa* koji su pohranjeni u web pregledniku Mozilla Firefox. Nakon krađe potrebnih podataka, podaci se kriptiraju i prenose na Citadel server. Uporabom određenih značajki ukazuje na to da napadači ulažu resurse kako bi njihova infrastruktura bila ažurirana i prate razvoj tehnologije, a sve u to u svrhu profita od kriminalne aktivnosti.

Meta ovakve vrste napada su, prvenstveno, podaci o kreditnim karticama pomoću web injektiranja. Ciljevi napada zemljopisno su rasprostranjeni, čime se želi stvoriti globalna prijetnja, a tomu u prilog ide i višejezičnost zlonamjernog programa. Kao što je ranije spomenuto, prvenstveno su bitne financijske institucije, međutim od velikog interesa pokazuje se da ciljaju na društvene mreže i stranice koje su vezane uz e-poštu. Koriste kompleksnu infrastrukturu vezanu uz domene koje se mijenjaju gotovo svakodnevno. Primjer skočnog prozora ovoga zlonamjernog virusa, kojeg je potrebno ispuniti osobnim podacima prikazan je na slici 4, a bit će prezentiran kao ovlaštena stranica renomiranih platnih mreža kao što su Visa ili MasterCard. Citadel je također pokazao sposobnost bilježenja lozinki za ciljane aplikacije koje mogu sadržavati osjetljive podatke, a to ovisi o nazivima procesa koji se obrađuju. U slučaju podudaranja naziva procesa, sve znakove koje je korisnik unio u aplikaciju bivaju zabilježene u onim intervalima koji su navedeni u njegovoj konfiguracijskog datoteci. Ovakvi obrasci napada zabilježeni su na aplikacijama koje koriste daljinski pristup, POS-ovim uređajima u trgovinama i elektroničkim načinima plaćanja, [19].



Slika 4. Skočni prozor koji se koristi u napadima Citadela, [19]

Krajem rujna 2012., prema [19], kampanja ovih napada uključivala je više od 400 različitih URL uzoraka s web injektiranjem. U sljedećem mjesecu, aktivnost mu je bila usporena te se tijekom studenog te godine pojavio se s 200 novih URL uzoraka. Razlog velikom broju URL-ova ukazuje na postojanje više grupa napada te kako svaka od njih ima svoj vlastiti skup za napade na određene ciljeve.

4.3.2. Preporuke

Karakterističan za razdoblje od prije nekoliko godina, slovio je kao jedan od uglednih alata u zločinačkom kibernetičkom svijetu. Njegov rast omogućio je napredovanje tehnika prijevare. Citadel ne predstavlja samo prijetnju korisnicima online bankarstva i financijskih usluga nego je i opasna prijetnja sigurnosti osjetljivih podataka. Organizacije trebaju procijeniti rizik koji predstavlja ovaj zlonamjerni softver prema njihovoj informacijskoj sigurnosti i poslovnim linijama. Uz razne analize Citadela, postoje poznati pokazatelji prijetnji koje je jednostavno rješenje za otkrivanje zaraženih uređaja, [19]. To danas ne garantira da se korisnici neće susresti s ovakvom prijetnjom, ali detaljnim proučavanjima koja su zatim implementirana u razne antivirusne softvere, mogu ga prepoznati i ukloniti sa zaraženog uređaja.

4.4. Sakula

Pod nazivom Sakula, pojavljuje se jedna od verzija daljinski upravljanog trojanskog napada koji su poznatiji kao RAT virusi. Saukla je također poznat i pod drugim nazivima, Sakurel i Viper. Značajne prve rezultate korištenja postigao je u razdoblju

mjeseca studenog 2012. godine, a u 2015. godini korišten je za mnoge ciljane napade. Spomenuti zlonamjerni softver omogućuje napadaču pokretanje interaktivnih naredbi (jer se njime upravlja na daljinu), kao i preuzimanje datoteka i izvršavanje dodatnih komponenti na zaraženom uređaju. U svijetu je poznato oko 346 različitih uzoraka Sakule, [20].

Sakula se skriva unutar web preglednika u varijantama gdje je digitalno potpisan (potpis je pribavljen pomoću aplikacija Kaspersky ili McAfee, koji slove kao jedne od ponajboljih antivirusnih softvera, [21]), što mu omogućuje da zaobiđe sigurnosne kontrole i pružajući korisnicima lažni osjećaj sigurnosti da je softver koji koriste legitiman. Zlonamjerni softver se maskirao u programe za instalaciju pouzdanih tvrtki (poput Adobea ili Microsofta), kako bi putem socijalnog inženjeringa uvjerio korisnike da su potrebni za instaliranje i daljnje korištenje. Prilikom postupka instalacije ovoga zlonamjernog softvera, izmjenjuju se originalne datoteke na uređaju sa zlonamjernima kako bi se mogao proširiti na više IP adresa unutar organizacije u kojoj se žrtva nalazi. Tijekom instaliranja se pokreće provjera datoteka koja je inicirana zlonamjernim softverom i utvrđuje se kako nema nikakvih opasnosti za uređaj.

Ova vrsta RAT virusa, koja je u upotrebi od 2012. godine, u svome izvornom programskom kodu doživio je vrlo malo promjena, što ukazuje da je učinkovit u ciljanim napadima. U njegovoj prirodi je, da mala naredba koja je postavljena u Sakulu omogućuje svojim operativcima aktivno upravljanje kompromitiranim sustavom, preuzimanje i izvršavanje dodatnih komponenti i skrivanje unutar napadnutog uređaja, [20].

4.5. TeslaCrypt

U prvom dijelu 2015. godine, istražena je nova obitelj *ransomwarea* koja je namijenjena šifriranju datoteka pod nazivom TeslaCrypt. Nakon šifriranja popularnih vrsta datoteka na zaraženom uređaju pomoću algoritama za šifriranje AES, TeslaCrypt drži datoteke i za otkupninu traži novac u vrijednosti 250 do 1000 USD. Zlonamjerni softver koristi anonimnu mrežu pod nazivom Tor koja upravlja naredbenim i kontrolnim poslužiteljem te ne zahtijeva mrežnu povezanost da bi proces šifriranja bio obavljen što uvelike komplicira njegovo otkrivanje na uređajima i samim tim i prevenciju. TeslaCrypt u početnoj fazi nije bio široko rasprostranjen i oponašali su zaslon upozorenja CryptoLockera (prikazano na slici 5), koji je ranije spomenut, a u pozadini zaslona ustvari se izvodio TeslaCrypt, [22].

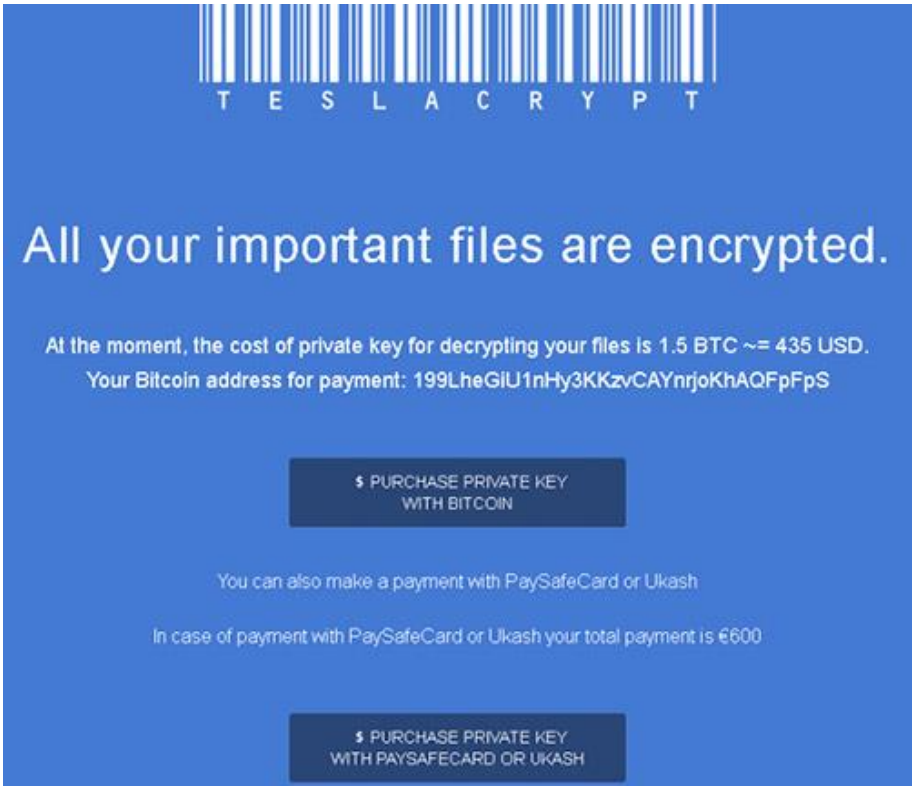
Slika 5. TeslaCrypt zaslon prezentiran žrtvama, [22]

Kao što prikazuje slika 6, tek je kasnijim nadogradnjama stvoren karakterističan zaslon s porukom na zaraženim uređajima.

Slika 6. Poruka postavljena od strane TeslaCrypta kao pozadina radne površine na zaraženom uređaju, [22]

Ovaj zlonamjerni softver iskoristio je ranjivosti u web tehnologijama kao što su Internet Explorer (web preglednik), Adobe Flash i Adobe Reader. Vrste datoteka koje zaključava ne ovise o uređaju i sustavu na kojemu se nalazi. Zanemaruje glazbene i video datoteke poput MP3 i MP4 formata, kao i mnoge ekstenzije datoteka koje su povezane s uobičajenim aplikacijama namijenih poslovnoj klasi. Formati datoteka koji su mu zanimljivi te prvenstveno cilja na grupu produktivnosti kao što su Open Office i Microsoft Office, kao i formati povezani s videoigrama (npr. „spremi“ (engl. *save*) datoteke) i kreativne aplikacije (npr. Adobe Photoshop). Proces enkripcije započinje tako da skenira sve pogonske sustave na uređaju i selektivno cilja određene pogone. TeslaCrypt ne napada prijenosne memorije za pohranu (npr. USB ili dodatne eksterne diskove). Zlonamjerni softver tada rekurzivno skenira pogone s datotekama na kojima se nalaze ciljani formati datoteka, zatim ih otvara, čita i šifrira svaku datoteku. Šifrirani podaci zapisuju se u izvornu datoteku, što smanjuje vjerojatnost da forenzički alati mogu opraviti izvorne datoteke.

Većina otkupnine plaćena je Bitcoinom, a jedan od razloga je i taj što su napadači poticali žrtve na taj način plaćanja zbog anonimnosti, ali prihvaćani su i *prepaid* kuponi ili kartice. U Sjedinjenim Američkim Državama žrtve imaju mogućnost plaćanja PayPal My Cash karticama, a u Europi s PaySafe karticom ili uCash opcijom naplate, što je prikazano na slici 7. U travnju 2015. godine, tvrtka Cisco Talos stvorila je alat za dešifriranje koji je mnogim žrtvama omogućio oporavak datoteka i izbjegavanje plaćanja otkupnine, [22].



Slika 7. Europski izgled zahtjeva za otkupninom, [22]

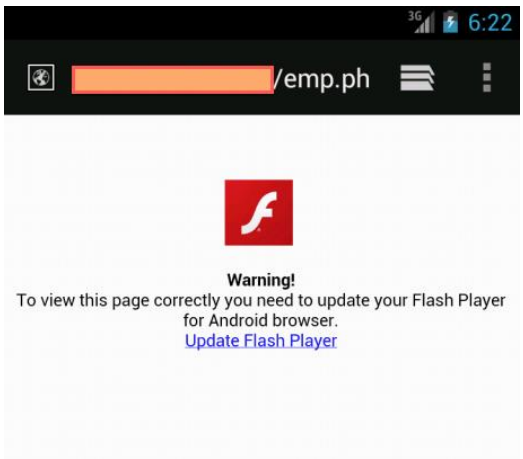
Iako postoji alat za dešifriranje i omogućuje opravak datoteka, prema [22], navode se neke radnje koje mogu ublažiti izlaganje ili štetu TeslaCrypta:

- blokiranje izvršnih datoteka i komprimiranih arhiva koji ih sadrže
- održavanje redovitih ažuriranja operativnih sustava uređaja, web preglednika i njegovih dodataka
- sprječavanje neprivilegiranih osoba da modificiraju datoteke
- implementiranje pravila softverskih ograničenja kako bi se spriječilo izvođenje programa poput TeslaCrypt u zajedničkim direktorijima

4.6. Stels

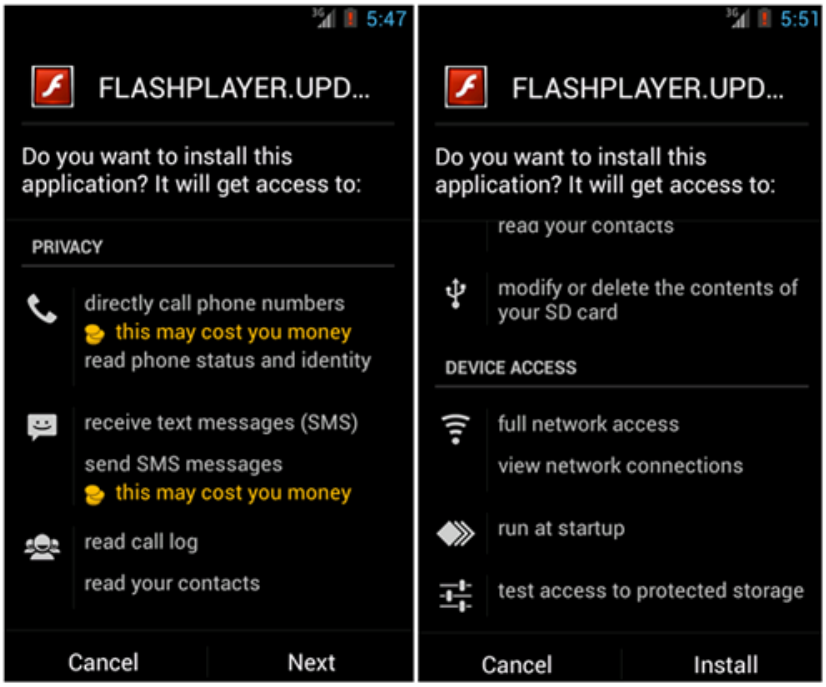
Zlonamjerni softver, Stels, višenamjenski je trojanski napad koji može prikupiti žrtvine popise kontakata, slati i presretati SMS (tekstualne) poruke, upućivati telefonske pozive (uključujući pozive na premium brojeve) i instalirati dodatne pakete zlonamjernog programa. Ovakva vrsta kampanje obično privlači korisnike da kliknu na link, nakon čega se preusmjeravaju na eksploatacijske pakete pod nazivom Blackhole, koji ciljaju na ranjivosti web preglednika i dodataka u operacijskom sustavu Windows. Međutim, zbog toga što se Blackhole ne može iskoristiti na Android uređajima, napadači upotrebljavaju lažno ažuriranje Adobe Flash Playera kako bi privukao korisnike da ga preuzmu i izvrše zlonamjerni program Stels. Stels koristi i mamce kao što su lažne poruke e-pošte iz američke porezne administracije (IRS) i preporuke „prijatelja“. Mnoge kampanje zlonamjernog softvera upotrebljavale su IRS kao mamac zbog roka za korporativno vraćanje poreza i roka za podnošenje pojedinačne prijave.

Uzorak Stelsa, koji se pojavio 12. ožujka 2013. godine, nije bio prepoznat od strane niti jednog od 44 antivirusna softvera. U e-mail porukama se nalazio URL koji se povezivao s ugroženom web stranicom koja otiskuje web preglednik i operativni sustav koji žrtva koristi, a to je ostvarivao pomoću PHP skripte koju se prenijeli napadači. U slučaju da uređaj žrtve pokreće Google Android, hakirana web stranica će prikazivati ažuriranje za Adobe Flash Player, kao što je prikazano na slici 8, koja pruža vezu s izvršnom datotekom zlonamjernog programa Stels, [23].



Slika 8. Lažna stranica za ažuriranje Adobe Flash Playera, [23]

U trenutku kada žrtva klikne na link „Update Flash Player“, njihov Android uređaj preuzima zlonamjerni program Stels i traži se korisnikovo odobrenje za njegovu instalaciju. Na temelju toga, kako je prikazano na slici 9, potrebna je interakcija s korisnikom kako bi se Android uređaji zarazili. Osim toga, aplikacija ne potječe iz službene trgovine aplikacijama Google Play pa korisnik mora omogućiti opciju instaliranja nepoznatih izvora (odnosno dopuštanje instaliranja neslužbenih aplikacija), [23].



Slika 9. Dopuštenje za instalaciju Stelsa na operativnom sustavu Android, [23]

Nakon instalacije Stelsa, pojavljuje se ikona Flash aplikacije u izborniku aplikacija te nakon pokretanja, Stels prikazuje lažnu poruku o pogrešci: „Vaša Android verzija ne podržava ovo ažuriranje! Postavljanje je otkazano.“ i briše ikonu Flasha iz izbornika aplikacija. U slučaju ako žrtva koristi Internet Explorer, Mozilla Firefox ili Opera web preglednik, PHP skripta prikazivat će lažnu IRS web stranicu prikazanu na slici 10. Uz to su napadači izmijenili URL-ove na lažnoj IRS web stranici kako bi se žrtve lakše mogle povezati sa zlonamjernom PDF datotekom, koja iskorištava ranjivosti u programima Adobe Reader i Adobe Acrobat. Zanimljiva je činjenica da su samo dva od 46 antivirusnih dobavljača označila PDF datoteku kao zlonamjernu u trenutku pojavljivanja u zlonamjernom svijetu mobilnih terminalnih uređaja, [23].

Slika 10. Lažna IRS stranica koju učitava Blackhole eksploatacijski paket, [23]

U slučaju da uređaj žrtve nije pokretan od strane Android operacijskog sustava ili jednog od ciljanih web preglednika, PHP skripta na ugroženoj web stranici preusmjerava web preglednik na stranice koje su povezane s prijevarama vezanim uz rad od kuće, prikazanog na slici 11, [23].

Slika 11. Prijevara vezana uz rad od doma, [23]

4.6.1. Mogućnosti i prepoznavanje

Stels radi gotovo na svim verzijama Android operacijskog sustava. Trojanski napad ne može *rootati* uređaj, međutim, prema [23] može obavljati sljedeće zadatke:

- preuzimati i izvršavati datoteke
- ukrasti popise kontakata

- prijaviti informacije o sustavu kojim se uređaj koristi:
    - IMEI (međunarodni broj mobilne opreme)
    - ID pretplatnika
    - instalirane aplikacije
    - broj telefona
    - model telefona
    - proizvođač telefona
    - operacijski sustav
- upućivanje telefonskih poziva
- slanje SMS poruka
- praćenje i bilježenje SMS poruka
- prikazivanje obavijesti
- deinstaliranje aplikacija

Stles zadržava nizak profil na uređaju, sve u svrhu toga kako ne bi bio otkriven. Međutim postoji nekoliko metoda za prepoznavanje infekcije. Konkretno, zlonamjerni softver instalira ikonu na izborniku aplikacija pod nazivom „APPNAME“ (prije nego što je prvi put izvršena). Stels se također konfigurira kao aplikacija koja je pokrenuta te se može vidjeti unutar postavki uređaja pod pokrenutim procesima, što prikazuje slika 12. Iako se ikona uklanja iz izbornika nakon prvog pokretanja ona se i dalje pojavljuje na popisu pokrenutih procesa. Uz to što se može vidjeti na popisu pokrenutih procesa, postoji i drugi indikator koji može otkriti prisutnost, a to je mrežni promet generiran od strane Stelsa, [23].

Slika 12. Ikona Flash prikazana na popisu pokrenutih procesa na uređaju, [23]

4.6.2. Preporuke i uklanjanje

Kako se navodi prema [23], sljedeće preporuke imaju utjecaj na sprječavanje pojavljivanja Stelsa na uređajima:

- ne dopuštanje instalacija aplikacija na uređajima koje se ne distribuiraju putem službenih trgovina

- prilikom instalacije aplikacija na uređaju, potrebno je obratiti pažnju na dozvole koje se traže od strane aplikacija
- ovisno o vrsti i svrsi aplikacije, neke dozvole mogu povećati sumnju vezanu uz sigurnost korisnika (npr. aplikacija Flash ne bi trebala imati dozvole za telefonske pozive ili primanje SMS poruka)
- obrazovanje korisnika o prijetnjama koje su prisutne putem raznih privitaka u SMS porukama i e-mail porukama

Za razliku od zlonamjernog softvera koji dobiva *root* pristup uređaju, Stels se može relativno lako ukloniti. Potrebno je otići u odjeljak postavke uređaja i na popisu procesa pokrenutih aplikacija pronaći „FLASHPLAYER.UPDATE“ (koji je u stvari zlonamjerni program Stels). Zatim treba prihvatiti opciju deinstalacije. Opcija uklanjanje ne predstavlja veliki problem za razliku od štete koju ovaj zlonamjerni softver može učiniti, [23].

4.7. CryptoWall

Jedan od najvećih i najdestruktivnijih *ransomwera* koji se pojavio na Internetu te koji zaključava datoteke predstavlja upravo CryptoWall. Iako se pojavio u zadnjem kvartalu 2013. godine, tek je u veljači 2014. godine zapažen te detaljnije analiziran i mogao se dobiti uvid u njegov rad. Nakon pojave CryptoLockera, u rujnu 2013. godine, istraživači su opazili sve veći broj zlonamjernog *ransomwer* programa koji su uništili zaključane podatke, unatoč tome što je otkupnina bila podmirena.

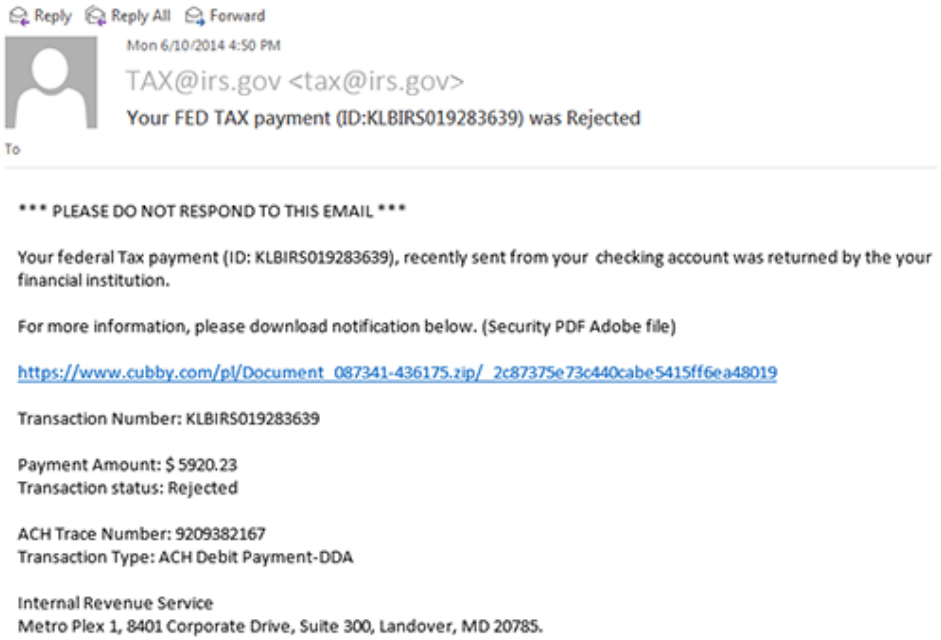
Rane CryptoWalla verzije imale su izrazito sličan izgled (vidi sliku 13) i ponašanje kao originalni CryptoLocker. Točan vektor infekcije kojim se širio ovaj zlonamjerni softver nije poznat, no izvješća zaraženih korisnika navode da je dolazio u obliku privitka unutar e-mail poruke, [24].

Slika 13. Imitacija CryptoWall verzije (lijevo) sa CryptoLockerom (desno), [24]

CryptoWall je tijekom razdoblja distribucije imao više imena. U najranijoj fazi, nazivaju ga CryptoClone zbog nedostatka jedinstvenog naziva i karakteristika koje je prikazivao, a izgledao je slično drugima. U ožujke 2014. godine, računalni stručnjaci su otkrili njegov pravi naziv CryptoDefense, a početkom srpnja iste godine promijenjen je u CryptoWall te se kao takav zadržao.

Iako infrastruktura CryptoWalla nije bila toliko sofisticirana, kao što je primjer kod CryptoLockera, napadi su pokazali iznimnu dugotrajnost i stručnost u njegovoj distribuciji. Od svojih početaka, CryptoWall se širio putem različitih vektora, uključujući web preglednike, opcije preuzimanja s određenih pogona i kao privitak unutar e-mail pošte. Od kraja ožujka 2014. godine, prvenstveno je prenošen putem zlonamjernih privitaka unutar e-mail poruka i linkova.

U lipnju 2014. godine, pokrenuta je agresivna kampanja vezana za neželjenu poštu koja je dovela do najvećih jednodnevnih infekcija koje su do tada bila zabilježene. Ove poruke sadržavale su uobičajeni mamac koji je korisnicima govorio da imaju „propušteni fax“ te je uključivao link koji ih je povezivao na Dropbox. U jednom trenutku ova kampanja je zastala, da bi par dana kasnije nastavila s e-mail porukama za koje se tvrdi da dolaze iz financijskih institucija ili vladinih agencija, kao što je prikazano na slici 14, [24].


Reply Reply All Forward

Mon 6/10/2014 4:50 PM

TAX@irs.gov <tax@irs.gov>

Your FED TAX payment (ID:KLBIRS019283639) was Rejected

To

*** PLEASE DO NOT RESPOND TO THIS EMAIL ***

Your federal Tax payment (ID: KLBIRS019283639), recently sent from your checking account was returned by the your financial institution.

For more information, please download notification below. (Security PDF Adobe file)

https://www.cubby.com/pl/Document_087341-436175.zip/_2c87375e73c440cabe5415ff6ea48019

Transaction Number: KLBIRS019283639

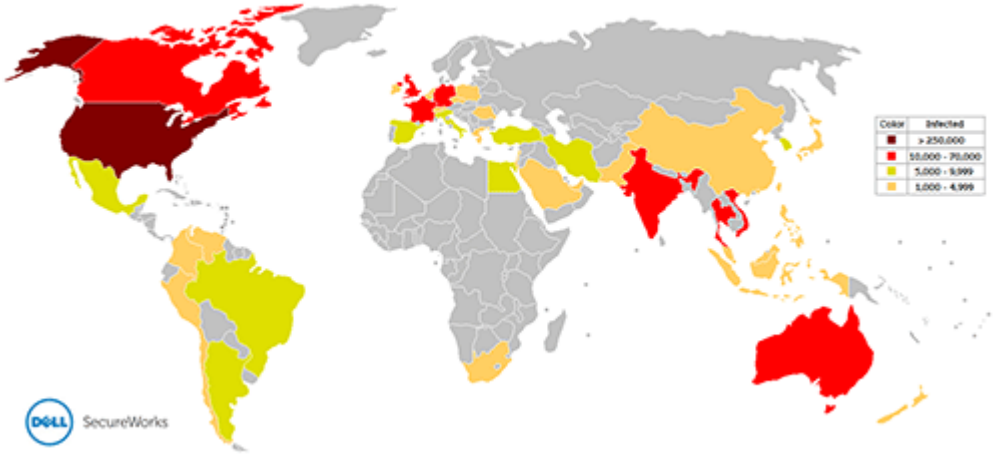
Payment Amount: $ 5920.23
Transaction status: Rejected

ACH Trace Number: 9209382167
Transaction Type: ACH Debit Payment-DDA

Internal Revenue Service
Metro Plex 1, 8401 Corporate Drive, Suite 300, Landover, MD 20785.

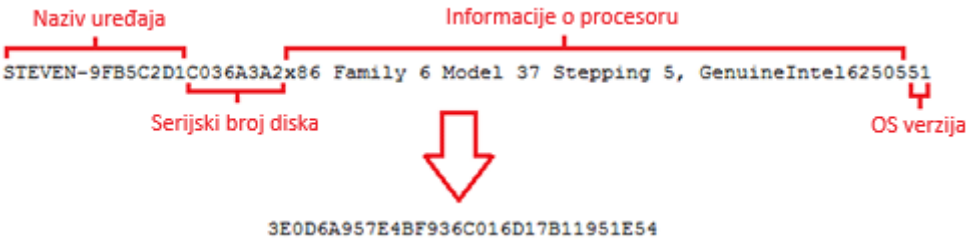
Slika 14. Lažna obavijest o odbijanju plaćanja poreza povezana sa CryptoWallom, [24]

Svakoj novoj infekciji koja je zabilježena, dodjeljuje se jedinstveni alfanumerički kod, koji se dodjeljuje uzastopno pomoću CryptoWall pozadine. Od sredine ožujka do kolovoza 2014. godine, gotovo je bilo zaraženo 625 000 uređaja. U tom istom vremenskom okviru, CryptoWall je šifrirao više od 5,25 milijardi datoteka. Na slici 15, prikazana je geografska distribucija zaraženih uređaja u prethodno navedenom vremenskom razdoblju. Zanimljivo je to da je svaka nacija na svijetu imala barem jednu žrtvu. Većina infekcija zabilježena je u Sjedinjenim Američkim Državama zbog česte distribucije CryptoWalla putem *spama* koji cilja na korisničke uređaje s engleskim jezikom, [24].



Slika 15. Globalna distribucija CryptoWall infekcije, [24]

Kada se CryptoWall izvodi prvi put, on se raspakira u memoriju uređaja i ubacuje zlonamjerni kod u nove procese koje sam generira. Procesi koji se stvaraju, mapiraju se i izvode zlonamjerni kod u adresnom prostoru procesa. Kad je jednom šifrirao datoteke, koristi se određenim tehnikama koje sprječavaju oporavljanje tih istih datoteka. Naposljetku, zlonamjerni kod stvara proces koji je anoniman (jer se izvodi s privilegijama sustava korisnika koji je zaražen), a ne kao proces sustava te se izvodi samostalno. Postoji mogućnost da se zlonamjerni program neće izvršiti u memoriji sustava u trenutku kada je dospio u sustav, već postoje mehanizmi koji mu omogućuju postojanost i osiguravaju da se on pokrene nakon ponovnog pokretanja sustava. Za razliku od ostalih prevladavajućih obitelji zlonamjernog softvera, CryptoWall ne koristi napredne tehnike kao što su algoritmi za generiranje domene (DGA) ili sustave brzog protoka DNS-a. Zlonamjerni softver stara jedinstven niz, prikazan na slici 16, od 32 heksadecimalnih znakova, koji je izveden iz naziva uređaja ugroženog sustava, serijskog broja diska, informacija o procesoru i verzije operacijskog sustava. Ovaj se niz može koristiti u svrhu sprječavanja stvaranja više istih kopija jednog zaraženog sustava, [24].

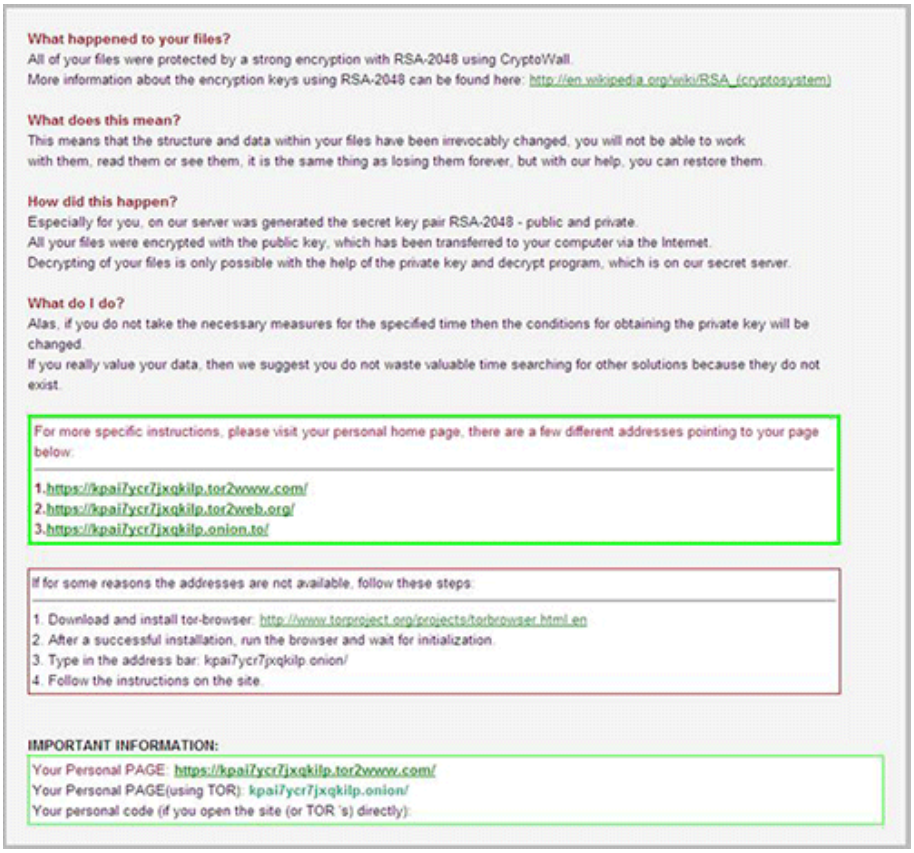


Slika 16. Jedinstveni identifikacijski generirani niz znakova infekcije
Izvor: [24]

4.7.1. Enkripcija datoteka

Šifriranje i zaključavanje datoteka počinje nakon što CryptoWall uspješno preuzme RSA javni ključ s aktivnog naredbenog i kontrolnog poslužitelja. Stoga, pomoću mrežnih kontrola za blokiranje ove komunikacije može se spriječiti da se ugroženi

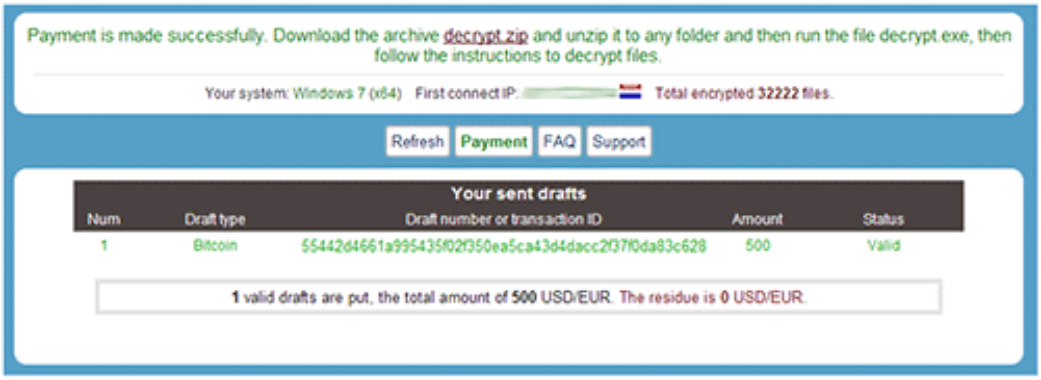
sustavi šifriraju. Za razliku od CryptoLockerove uporabe simetričnog šifriranja, kao što je AES, za šifriranje skupa podataka CryptoWall koristi javni ključ RSA za izravno šifriranje datoteka. Budući da je RSA algoritam daleko više intenzivniji od simetričnih, kompromitirani sustavi imaju značajno opterećenje procesora nakon kompromitacije CryptoWallom, jer su datoteke šifrirane. Prvi eksplicitni pokazatelj aktivne infekcije predstavljen žrtvi upravo je web stranica koju CryptoWall otvara nakon šifriranja datoteka, kako je prikazano na slici 17, [24].



Slika 17. Zaslon predstavljen žrtvama od strane CryptoWalla, [24]

Inačice CryptoWalla koje su implementirane prije travnja 2014. godine, sadržavale su slabosti u kriptografskoj implementaciji koja je omogućila oporavak ključa koji se koristi za šifriranje datoteka. U kasnijim verzijama zlonamjernog softvera taj je nedostatak ispravljen. CryptoWall koristi rekurzivno kretanje datotečnim sustavom te pritom selektivno šifrira određene vrste datoteka (npr. tekstualne datoteke, dokumente, izvorne kodove). Datoteke na fiksnim (npr. tvrdim diskovima), prijenosnim (npr. USB memorije) i mrežnim pogonima ciljane su za šifriranje. Nadalje, usluge za pohranu u oblaku, kao što su Dropbox ili Google Drive, koji su mapirani na određeni datotečni sustav također će biti šifrirani.

Računalni stručnjaci obeshrabrili su žrtve od plaćanja otkupnine, a razlog tomu je, kako navode rast poduzeća u području kibernetičkog kriminala. Žrtve koje odluče platiti otkupninu, moraju podnijeti plaćanje i čekati neko proizvoljno vrijeme da napadači potvrde plaćanje. Nakon što je plaćanje potvrđeno, žrtvina stranica na platnom poslužitelju poprima promjene i novi izgled, što prikazuje slika 18, [24].



Slika 18. Odredišna stranica nakon potvrde plaćanja otkupnine, [24]

4.7.2. Opcije plaćanja otkupnine i ublažavanje štete

Poput CryptoLockera, u ranijim verzijama CryptoWalla bile su brojne mogućnosti plaćanja, uključujući i *prepaid* kartice kao što su Paysafecard, cashU i Ukash, uz Bitcoin kriptovalutu. Za razliku od CryptoLockera, prikazano na slici 19, napadači su izvorno prihvaćali opciju kriptovalute Litecoin, [24].

Slika 19. Litecoin opcija plaćanja u ranijim CryptoWall verzijama, [24]

Cijene otkupnine često su oscilirale i nije utvrđen točan uzrok koji određuje koliku će cijenu otkupnine morati platiti određena žrtva. CryptoWall operatori zahtijevali su vrijednost otkupnine u rasponu od 200 do 2000 USD. Veće otkupnine obično su bile rezervirane za žrtve koje ne plaćaju u određenom vremenskom razdoblju (obično od četiri do sedam dana). U jednom slučaju, zabilježeno je da je žrtva platila čak 10 000 USD za oslobađanje svojih datoteka.

Web stranica koja upućuje žrtve na plaćanje otkupnine pomoću opcije Bitcoin, mijenja se jedanput dnevno. Ukupni priljev koji je zabilježen prema ovoj opciji iznosi 939 Bitcoina. Prema tečaju u kolovozu 2014. godine, jedan (1) Bitcoin iznosio je 520 USD, tako da su napadači prikupili više od 488 000 USD pomoću otkupnina. Prikupljeni podaci s poslužitelja otkrivaju točan broj žrtava i iznos koji su platili. Od gotovo 625 000 infekcija, 1683 žrtvi platile su otkupninu u vrijednosti od 1 101 900 USD. CryptoWall je manje učinkovit što se prihoda tiče, u odnosu na CryptoLocker, a razlog tomu su više prosječne cijene otkupnine i tehničke prepreke s kojima su se žrtve suočavale prilikom nabavljana Bitcoina, [24].

Sljedeće radnje, prema [24] mogu ublažiti izloženost ili štetu nastalu zlonamjernim programom CryptoWall:

- redovno sigurnosno kopiranje podataka
- održavanje operacijskih sustava, web preglednika i raznih dodataka ažuriranim
- sprječavanje neprivilegiranih korisnika da izmjenjuju datoteke
- blokiranje izvršnih datoteka zlonamjernog programa prije nego što dođu do e-mail poruka

4.8. Stegoloader

Autori zlonamjernog programa razvijaju svoje tehnike kako bi izbjegli mehanizme otkrivanja. Stegoloeader predstavlja jedan novi trend zlonamjernog softvera: koristi digitalnu steganografiju za skrivanje zlonamjernog koda, [25]. Steganografija, prema [26], predstavlja znanstvenu disciplinu koja se bavi skrivanjem informacija, odnosno tajna se poruka skriva unutar neke druge bezazlene poruke tako da se postojanje tajne poruke ne može uočiti. Steganografija strogo gledajući nije enkripcija, jer ona prikriva postojanje poruke, dok metode kriptografije čine poruku nerazumljivu vanjskim akterima različitim preobrazbama teksta, [27]. Stegoloader prvi put je identificiran u rujnu 2013. godine, ali privukao je mali interes javnosti. Ovaj zlonamjerni softver kradom krade podatke iz ugroženih sustava, a bilježi se svaki pristup određenim dokumentima, instalacije raznih programa i aplikacija, posjećene web stranice te krade lozinke, [25].

Stegoloaderov modul za implementaciju preuzima i pokreće glavni modul. Ovaj zlonamjerni softver ne izvršava svoj glavni programski kod ako detektira analize ili sigurnosne alate na zaraženom sustavu. Modul za implementaciju preuzima sliku s legitimne web stranice. Nakon preuzimanja, koristi se dekompresija slike. U ovom slučaju je teško otkriti lokaciju preuzete slike i zlonamjernog koda putem tradicionalnih načina, jer nisu spremljeni na disk. Nakon što se glavni modul učita i dešifrira, modul za implementaciju prenosi izvršenje na glavni modul koji se nalazi u memorijskom području dodijeljenom za tu svrhu. Modul za implementaciju postaje latentan sve dok se glavni modul ne izvrši. Kada glavni modul terminira, implementacijski modul šalje posljednje izvješće kontrolnom i naredbenom poslužitelju s porukom da je glavni modul završen, a zatim i on također terminira. Glavni Stegoloader modul prikuplja informacije ugroženim sustavima. Ako podaci odgovaraju određenim kriterijima, operater

zlonamjernog softvera može implementirati dodatne module, koji se također izvršavaju direktno u memoriji i nikad se ne spremaju na disk.

Podaci, prema [25], pokazuju da je ovaj zlonamjerni program utjecao na područja poput zdravstva, obrazovanja i proizvodnje. Zlonamjerni program ima karakteristike nevidljivosti i oportunističkog kradljivca informacija. Stegoloader je u mnogim aspektima čudan, izbjegava alate za analizu i sigurnosne softvere te postavlja samo potrebne module, bez njihova zapisa na disku, a izvršavanje se događa kada napadač to odluči.

4.9. Ztorg

Istraživanje ovog zlonamjernog softvera započeto je kada je otkrivena Pokemon GO Guide aplikacija na Google Play trgovini, [28]. Popularnost ove aplikacije bila je golema upravo zbog toga što je igra Pokemon GO pokrenula revoluciju i bilježila je izrazito velik broj korisnika u cijelom svijetu, čak njih oko 45 000 000, [29]. Također, valja napomenuti kako Pokemon Go Guide nije bila jedina zaražena aplikacija. Prva aplikacija zaražena ovim zlonamjernim softverom bila je Privacy Lock, koja se pojavila na Google Play trgovini u prosincu 2016. godine, ujedno je to bila i jedna od najpopularnijih modifikacija zlonamjernog softvera Ztorg, koja je instalirana u više od milijun navrata. Zabrinjavajući podatak je upravo taj kako su te zaražene aplikacije brzo postajale popularne, svakog dana je bilježeno tisuće novih korisnika, [28].

Ztorg predstavlja zlonamjerni softver kojemu je cilj, čim se aplikacija preuzme, dobiti administratorska prava na uređaju. Korisnike je najviše privukla obavijest da u slučaju instaliranja aplikacije (koje je bila zaražena Ztorgom, a da to nisu znali) s Google Play trgovine dobiju 0,04 ili 0,05 USD. Aplikacija prima razne ponude koje dolaze s poslužitelja. Zlonamjerne ponude šalju se iz poznatih oglasnih usluga. Kada se klikne na instaliranje, obaviti će se preusmjeravanja (u jednom slučaju ih je zabilježeno 27) do stranice na kojoj se nalazi konačni URL koji vodi do Google Play trgovine.

Zlonamjerni virus Ztorg prenesen je u Google Play trgovinu kroz više od 100 različitih aplikacija. Najnovije aplikacije koje sadrže Ztorg pojavile su se u travnju 2017. godine. Sve vrste ovoga zlonamjernog softvera distribuirane su putem mreža za oglašavanje. Sve su kampanje sadržavale isti URL, tako da je bilo lako otkriti sve nove zaražene aplikacije. Ztrog nije u potpunosti iskorijenjen s Interneta, ali u velikoj većini je, međutim ima modularnu arhitekturu i koristi nekoliko različitih modula s raznim funkcionalnostima, a svaki do njih se može ažurirati putem Interneta, [24].

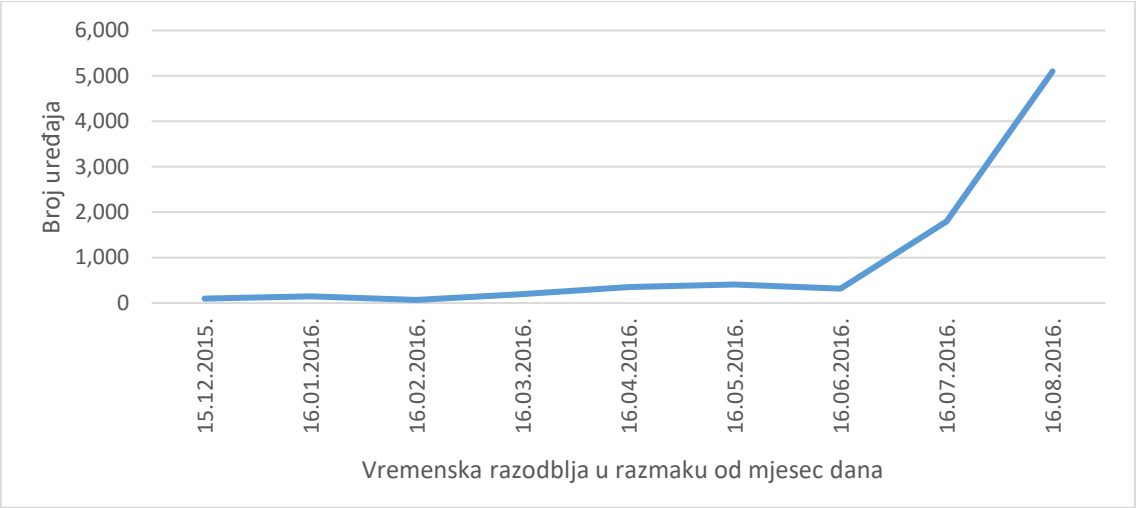
4.10. Gugi

Nove izmjene koje su se dogodile unutar zlonamjerne obitelj trojanskog zlonamjernog softvera namijenih mobilnom bankarstvu predstavlja Gugi. U tada novom operativnom sustavu Android 6, mogao je zaobići dvije nove sigurnosne značajke: prekrivanje aplikacija temeljnih na odobrenju i zahtjev za dinamičkim dopuštanjem opasnih aktivnosti unutar aplikacija kao što su SMS ili pozivi. Izmjena ne koristi nikakve ranjivosti sustave, veće se bazira na socijalnom inženjeringu.

Trojanski napad Gugi se uglavnom širi putem SMS poruka koje korisnike preusmjeravaju na *phishing* web stranice s karakterističnom porukom: „Dragi korisnici, dobivate MMS fotografiju! Možete pogledati klikom na sljedeći *link.*“ Klikom na tu vezu započinje preuzimanje Gugi Trojanskog napada na korisnikov Android uređaj. Kako bi zaštitio korisnike od utjecaja *phishing* i *ransomware* napada, operacijski sustav Android 6 je predstavio zahtjev za aplikacije da zatraže dopuštenje za dodavanje svojih vlastitih prozora nad drugim aplikacijama. U ranijim verzijama operacijskog sustava događalo se to da su automatski uspjeli prekrivati druge aplikacije. Konačni cilj ovoga zlonamjernog softvera je preklapanje bankovnih aplikacija s prozorima za zaštitu od krađe identiteta kako bi ukrali vjerodajnice korisnika za mobilno bankarstvo, a također prekriva i službenu aplikaciju Google Play trgovine da ukrade pojedinosti o kreditnim karticama za platne usluge. Gugi dobiva potrebna dopuštenja za preklapanje prisiljavajući korisnike da mu to omoguće te se zatim koristi za blokiranje zaslona dok traži sve opasnije pristupe.

Prva stvar koju zaražen korisnik vidi je prikazan prozor s tekstom „Dodatna prava potrebna su za rad s grafikom i prozorima“ i jednim gumbom kojeg je moguće kliknuti „Omogući“. Nakon što se klikne taj gumb, korisniku se otvara dijaloški okvir koji autorizira prekrivanje aplikacije. No, čim korisnik dozvoli zlonamjernom softveru to dopuštenje, automatski će mu blokirati uređaj i prikazati svoj prozor nad svim ostalim prozorima. Korisniku nije pružena niti jedna druga mogućnost osim da klikne na jedini gumb „Aktiviraj“. Kad korisnik ponovno klikne na ovaj gumb, dobiti će kontinuirani niz zahtjeva za sva prava koja traži zlonamjerni softver, a dok mu ih sve ne odobri ne vraća se na glavni izbornik. Primjerice, pojavljuje se zahtjev za administratorskim pravima na uređaju, što Gugi koristi kao samoobranu u svrhu teže deinstalacije aplikacije. Zatim slijede zahtjevi za odobravanjem slanja i pregleda SMS poruka te upućivanje poziva. U slučaju da se zahtjevi ne odobre, Gugi onemogućuje zatvaranje tog prozora, a nakon nekog izgledno vremena potpuno će blokirati zaraženi uređaj. U takvom slučaju, korisnikova jedina opcija je ponovno pokretanje uređaja u sigurnosnom načinu rada i pokušati deinstalirati zlonamjerni softver.

S izuzetkom sposobnosti da zaobiđe sigurnosne značajke operacijskog sustava Android 6, Gugi je tipični predstavnik zlonamjernog bankarskog softvera. Obuhvaća aplikacije s *phishing* prozorima kako bi ukrao vjerodajnice za mobilno bankarstvo ili informacije o platnim karticama te također krade SMS poruke i kontakte. Obitelj ovoga zlonamjernog softvera poznata je od prosinca 2015. godine, dok je ova verzija prvi put otkrivena u lipnju 2016. godine. Gugi uglavnom napada korisnike u Rusiji, više od 93% žrtava je baziranu upravo u toj zemlji, a tijekom kolovoza 2016. godine zabilježeno je deset puta više žrtava nego u travnju te iste godine, što prikazuje grafikon 5, [30].



Grafikon 5. Broj zaraženih uređaja od strane zlonamjernog softvera Gugi
Izvor: [31]

4.11. SMiShing

U Južnoj Americi kiberetičkim kriminalcima interesantno područje predstavljaju korisnici koji koriste mobilno bankarstvo, a uz tu granu vezan je ogroman porast registriranih incidenata, pogotovu u Brazilu, u zadnje dvije godine. Kako bi izvršili ovakve vrste napada služe se opcijom SMiShing koja predstavlja *phishing* napade koji su producirani putem SMS-a, [32].

U 2015. godini, upotreba mobilnog bankarstva u Brazilu dosegla je 11,2 milijardi transakcija, što je povećanje od 138 posto u odnosu na 2014. godinu. Mobilno bankarstvo trenutno je druga najpopularnija metoda za pristup bankovnim računima u toj zemlji. Ogroman broj korisnika i ovakve zapažene brojke privlačne su kibernetičkim kriminalcima koji ulažu svoje vrijeme i napore u stvaranju novih napada, a SMS poruke predstavljaju im najjednostavniju i najjeftiniju metodu da obuhvate toliku količinu uređaja, [32]. Ovaj zlonamjerni softver zastupljen je u Brazilu, no postoji mogućnost da se pojavi u bilo kojem dijelu svijeta i bude prilagođen određenoj zemlji.

Prilikom provođenja ovoga zlonamjernog programa, prvi koraci ne zahtijevaju puno novca ili pripreme: prvo je potrebno registrirati domenu (obično se koristi .mobi domena), pripremiti stranicu za krađu identiteta (*phishing* stranicu) namijenjenu mobilnom formatu te angažirati skupnu SMS uslugu. Telefonski brojevi korisnika, koji predstavljaju jednu od važnijih karika u ovakvom napadu, mogu se pribaviti na crnom tržištu ili se mogu dobiti u napadima gdje se aplikacija WhatsApp, koja je namijenjena komuniciranju, koristi kao mamac. Poruke koje SMiShing šalje primatelju, obavještavaju ga da su bankovni račun ili kreditna kartica blokirani te se na kraju poruke nalazi link koji će korisnika, u slučaju da klikne na njega, preusmjeriti na *phishing* stranicu. Mobilne verzije ovih *phishing* web stranica za bankarstvo otvaraju se ispravno, što olakšava krađu korisničkih akreditiva. Taktika napadača je prisiliti korisnika da pristupi web stranici putem svojeg mobilnog uređaja, a ne putem radne površine odnosno računala, no ako se pokuša spojiti na taj način, stranica će pokazati

da usluga nije dostupna. Jedina preostala opcija im upravo ona koja će im nanijeti štetu, a to je ujedno i jedni način da se stranica ispravno i kompletno pokrene, a to su mobilni uređaji. Kibernetički kriminalci stvaraju *phishing* stranice za nekoliko bankarskih tvrtki kako bi postigli jednu opsežnost korisnika i time si povećali šanse za uspješnim napadom, [24].

4.12. Fusob

U travnju 2016. godine, Fusob je postao najpopularniji mobilni trojanski napad: korisnici u više od 100 zemalja širom svijeta bili su meta napada ovoga zlonamjernog programa. Potrebno je napomenuti da se prilikom izvršavanja ovoga zlonamjernog programa prvo provjerava jezik uređaja, jer postoje neki jezici odnosno zemlje za koje je programiran da ne izvršava zlonamjerne radnje, a u te države spadaju: Kazahstan, Azerbajdžan, Bugarska, Gruzija, Mađarska, Ukrajina, Rusija, Armenija i Bjelorusija. Ako se zemlja u kojoj se uređaj nalazi nije jedna od ranije navedenih, program traži administratorska prava na uređaju i prikazuje poruku da se uređaj ažurira, a uređaj se može i dalje koristiti, ali zlonamjerni softver blokira pristup postavkama tako da ih prekriva sa svojim vlastitim prozorom i na taj način se štiti od uklanjanja.

U međuvremenu, zlonamjerni softver prikuplja informacije o uređaju i šalje ih napadačima. Prvi set podataka sadrži informacije o uređaju, kao što su: model uređaja, operacijski sustav, inačica operacijskog sustava, itd. Drugi set podataka sastoji se od lokacije uređaja odnosno korisnika i zapisa poziva s imenima s popisa kontakata. Nakon prikupljanja podataka, čeka se naredba napadača kako bi se uređaj blokirao. Nakon što je uređaj blokiran pojavit će se pripadajući zaslon, kako je prikazano na slici 20, te uz blokiranje postoje i druge raspoložive funkcije kojima se ovaj zlonamjerni softver služi, ali dvije uzrokuju posebnu zabrinutost. To su: mogućnost fotografiranja pomoću prednje kamere uređaja i mogućnost instaliranja prethodno preuzetih datoteka, [33].

Slika 20. Poruka na zaslonu uređaja prikazana od strane Fusob *ransomwera*, [33]

Napadači obično traže otkupninu u vrijednosti između 100 i 200 USD za deblokiranje uređaja. Način plaćanja otkupnine je u obliku kodova s *prepaid* iTunes kartica. Obitelj ovakvog zlonamjernog softvera se širi putem web stranica (uglavnom stranice sa sadržajem za odrasle). Prema [33], kao vrste zaštite od Fusoba navode se:

- *back-up* (stvaranje sigurnosne kopije) podataka na uređaju
- korištenje pouzdanog sigurnosnog rješenja odnosno antivirusnog softvera
- redovito ažuriranje uređaja i njegovih pripadajućih aplikacija
- obraćanje pažnje na datoteke koje se preuzimaju putem Interneta i na izvore s kojih se preuzimaju
- informiranje o novim načinima napada kojima se kriminalci služe

4.13. Dvmap

Dvmap, zlonamjerni program koji se distribuira putem Google Play trgovine što jasno upućuje na to da su meta Android uređaji, predstavlja jedan od naprednijih vrsti *rooting* zlonamjernog softvera. Ono što ga čini zanimljivim je mogućnost, ne samo instaliranja njegovih zlonamjernih modula u sustav nego i u knjižnice sustava (engl. *System libraries*) te ga je upravo ova potonja mogućnost učinila prvim zlonamjernim softverom za Android koji ubacuje zlonamjerni kod u knjižnicu sustava i s Google Play trgovine preuzet je više od 50 000 puta.

Autori ovoga zlonamjernog softvera koristili su jednu zanimljivu metodu pomoću koje su zaobišli sigurnosne provjere od strane Google Play trgovine: u početku su prenijeli „čistu“ aplikaciju na trgovinu krajem ožujka 2017. godine, a zatim su je u kratkom vremenskom razdoblju ažurirali zlonamjernom verzijom. Upravo je ovakva prijevara bila izvedena najmanje pet puta u razdoblju između 15. travnja i 15. svibnja iste godine.

Ovaj zlonamjerni softver prolazi kroz dvije faze koje se dijele na: početnu i glavnu fazu. Unutar početne faze, pokušava dobiti *root* prava na uređaju i instalirati zlonamjerne module s različitim funkcionalnostima u sustavu. Ovisno o verziji sustava, mogu biti instalirana tri ili četiri paketa datoteka, a ako te datoteke steknu *root* prava, Dvmap će instalirati nekoliko alata u sustav skupa sa zlonamjernom aplikacijom. U drugoj fazi, odnosno glavnoj, pokreće se zlonamjerna datoteka koja provjerava verziju instaliranog sustava i odlučit će koja bi se knjižnica sustava trebala ažurirati novom zakrpom. Tijekom instaliranja zakrpe, zlonamjerni softver će prebrisati postojeći kod sa zlonamjernim, a ova faza se smatra opasnom i može uzrokovati gašenje uređaja koji će zatim zlonamjerni softver ponovno pokrenuti i u startu zamijeniti originalne datoteke sa zlonamjernim.

Tvrtka Kaspersky Lab prijavila je prijetnju, koja je uočena u travnju 2017. godine, Googleu i uklonjena je iz službene trgovine u najkraćem roku. Pretpostavlja se da je glavna svrha ovoga zlonamjernog softvera bila je ta da mu se omogući pristup sustavu i izvršavanje određenih datoteka s *root* pravima. Međutim, smatra se kako se ovaj zlonamjerni softver još uvijek testira jer postoje neke tehnike koje doslovno mogu

uništiti zaražene mobilne uređaje, ali unatoč tome velik je broj uređaja korisnika koji su već zaraženi tako da je na njima moguće isprobati novitete, [34].

4.14. Svpeng

Sredinom srpnja 2017. godine pronađena je nova modifikacija već poznate obitelji zlonamjernog softvera za mobilno bankarstvo, a to je Svpeng Trojan - Banker.AndroidOS.Svpeng.ae. U ovoj izmjeni kibernetički kriminalci su dodali novu funkcionalnost koja se odnosi da ima mogućnost rada i kao *keylogger*, kradući uneseni tekst kroz korištenje usluga pristupačnosti.

Usluge pristupačnosti uglavnom pružaju poboljšanja korisničkog sučelja korisnicima s invaliditetom ili onima koji privremeno ne mogu biti u potpunoj interakciji s uređajem primjerice zbog vožnje. Zlouporaba ove značajke sustava omogućuje trojanskom napadu, ne samo da ukrade uneseni tekst iz aplikacija instaliranih na uređaju, već i da sam odobri ovlasti i prava te se suprotstavlja pokušajima deinstalacije trojanskog softvera, [33].

Aktualni podaci o napadu upućuju na to da ovaj zlonamjerni softver još uvijek nije široko rasprostranjen. U razdoblju od tjedan dana, kako navodi [35], uočen je mali broj korisnika koji su napadnuti, a što se zemalja tiče obuhvaćeno je njih 23. Većina korisnika bila je u Rusiji (29%), Njemačkoj (27%), Turskoj (15%), Poljskoj (6%) i Francuskoj (3%). Zanimljiva je činjenica i važno je za napomenuti, iako se većina napadnutih korisnika nalazila u Rusiji, ovaj zlonamjerni softver ne funkcionira na uređajima koji se izvode na ruskom jeziku.

Svpeng, kao zlonamjerna programska obitelj, poznata je po inovativnosti. Počevši od 2013. godine, među prvima počela je napadati SMS bankarstvo, upotrebljavajući *phishing* stranice za krađu identiteta kako bi prikrile druge aplikacije i ukrali vjerodajnice te blokirali uređaje i potraživali novac. Godine 2016., kibernetički kriminalci su aktivno distribuirali Svpeng putem AdSense programa koristeći ranjivosti u Internet pregledniku Google Chrome te zbog toga Svpeng postaje jedna od najopasnijih mobilnih vrsta zlonamjernog programa, [33].

4.14.1. Postupak napada

Nakon pokretanja, Trojan - Banker.AndroidOS.Svpeng.ae provjerava se jezik uređaja i ako nije ruski, pita uređaj za dopuštenje za korištenje usluga pristupačnosti. Prilikom zloupotrebe ove privilegije, može se učiniti mnogo štetnih stvari. On sam odobrava administratorska prava na uređaju, instalira se kao zadana SMS aplikacija i dodjeljuje si neka dinamička dopuštenja koja uključuju mogućnosti slanja i primanja SMS poruka, upućivanja poziva i čitanje kontakata. Nadalje, korištenjem novonastalih sposobnosti trojanski napad može blokirati svaki pokušaj uklanjanja administratorskih ovlasti na uređaju, čime se sprječava njegova deinstalacija, a to nam govori koliko njegova struktura kompleksna i konkretno napravljena da se ugrozi korisnika. Zanimljivo je da time i blokira svaki pokušaj dodjeljivanja ili uklanjanja administratorskih ovlasti uređaja za bilo koju drugu aplikaciju.

Korištenje usluga pristupačnosti Svpengu omogućuje pristup korisničkom sučelju drugih aplikacija i da ukrade njihove podatke, kao što su elementi sučelja i njihov sadržaj, ako je dostupan, a to uključuje unesene tekstualne podatke. Osim toga, snimka zaslona pravi se svaki put kada korisnik pritisne gumb na tipkovnici i prenosi se na poslužitelja kojim upravlja zlonamjerna strana, a moguće je i korištenje fotoaparata uređaja. Veliki problem predstavlja to što, ne samo da podržava Android tipkovnicu, već i tipkovnice trećih strana. Neke aplikacije, prvenstveno vezane za bankarstvo, ne dopuštaju snimanje zaslona. U takvim slučajevima, Svpeng ima još jednu opciju kojom se može poslužiti kako bi ukrao podatke - pokreće vlastiti *phishing* prozor preko napadnute aplikacije, [33].

4.14.2. Distribucija i zaštita

Trojan - Banker.AndroidOS.Svpeng.ae se distribuira od strane malicioznih web stranica kao lažni *flash player*. Njegove zlonamjerne tehnike rade čak i na potpuno ažuriranim uređajima s najnovijom inačicom Androida i svim instaliranim sigurnosnim ažuriranjima. Trenutno je napravljen samo za uređaje koji dolaze s Android operativnim sustavom. Najbolje zaštita su razni antivirusni softveri koji imaju mogućnost njegova deinstaliranja, ali prvenstveno pažanja korisnika koja se odnosi na aplikacije koje instaliraju na svoje uređaje te koje web stranice posjećuju, [33].

4.15. Tablice karakteristika zlonamjernog softvera

Tablica 1. Osnovne karakteristike zlonamjernog softvera

Zlonamjerni softver	Karakteristike					
	Daljinsko upravljanje	Krađa podataka	Snimanje zaslona	Zaključavanje uređaja	Šifriranje datoteka	Bilježenje lozinki
Zeus	DA	DA	DA	NE	NE	DA
CryptoLocker	NE	NE	NE	DA	DA	NE
Citadel	DA	DA	NE	NE	NE	DA
Sakula	DA	NE	NE	DA	DA	NE
TeslaCrypt	NE	NE	NE	DA	DA	NE
Stels	NE	DA	NE	NE	NE	NE
CryptoWall	NE	DA	NE	NE	DA	NE
Stegoloader	NE	DA	NE	NE	NE	DA
Ztorg	NE	NE	NE	NE	NE	NE
Gugi	NE	DA	NE	DA	NE	DA
SMiShing	NE	DA	NE	NE	NE	DA
Fusob	NE	NE	NE	DA	NE	NE
Dvmap	NE	NE	NE	NE	NE	NE
Svpeng	NE	DA	DA	DA	NE	NE

Tablica 2. Dodatne karakteristike zlonamjernog softvera

Zlonamjerni softver	Karakteristike		
	Administratorska prava	Dodatne mogućnosti	Distribucija
Zeus	NE	NE	e-mail, web
CryptoLocker	NE	NE	e-mail
Citadel	NE	NE	e-mail, web
Sakula	NE	preuzimanje datoteka, izvršavanje dodatnih komponenti	aplikacije, web
TeslaCrypt	NE	NE	web
Stels	NE	upravljanje pozivima i SMS uslugom, instaliranje dodatnih komponenti	aplikacije, e-mail, web
CryptoWall	NE	NE	e-mail, web
Stegoloader	NE	bilježi sve aktivnosti	web
Ztorg	DA	NE	aplikacije, web
Gugi	DA	upravljanje pozivima, SMS uslugom i kontaktima	SMS, web
SMiShing	NE	NE	SMS, web
Fusob	NE	bilježi lokaciju i popise poziva, koristi kameru	web
Dvmap	DA	NE	aplikacije
Svpeng	DA	upravljanje pozivima i SMS uslugom, bilježi uneseni tekst putem tipkovnice, koristi kameru	web

5. Mogućnosti zaštite terminalnih uređaja

U cilju da korisnici bezbrižno koriste terminalne uređaje, potrebna je određena vrsta zaštite. Sigurnost koja se prezentira putem određenih vrsta zaštite nalazi se na visokoj razini. Korisnici u velikoj mjeri nisu svjesni prijetnji s kojima se danas mogu susresti u tehnološkom svijetu, a da ne govorimo o njihovim posljedicama. Svijest korisnika o prijetnjama može se podignuti informiranjem i njihovom edukacijom.

5.1. Sigurnost mreža

S brzim porastom interesa za pristupom Internetu, sigurnost mreža postala je glavna briga tvrtki širom svijeta. Činjenica je da su informacije i alati, potrebni za prodiranje sigurnosti korporativnih mreža pa tako i privatnih, široko dostupni te su povećali zabrinutost. Zbog povećanog fokusa na mrežnu sigurnost, mrežni administratori ulažu velike napore prilikom zaštite mreža, a također moraju biti u toku s novim prijetnjama jer alati ne pružaju stopostotnu zaštitu od svih napada, [36]. Stvaranjem nove mreže, mrežni rukovoditelj mora napraviti mrežnu sigurnosnu policu, a svaka mreža mora biti klasificirana, prema [37], kao jedna od sljedećih:

- pouzdana
- nepouzdana
- nepoznata

5.1.1. Pouzdana mreža

Pouzdane mreže su one mreže koje se nalaze unutar sigurnosnog mrežnog perimetra. Ovakve mreže su one koje se nastoje zaštiti. Unutar pouzdanih mreža, netko je administrator koji nadgleda računala koja se priključuju na ovakvu mrežu, a netko tko nadgleda mrežu upravljanja njihovim sigurnosnim mjerama. Prilikom postavljanja ovakvog tipa mreže, postavlja se vatrozid (engl. *firewall*) koji je često povezan s poslužiteljem, kojim se utvrđuje identitet određene mreže koje su vezane za sam server pomoću mrežnih kartica adaptera. Nakon postavljanja konfiguracije, pouzdana mreža uključuje vatrozid server i sve mreže koje dolaze nakon njega.

Iznimka kod ovakvog pravila je VPN, virtualna privatna mreža, koja je pouzdana mreža koja prenosi podatke preko nepouzdane mrežne infrastrukture. Mrežni paketi koji se pojavljuju na virtualnoj mreži smatraju se kao da dolaze unutar mrežnog perimetra koji je ranije spomenut. Porijeklo je ustvari logično zbog samog načina na koji su VPN mreže uspostavljene. Za komunikaciju koja dolazi od ovakvih mreža, sigurnosni mehanizmi moraju postojati da bi vatrozid servera mogao dokazati autentičnost porijekla, ispravnost podataka i druge sigurnosne principe unutar mrežnog prometa da bi se dokazala sigurnost ovakve mreže, [37].

5.1.2. Nepouzdana mreže

Nepouzdana mreža je mreža koje se nalazi izvan sigurnosnog perimetra. One su nepouzdane iz razloga što su izvan područja kontrole. Ne postoji kontrola nad administracijom ili sigurnosna polica. To su privatne, dijeljene mreže od kojih se nastoji zaštiti određena mreža, iako postoji mogućnost komunikacije između pouzdanih i nepouzdanih mreža, [37].

5.1.3. Nepoznata mreža

Nepoznate mreže su mreže koji nisu niti pouzdane niti nepouzdane. Nepoznate su vatrozidu upravo zbog toga što se ne mogu odrediti kojeg su tipa pa spadaju u zasebnu kategoriju. Nepoznate mreže postoje izvan sigurnosnog perimetra. Sve nepouzdane mreže smatraju se kao nepoznate mreže i vatrozid primjenjuje sigurnosna pravila unutar Internet čvora u korisničkom sučelju, koji određuje sve nepoznate mreže, [37].

5.2. Sigurnosni nedostaci spajanja na Internet

Spajanjem određenom mrežom na Internet, fizički se povezujemo na nekoliko desetaka tisuća nepoznatih mreža. Otvoren pristup takvim mrežama omogućuje dijeljenje raznovrsnih korisnih aplikacija i veliku priliku za dijeljenje informacija, ali većina privatnih mreža sadrži podatke koji nisu namijenjene dijeljenju ostalim korisnicima na mreži, jer nisu svi korisnici vezani uz zakonske akte i podatke bi mogli iskoristiti u ilegalne svrhe.

Povjerljive informacije obitavaju na dvije lokacije u mreži. Jedan način je da se one nalaze na fizičkom mediju, kao što su hard disk ili memorija, ili mogu se nalaziti u prijenosu preko fizičkog medija u formi paketa. Ova dva stanja informacija predstavljaju višestruku mogućnost za napade od korisnika na istoj mreži ili od onih koji se koriste Internetom. Postoji pet uobičajenih metoda napada koji predstavljaju mogućnost kompromitiranja informacija na mreži, [37]:

- presretanje mrežnih paketa
- IP *spoofing*
- napad na šifre
- distribucija osjetljivih informacija prema vanjskih izvorima
- napadi „čovjek u središtu“

Presretanje mrežnih paketa je presretanje paketa u mreži prilikom komunikacije unutar mreže. Prilikom slanja podataka oni se dijele u manje dijelove i oni se nazivaju paketi, međutim slanjem takvih paketa određenim mrežnim aplikacijama ne omogućuje enkripciju tih istih paketa i oni se mogu presresti od neke druge aplikacije i proslijediti u drugu mrežu.

IP *spoofing* napadi se pojavljuju kada se napadač izvan mreže pokušava prikazati kao pouzdano računalo. Ovakav napad olakšan je koristeći IP adresu koja je unutar raspona IP adrese određene mreže ili korištenjem autorizirane vanjske IP adrese koja je pouzdana i kojom se želi omogućiti pristup određenom izvoru na mreži.

Napadi na šifre mogu se implementirati na nekoliko načina, uključujući *brute-force* napade (koji uključuje program sličan rječniku i pokušava određenim kombinacijama unaprijed definiranim izrazima ostvariti upad), trojanske napade, IP *spoofing* i presretanje mrežnih paketa.

Distribucija osjetljivih podataka, posebno je zanimljiva u poslovnim okruženjima, a predstavlja izrazito bitne podatke čija je zaštita prioritet.

Napadi „čovjek u središtu“ opisuju se kao napadi u kojima je čovjek koji je zadužen za nadzor mreže i ima pristup sustavu, neovlašteno ostvari pristup podacima na samoj mreži.

5.3. Antivirusna zaštita

Antivirusna zaštita, odnosno antivirusni softveri, navedeni su kao [13] posebna kategorija programa čija je osnovna namjena identifikacija, neutralizacija i eliminacija zlonamjernog programa koji se mogu infiltrirati u korisničke uređaje i napraviti štetu. Kao temeljna zadaća antivirusnog programa navodi se prepoznavanje zlonamjernog programa i zaštita sustava od njegovog daljnjeg djelovanja. Ako je uređaj zaražen zlonamjernim programom, tada ga antivirusni program mora izolirati i ukloniti. Upravo za njihovo prepoznavanje koriste se unaprijed definirane definicije određenih tipova zlonamjernog softvera.

Svaki zlonamjerni program karakteriziran je određenim slijedom znakovnih kodova, zbog toga što je i sam zlonamjerni softver u osnovi računalni program. Nakon detekcije sekvenci zlonamjernog softvera u određenoj datoteci na uređaju, prema [13], antivirusni program će pokušati napraviti jedan od sljedećih koraka:

- popraviti datoteku brišući iz nje zlonamjerni program
- staviti datoteku u karantenu te joj tako onemogućiti pristup dostupnim programima pa se samim tim ni infekcije dalje ne može širiti
- te naposljetku izbrisati inficiranu datoteku

Zlonamjerni softver nije uvijek jednak, on se razvija i dobiva poboljšane inačice što za korisnike predstavlja velik problem. Bazu definicije zlonamjernog softvera i njihovih kodova potrebno je stalno osvježavati i nadopunjavati, uglavnom više puta dnevno. Taj posao umjesto korisnika odrađuje sam antivirusni program. U slučaju da se definicije ne bi osvježavale, antivirusni program neće biti u mogućnosti prepoznati novonastale inačice zlonamjernog programa. Problem ne osvježavanja njihovih definicija je glavni razlog stalnog širenja ranije poznatih vrsta zlonamjernog programa.

U igri između mehanizama za detekciju zlonamjernog programa i samih virusa, programeri kao njihovi tvorci, često stvaraju oligomorfne, polimorfne ili metamorfne verzije. Pojašnjenje takvih virusa je taj da oni mijenjaju oblik i programski kod, nastojeći ostati nezapaženi kako nastaju njihovi novi oblici i verzije.

Drugi način rada antivirusnog programa je nadzor ponašanja svih programa. Ako neki program pokuša zapisivati podatke u izvršni kod nekog drugog programa, pristupati mreži ili pokušati slati podatke, antivirusni program će to dojaviti korisniku. Ovakvim pristupom zaštita se proširuje i na one zlonamjerne programe čije definicije nisu ranije navedene u bazi podataka. Problem ovakvog pristupa je u tome što se može dogoditi da se sasvim legitimne akcije okarakteriziraju sumnjivima, [13].

5.4. Kriptografija

U svijetu umrežavanja i telekomunikacija, kriptografija, kako navodi [27], je proces sigurnog prijenosa podataka preko mreže na takav način da, ako su podaci presretnuti, ne može ih se pročitati od strane neovlaštenih korisnika. Kriptografija uključuje dva komplementarna procesa:

- enkripciju/šifriranje: proces preuzimanja podataka i njihovo modificiranje tako da ih nepoželjni korisnici ne mogu čitati
- dekripciju/dešifriranje: proces preuzimanja šifriranih podataka i pretvaranje u čitljiv oblik pouzdanim korisnicima

Enkripcija i dekripcija podataka obavljaju se pomoću algoritama i ključeva. Algoritam, kao niz matematičkih koraka koji izokreću podatke, temeljni je matematički proces koji stoji iza kriptografije. Postoji niz kriptografskih algoritama koji su razvijeni na temelju različitih matematičkih procesa pa tako neki algoritmi rezultiraju jačom enkripcijom naspram drugih – što je algoritam jači to je teže dešifrirati podatke. Enkripcijski algoritmi uključuju matematičke vrijednosti koje se nazivaju ključevi.

Raniji kriptografski sustavi bili su se enkripcijski sustavi tajnih ključeva u kojima su samo sudionici, uključeni u prijenos i primanje, znali tajne ključeve. Taj ključ se morao na neki način sigurno prebaciti svakome tko je trebao dešifrirati poruku. To je bio glavni nedostatak kriptografskog sustava tajnih ključeva. Danas, većina kriptografije uključuje proces nazvan šifriranje javnog ključa, koji koristi dvije različite vrste ključeva, [27]:

- javni ključ, koji se distribuira svakom korisniku koji ga potražuje
- privatni ključ, koji je poznat samo vlasniku

Da bi šifrirana poruka bila poslana, pošiljatelj koristi svoj privatni ključ za šifriranje podataka, a primatelj koristi javni ključ pošiljatelja za dekriptiranje. Slično tome, primatelj može vratiti odgovor izvornom pošiljatelju pomoću javnog ključa pošiljatelja za šifriranje odgovora, a izvrni pošiljatelj koristi njegov privatni ključ za dekriptiranje. Dvije vrste napada mogu ugroziti enkripciju, a to su: kriptoanaliza, koja je temeljena na svojstvima algoritama za šifriranje i *brute-force* napadi, koji uključuju pokušaje implementiranja svih mogućih kombinacija ključeva.

Simetrična enkripcija, poznata i pod nazivima kao konvencionalna enkripcija ili enkripcija jednim ključem, bila je jedina vrsta enkripcije u upotrebi prije razvoja šifriranja pomoću javnih ključeva sedamdesetih godina 20. stoljeća. Ova vrsta enkripcije ostaje daleko najčešće korištena metoda enkripcije. Simetrično šifriranje pretvara čiste podatke ili tekst u šifrirane, koristeći tajni ključ i algoritme šifriranja. Upotrebljavajući taj isti tajni ključ i algoritme za dešifriranje te se iz šifriranog dobiva se prvobitni oblik podatka ili teksta.

S druge strane imamo asimetričnu enkripciju, koja pretvara čiste podatke ili tekst u šifrirani koristeći jedan od dva ključa i algoritam šifriranja. Korištenjem drugog uparenog ključa i algoritama za dešifriranje, kriptirani podaci vraćaju se u prvobitno stanje. Naziva se još i kriptografija s javnim ključem. Upravo korištenje dvaju ključeva

ima duboke posljedice u područjima povjerljivosti i autentifikacije, čime je sigurnost dobila nove razine, [38].

5.5. Svijest korisnika

Zlonamjerni softver postaje sve sofisticiraniji i njihovi napadi imaju za cilj ostati neotkriveni i napraviti štetu unutar sustava u kojem se nalaze. Infiltracijom u određene sustave, sigurnost korisničkih podataka dolazi u pitanje. Sveobuhvatnim korištenjem mobilnih uređaja u svakodnevnom životu korisnici pohranjuju osobne podatke unutar njih, kao i ostale multimedijalne sadržaje, a to predstavlja primamljivu metu za hakere. Krajnji korisnici teško mogu sami prepoznati zlonamjerne napade, osim u slučaju zaključavanja zaslona uređaja, što znači da tijekom korištenja uređaja mogu biti u središtu napada, a da pritom nisu toga svjesni. Svijest korisnika o prisustvu zlonamjernog softvera u tehnološkom svijetu mobilnih uređaja, potrebno je podignuti na višu razinu.

Sigurnost sustava i uređaja se ne može jamčiti, a potencijalni rizici koji se pojavljuju sa zlonamjernim napadima mogu imati značajne posljedice za krajnje korisnike. Upravo je svijest korisnika jedan od načina obrane od zlonamjernog softvera čime bi korisnici bili upoznati za zlonamjernim softverom koji prijeti njihovim uređajima i podacima. Korisnici ne razmišljaju o tome da mogu biti žrtve zlonamjernih napada, a upravo je ljudski faktor jedna od najvećih prijetnji informacijskim sustavima i uređajima. Podizanjem svijesti korisnika određenim educiranjem o opasnostima koje nam donosi tehnologija moguće je smanjiti vjerojatnost zlonamjernih napada sa nepovoljnim ishodom za korisnike. U međuvremenu krajnji korisnici se moraju pouzdati u antivirusnu zaštitu na svojim uređajima i nadati se da svojom nepažnjom neće postati žrtve zlonamjernog softvera, [39].

6. Zaključak

Zlonamjerni softver, tzv. *malware*, predstavlja sve prisutniju opasnost od napada koji za cilj imaju infiltraciju određenih sustava i nanošenja štete krajnjim korisnicima. S razvojem tehnologije dolazi i do razvoja zlonamjernog softvera, koji tako održavaju korak s tehnološkim napretkom te pokušavaju iskoristiti njezine slabosti i mane. Značajnim rastom broja korisnika mobilnih uređaja otvara se šire područje djelovanja zlonamjernog softvera, što predstavlja sve veću prijetnju sigurnosti mobilnih uređaja. Kao krajnji cilj zlonamjernog softvera ističe se financijska profitabilnost i krađa identiteta, što donosi velike financijske gubitke kako pojedincima, tako i svjetskom gospodarstvu.

Učestalost pojavljivanja zlonamjernog softvera predstavlja sve veći izazov za korisnike kada je riječ o sigurnosti mobilnih uređaja. Mobilni uređaji sadrže niz pogodnosti za korisnike, no isto tako i sigurnosne nedostatke. Današnjim korisnicima omogućeno je da putem mobilnih uređaja obavljaju svakodnevne aktivnosti, od pristupa e-pošti do osjetljivih transakcija kao što su internetsko bankarstvo i plaćanja. Budući da korištenje mobilnih uređaja postaje masovno i korisnici postaju sve više ovisni o upotrebi istih, aktivnosti kibernetičkog kriminala su sve prisutnije što predstavlja izazov za sigurnosne stručnjake u borbi protiv zlonamjernog softvera. Obrađene vrste zlonamjernog softvera u ovome radu prikazane su međusobnom usporedbom pokazujući na različite karakteristike i drugačije ponašanje što potvrđuje njihovu raznovrsnost.

Razumijevanjem zlonamjernog softvera, od kojih su neki opisani u ovome radu, moguće je pružiti sigurnosnu zaštitu krajnjim korisnicima te tako smanjiti sigurnosne rizike s ciljem zaustavljanja ili onemogućavanja zlonamjernog softvera. Također bitno je podizanje svijesti krajnjih korisnika kroz edukaciju te informiranjem o novim, sve učestalijim, napadima putem zlonamjernog softvera. Time bi se korisnike upozorilo na načine prijenosa zlonamjernog softvera te ukazalo na mogućnosti zaštite i upotrebu antivirusnih softvera, kako bi se preveniralo njihovo daljnje širenje. Kroz razvoj alata za rano otkrivanje znakova prisutnosti zlonamjernog softvera osigurala bi se rana reakcija i odgovor na napad, čime bi se spriječio nastanak štete za sustav mobilnog uređaja, ali i korisnika.

Literatura

[1] Fling, B.: *Mobile Design and Development*, O'Rilley Media, SAD, 2009.

[2] URL: http://e-student.fpz.hr/Predmeti/T/Terminalni_uredaji/Materijali/03_Ranolikost_i_klasifikacija_terminalnih_uredjaja.pdf (pristupljeno: svibanj 2017.)

[3] URL: https://www.wareable.com/wearable-tech/what-is-wearable-tech-753 (pristupljeno: kolovoz 2017.)

[4] URL: https://www.statista.com/topics/3837/mobile-device-usage-in-europe/ (pristupljeno: lipanj 2017.)

[5] URL: http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals (pristupljeno: lipanj 2017.)

[6] URL: https://www.statista.com/statistics/430830/share-of-mobile-internet-traffic-countries/ (pristupljeno: srpanj 2017.)

[7] URL: https://www.statista.com/statistics/219030/mobile-traffic-per-year-in-europe-since-2010/ (pristupljeno: lipanj 2017.)

[8] URL: https://www.statista.com/statistics/271405/global-mobile-data-traffic-forecast/ (pristupljeno: lipanj 2017.)

[9] Laboratorij za sustave i signale, Fakulteta elektrotehnike i računarstva, Sveučilišta u Zagrebu: *Modeliranje sigurnosnih prijetnji (Threat modeling)*, Centar Informacijske Sigurnosti, Zagreb, 2012.

[10] URL: http://e-student.fpz.hr/Predmeti/T/Terminalni_uredaji/Materijali/10_-_Sigurnost_primjene_terminalnih_uredjaja_-_09122013.pdf (pristupljeno: svibanj 2017.)

[11] URL: https://ist.mit.edu/security/data_risks (pristupljeno: kolovoz 2017.)

[12] URL: http://www.electronicstakeback.com/wp-content/uploads/Facts_and_Figures_on_EWaste_and_Recycling.pdf (pristupljeno: svibanj 2017.)

[13] Bažant, A., Car, Ž., Gledec, G., Jevtić, D., Ježić, G., Kunštić, M., Lovrek, I., Matijašević, M., Mikac, B., Skočir, Z.,: *Telekomunikacije - tehnologija i tržište*, Element, Zagreb, 2007.

[14] Tulloch, M.: *Microsoft Encyclopedia of Security*, Microsoft, SAD, 2003.

[15] Peraković, D., Husnjak, S., Remenar, V.: *Research Of Security Threats In The Use Of Modern Terminal Devices*, DAAAM International, vol. 23, no. 1, 2012.

[16] URL: https://www.secureworks.com/research/zeus (pristupljeno: svibanj 2017.)

[17] URL: https://www.secureworks.com/research/cryptolocker-ransomware (pristupljeno svibanj 2017.)

[18] URL: https://www.bitcoin.com/ (pristupljeno: lipanj 2017.)

[19] URL: https://www.secureworks.com/research/updates-to-the-citadel-trojan (pristupljeno: svibanj 2017.)

[20] URL: https://www.secureworks.com/research/sakula-malware-family (pristupljeno: svibanj 2017.)

[21] URL: http://www.techadvisor.co.uk/test-centre/security/best-antivirus-2017-3651652/ (pristupljeno: lipanj 2017.)

[22] URL: https://www.secureworks.com/research/teslacrypt-ransomware-threat-analysis (pristupljeno: svibanj 2017.)

[23] URL: https://www.secureworks.com/research/stels-android-trojan-malware-analysis (pristupljeno: svibanj 2017.)

[24] URL: https://www.secureworks.com/research/cryptowall-ransomware (pristupljeno: svibanj 2017.)

[25] URL: https://www.secureworks.com/research/stegoloader-a-stealthy-information-stealer (pristupljeno: svibanj 2017.)

[26] URL: http://e.math.hr/stegano/index.html (pristupljeno: lipanj 2017.)

[27] URL: http://flylib.com/books/en/3.370.1.18/1/ (pristupljeno: svibanj 2017.)

[28] URL: https://securelist.com/ztorg-money-for-infecting-your-smartphone/78325/ (pristupljeno: svibanj 2017.)

[29] URL: https://zimo.dnevnik.hr/clanak/popularnost-igre-pokemon-go-u-stalnom-padu---448186.html (pristupljeno: srpanj 2017.)

[30] URL: https://securelist.com/banking-trojan-gugi-evolves-to-bypass-android-6-protection/75971/ (pristupljeno: svibanj 2017.)

[31] URL: https://securelist.com/gugi-from-an-sms-trojan-to-a-mobile-banking-trojan/76023/ (pristupljeno: svibanj 2017.)

[32] URL: https://securelist.com/smishing-and-the-rise-of-mobile-banking-attacks/75575/ (pristupljeno: svibanj 2017.)

[33] URL: https://securelist.com/ksn-report-mobile-ransomware-in-2014-2016/75183/ (pristupljeno: svibanj 2017.)

[34] URL: https://securelist.com/dvmap-the-first-android-malware-with-code-injection/78648/ (pristupljeno: svibanj 2017.)

[35] URL: https://securelist.com/a-new-era-in-mobile-banking-trojans/79198/ (pristupljeno: svibanj 2017.)

[36] URL: http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook#Security_Technologies (pristupljeno: lipanj 2017.)

[37] URL: http://docwiki.cisco.com/wiki/Security_Technologies#Trusted.2C_Untrusted.2C_and_Unknown_Networks (pristupljeno: lipanj 2017.)

[38] Stallings, W.: *Cryptography and Network Security: Principles and Practice, Fifth Edition*, Prentice Hall, SAD, 2010.

[39] URL: http://www.nativeintelligence.com/ni-programs/whyaware.asp (pristupljeno: kolovoz 2017.)

Popis kratica

ACH	(Automatic Clearing House) elektronička mreža za financijske transakcije
AES	(Advanced Encryption Standard) napredni enkripcijski standard
DNS	(Domain Name System) protokol za davanje imena mrežnim adresama
DoS	(Denial of Service) uskraćivanje usluge
FTP	(File Transfer Protocol) protokol za prijenos podataka
HTML	(HyperText Markup Language) prezentacijski jezika za izradu internetskih stranica
HTTP	(HyperText Transfer Protocol) protokol za prijenos informacija na webu
ID	(Identifier) identifikator
IMEI	(International Mobile Equipment Identity) međunarodni broj mobilne opreme
IoT	(Internet of Things) Internet stvari
IP	(Internet Protocol) Internet protokol
IRS	(Internal Revenue Service) američka porezna administracija
MP3	(MPEG-1 Audio Layer 3) zvučni digitalni format
MP4	(MPEG-4 Part 14) multimedijski digitalni format
NFC	(Near Field Communication) komunikacija bliskog polja
PDF	(Portable Document Format) prenosivi format dokumenta
PHP	(Hypertext Preprocessor) programski jezik za web stranice
POP	(Post Office Protocol) protokol za pristup e-pošti
RAT	(Remote Access Trojan) daljinski upravljani trojanski napad
RSA	(Public-key encryption) algoritam šifre javnog ključa
SMS	(Short Message Service) slanje kratkih tekstualnih poruka
SQL	(Structured Query Language) upitni jezik za rad s relacijskim bazama podataka
URL	(Uniform Resource Locator) ujednačeni lokator sadržaja
USB	(Universal Serial Bus) standard za povezivanje elektroničkih uređaja kabelom
USD	(United States Dollar) američki dolar
VPN	(Virtual Private Network) virtualna privatna mreža
ZIP	(File format) format datoteke

Popis slika

Popis grafikona

Popis tablica