Značajke ucjenjivačkog softvera usmjerenog terminalnim uređajima

Kletuš, Tomislav

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Tomislav Kletuš

ZNAČAJKE UCJENJIVAČKOG SOFTVERA USMJERENOG TERMINALNIM UREĐAJIMA

ZAVRŠNI RAD

Zagreb, 2018.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

ZAVRŠNI RAD

ZNAČAJKE UCJENJIVAČKOG SOFTVERA USMJERENOG TERMINALNIM UREĐAJIMA

FEATURES OF RANSOMWARE ATTACKS TARGETED AT TERMINAL DEVICES

Mentor: dr. sc. Siniša Husnjak

Student: Tomislav Kletuš
JMBAG: 0135236817

Zagreb, rujan 2018.

SAŽETAK

Ucjenjivački softver (engl. *Ransomware*) je vrsta malicioznog programa ili koda koja pokušava doprijeti do osobnih podataka krajnjih korisnika terminalnih uređaja. Krajnji cilj su korisnici te okorištavanje njima u financijskom smislu. Ucjenjivački softver radi na principu zaključavanja terminalnog uređaja te kriptiranja korisničkih podataka koji se nalaze na memorijskoj pohrani terminalnih uređaja, nakon čega oni postaju nedostupni krajnjem korisniku. Od korisnika se zatim iznuđuje novac raznim kanalima, vrlo često putem kriptovaluta, kako bi povratili, tj. otkupili vlastite podatke. U radu je ucjenjivački softver opisan pored ostalog zlonamjernog softvera te su iznesene razlike između podvrsti zaključavajućeg i kriptografskog ucjenjivačkog softvera uz njihove temeljne načine funkcioniranja. Uspoređene su karakteristike nekih od aktualnih i poznatijih ucjenjivačkih softvera poput *WannaCry* i *Petya* te je cjelovita usporedba izražena pomoću tabličnog prikaza. Upravo činjenice i iznesene karakteristike te statistički pokazatelji stvaraju sliku i otvaraju svijest o problemu ucjenjivačkog softvera. Iz tih praktičnih razloga na kraju rada nalaze se savjeti i preporuke kako zaštiti terminalni uređaj te kako promijeniti obrasce ponašanja i loše navike korištenja terminalnih uređaja jer sigurnosni rizici drastično opadaju s kvalitetnom prevencijom i samim prestankom širenja ucjenjivačkog softvera.

KLJUČNE RIJEČI: ucjenjivački softver; terminalni uređaji; sigurnost; zaštita

SUMMARY

Ransomware is a kind of malicious program or a code that tries reach and impact to the personal data of end-users of terminal devices. The ultimate goal are end users and exploiting them in a financial sense through blackmail. The blackmailing software works on the principle of locking terminal devices and encrypting user data stored on the same devices after which they become unavailable to the end user. In the second stage of attack money is drawn from the end users through various channels, very often through cryptocurrency to regain or repurchase their own data. In this paper, blackmail software is described beside other malicious software and the differences between the underlying locking and cryptographic blackmail software are outlined with their basic ways of functioning. The features of some of the current and well known blackmailing software such as WannaCry and Petya have been compared, and a complete comparison is expressed by a table. The facts and the characteristics that are presented, as well as the statistical indicators, create a picture and open the awareness of the main problem, named blackmailing software. For these practical reasons at the end of the work, there are tips and recommendations on how to protect the terminal device and how to change behavioral patterns and bad habits of using these existing terminal devices because security risks drastically fall off with quality prevention and with the end of the blackmail software expansion.

KEY WORDS: blackmail software; ransomware; terminal devices; security; protection

Sadržaj

1. Uvod

Samim razvojem tehnologije u zadnjih dvadesetak godina, navike u određenim životnim aspektima su se promijenile. Razvoj terminalnih uređaja od klasičnih stolnih računala pa sve do mobilnih pametnih telefona te razvitak informacijsko-komunikacijskih mreža i usluga, promijenio je način na koji danas živi. Primjerice, korištenje pametnog mobilnog telefona kao organizatora ili korištenje internet bankarstva putem njega, danas je sasvim uobičajeno i svima prihvatljivo. Upravo tom spoznajom vode se počinitelji kibernetičkih napada, tzv. crni hakeri. Oni iskorištavaju tu činjenicu zajedno s nedovoljnom educiranošću krajnjih korisnika, kako bi im oteli podatke, iznudili novac te općenito se njima okoristili kroz ilegalne radnje, poput izrade i napada malicioznim prijetnjama poput ucjenjivačkog softvera tzv. *ransomwarea*.

Analizom karakteristika i shvaćanjem principa napada raznih tipova ucjenjivačkog softvera tj. prijetnji, može se stvoriti slika o tome koje su kritične točke terminalnih uređaja najviše izložene napadima uz određene korisničke aktivnosti. Tim se pristupom razumijeva sam problem i dolazi se do spoznaja o aktualnim i najkvalitetnijim načinima zaštite i prevencije od tzv. *ransomware* prijetnji i napada.

Naslov završnog rada je *Značajke ucjenjivačkog softvera usmjerenog terminalnim uređajima*, a njegov cilj je detaljnije objasniti aktualne ucjenjivačke prijetnje i napade prema terminalnim uređajima te principe i postupke njihove zaštite i prevencije napada. Rad se sastoji od šest cjelina:

1. Uvod
2. Zlonamjerni softver umjeren terminalnim uređajima
3. Značajke prijetnji ucjenjivačkog softvera prema terminalnim uređajima
4. Žrtve i ciljevi napada ucjenjivačkim softverom
5. Mogućnosti zaštite terminalnih uređaja i prevencije prijetnji ucjenjivačkim softverom
6. Zaključak

U drugom poglavlju govori se o osnovnim informacijama raznih vrsta malicioznih softvera koji predstavljaju prijetnju prema korisnicima te njihovim terminalnim uređajima. Kako bi se stvorila jasnija razlika između učestalih zlonamjernih softvera i samog ucjenjivačkog softvera te kako bi se dobio dojam o povezanosti tih dvaju termina važnih za shvaćanje nastavaka rada, ovo poglavlje će imati informativan karakter.

Treće poglavlje tvori ključni dio analize ovog rada, tj. sadrži detalje o tome što je ucjenjivački softver, na koji način se distribuira u korisnički sustav te kako funkcionira uz pregled aktualnih ucjenjivačkih prijetnji. Kako bi se pokazala ozbiljnost

ucjenjivačkih prijetnji, u ovom poglavlju bit će prikazani statistički podatci te usporedna tablica karakteristika aktualnih tipova ucjenjivačkog softvera.

U četvrtome poglavlju konkretno su navedeni najčešći primjeri napadanih subjekata i sustava, uz pojašnjenja zašto se napadači, *cyber* kriminalci, baš opredjeljuju za napade na određen profil krajnjih korisnika te određene tipove terminalnih uređaja i njima pokretanih operacijskih sustava.

Napadi i prijetnje ucjenjivačkim softverom u petom su poglavlju podijeljeni po fazama. Upravo takvo raščlanjivanje napada na faze i prikaz njegovih kritičnih točaka omogućuje njihovo lakše razumijevanje te na kraju i implementaciju praktičnih savjeta, detalja o prevenciji i zaštiti od ucjenjivačkih prijetnji i napada.

2. Zlonamjerni softver usmjeren terminalnim uređajima

Kada se govori o zlonamjernom softveru, obično se misli na sve tzv. maliciozne prijetnje u vidu aplikacija te dijelova tih aplikacija, tj. programskog koda. Takav zlonamjerni softver (engl. *malware)* označava sve aplikacijske prijetnje prema korisnicima i njihovim terminalnim uređajima koji imaju za cilj nanijeti svojevrsnu štetu korisniku ili terminalnim uređajima koje on posjeduje. Šteta se očituje u vidu uništenja, krađe korisničkih podataka, kompromitiranja hardverskih mogućnosti terminalnih uređaja (smanjenje procesorske mogućnosti obrade, zagrijavanje komponenata, zagušenje prostora pohrane itd.), onemogućavanja korištenja aplikacijskih rješenja i osnovnih funkcija terminalnih uređaja (npr. zaključavanje radne površine i pristup pohranjenim podatcima) te kao posljedica svega na kraju ucjene i iznuđivanje financijskih sredstava. Kako bi se stekao dojam i slika što je tzv. *ransomware* te u kakvoj je korelaciji s ostalim *malware* softverom, u nastavku će biti predstavljeni neki od osnovnih tipova zlonamjernih softvera kao što su: *adware*, crv, *keylogger*, *rootkit*, *spyware*, trojanski napad te virus, [1], [2].

Spomenute maliciozne prijetnje distribuiraju se na različite načine dok su sljedeći slučajevi, prema [1], najučestaliji:

- *Drive-by-Downloads* - nesvjesno preuzimanje zlonamjernog softvera nakon otvaranja web stranice na kojoj se isti nalazi
- *E-mail* – infekcija terminalnog uređaja zlonamjernim softverom nakon otvaranja sadržaja poruke unutar *e-mail* sandučića
- Mrežni upad – pozadinski mrežni procesi koji se odvijaju unose maliciozni softver nakon što je jedan od tih procesa kompromitiran istim
- Socijalni inženjering – iskorištavanje te manipulacija krajnjih korisnika zbog nedostatka znanja i informacija o informacijskoj sigurnosti
- Automatsko preuzimanje tzv. *downloaders* – nakon što maliciozni softver kompromitira sustav, terminalni uređaj, pokreće se niz automatskih preuzimanja dodatnih zlonamjernih softvera koji će biti objašnjeni u nastavku

2.1. *Adware*

Adware je vrsta softvera koji po prirodi ne mora nužno biti zlonamjeran. *Adware* dolazi od engleske riječi „*advertisement“* što u prijevodu označava reklame tj. oglase. To je samo dio programskog koda koji se obično nalazi unutar aplikacija namijenjenih krajnjim korisnicima kako bi reklamirao određeni proizvod, uslugu i sl. Kao takav, može se reći kako predstavlja smetnju jer prikazane reklame odvraćaju i smetaju pri korištenju terminalnog uređaja. Vrlo često ga karakteriziraju i skočni prozori (engl. *pop-up window*) zbog kojih stariji terminalni uređaji s manje radne memorije znaju usporiti svoj rad. Nerijetko se pojavljuje kod besplatnih aplikacija za pametne mobilne terminalne uređaje gdje ometa korisnike pri korištenju aplikacije s namjerom prelaska s besplatne na komercijalnu verziju te aplikacije. U punom smislu

zlonamjernost se očituje kada se *adware* pojavljuje u kombinaciji sa *spywareom* prilikom čega se prati aktivnost korisnika i postoji mogućnost od krađe i zlouporabe korisničkih podataka, [3].

2.2. Crv

Poznat pod engleskim nazivom „*worm*“, ovakav tip malicioznog softvera distribuira se mrežom, najčešće putem *e-maila* kroz priložene datoteke. Iskorištavajući sigurnosne propuste u kodu operacijskog sustava zahvaća terminalni uređaj te mu uzrokuje štetu u vidu zagušenja lokalne mreže. Radeći u pozadini zauzima velik dio dostupnog mrežnog kapaciteta onemogućujući komunikaciju između terminalnog uređaja i servera kojem se želi pristupiti. Također mogu sadržavati i dijelove programskog koda koji na zaraženom terminalnom uređaju samostalno pokreću određene procese kojima se korisnički podatci mogu izbrisati, otuđiti te stvoriti tzv. *botnets*, mreže zaraženih računala kojima tvorci crva mogu upravljati primjerice kroz slanje *spam* poruka. Jedna od njegovih karakteristika je i to što se samostalno umnožava i širi po zaraženom terminalnom uređaju stvarajući time vlastite kopije koje dodatno umanjuju performanse rada terminalnog uređaja i mreže koju koristi, [4].

2.3. *Keylogger*

Prijetnje u vidu *keyloggera* za krajnje korisnike terminalnih uređaja mogu biti vrlo opasne i štetne. One mogu biti izvedene ili hardverski ili softverski dok je potonji učestaliji. Nakon prvotne distribucije na terminalni uređaj on pokreće pozadinski proces koji stvara *log* datoteku. Ta *log* datoteka bilježi sve podatke koje je korisnik unio kroz ulazne uređaje poput tipkovnice te se dalje njen sadržaj prosljeđuje na poslužitelj (engl. *server*) kojemu napadači imaju pristup. Zlonamjerno korištenje *keyloggera* korisnicima može prouzročiti štetu u vidu krađe informacija (*log in* podatci, korisničko ime i lozinka) ili u većini slučajeva dovodi do financijskog okorištavanja zbog implementacije *keyloggera* na sučeljima za unos broja kreditnih kartica i PIN-a kod web stranice za *online* kupovinu. Dovodi ih se u korelaciju s tzv. *phishing* napadima, kojima se manipulacijom i obmanom korisnika nastoji doći do njihovih podataka, [5].

2.4. *Rootkit*

Ova skupina zlonamjernog softvera u velikoj mjeri je povezana s drugim tipom takvog softvera, *spywareom*. *Rootkit* nakon zahvaćanja sustava i terminalnog uređaja nastoji kroz prikriveno djelovanje u pozadini omogućiti njegovim tvorcima praćenje, bilježenje korisničke aktivnosti, otuđivanje osjetljivih korisničkih podataka te upravljanje hardverskim resursima terminalnog uređaja i dodatnim mrežnim uređajima koji su na njih spojeni za određene vlastite radnje (primjerice tzv. rudarenje kriptovaluta). Kako takav maliciozni softver ima za cilj ostati prikriven u pozadini te vladati terminalnim uređajem, sve informacije i karakteristike koje korisnik može pronaći o radu vlastitog terminalnog uređaja mogu biti lažne i iskrivljene, [6].

2.5. *Spyware*

U osnovi nakon što ga korisnik nesvjesno ubaci u terminalni uređaj preuzimanjem sadržaja s mreže, otvaranjem kroz e-mail ili pak instalacijom određenih aplikacija i programa unutar kojih je ugrađen, *spyware* počinje prikupljati podatke o aktivnosti korisnika na mreži, te ih šalje trećoj strani tj. autoru takvog malicioznog softvera. Navedeno vrijedi za najjednostavniju verziju *spywarea* dok je on često implementiran s drugim zlоćudnim softverom poput *adwarea*, *keyloggera* te trojanskih virusa. U takvoj kombinaciji predstavlja puno veću opasnost zbog šireg spektra korisničkih podataka koje prikuplja, što može rezultirati izradom kopije profila nekog korisnika, odnosno krađom identiteta. Dodatno može izazvati štetu i na samim terminalnim uređajima , tj. u njihovom radu, iskorištavajući resurse te zagušujući mrežne kapacitete na koje su isti povezani. Preuzimanjem podataka ili aplikacija od nepouzdanih izvora rizik zaraze *spywareom* raste, [7].

2.6. Trojanski napad

Poznat i kao trojanski konj ili trojanski virus iz razloga što ovakva vrsta počinje stvarati štetu nakon što ga neoprezni korisnik samostalno distribuira unutar vlastitog terminalnog uređaja iz neznanja ili misleći kako je riječ o legitimnom programu, aplikaciji. Prema [1], njegova arhitektura se sastoji od dva dijela:

- Poslužiteljska strana – izvršava se na terminalnom uređaju žrtve
- Klijentska strana – izvršava se na uređaju napadača putem konzole

Nakon što napadač uspostavi opisanu vezu, u mogućnosti je instalirati neke od ostalih malicioznih, prethodno navedenih softvera, kako bi ostvario svoj naum. Također se šteta po korisnika javlja kroz krađu povjerljivih korisničkih informacija ili iskorištavanja resursa terminalnog uređaja i njemu povezanih mrežnih uređaja.

2.7. Virus

Prema svojstvu širenja unutar sustava terminalnog uređaja, virusi se razlikuju od ostalih zlonamjernih aplikacija i programskih kodova. Nakon inicijalne distribucije i infekcije virus se veže uz određenu datoteku na korisničkom terminalnom uređaju te se širi i zahvaća ostale datoteke otvaranjem zaraženog podataka. Takvim lančanim reakcijama virus može stići do datoteka iz registra ili pokretačkih datoteka operativnog sustava te nad njima izvršavati promjene, kopirati ih, brisati, dodavati *adware*, stvarati tzv. *botnets* i sl. Osim što može uništiti korisničke podatke, šteta može biti prouzročena i na operativnom sustavu kojeg je često potrebno ponovo instalirati zbog oštećenih *.exe* datoteka. Termin „virus“ je u najširoj uporabi te predstavlja neispravan sinonim za sve tipove malicioznih softvera, [1].

3. Značajke prijetnji ucjenjivačkog softvera prema terminalnim uređajima

Vidljiva je nezaustavljiva ekspanzija i razvitak tehnologije u vidu digitalizacije te informatizacije društva pa na kraju i pojedinca kao njegovog temelja. Tijekom zadnjih dvaju desetljeća elektronički sklopovi, uređaji i računala doživjeli su procvat - primarno kroz povećanje njihovih performansi (procesorskih, grafičkih, memorijskih…) što je rezultiralo približavanjem tehnologije običnim ljudima. Taj tehnološki razvoj uređaja, njima pripadajućeg softvera te informacijsko-komunikacijskih sustava i mreža doveo je do revolucije u svim društvenim djelatnostima što su krajnji korisnici vrlo dobro prihvatili. Može se reći da je daljnjim razvojem i povezivanjem tih uređaja i sustava došlo do pojave terminalnih uređaja kakve danas poznajemo.

Kao što je spomenuto, velik broj ljudskih djelatnosti danas se odvija putem terminalnih uređaja i informacijsko-komunikacijskih sustava što njihove krajnje korisnike dovodi u situaciju da postaju mete kriminalaca odnosno žrtve tzv. *cyber* kriminala. Kada se govori o *cyber* kriminalu, isti se obično povezuje s hakerima i malicioznim prijetnjama. Jedna od mnogih malicioznih prijetnji koja je popularna među napadačima prošlih godina jest napad ucjenjivačkim softverom, kodom ili programom poznatijim pod engleskim terminom *ransomware*. Takav ucjenjivački softver, program ima vrlo slične karakteristike distribucije prethodno opisanim malicioznim prijetnjama ili je njihov sastavni dio.

Ucjenjivački softver ima za cilj okoristiti se žrtvom kroz ucjenu na način da se žrtvin terminalni uređaj zaključa te u smislu korištenja postane nedostupan ili da žrtvini podatci nakon kriptiranja njoj na neki način postanu nedostupni. Najširi oblik ovakvih napada uključuje zastrašujuću poruku prilikom podizanja operativnog sustava terminalnog uređaja koja sadrži zahtjev za uplatom određene svote novaca najčešće izraženom u jednoj od kriptovaluta poput *Bitcoina*. Kriptovalute su digitalne valute koje se čuvaju elektronski (ne postoje fizički, ne printaju se) te nisu ni u čijem vlasništvu. Nastaju putem posebnih računala koja rješavanjem kompleksnih matematičkih zadataka stvaraju određenu vrijednost tj. digitalnu valutu. U svijetu postoji velik broj različitih kriptovaluta ali najpoznatija je svakako *Bitcoin* (BTC). Ne postoji garancija da će kriptirani korisnički podatci ili terminalni uređaji biti dostupni nakon uplate otkupnine te je samim *cyber* kriminalcima tzv. crnim hakerima teško ući u trag, [8].

Tipovi napada prema distribuciji mogu biti, [8]:

- Usmjereni prema točno određenom cilju, žrtvi
- Usmjereni prema širokom spektru korisnika terminalnih uređaja

Kada se govori o samom napadu, napadači se obično koriste sljedećim tehnikama, [8]:

- Prijetnja ucjenom, iznudom – zaključavanje korisničkih podataka ili dijelova programskog koda za podizanje operacijskog sustava sve dok korisnik ne uplati otkupninu
- Prijetnja objavljivanjem – korisnika se zastrašuje prijetnjama kako će njegovi osobni i povjerljivi podatci biti javno objavljeni ukoliko ne uplati otkupninu

3.1. Razvoj ucjenjivačkog softvera

Prva pojava ovakvog tipa ucjenjivačkog malicioznog softvera zabilježena je 1989. godine na konferenciji Svjetske zdravstvene organizacije gdje je Joseph Popp realizirao svoju ideju da među sudionicima događaja distribuira tzv. *ransomware*. Konferencija je bila na temu svjetskog problema AIDS-a pa je na temelju toga prvi poznati ucjenjivački maliciozni softver dobio ime AIDS trojan. Kao način distribucije, Popp je odabrao tadašnje disketne pogone (diskete, engl. *floppy disk*) koji su podijeljeni sudionicima. Nakon što su žrtve pokrenule disketne pogone na vlastitim računalima na zaslonima se pojavilo sučelje s porukom kako je računalo zaraženo te ukoliko se maliciozni softver želi ukloniti, žrtva mora uplatiti 189 američkih dolara na račun jedne korporacije u Panami. Unutar samog programskog koda AIDS trojan ucjenjivačkog softvera nalazio se brojač pokretanja operativnog sustava koji se izvršavao u pozadini. Nakon 90 iteracija pokretanja operativnog sustava AIDS trojan bi podatke datotečnog sustava s C:// particije zaključao ili kriptirao. Kako je bila riječ o 1989. godini, ovaj *ransomware* nije bio široko rasprostranjen zbog malog broja krajnjih korisnika terminalnih uređaja tj. računala, [9].

Koncept malicioznih ucjenjivačkih prijetnji popularizirao se 2005. i 2006. godine. U Rusiji se javljaju prvi širi slučajevi ucjenjivačkih prijetnji softverom koje putem kompresije, a potom zaključavanja korisničkih podataka na napadnutim računalima od žrtve traže otkupninu u iznosu od 300 američkih dolara. Neki od formata korisničkih podataka koji su bili na udaru: .DOC, .JPG, .PDF, .XML te .ZIP. Takav *malware* često je inficirao zapis za podizanje operativnog sustava (engl. *Master Boot Record* - MBR) te onemogućavao pravilno podizanje operativnog sustava i prikaz početnog zaslona, [10]. Također, u to vrijeme prijetnje ucjenjivačkog softvera bile su izvedene u oba oblika raznih antivirusnih, *antispyware* alata uz pomoć kojih su se korisnicima lažno predstavljali bilo kao sigurnosni programi ili bilo kao programi za optimizaciju rada terminalnih uređaja (npr. Spysheriff, Performance Optimizer i Registry Care). Žrtvama bi se na zaslonu prikazalo sučelje s porukom upozorenja kako njihovo računalo sadrži neispravne datoteke kao i oštećene datoteke unutar registra operativnog sustava. Cilj takvih poruka bio je izazivanje panike među žrtvama što bi ih nagnalo na kupovanje lažnih licenci za određene sigurnosne programe i alate koji ne bi koristili ni za što, [9]. Ti napadi su obično bili usmjereni prema tada najzastupljenijim platformama koje su pokretale korisničke terminalne uređaje, Windows i Macintosh operativne sustave.

Prvi ucjenjivački softver koji je imao karakteristike svih trenutno aktualnih zvao se Trojan.Gpcoder. Iako je imao algoritam zaključavanja podataka koji je brzo i jednostavno dešifriran, svi nadolazeći ucjenjivački softveri sadrže identičan temelj uz tematski slične ili drugačije ciljeve. 2006. godine, u početcima se još pojavljuju Trojan.Cryzip za kojeg se ubrzo otkrilo kako u svome programskom kodu sadrži kombinaciju znakova za otključavanje stvorene arhive, .ZIP datoteke te Trojan.Archiveus koji je po radu bio sličan Trojan.Cryzip-u ali je od žrtava zahtijevao kupovanje lijekova u web trgovini određene ljekarne te dostavljanje potvrde o kupnji umjesto tradicionalnog iznosa otkupnine, [9]. Upravo ovim primjerom ostavlja se prostor za sumnju kako postoji povezanost kriminalaca (hakera) te velikih kompanija ili čak politike kako bi obje strane imale koristi štiteći istovremeno jedni druge.

3.2. Osnovna podjela ucjenjivačkog softvera

Kada se govori o modernim, aktualnim verzijama ucjenjivačkog malicioznog softvera, tada ih dijelimo na dva glavna podtipa:

- Zaključavajući ucjenjivački softver (*locker ransomware*)
- Kriptografski ucjenjivački softver (*crypto ransomware*)

Oba služe istoj svrsi, okoristiti se nezaštićenim sustavima terminalnih uređaja, propustima u mrežnom dijelu te neinformiranošću, nesvjesnošću krajnjih korisnika o digitalnoj sigurnosti kako bi se njihovim svakodnevnim digitalnim djelatnostima došlo do financijske koristi ili kako bi pravnoj ili fizičkoj osobi nanijeli štetu kroz narušavanje ugleda. Također treba naglasiti potencijalno postojanje tzv. hibridnih ucjenjivačkih softvera kao kombinacije prethodno navedenih podtipova koji su kao takvi složeniji i time opasniji i štetniji po svoje žrtve. Iako hibridni ucjenjivački softver nije raširen u velikoj mjeri, pitanje je vremena kada će trenutne verzije napredovati i evoluirati iz razloga što kriminalci besprekidno rade na novim malicioznim prijetnjama, [9].

3.2.1. Zaključavajući ucjenjivački softver (*locker ransomware*)

Poznatiji pod engleskim terminom *computer locker* te kao što mu i naziv govori zaključava tj. onemogućuje pristup (u cijelosti ili pojedinim resursima) terminalnom uređaju ili pristup korisničkom sučelju i kao takvog ga ostavlja neuporabljivog za krajnjeg korisnika, žrtvu. Kako se od žrtve potražuju financijska sredstva za ponovni pristup terminalnom uređaju, ona često može upravljati samo ulaznim uređajima poput tipkovnice i to numeričkim dijelom za unos broja kreditne kartice ili sl.

Locker ransomware po svojoj prirodi ne uništava i ne oštećuje datoteke operativnog sustava niti korisničke podatke pa ga je prema tome vrlo lako ukloniti implementacijom sigurnosne kopije prošlog stanja računala ili komercijalnim sigurnosnim alatima. Iz tog razloga napadači se služe metodom socijalnog inženjeringa računajući na izazivanje straha i panike kod žrtve što će rezultirati njihovom uplatom otkupnine. Najčešće je to u vidu poruke na zaslonu kako je terminalni uređaj zaključan od strane policije ili sličnih sigurnosno-pravosudnih državnih tijela zbog preuzimanja piratskog sadržaja, prodaje narkotika putem interneta ili recimo posjedovanja dječje pornografije. Sam uspjeh takvog napada

ovisi o znanjima i sposobnostima žrtve. Ukoliko je riječ o tehnički sposobnoj osobi koja se zna služiti računalom i internetom, sam ucjenjivački softver je lako uklonjiv te ne predstavlja veću prijetnju osim gubljenja određenog vremena za njegovu eliminaciju. Ako je pak riječ o osobi koja nema tolika znanja i sposobnosti, postoji vjerojatnost kako će ona platiti otkupninu radi toga što je uvjerena u istinitost prikazane poruke (primjerice ispunjava tezu o posjedovanju piratskog softvera) ili sumnja u njenu vjerodostojnost ali nema dovoljna znanja za uklanjanje tog malicioznog programa.

Slika 1. Primjer sučelja zaključavajućeg ucjenjivačkog softvera, [12]

Iako je ovaj tip napada ucjenjivačkim softverom u padu zbog široke informiranosti korisnika o takvim napadima, pretpostavlja se da će se oni u budućnosti ponovo aktivirati radi činjenice kako raste tržište IoT (engl. *Internet of Things*) terminalnih uređaja. Primjerice, za hladnjake, pametne televizore i sl. terminalne uređaje koji su povezani na mrežu ne postoje opcije izrade sigurnosnih kopija operativnog sustava pa žrtva ma koliko dobro bila informirana nema drugih mogućnosti već ili platiti traženi iznos otkupnine ili pronaći neko sigurnosno rješenje kroz komercijalne alate te u njih uložiti vrijeme i novac kako bi na koncu uklonila prijetnju, [9], [11].

3.2.2. Kriptografski ucjenjivački softver (*crypto ransomware*)

Tzv. *data locker*, ovaj tip ucjenjivačkog softvera je raširenji a samim tim predstavlja veću prijetnju prema krajnjim korisnicima. On kao i zaključavajući ucjenjivački softver ne oštećuje ili uništava datoteke operativnog sustava niti korisničke podatke već isključivo potonje zaključava, kriptira ih implementacijom određenog enkripcijskog algoritma. Na taj način žrtva ne može pristupiti svojim

podatcima (poput dokumenata, projekata, slika, audio datoteka, videozapisa i sl.) bez odgovarajućeg ključa za dešifriranje ali i dalje može koristiti resurse terminalnog uređaja kao npr. povezivanja i pretraživanja weba. Takvi ucjenjivački softveri često potražuju plaćanje otkupnine u kriptovalutama, obično u *Bitcoinu* protuvrijednosti od nekoliko stotina američkih dolara (ovisno o tipu). Upravo je to razlog zašto kriptografski ucjenjivački softver žrtvi omogućuje korištenje resursa terminalnog uređaja. Neki tipovi čak korisniku pružaju upute kako i na kojim web adresama kupiti te uplatiti potraživani iznos u kriptovaluti. Nadalje, nakon infekcije terminalnog uređaja tzv. *crypto ransomware* radi neprimjetno u pozadini kriptirajući korisničke datoteke te kad jednom s njima završi korisniku se na zaslonu pojavljuje obavijest kako su njegovi podatci zaključani s uputom kako uplatiti otkupninu. Dodatan faktor panike kod žrtve izaziva i ugrađeni brojač vremena kojeg korisnik ima za realizaciju uplate. Kada on istekne žrtvini podatci ostaju trajno zaključani i nedostupni jer se ključ za dešifriranje briše. Prvotne verzije ovakvog ucjenjivačkog softvera nisu postizale očekivani učinak kod žrtvi jer su koristile jednostavnije algoritme za zaključavanje podataka te su sigurnosni stručnjaci lako dolazili do ključa za dešifriranje koji se ponekad nalazio na terminalnom uređaju žrtve ili u samom programskom kodu *ransomwarea*. Jednom kada je ključ za dešifriranje postao javan sve zaražene žrtve mogle su iskoristiti taj ključ ukoliko se radilo o istoj inačici ucjenjivačkog softvera.

Slika 2. Primjer sučelja kriptografskog ucjenjivačkog softvera, [13]

Kod izrade malicioznog koda, napadači se često koriste Tor (engl. *The Onion Router*) programom i kriptovalutama kako bi očuvali svoju anonimnost. Takav program iskusnijim korisnicima poznat je kao sinonim za pretraživanje tzv. *dark weba*, nekontroliranog sadržaja interneta kojem prosječan korisnik nema pristup bez

Tor softvera jer upravo on usmjerava na nekontrolirane web adrese sakrivajući svoju prisutnost kroz anonimne *proxy* poslužitelje diljem svijeta.

Slika 3. Primjer upute plaćanja otkupnine kriptografskog ucjenjivačkog softvera, [14]

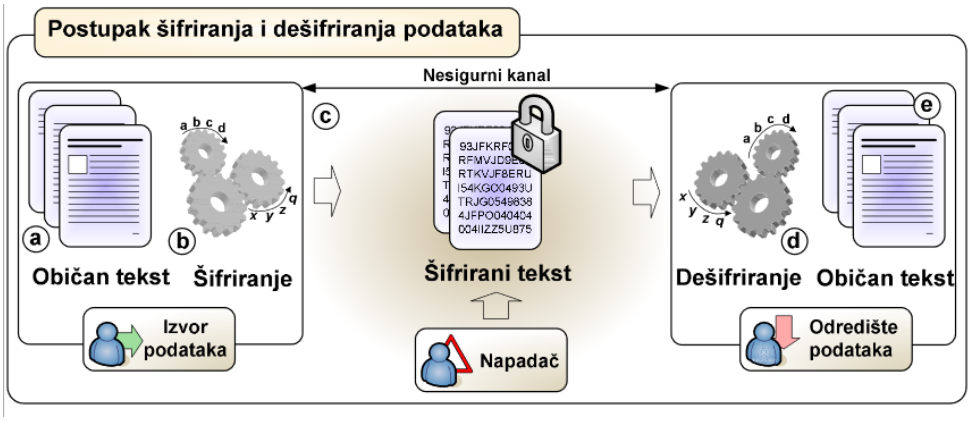
Kako je izrada sigurnosnih kopija vremenski zahtjevan posao zbog količine podataka koje prosječan korisnik pohrani na terminalnom uređaju, vrlo često korisnici ne primjenjuju ovu važnu sigurnosnu opciju. Takav obrazac ponašanja poznat je napadačima te se upravo na njega oni fokusiraju da bi ostvarili svoj cilj. Kako je današnji tempo života vrlo usko vezan uz rad i pohranu svakodnevno važnih podataka na terminalne uređaje, lako je za pretpostaviti da će trend rasta broja ovakvih kriptografskih ucjenjivačkih napada i prijetnji konstantno rasti, [9], [11].

3.3. Način rada ucjenjivačkog softvera

Kako je trenutno aktualno više inačica, verzija ucjenjivačkih softvera u nastavku će biti izneseno tehničko objašnjenje o principima funkcioniranja dva osnovna podtipa prethodno opisanih *ransomwarea*, kriptografski ucjenjivački softver te zaključavajući ucjenjivački softver.

3.3.1. Enkripcija datoteka

Kod ovog načina djelovanja važno je poznavati opće principe enkripcije te poznatije algoritme korištene kod iste. Prilikom govora o terminu kriptografije moramo znati što on označava. Kriptografija je znanost koja se bavi štićenjem podataka, informacije te očuvanjem njihovog integriteta te povjerljivosti. Njen glavni postupak naziva se kriptiranje ili enkripcija a označava izvođenje matematičkih i logičkih funkcija na izvornim podatkom kako bi njegova izlazna verzija bila jasna samo osobi koja je kriptiranje izvršila, poznajući korištenu matematičko logičku funkciju. Ta funkcija se naziva ključ te se bez njega ne može dešifrirati podatak tj. vratiti ga (pregledati) u izvoran oblik. Kriptiranje se koristi kada osjetljivu informaciju želimo zaštititi, osigurati njenu povjerljivost te prenijeti preko nesigurnog prijenosnog kanala, [15].



Slika 4. Ilustrirani prikaz postupka kriptiranja, [15]

Nadalje, postoje dva načina izvedbe enkripcije. Prva izvedba naziva se simetrična enkripcija. Kod nje postoji samo jedan ključ koji se koristi i za šifriranje i dešifriranje podataka te se on šalje na odredište zajedno s šifriranim podatkom što općenito nije pouzdana metoda ukoliko netko presreće, prisluškuje slanje na prijenosnom kanalu. Govoreći o simetričnoj enkripciji korisničkih podataka kod ucjenjivačkog softvera, ona će generirati ključ na žrtvinom terminalnom uređaju te ga proslijediti napadaču ili će ucjenjivački softver tražiti unos ključa od napadača prije nego se izvrši enkripcija žrtvinih podataka. Prednost za napadača kod ovakvog načina enkripcije je brz i jednostavan postupak što je bitno kod pregledavanja i kriptiranja velike količine korisničkih podataka u kratkom periodu (korištenje malih, kratkih ključeva dužine 256-bita).

Druga izvedba enkripcije naziva se asimetrična. Ona sadrži dva ključa; javni za šifriranje podatka te privatni za suprotan postupak dešifriranja. Predajna strana šifrira podatak javnim ključem te ga šalje putem prijenosnog kanala zajedno s tim ključem dok samo prijemna strana poznaje privatni ključ i dešifrira podatak. Ovaj postupak je općenito znatno sigurniji jer ako i napadač presretne podatak na prijenosnom kanalu i sazna javni ključ, s njime ne može dešifrirati podatak i saznati njegov sadržaj. Kod asimetrične enkripcije ucjenjivačkog softvera, napadač jedini poznaje privatni ključ te žrtva ma koliko stručna bila ne može dohvatiti taj ključ pa samim tim niti dešifrirati svoje podatke. Za napadača je ovakav tip enkripcije potencijalno problematičan zato što je postupak dugotrajan što može rezultirati otkrivanjem te prevencijom napada od strane žrtve.

Određene vrste ucjenjivačkog softvera koriste kombinaciju navedenih izvedbi enkripcije kako bi se smanjila mogućnost da žrtva shvati kako je ključ za dešifriranje stvoren na njenom terminalnom uređaju te preventivno djeluje. Primjerice, za primarnu enkripciju žrtvinih podataka koristi se simetrična enkripcija s jednim ključem koji koristi AES (engl. *Advanced Encryption Standard*) algoritam dug 256-bita. Zatim se nad AES ključem i kriptiranim podatcima vrši dodatna, asimetrična RSA (autori Rivest–Shamir–Adleman) enkripcija javnim ključem koji je preuzet s napadačevog poslužitelja dok on zadržava privatni ključ na svojem terminalnom uređaju. Nadalje,

postoji slična kombinacija gdje se žrtvini podatci simetrično kriptiraju te se taj ključ dodatno kriptira asimetrično putem RSA javnog ključa koji se nalazi u samom programskom kodu ucjenjivačkog softvera. Ovakav pristup smanjuje potencijalnu nemogućnost povezivanja na napadačev poslužitelj te izbacuje nepouzdanu kariku mreže iz cijelog lanca. Nedostatak je potreba za izradom novog privatnog ključa za svaki novi napad, [11].

3.3.2. Zaključavanje radne površine

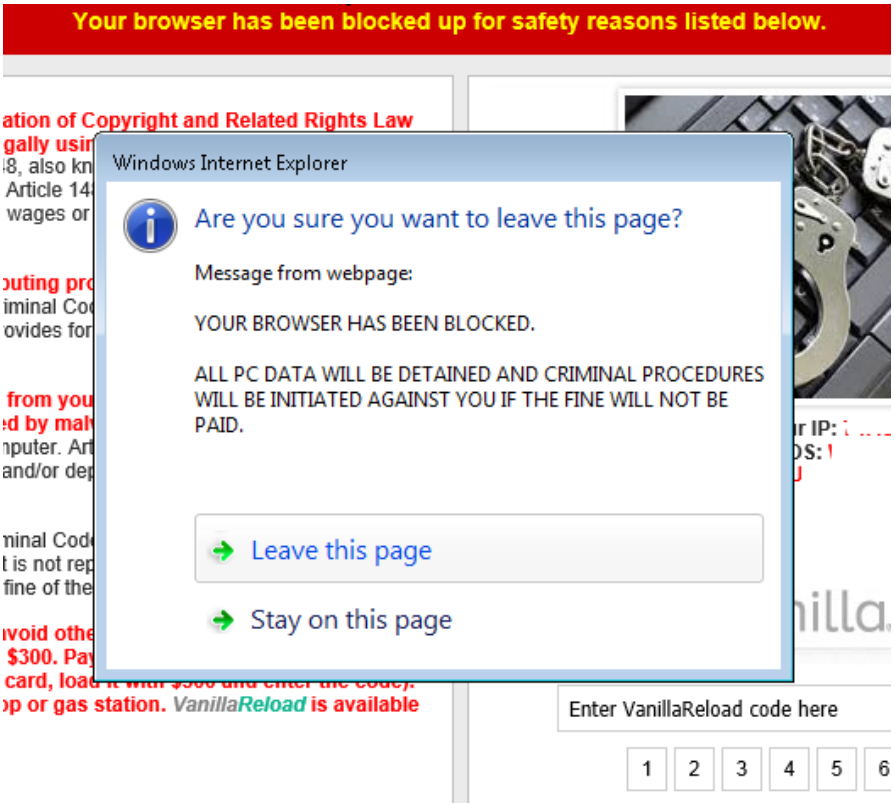
Jedan od načina hakera kako navesti korisnika da uplati željeni iznos otkupnine je i oduzimanje dostupnosti i mogućnosti korištenja njegovih terminalnih uređaja u vidu zaključavanja radne površine, zaslona. Prikaz poruke na zaključanoj radnoj površini kod žrtve može izazvati strah te paniku ostavljajući dojam kako je ta poruka trajna i stalno prisutna. No ono što žrtve ne znaju je to da se sučelje s uznemirujućom poruku vrlo često vrti u petlji programskog koda ucjenjivačkog softvera. Petlju je moguće prekinuti na određenim dijelovima. Takav tip *ransomwarea* obično iskorištava određene značajke operativnog sustava ili sučelja za programiranje aplikacija (engl. *Application Programming Interface* - API).

Postoje tri tipa zaključanih radnih površina terminalnih uređaja putem ucjenjivačkog softvera:

- Zaključavanje prozora radne površine *desktop* platformi
- Zaključavanje prozora radne površine putem web preglednika
- Zaključavanje prozora radne površine mobilnih platformi

Najpoznatiji tip zaključanog zaslona, radne površine je onaj kod Windows operativnog sustava gdje korisnik ima pristup samo sučelju s ucjenjivačkom porukom te uputama za uplatu otkupnine. To sučelje je prikazano preko cijelog ekrana ali ucjenjivački softver može sam stvoriti takav prozor ili iskoristiti prozor nekog Windows procesa ili programa poput prozora za pretraživanje sustava (engl. *browser window*). Ucjenjivački softver može kontrolirati radnu površinu kroz dijelove određenih procesa operativnog sustava (tzv. *thread*) koji se pozadinski izvršavaju u nekim intervalima. Kada se govori o sadržaju ucjenjivačke poruke, obično se on preuzme s napadačevog poslužitelja nakon izvršene infekcije žrtvinog računala ali ponekad (ovisno o varijanti ucjenjivačkog softvera) sadržaj poruke može biti sadržan unutar programskog koda *ransomwarea* tj. unutar njegove izvršne datoteke (*.EXE*). Takav mrežni pristup postavljanja sadržaja napadačima omogućava njegovu izmjenu prema potrebi, odnosno postavljanje slika policijskih organa države iz koje je žrtva te postavljanje teksta na točno određenom jeziku kako bi sam napad izgledao što uvjerljiviji i relevantniji. Kako bi ucjenjivački softver zaštitio sam sebe od ostalih procesa operativnog sustava koji imaju mogućnost gašenja neaktivnih ili nepotrebnih procesa (npr. Task Manager), on uz nadzor svih procesa te korištenje dijelova pozadinskih procesa (tzv. *thread*) ostalima može izdati naredbe za njihovo gašenje i prestanak rada.

Zaključavanje pristupa nekom resursu terminalnog uređaja poput radne površine može se ostvariti kroz web preglednik. Dok tzv. *browlock* (engl. *browser* + *locker*) ne onemogućava pristup operativnom sustavu jer ne sadrži nikakvu izvršnu datoteku, on djeluje tj. inficira uređaj nakon što korisnik putem web preglednika otvori zaraženu web stranicu. Sama web stranica nalazi se na poslužitelju s *browlock* ucjenjivačkim softverom te su na njoj implementirani dijelovi JavaScript koda koji je zadužen da se korisniku konstantno pojavljuje sučelje ucjenjivačkog karaktera. Tada se korisniku prikazuje sučelje s ucjenjivačkom porukom. To sučelje je temeljeno na HTML (engl. *HyperText Markup Language*) kodu te na određenom dijelu JavaScript koda koji je zadužen za pokretanje *onbeforeuload* funkcije. Prilikom korisničkog pokušaja zatvaranja tog sučelja, aktivira se *onbeforeunload* funkcija koja otvara skočni prozor nakon čega korisnik dobiva upit o zatvaranju, izlasku sa stranice ili prikazu krajnje ucjenjivačke poruke, [11]. Ukoliko je odabrana opcija izlaska sa stranice pojavljuje se skočni prozor kao na slici u nastavku (Slika 5.).



Slika 5. Prikaz skočnog prozora nakon pokušaja zatvaranja web stranice zaražene *browlock* ucjenjivačkim softverom, [16]

Prilikom daljnjeg odabira izlaza, zatvaranja stranice stalno se pojavljuje isti skočni prozor. Ako se korisnik odluči na opciju ostanka na stranici, prikaže mu se cijelo sučelje ucjenjivačkog softvera s porukom i uputom o uplati otkupnine. Korisnik dobiva dojam kako mu se stalno pojavljuje ista stanica s istim skočnim prozorom dok u suštini zaražena web stranica unutar svojeg HTML koda sadrži tzv. *iframe tag* - oznaku koja se aktivira svakim odabirom opcije zatvaranja stranice. Ta oznaka, otvara drugu zaraženu web stranicu s *browlock* poslužitelja u roku od nekoliko

milisekundi što korisnik ne zamjećuje. Ovakav tip ucjenjivačkog softvera može se ugasiti (na dva načina) zato što je temeljen na web pregledniku. Ako je korisnik dovoljno uporan u klikanju opcije izlaz sa stranice, u jednom trenutku ona će se zatvoriti. Druga metoda je učinkovitija te uključuje gašenje procesa web preglednika kroz Windows Task Manager. Ovakav način zaključavanja nije učinkovit za same napadače ali je jednostavan za implementaciju te je trenutno jedini tip ucjenjivačkog softvera koji je primjenjiv na svim aktualnim platformama terminalnih uređaja.

Kod mobilnih platformi poput primjerice Android operativnog sustava ucjenjivački softver *locker* tipa, stvara prozor aktivnosti sa sučeljem, ucjenjivačkom porukom. Slično kao kod zaključavanja radne površine putem web preglednika, ucjenjivački softver na Android uređaju koristi nadzor i provjeru je li poruka i dalje prikazana na zaslonu te se on izvršava u vrlo kratkom roku pa žrtva ima dojam kako sučelje stoji na zaslonu. Isto se postiže objektima izvršnih usluga unutar programskog koda Android operativnog sustava, [11].

3.4. Distribucija prijetnji ucjenjivačkog softvera

Ucjenjivački softver, tzv. *ransomware* spada pod maliciozni softver ili program. Prema navedenom, on se distribuira slično ostalim malicioznim prijetnjama. Uz tehnike distribucije prema korisnicima, postoje i one među *cyber* kriminalcima te specifični slučajevi samoumnažajućih ucjenjivačkih softvera temeljenih na socijalnom inženjeringu.

Samoumnažajući ucjenjivački softver, obično posjeduje neke od karakteristika *malwarea* poznatijeg kao crv. Naime takav softver, dok radi svoju primarnu namjenu bilo kao kriptografski ili zaključavajući ucjenjivački softver, u pozadini stvara svoje kopije, tj. umnožava se i prenosi putem mreže šireći obujam infekcije. Dok je ovaj slučaj češći kod Windows platforme, druga vrsta osmišljena je za mobilne terminalne uređaje, primjerice Android platformu, također na principu samoumnožavanja. Android platforma za isto koristi socijalni inženjering slanjem sumnjivih *phisihing* SMS (engl. *Short Message Service*) poruka svim kontaktima pronađenim na uređaju žrtve.

Drugi tip distribucije, manje poznat krajnjim korisnicima je međusobna suradnja *cyber* kriminalaca, hakera. U tom kriminalnom miljeu postoje hakeri amateri te oni iskusniji. Kako prvi nemaju dovoljna znanja za izradu kompleksnijih tipova ucjenjivačkog softvera, a njihove jednostavnije verzije mogu prevenirati razni komercijalni sigurnosni alati, oni se za savjete i pomoć obraćaju iskusnijim kriminalcima. Ulaz u svijet ucjenjivačkog softvera postao je način zarade. Iskusniji kriminalci prodaju vlastiti *ransomware* amaterima, što njima ostavlja dovoljno prostora za daljnji razvitak svojih softvera te brigu o samoj distribuciji prepuštaju napadačima amaterima. Termin koji se koristi za navedeno je „ucjenjivački softver kao usluga“ (engl. *Ransomware-as-a-Service* - Raas). Taj sustav funkcionira tako da iskusniji kriminalci dostave svoj softver amaterima sa svim svojim značajkama ali zarada se dijeli u omjeru 70%-30% od 300 američkih dolara, tipičnog iznosa tražene

otkupnine. Drugi model pod kojim se navedena usluga prodaje među napadačima je PPI (engl. *Pay-Per-Install*), odnosno plaćanje po učinku samog napada, infekcije, [11].

U nastavku će biti opisani najčešći načini distribucije tj. oni usmjereni prema krajnjim korisnicima.

3.4.1. Širenje elektroničkom poštom

Najpoznatiji tip širenja malicioznog softvera je putem elektroničke pošte, točnije putem neželjenih tzv. *spam* poruka temeljenim na socijalnom inženjeringu. Sve takve poruke poslane su s nekog oblika *botneta* koje se također iznajmljuju među hakerima uz proviziju. Oblici tih elektroničkih poruka mogu biti raznoliki, od *phishing* napada, zaraženih priloga poruka koji sadrže kombinacije ucjenjivačkog softvera i ostalog *malwarea* (npr. programi za preuzimanje s interneta tzv. *downloaders*, koji nakon instalacije automatizirano preuzimaju *ransomware* i ostali *malware*) do poruka s poveznicama na druge zaražene web lokacije. Jedna *spam* poruka može sadržavati sve prethodno navedene elemente te kao takva predstavlja izuzetan rizik u korporativnom okruženju jer prilikom infekcije na jedan terminalni uređaj korporacije, cijela njezina mreža i sustavi postaju ranjivi i kompromitirani. Što se tiče socijalnog inženjeringa, on može biti širokog tematskog spektra. Poruke s obavijestima o dugovanju, kriminalnim aktivnostima korisnika, kupoprodaji stvari od korisničkog interesa i sl., [9], [11].

3.4.2. Širenje reklamama (*Malvertisments*)

Krajnji korisnici svoje terminalne uređaje često zaraze svoje terminalne uređaje neovisno o platformi putem zloćudnih oglasa. Model zaraze putem oglasa može se podijeliti u dvije skupine. Prva je infekcija otvaranjem reklama koje nesvjesnog korisnika (zbog neznanja ili nepažnje) usmjeravaju na zaražene web stranice s malicioznim sadržajem. Drugi tip infekcije je prisutan kada legitimne web stranice budu prevarene nakon dogovora sponzorstva s lažno predstavljenim hakerima pa na vlastitim web stranicama objavljuju maliciozne reklame. Ovakav tip napada je neočekivan i opasniji jer čak i informirani korisnici mogu zaraziti svoj uređaj ne sumnjajući u kompromitiranost pouzdanih web stranica. Nadalje, kod mobilnih terminalnih uređaja postoji rizik od zlonamjernih reklama unutar besplatnih aplikacija. Preporučljivo je instalirati programe koji blokiraju (tzv. *ad blocker* programi) reklame čime se poboljšavaju performanse lokalne mreže na koju je spojen terminalni uređaj što se očituje u vidu brzine učitavanja web stranica. Problem se javlja kod *ad blocker* aplikacija namijenjenih mobilnim platformama jer neke vrše odbijanje reklama samo unutar web preglednika, a ne istovremeno prilikom korištenja drugih aplikacija. Dodatan rizik predstavlja i mogućnost kupovanja informacija o mrežnim korisničkim aktivnostima što može poslužiti napadačima kao orijentacija za usmjerenje svojih napada s tematski organiziranim zloćudnim reklamama prema određenom obrascu korisnika, [9], [11].

3.4.3. Sustavi distribucije mrežnog prometa (*TDS*)

TDS (engl. *Traffic Distribution Systems*) sustavi su sustavi koje koriste hakeri kako bi preusmjerili promet s jedne mrežne lokacije, web stranice na drugu. Vrlo često se preusmjerava promet s web stranica neprimjerenog sadržaja, koji spada pod oznaku 18+, piratskog sadržaja (npr. ilegalan *streaming* filmova i serija) na web stranice koje na svojim poslužiteljima sadrže ucjenjivački softver, neki drugi maliciozni softver ili kombinaciju istih. U praksi, hakeri kupuju preusmjereni mrežni promet od davatelja usluga distribucije prometa koji zatim upućuju na vlastite web stranice s malicioznim softverom. Navedena aktivnost inficira terminalni uređaj i izvršava pozadinsko preuzimanje ucjenjivačkog softvera, [9], [11].

3.5. Primjeri aktualnih prijetnji ucjenjivačkog softvera

U ovom potpoglavlju bit će navedene neke od aktualnih ucjenjivačkih prijetnji uz njihove karakteristike te objašnjenja.

3.5.1. WannaCry

Trenutno najaktualniji tip ucjenjivačkog kriptografskog softvera poznat je pod imenom WannaCry. Iako je postojao i prije njegova tzv. 2.0 inačica proširila se je u svibnju 2017. godine kada je u jednom danu izvršeno 75000 napada i potvrđenih zaraza što se smatra jednim od napada najvećih razmjera ucjenjivačkim softverom u svijetu. WannaCry je prema arhitekturi maliciozni softver koji se sastoji od kombinacije crva i ucjenjivačkog, *ransomware* softvera. Upravo ta karakteristika crva zaslužna je za njegovu široku rasprostranjenost zbog mogućnosti samoumnožavanja i daljnjih infekcija unutar nekoliko sati. Napadačima su ciljevi bili primarno korisnici terminalnih uređaja, Windows platforme, nad kojima su početno zaraženi svi uklonjivi memorijski pogoni uz izradu klona, kopije ucjenjivačkog softvera za daljnju propagaciju prije samog kriptiranja korisničkih podataka. Sami napadi bili su izvjesni od travnja 2017. te su nekoliko dana prije izvršenja čak i najavljivani. Skupini tzv. bijelih hakera američke sigurnosne agencije (engl. *National Security Agency* - NSA) ukradeni su napadački alati EternalBlue i DoublePulsar od strane hakerske skupine pod imenom Shadow Brokers, koji su ih javno objavili nakon čega dolaze u posjed mnogih hakera diljem svijeta. Upravo ti alati služe kako bi se neopaženo zadobila kontrola nad žrtvinim terminalnim uređajem te kako bi se na njega potajno instalirao ucjenjivački softver.

EternalBlue i DoublePulsar funkcioniraju na način da za infiltraciju u uređaj iskorištavaju rupu u programskom kodu Windows operacijskog sustava, odnosno u njegovoj jezgri (engl. *kernel*). Nakon što alati ostvare sve privilegije u sustavu, počinje implementacija ucjenjivačkog softvera. Daljnja distribucija je također moguća ne samo kroz lokalnu mrežu, već i preko interneta. Ako je uređaj zaštićen vatrozidom, (engl. *firewall*) vjerojatnost infekcije putem internetske veze je manja. Mjesec dana prije objavljivanja navedenih alata, Windows je izdao sigurnosnu zakrpu kroz ažuriranje baš kako ranjivost unutar jezgre ne bi bila iskorištena. Na žalost, mnogi korisnici nisu ažurirali svoje sustave ili su čak koristili starije sustave

poput Windows XP verzije za koju ne postoji nikakav oblik podrške te je ucjenjivački softver zahvatio velik broj računala. Mnoge institucije i danas koriste starije inačice takvih sustava ili ne brinu o svojim uređajima te nemaju valjanu mrežnu zaštitu što hakeri lukavo iskorištavaju, [17], [18].

Primjerice, nakon što je preuzeta kontrola nad zaraženim terminalnim uređajem, crv izrađuje vlastitu kopiju koja se dalje distribuira putem mreže. Ako je riječ o nekoj lokalnoj mreži određene organizacije, daljnja infekcija među računalima odvija se bez problema pod pretpostavkom kako je međusobni promet unutar lokalne mreže često bez nadzora, tj. nema implementirane sigurnosne mehanizme za unutarnju zaštitu (npr. vatrozid). U slučaju da se WannaCry distribuira putem širokopojasne mreže, prema pojedinačnim računalima, manja je mogućnost infekcije zbog češćih implementacija vatrozida na takvim terminalnim uređajima. Jedna od manje spominjanih metoda infekcije, je korištenje alata za udaljeni rad na računalu, otvaranjem RDP sesije (engl. *Remote Desktop Protocol*). Kada se zaraženo računalo udaljeno poveže na drugo putem *remote* programa i sesije, automatski prenosi WannaCry ucjenjivački softver.

Zanimljiva je činjenica kako WannaCry u svojem programskom kodu sadrži mehanizam kojim se štiti protiv antivirusnih programa. Naime, svaki antivirusni program ima tzv. karantenu u koju sprema sve maliciozne prijetnje te ona nije povezana direktno na mrežu niti ima doticaj s bilo kojim resursom terminalnog uređaja. Karantena svojem sadržaju prezentira simulaciju, virtualno okruženje unutar kojeg *malware* može funkcionirati (autoriziran je za sve radnje na računalu) što ima za cilj praćenje načina na koji on radi kako bi se mogao proizvesti softver za njegovo uklanjanje. WannaCry prije izvršavanja enkripcije korisničkih podataka pokušava uspostavu veze s web adresom:

www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

Ako povezivanje uspije enkripcija se obustavlja te korisnički podatci ostaju netaknuti ali se to računalo i dalje koristi za daljnju infekciju, distribuciju. Ta činjenica da je povezivanje uspješno izvršeno značila bi kako se WannaCry nalazi u karanteni antivirusnog programa i da se prate njegovi koraci rada. Hakerima je poznat princip karantene pa su iz tog razloga uvrstili vlastiti mehanizam zaštite. Vrlo brzo nakon početnih napada antivirusni programi su napravljeni ali do tad su već brojna računala bila pogođena. Što se tiče samog načina kriptiranja podataka i prikaza ucjenjivačke poruke, WannaCry je identičan istovjetnim ucjenjivačkim programima. Njegova dodatna mogućnost je brisanje sigurnosnih kopija sustava i promjene registra Windowsa kako bi se osiguralo prikazivanje poruke prilikom svakog podizanja sustava te onemogućilo korisnika vraćanje stanja sustava u vrijeme normalnog rada.

Od korisnika se zahtjeva uplata 300 američkih dolara otkupnine u *Bitcoinu* u roku od 3 dana. Ako rok nije ispoštovan, otkupnina se povećava na protuvrijednost 600 američkih dolara s rokom od 7 dana nakon čijeg isteka se kriptirani podatci brišu. Korisnikov uređaj je u pozadini cijelo vrijeme povezan s napadačem putem

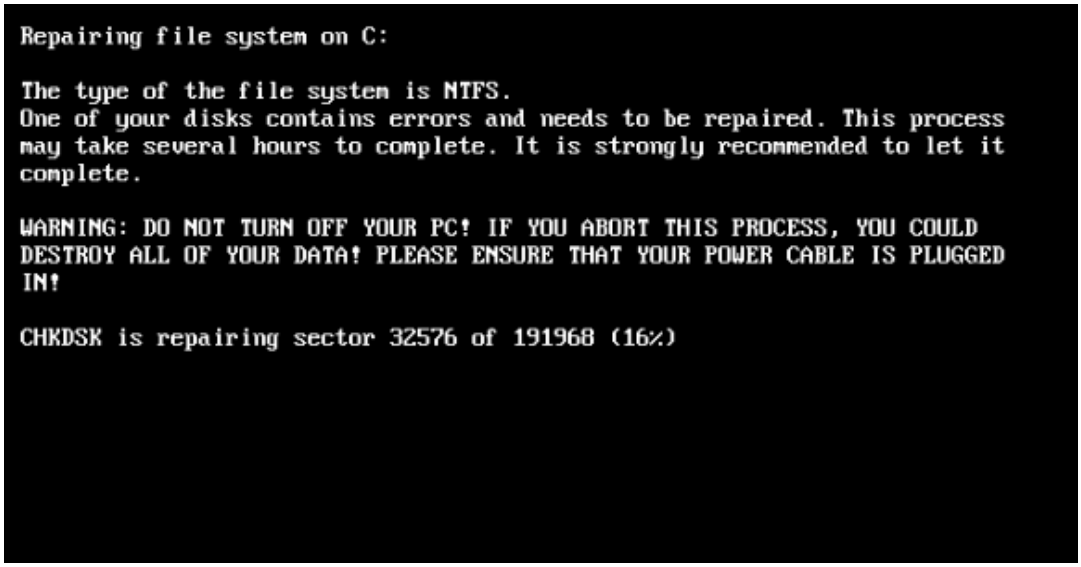
anonimne Tor mreže kako bi uplata otkupnine bila ostvariva uz tajnost IP (engl. *Internet Protocol*) adrese napadačevog računala, [17], [18].

3.5.2. Petya

Iako naizgled sličan tip *ransomwarea* WannaCry-u, Petya za svoje širenje koristi drugačiji način dok je za preuzimanje kontrole nad žrtvinim terminalnim uređajem također zadužen alat EternalBlue. Hakeri su implementirali trojanski *malware* u porezni i računovodstveni program MEDoc široko rasprostranjen među tvrtkama u Ukrajini gdje je većina napada i izvedena 2017. godine. Jednom kada je žrtvino računalo zaraženo, trojanski virus se pokreće kako bi našao žrtve za daljnju distribuciju. On skenira mrežne komponentne i sučelja unutar terminalnog uređaja te izdvaja liste sljedećih podataka: lokalne i vanjske IP adrese, DHCP (engl. *Dynamic Host Configuration Protocol*) poslužitelje te njihove klijente s mrežnih priključaka, DHCP klijente i poslužitelje ukoliko imaju otvorene *portove* 445 i 139, IP adrese definirane mrežnim maskama ukoliko imaju otvorene *portove* 445 i 139, IP adrese svih računala na koje je trenutno povezano zaraženo računalo, IP adrese računala povezane udaljenim pristupom sa zaraženim računalom i sl. Iz navedenog se može zaključiti kako Petya ima točno određene smjernice i odabrane ciljeve za napad.

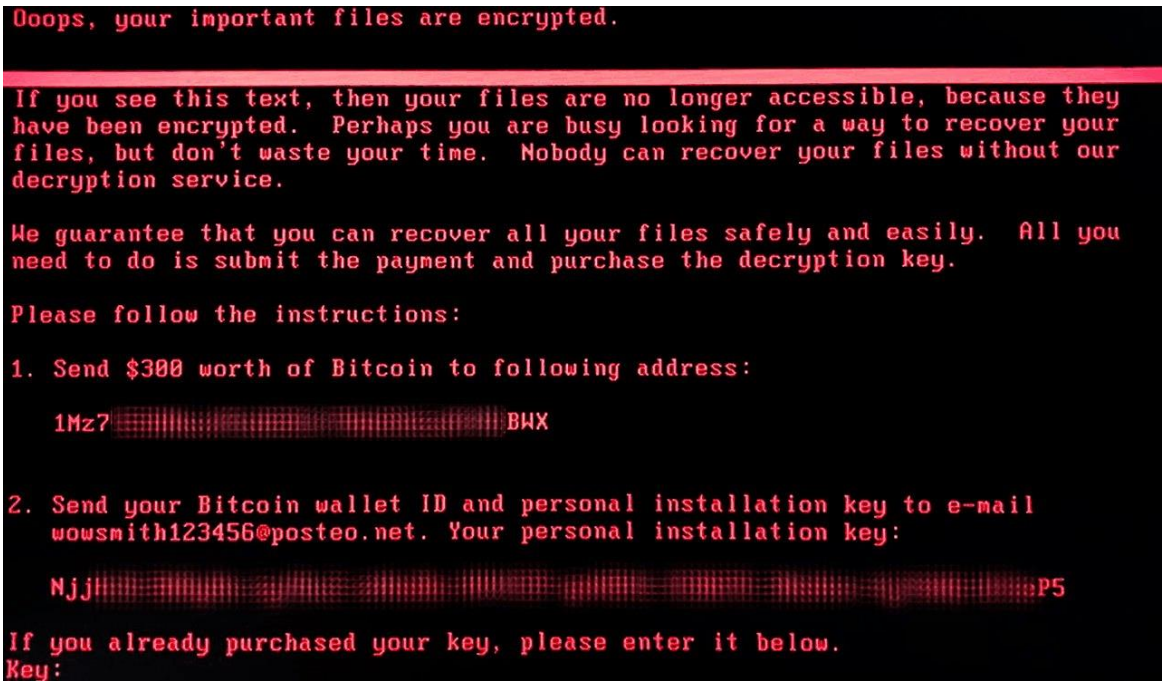
Nakon izrađene liste IP adresa, počinje se sa stvaranjem liste akreditacijskih podataka (korisničkih imena i lozinki) ukradenih sa svih računala pronađenih putem liste IP adresa. Akreditacijski podatci dohvaćeni su iz dijela operativnog sustava zaduženog za njihovu pohranu (engl. *Windows Credential Manager*).

Nakon izrađenih listi, Petya može izvršiti širenje na dva načina. Prvi je iskorištavanje EternalBlue alata na svim računalima s popisa IP adresa, a drugi je pokušaj pristupa (proces udaljenog pristupa PSExec) računalima s tih istih IP adresa ali putem korisničkog imena i lozinke. Pokušaj preuzimanje računala putem akreditacijskih podataka predstavlja prijetnju onim računalima koja su već instalirala sigurnosnu Windows zakrpu za onemogućavanje iskorištavanja jezgre operacijskog sustava. Hakeri su dodatno implementirali mehanizam koji na zaraženim računalima skenira aktivnost antivirusnih softvera te ukoliko isti budu pronađeni, ucjenjivački softver prestaje s radom i zamrzava se, [17], [19], [20]. Prije enkripcije, istovjetno WannaCry softveru, izmjenjuje registar operacijskog sustava, dio koda zaduženog za njegovo podizanje kako bi se osigurao konstantan prikaz ucjenjivačke poruke na zaslonu čak i nakon resetiranja uređaja (izmjena uključuje automatsko resetiranje uređaja u intervalu između 10 i 60 minuta). Računalo se ponovo pokrene te se korisniku prikaže sučelje kao na slici 6.



Slika 6. Početno sučelje Petya ucjenjivačkog softvera, [20]

Sučelje prikazuje lažnu obavijest o ispravljanju greške na tvrdom disku dok se u pozadini odvija kriptiranje korisničkih podataka s tog tvrdog diska. Koristi se tip asimetrične enkripcije s AES-128 (128-bit) algoritmom gdje se početni ključ (iz simetrične enkripcije) kriptira s javnim ključem koji je prethodno kodiran Base64 algoritmom. Kada se na ekranu završi postupak lažnog ispravljanja greške tvrdog diska, računalo se ponovo pokrene. Prilikom drugog pokretanja počinje druga faza enkripcije, Salsa20 algoritmom koji zaključava cijeli tvrdi disk. Korisnik nakon prikaza sučelja sa zaslona (slika 7.) shvaća kako je zaražen ucjenjivačkim softverom.



Slika 7. Završno sučelje Petya ucjenjivačkog softvera, [20]

Važno je napomenuti kako su elektronička adresa napadača i adresa za uplatu otkupnine lažni te da su svi korisnički podatci s tvrdog diska prebrisani. Čak i ako žrtva uplati otkupninu, neće dobiti povratni odgovor i ključ za dešifriranje a samim time niti će moći povratiti svoje podatke. Od Petya ucjenjivačkog softvera može se štititi samo preventivno.

3.5.3. CryptoLocker

Ova verzija *ransomwarea* kao što mu i ime označava, po tipu pripada kriptografskom ucjenjivačkom softveru. Njegova pojava zapažena je 2013. godine nad terminalnim uređajima platforme Windows. Cilj napada bile su poslovni subjekti te razne kompanije u najvećem broju s područja SAD-a i Velike Britanije. CryptoLocker se širio putem *botneta* pod imenom GameoverZeuS. *Botnet* bi poslovnim ciljevima slao cijeli maliciozni softver putem elektroničke pošte koji se nalazio unutar poruke kao prilog. Kako bi naveli žrtve da otvore poruku i preuzmu inficirani prilog na terminalni uređaj, napadači su se služili socijalnim inženjeringom. Kontekst je u pravilu sadržavao žalbu i nezadovoljstvo mušterija ciljanih kompanija. Nakon preuzimanja priloga .ZIP formata i njegovog raspakiravanja sama .PDF (engl. *Portable Document Format*) datoteka bila je prikrivena izvršna datoteka ucjenjivačkog softvera. Prema arhitekturi, CryptoLocker je trojanski tip prijetnje te se on instalira unutar registra Windows operacijskog sustava gdje modificira dio zadužen za pokretanje (tzv. *boot*) sustava kako bi prikaz ucjenjivačkog sučelja ostao konstantno prisutan pri svakom sljedećem pokretanju sustava. Nakon početnog prepoznavanja, usklađivanja ucjenjivačkog softvera i poslužitelja napadača pokreće se enkripcija žrtvinih podataka. Svaki podatak prvotno je kriptiran simetrično AES 128-bitnim algoritmom a zatim i asimetrično, RSA 2048-bitnom enkripcijom. Kod CryproLockera je specifično njegovo usmjerenje na poslovne podatke i dokumente tipičnih .DOCX, .TXT, .XLSX, .PPTX, .PDF i sl. formata dok su svi multimedijski podatci (foto, audio, video) zanemareni. Nakon što se žrtvu obavijesti kako su njeni podatci zaključani, aktivira se odbrojavanje od 72 do 100 sati što predstavlja rok za uplatu otkupnine. Nakon što otkupnina bude uplaćena, žrtvi se dostavlja jedinstveni ključ koji otklanja obje vrste enkripcije sa svake datoteke. Poznati su slučajevi gdje su niti nakon uplate otkupnine žrtvama nije dostavljen ključ za dešifriranje podataka dok također jedna od inačica CryptoLocker ucjenjivačkog softvera žrtvi omogućava dešifriranje 5 datoteka po njenom izboru (princip probaj prije plaćanja).

Kako je način distribucije ovog ucjenjivačkog softvera putem elektroničke pošte vrlo se je lako obraniti od napada mnogim *spam* filterima i drugim sigurnosnim antivirusnim alatima te na koncu i informiranjem krajnjih korisnika. Zanimljiv je podatak iznesen među iskustvima sistemskih administratora na popularnom forumu Reddit, kako je moguće saznati je li uređaj inficiran. Naime, oni su shvatili kako CryptoLocker počinje kriptirati poslovne datoteke prema abecednom redu te su na poslužiteljima kompanije stvorili direktorij s bespotrebnim datotekama. Taj trik su nazvali „*honeypot*“ (engl. posuda meda) što bi od takvog direktorija stvorilo mamac

te bi administratori znali da je sustav napadnut ukoliko je tome direktoriju pristupljeno ili ako je modificiran, [2], [9], [21].

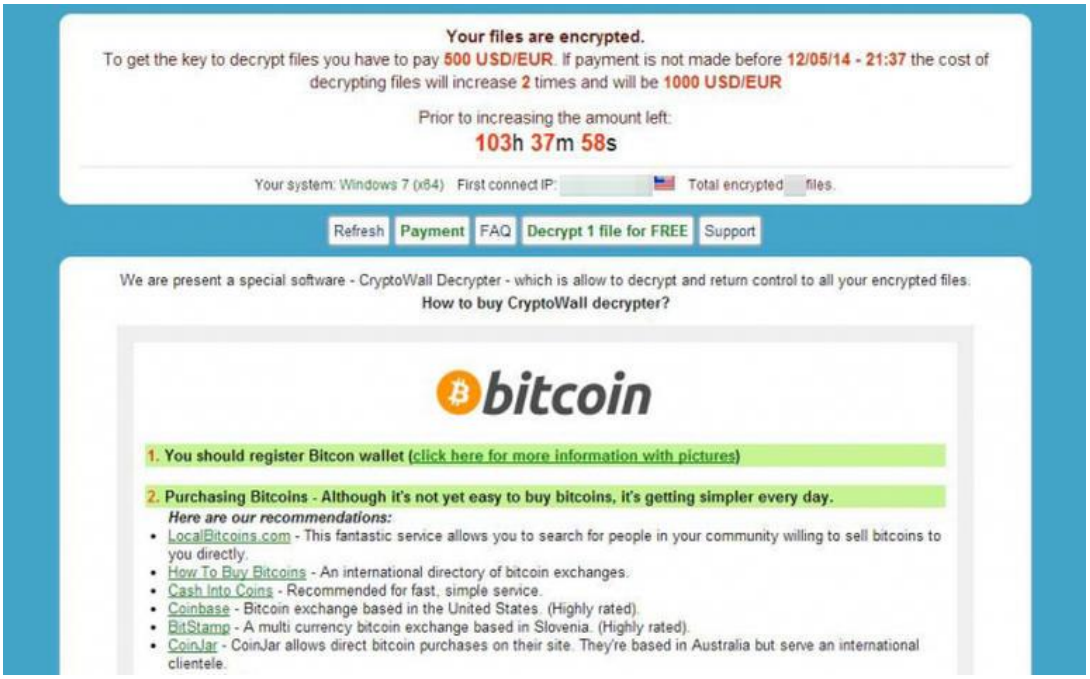
Nakon nekoliko godina otkriven je drugi slučaj CryptoLocker napada. Ovog puta ucjenjivački softver bio je u kombinaciji s crvom koji bi se samoumnožavanjem širio dalje po mreži. Sam princip je bio identičan opisanom napadu iz 2013. godine uz dodatak da su se žrtvini terminalni uređaji, njihovi procesorski resursi unutar otkupnog roka (72-100h) potajno koristili za druge kriminalne aktivnosti hakera poput distribuiranih napada za sprečavanje pristupa (engl. *Distributed Denial-of-Service* - DDoS) te za rudarenje kriptovaluta, [21].

3.5.4. Locky

Locky je po tipu kriptirajući ucjenjivački softver koji se pojavio 2016. godine. Širi se putem *spam* poruka elektroničke pošte sadržavajući inficirani prilog (tzv. *macro* virus) u obliku MS Word dokumenta. Nakon što žrtva preuzme dokument od nje se traži da omogući određene postavke na njemu čime ga nesvjesno aktivira. Trojanski virus zatim se aktivira te prvotno briše sve datoteke sigurnosnih kopija operacijskog sustava ukoliko one postoje. Zatim se povezuje na poslužitelj napadača te kriptira korisničke podatke slično kao i CryptoLocker, koristeći kombinaciju simetrične i asimetrične enkripcije (AES-128 i RSA-2048). Žrtvi se tada prikazuje ucjenjivačko sučelje s uputama o načinu korištenja Tor mreže kako bi se uplatila otkupnina. Otkupnina je od 2016. godine do sada obično varirala od 0,5 do 1 Bitcoina u protuvrijednosti američkih dolara. Prepoznatljiv je po tome što kriptirane datoteke preimenuje u nasumično odabrane alfanumeričke znakove s nastavkom .locky i .osiris (npr. 67dh3—jah342.osiris). U novijoj inačici zapaženo je kako se širi drugačijim načinom nego inače, putem *exploit kita* unutar Facebook Messenger servisa. Ukoliko žrtva ima na Windows platformi aktiviranu opciju Shadow Copy koja automatski prema određenom rasporedu izrađuje sigurnosnu kopiju sustava i tvrdog diska u NTFS (engl. *New Technology File System*) formatu, postoji mogućnost kako Locky neće obrisati takvu vrstu *back up-a*. U nekim slučajevima Shadow Copy ne bi bio obrisan te bi žrtva samostalno mogla vratiti sustav na prijašnje stanje te tako ukloniti ucjenjivački softver s mogućnošću vraćanja određenih podataka na stanje prije kriptacije, [9], [22].

3.5.5. CryptoWall

Prvi napadi CryptoWallom zabilježeni su 2014. godine a najšire razmjere infekcije je imao u Nizozemskoj, Njemačkoj, SAD-u i Velikoj Britaniji te je kao takav jedan od najraširenijih malicioznih softvera u Europi. Prema imenu vidljivo je kako je riječ o kriptografskom ucjenjivačkom softveru a njegov način distribucije je putem elektroničke pošte te web stranicama sa zloćudnim oglasima koje sadrže hakerske iskorištavačke programe (*exploit kits*).



Slika 8. Izgled ucjenjivačkog sučelja CryptoWalla, [23]

Po svojim karakteristikama najsličniji je CryptoLocker *ransomwareu*. Nakon otvaranja zaražene datoteke na žrtvinom računalu ona se sprema u privremeni direktorij Windows platforme, pokreće novi explorer.exe proces i maliciozni softver počinje s povezivanjem na kontrolno-naredbeni poslužitelj napadača. Koristi se kombinacija RSA-2048 i AES-256 enkripcija ali nasumično odabranih pojedinih korisničkih podataka. Za to vrijeme u pozadini se aktivira *spyware* koji traži korisničke podatke o kreditnim karticama i lozinke. Razlog ne kriptiranja svih podataka je postizanje veće brzine izvođenja napada (posljedica je mogućnost postizanja više napada u kraćem roku) te kako bi žrtva stekla dojam da je njene podatke moguće dešifrirati nakon uplate otkupnine koja vrlo često iznosi 1 Bitcoin u protuvrijednosti američkih dolara, [9], [22].

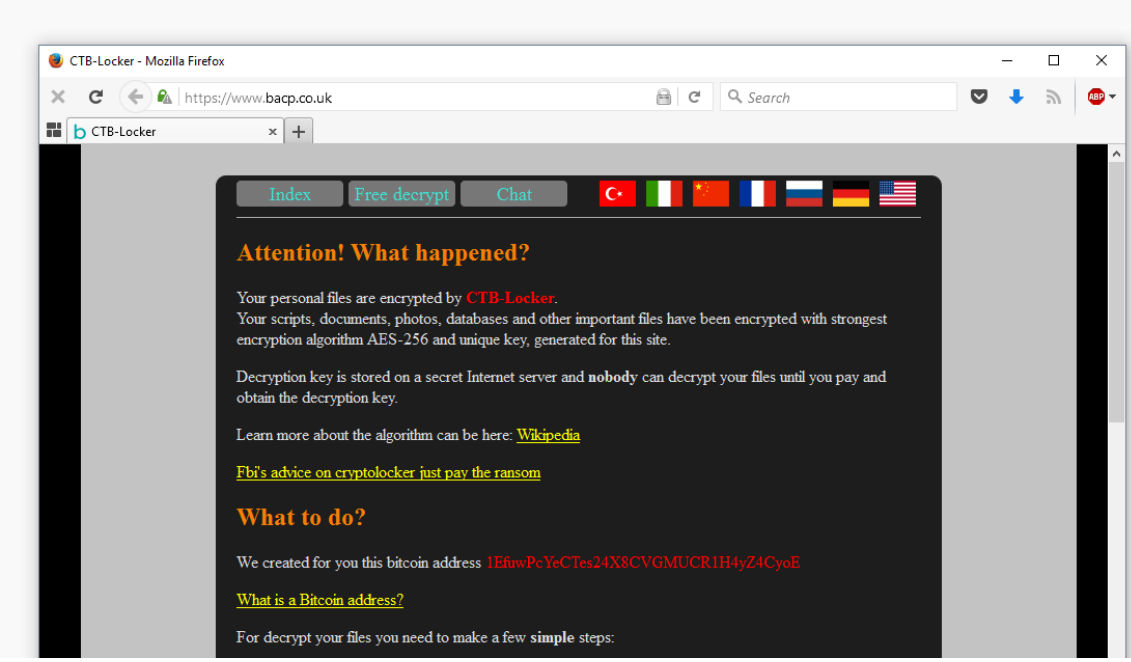
3.5.6. CTB-Locker

Kriptografski ucjenjivački softver koji se pojavio 2014. godine. CTB stoji kao kratica od engl. *Curve-Tor-Bitcoin*, što ga opisuje kao ucjenjivački softver kojeg iskusniji hakeri pružaju hakerima početnicima i upravljačima *botnet* mreža bilo uz određenu novčanu naknadu za uslugu, tzv. RaaS ili po principu plaćanja po ostvarenoj infekciji, tzv. PPI. Načini distribucije CTB-Locker ucjenjivačkog softvera uključuju korištenje izravno slanje *spam* poruka kroz elektroničku poštu, programa za iskorištavanje ranjivosti određenih programa i servisa tzv. *exploit kits*, programa za preuzimanje (*downloaders*) te *botnet* mreža za automatizirano slanje *spam* elektroničke pošte. Neki od *exploit kit*-ova koje koristi su Rig i Nuclear dok su nazivi programa za preuzimanje Dalexis (.CAB format) i Elenoocka (.ZIP i .RAR formati). Ti programi sadrže trojanski virus koji se pokreće nakon njihovog izvršavanja. Ovo je jedan od prvih ucjenjivačkih softvera temeljen na trojanskoj prijetnji tj. klijentsko-poslužiteljskoj arhitekturi koja omogućava kriptiranje žrtvinih podataka. Enkripcija je

moguća i bez mrežne povezanosti klijentske aplikacije (trojanskog virusa) i kontrolno-naredbenog poslužitelja napadača. Za nju se koriste simetrične tehnike, AES te asimetrične ECC (engl. *Elliptic Curve Cryptography*) tehnike. Razlika između učestalije RAS i ECC asimetrične enkripcije je u tome što se s ECC algoritmom postiže puno veća snaga enkripcije za identičnu dužinu algoritma u bitovima, odnosno ECC-256 po snazi je istovjetan onoj RAS-3072. Prethodne dvije činjenice razlikuju CTB-Locker od ostalih kriptografskih ucjenjivačkih softvera i čine ga ozbiljnijom prijetnjom. Nakon enkripcije korisniku se pojavljuje sučelje s ucjenjivačkom porukom uz dodatnu stavku, pozadinska slika uređaja je promijenjena te se na njoj nalaze upute kako uplatiti otkupninu. Tom promjenom pozadinske slike pokušava se ostaviti ozbiljniji dojam prema korisniku. Vrijeme za uplatu otkupnine obično iznosi 96 sati dok njen iznos oscilira prema vrijednosti kriptovaluta na tržištu.

Slika 9. Prikaz CTB-Locker ucjenjivačke poruke s računala, [25]

Novije inačice ovog ucjenjivačkog softvera temelje se na PHP (engl. *Hypertext Preprocessor*) programskom jeziku pod nazivom Critroni. Pomoću takvog softvera izvršeni su napadi na web stranice manjih kompanija koje su bile ne zaštićene ili izrađene na starijim verzijama WordPress alata. Njihove datoteke poput onih za prikaz glavnih stranica (index.php i indeks.html) zamijenjene su malicioznim koje su zahvatile cijeli poslužitelj i simetrično ga (AES-256) kriptirale.



Slika 10. Prikaz web stranice zaražene CTB-Locker/Critroni ucjenjivačkim softverom, [26]

Takva zaražena web stranica s ucjenjivačkom porukom bila je vidljiva i administratorima tih stranica kao i samim korisnicima. Iako je Critroni nedugo nakon toga smanjio svoju raširenost, ostaje pitanje hoće li u budućnosti hakeri moći putem zaražene web stranice inficirati i njezine pristupnike. Time bi se distribucija takvog softvera znatno povećala te bi predstavljala opasnost za širi spektar korisnika (npr. kompanija te svi njeni partneri i klijenti), [9], [24].

3.6. Usporedna analiza karakteristika aktualnih ucjenjivačkih prijetnji

U nastavku slijedi usporedni tablični prikaz karakteristika poznatijih ucjenjivačkih prijetnji i napada zadnjih nekoliko godina. Prijetnje su kronološki prikazane prema aktualnosti, tj. vremenu pojave prema unazad te su sve predstavnice aktualnog kriptografskog tipa ucjenjivačkog softvera. Iz same tablice moguće je vidjeti na koje načine su sustavi iskorištavani kako bi se prijetnje prvotno distribuirale te potom i izvršile na terminalnim uređajima. Također prikazani su potraživani iznosi otkupnine od strane napadača uz karakteristične osobine pojedinih prijetnji.

Tablica 1. Karakteristike aktualnih ucjenjivačkih softvera

Naziv (pojava)	Ciljana platforma	Distribucija	Infekcija	Otkupnina	Specifičnosti
WannaCry (2017.god.)	Windows	e-pošta, *botnets*, crv, *remote desktop* alati	*exploit kit* (EternalBlue), *backdoor* alat (DoublePulsar)	300 USD (BTC)	Testiranje okuženja (unutar karantene antivirusnog programa ili ne)
Petya (2016.god.)	Windows	e-pošta, *remote desktop* proces PSExec	*exploit kit* (EternalBlue), trojanski virus	Ovisno o inačici	Skeniranje IP adresa i akreditacijskih informacija povezanih računala te napad na njih (EternalBlue i korištenje akreditacijskih podataka za prijavu)

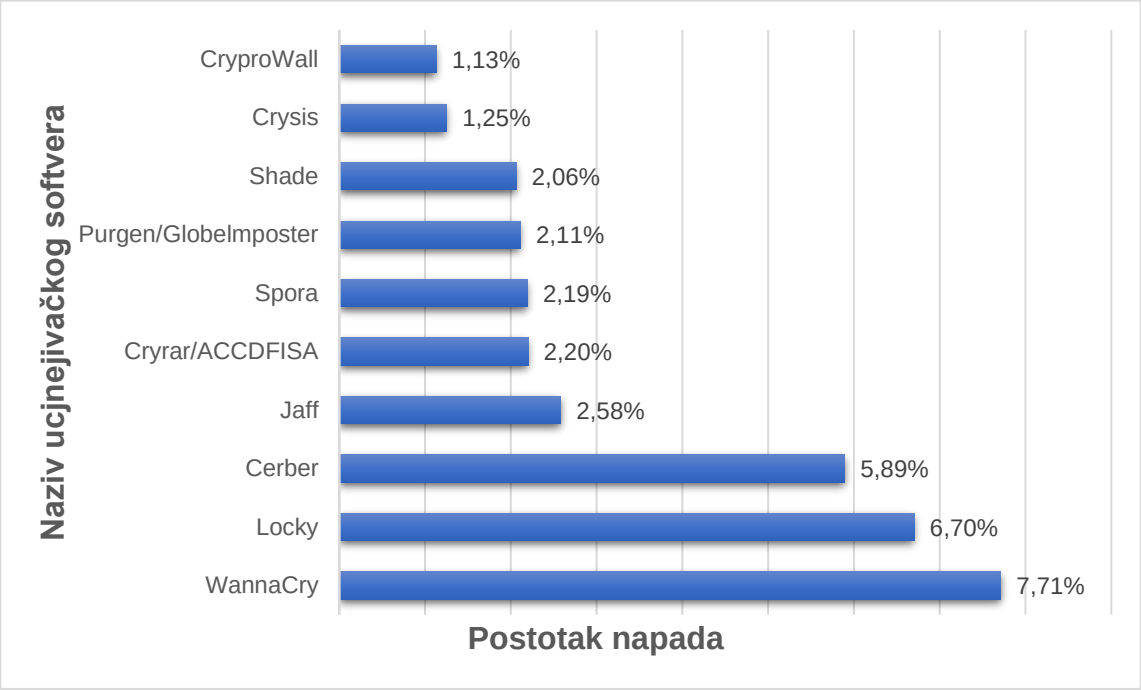
CryptoLocker (2013.god.)	Windows	e-pošta, *botnet* (GameoverZeus)	trojanski virus	400 USD (BTC)	Enkripcija poslovnih podataka, iskorištavanje resursa računala za DDoS i rudarenje kriptovaluta
Locky (2016.god.)	Windows	e-pošta	macro virus, trojanski virus	0,5 – 1 BTC	Mogućnost prevencije napada uz Shadow copy sigurnosnu kopiju
CryptoWall (2014.god.)	Windows	e-pošta, *malvetisments*	trojanski virus, *spyware*, *exploit kits*	1 BTC	Brisanje sigurnosne kopije Shadow copy prije enkripcije
CTB-Locker (2014.god.)	Windows	e-pošta, RaaS, *botnets*, kompromitirane web stranice, *downloaders* (Dalexis, Elenoocka)	Trojanski virus, *exploit kits* (Rig i Nuclear)	Ovisno o inačici	Korištenje ECC sheme enkripcije, mogućnost napada na web stranice (WordPress)

Ova usporedna tablica pokušava predočiti različitosti aktualnih prijetnji kako bi čitatelj shvatio koje se potencijalne slabe točke nastoje iskoristiti unutar vlastitih, implementiranih sigurnosnih rješenja i terminalnih uređaja.

3.7. Statistički pokazatelji obujma prijetnji ucjenjivačkim softverom

Kako bi se stvorila cjelovita slika o problemu prijetnji ucjenjivačkih softvera, važno je prikazati određene statističke podatke vezane uz tu tematiku. U nastavku slijedi nekoliko relevantnih pokazatelja u kojem smjeru se kreću trendovi vezani uz zlonamjerni ucjenjivački softver.

Kako je u prethodnim poglavljima bilo više riječi o pojedinim aktualnim prijetnjama važno je iste statistički prikazati. Udio napada ucjenjivačkim softverom izražen u postotcima vidljiv je s grafikona 1, među kojima su određeni navedeni u prethodnim poglavljima.

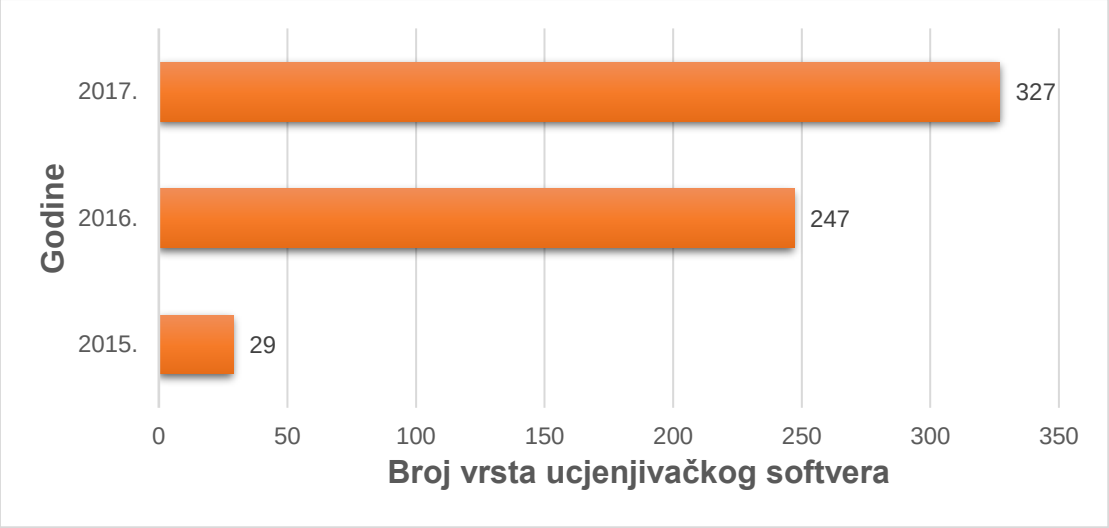


Grafikon 1. Udio napada pojedinih kriptografskih ucjenjivačkih softvera u 2017. godini

Izvor: [27]

Grafikon 1 prikazuje koliki je udio pojedinih aktualnih prijetnji od ukupnog broja bilo zastupljen među žrtvama u 2017. godini. Vidljivo je kako su prijetnje WannaCry te Locky bile na samom vrhu najraširenijih ucjenjivačkih softvera. Ovdje navedene najaktualnije prijetnje čine otprilike trećinu svih *ransomware* napada zabilježenih tijekom 2017. godine.

Ovdje prikazani tipovi kriptografski ucjenjivačkih softvera predstavljaju samo mali dio od svih vrsti i ukupnog broja ucjenjivačkog softvera. Ne moguće ih je sve nabrojati i prikazati, što kao činjenica dovoljno govori o njihovoj problematici i opasnosti. Među tim velikim brojkama, vrijedno je istaknuti podatak o novo otkrivenim prijetnjama u periodu od jedne godine te ga usporediti s podatcima prethodnih godina. Slijedi prikaz grafikona 2. Na njemu su vidljive novo otkrivene vrste ucjenjivačkog softvera u nazad nekoliko godina.

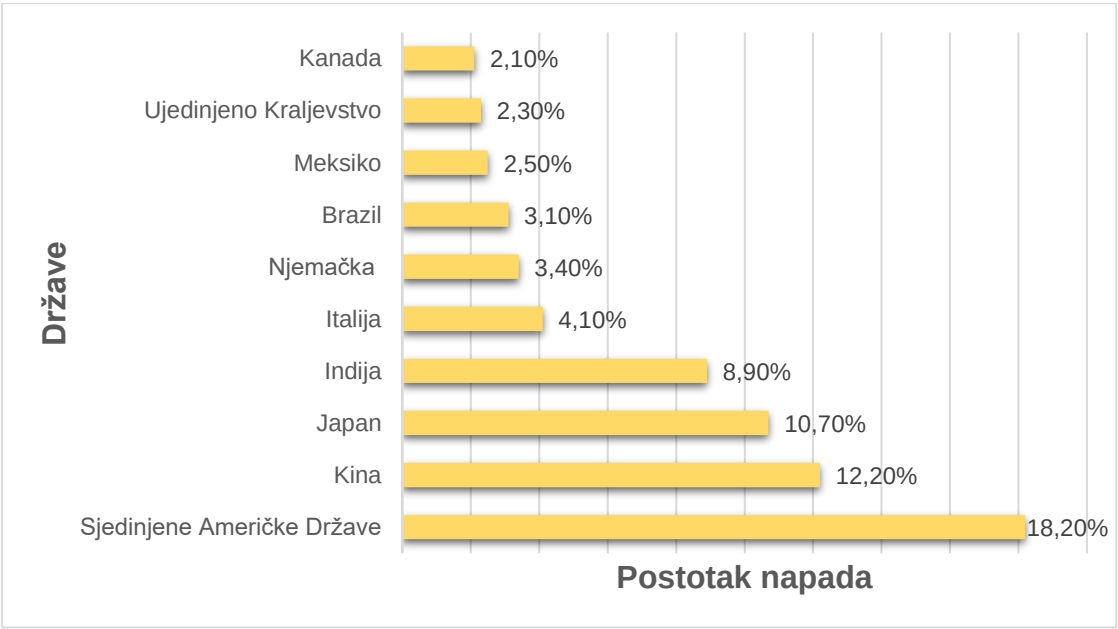


Grafikon 2. Prikaz otkrivenih vrsta ucjenjivačkih softvera po godinama

Izvor: [28]

Na grafikonu 2 iznesena je količina ukupno otkrivenih ucjenjivačkih prijetnji u protekle tri godine. Sam prikaz svjedoči o popularizaciji negativnog trenda, rasta *ransomware* napada što samo po sebi predstavlja ozbiljan problem i zabrinutost.

Kako je sam ucjenjivački softver globalno veoma rasprostranjen, prema statističkim pokazateljima gdje je on najviše zastupljen može se shvatiti zašto napadači odabiru žrtve s točno određenih geografskih područja. Slijedi prikaz grafikona 3. On pruža informacije o najvećem udjelu napada po državama u odnosu na svijet izražene u postotcima.

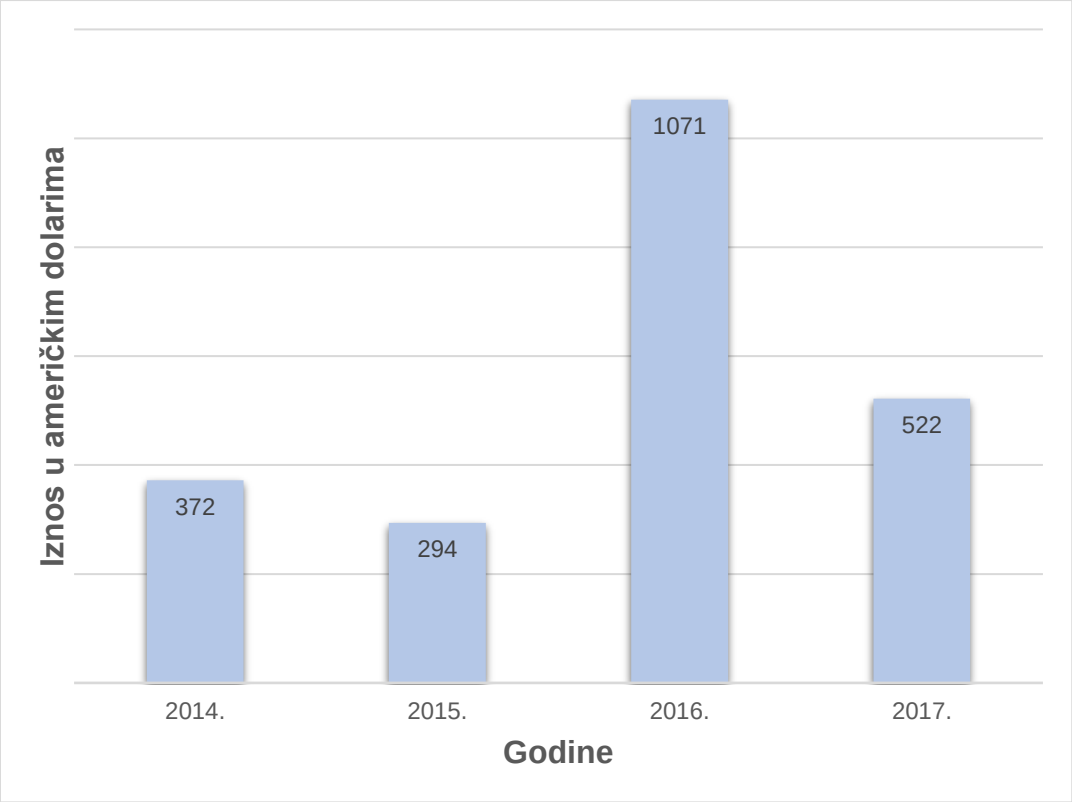


Grafikon 3. Najveći udio napada ucjenjivačkim softverom po državama u odnosu na svijet kroz razdoblje od ožujka 2017. do ožujka 2018. godine

Izvor: [29]

Grafikon 3 prikazuje države s najvećim ukupnim postotkom zahvaćenih napada ucjenjivačkim softverom u cijelom svijetu. Podatci se odnose na sve tipove korisnika, operacijske sustave i vrste terminalnih uređaja. Iz grafičkog prikaza vidljivo je kako je se taj najveći udio napada u postotcima odnosi na zemlje s najvećim brojem stanovništva. Razlog tome može se tražiti u velikoj informatički pismenoj populaciji koja koristi raznolike terminalne uređaje zajedno s njihovih pripadajućim sustavima.

Kao glavni cilj napadača obično se ističe financijsko okorištavanje žrtvom te zarada. Vođeni tom tezom, napadači često mijenjaju taktike kod izrade ucjenjivačkih prijetnji pa prema tome i iznose potraživane otkupnine. Trend rasta potraživanja stabilizirao se u usporedbi proteklih nekoliko godina što je vidljivo na grafikonu 4. On prikazuje prosječni iznos potraživane otkupnine prema žrtvama izražen u američkim dolarima.

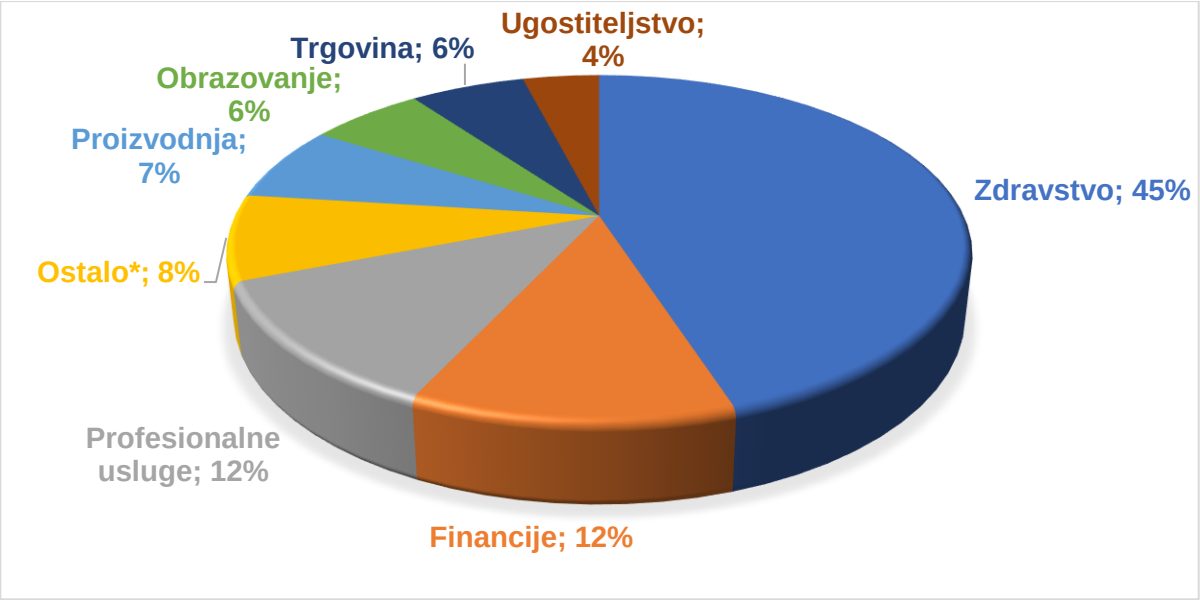


Grafikon 4. Prosječan iznos tražene otkupnine od strane napadača po godinama
Izvor: [29]

Iz prethodnog prikaza grafikona 4, može se zaključiti kako se visina tražene otkupnine ucjenjivačkog softvera s vremenom stabilizira. Ne realne, visoke cijene ne dovode do krajnjeg cilja *cyber* kriminalaca a to je profit. Složeniji *ransomware* i manja otkupnina pruža veću šansu za uspjeh napadača.

Kada je riječ o motivu tj. zaradi, napadači pokušavaju prodrijeti u sve sektore industrije, ne prezajući ni pred čime. Svaki industrijski sektor je pogođen u većoj ili manjoj mjeri. Napadači pažljivo biraju industriju u kojoj postoji najveća vjerojatnost kako će žrtve uplatiti potraživanu otkupninu. Prikaz industrijskih sektora najviše

pogođenih ucjenjivačkim prijetnjama vidljiv je na grafikonu 5. Pod kategorijom *Ostalo*, ubrajaju se sektori kao što su komunalne usluge, građevinska industrija, nekretnine te državne službe.



Grafikon 5. Industrijski sektori najviše pogođeni ucjenjivačkim softverom u 2017. godini

Izvor [30]

Iz prethodnog grafikona 5, vidljivo je kako su mete *cyber* kriminalaca najčešće bile zdravstvene ustanove u odnosu na ostale industrijske sektore. Upravo je zdravstveni sektor najosjetljiviji iz razloga što nedostupnost njegovih informacijsko-komunikacijskih sustava te terminalnih uređaja može rezultirati ljudskim žrtvama. Ta činjenica zdravstvenom sektoru ne ostavlja mnogo manevarskog prostora kod zaraze ucjenjivačkim softverom osim plaćanja tražene otkupnine što koriste sami napadači.

Kako bi se na kraju ovog dijela stvorila cjelovita slika problema, pametno je ucjenjivački softver staviti u kontekst s ostalim zlonamjernim softverom. Uspoređujući te gledajući omjere rasprostranjenosti tih dvaju oblika prijetnji, vidljivo je kako je upravo ucjenjivački softver dobio na popularnosti prethodnih godina što ga izdvaja kao jednog od najopasnijih izvora prijetnji današnjice. Tablični prikaz država s najvećim udjelom napada kriptografskim ucjenjivačkim softverom u svijetu prikazanim u postotcima vidljiv je na tablici 2. Taj iznos je prikazan u odnosu na sve korisnike te države koji su napadnuti bilo kojim, drugim tipom zlonamjernog softvera:

Tablica 2. Usporedba godišnje promjene stope napada kriptografskim ucjenjivačkim softverom kod država s najvećim omjerom zaraze ucjenjivačkim softverom na ostali zlonamjerni softver u razdoblju 2016.-2017. te 2017.-2018. godine

Država	Postotak napada u razdoblju 2016.-2017. godine	Postotak napada u razdoblju 2017.-2018. godine
Tajland	3,43%	9,57%
Ujedinjeni Arapski Emirati	6,08%	8,67%
Iran	5,86%	8,47%
Bangladeš	6,25%	7,62%
Vijetnam	7,52%	6,17%
Saudijska Arabija	3,48%	5,45%
Kina	3,78%	5,36%
Indija	7,06%	4,28%
Alžir	3,84%	3,59%
Turska	7,93%	3,22%
Ostale države	44,77%	37,60%

Izvor: [31]

Iz tablice 2 se može zaključiti kako su najozbiljnije ugrožene azijske zemlje s relativno velikom populacijom. Dodatno tome, unutar tog velikog broja korisnika pozamašan udio je onih koji nisu svjesni opasnosti ucjenjivačkih prijetnji niti su o njima informirani što ih svrstava u idealan profil žrtve. U većini iznad navedenih država vidljiva je trend rasta napada kroz godinu što ukazuje kako se ne radi na edukaciji korisnika u svrhu prevencije prijetnji. Ukupno gledajući ostale zemlje svijeta, trend samih napada je u padu ali je i dalje na vrlo visokoj stopi od približno četvrtine svih ostalih zlonamjernih napada i prijetnji te kao takav i dalje predstavlja velik problem za sigurnost terminalnih uređaja i krajnjih korisnika.

4. Ciljevi i žrtve napada ucjenjivačkim softverom

U nastavku će biti iznijete informacije o tome koje tipove korisnika terminalnih uređaja hakeri imaju na meti te putem kojih terminalnih uređaja oni postaju žrtve uz segmentaciju korisnika, uređaja te na kraju njihovih platformi (operativnih sustava).

4.1. Subjekti napada

Kada se govori o subjektima napada obično se misli na sve tipove korisnika koji će na kraju njime biti zahvaćeni. Prilikom realizacije napada, najčešći plan hakera je zahvatiti širok spektar korisnika što im kao rezultat može pružiti ili barem povećati šanse za većom zaradom, profitom. Napadi na pojedinačne ciljeve nisu u tolikoj mjeri profitabilni ali se ipak događaju kao kampanje s namjerom nanošenja nekog oblika štete ili kako bi se narušio ugled tog pojedinca.

4.1.1. Rezidencijalni korisnici

Krajnji, rezidencijalni korisnici su jedni od najčešćih žrtava pogođenih napadima ucjenjivačkim softverom. Iako nisu primarna meta hakera, među ucjenjivačkim softverom koji se automatizirano distribuira i širi svakako čine najveći broj. Uzrok tome leži u činjenici kako se u njihove sustave zlonamjerni ucjenjivački softver vrlo lako implementira zbog manjka, nedostatka korištenja sigurnosnih rješenja te znanja i informacijama o prijetnjama kako bi bili u stanju poduzeti preventivne korake i na taj način se zaštititi. Njihova nedovoljna informiranost pogoduje napadačima jer uz prikazane ucjenjivačke poruke i vrijeme koje odbrojava postižu efekt panike i straha te se na temelju njih, korisnici odlučuju za uplatu otkupnine. Za neke iznose otkupnine koji su izvan granica mogućnosti rezidencijalnih korisnika postoji vjerojatnost kako neće biti uplaćeni jer se njihovi kriptirani podatci sastoje od multimedijskih datoteka (slike, videozapisi, glazba i sl.) a rjeđe od podataka bitnih za poslovanje, [9], [11].

Korištenje raznih nesigurnih internetskih usluga i servisa poput posjećivanja web stranica za gledanje *online* filmova i serija te web stranica za preuzimanje ilegalnih piratskih datoteka (npr. *torrent*) te općenito manjak pažnje može dovesti do infekcije ucjenjivačkim softverom u suprotnosti s ograničenim korištenjem takvih usluga propisanih sigurnosnim politikama kod većih korporacija. Također, vrlo mali broj prosječnih korisnika ima naviku stvarati sigurnosne kopije sustava, podataka i važne datoteke čuvati na posebnim tvrdim diskovima ili drugim načinima pohrane. Zanemarivanje sigurnosnih ažuriranja računalnih komponenti (prevencija od *exploit kit* prijetnji), ažuriranja antivirusnih programa, korištenje zastarjelih terminalnih uređaja s operativnim sustavima bez adekvatne programske podrške (npr. Windows XP) te korištenje piratskih programa spada pod još jedan obrazac ponašanja karakterističan za prosječne rezidencijalne korisnike. Taj obrazac ih dodatno svrstava u najrizičniju skupinu, [9]. Jedan od primjera napada na rezidencijalne korisnike dogodio se u prosincu 2017. godine kada su prema izvoru [32], korisnici u Hrvatskoj, Bosni i Hercegovini te Srbiji zaprimali *phising* e-mail poruke koje navodno sadržavaju potraživanje duga od strane državnih financijskih agencija, poput

hrvatske FINE. Riječ je bila o napadu File Spider kriptografskim ucjenjivačkim softverom.

4.1.2. Poslovni korisnici

Principi današnjeg poslovanja izgrađeni su na korištenju terminalnih uređaja, mrežne infrastrukture te njenih usluga i servisa. Upravo to poslovne korisnike čini primamljivom metom ucjenjivačkih napada. Svaki gubitak vremena i prilika za rad, poslovne korisnike stoji puno financijskih sredstava stoga u slučaju uspješno provedenog napada ucjenjivačkim softverom postoji velika vjerojatnost kako će korporacije uplatiti otkupninu da bi čim prije mogli nastavi radom uz što manje daljnje poslovne gubitke. Takve su otkupnine vrtoglavih iznosa jer *cyber* kriminalci znaju da za dobro poslovanje ne postoji cijena. Kako se u poslovnom okruženju velik broj djelatnosti temelji na digitalnim podatcima, informacijama i bazama podataka, poslovne kompanije često posjeduju dodatne, redundantne terminalne uređaje poput poslužiteljskih računala za njihovo čuvanje i za izradu sistemskih sigurnosnih kopija. Također, dodatni poslužitelji mogu biti i jedan model sigurnosnog rješenja ako dođe do napada ucjenjivačkim softverom.

Veće kompanija uz redundantne poslužitelji posjeduje ozbiljnija komercijalna sigurnosna rješenje implementirana u svoje sustave s robusnijom infrastrukturom te su kao takva otpornija na napade u suprotnosti s manjim i skromnijim poslovnim kompanijama. Unatoč navedenome, iskusnijim hakerima veće kompanije i korporacije postaju jedna od primarnih meta te za njih razvijaju inačice ucjenjivačkih softvera sa sposobnošću prodiranja i infekcije takvih složenijih sustava. Uz današnje sigurnosne standarde koji su u konstantnom razvoju, veće kompanije u manjoj su mjeri pogođene takvim naprednijim ucjenjivačkim softverom ali ako grupa hakera uspije provaliti u sustav ili dio sustava jedne ili dvije kompanije, može ostvariti dobit te isplatiti svoj trud i vrijeme uloženog u takav softver. Dodatno, infiltracijom u cjelovit ili dio sustava osim mogućnosti zarade, kriminalcima pruža i drugu mogućnost širenja na ostale sestrinske tvrtke i kompanije putem kompromitirane informacijsko-komunikacijske mreže, [9].

Primjer nedavnog napada na jednu od većih kompanija, Taiwan Semiconductor Manufacturing Company (TSMC) pokazuje kako nitko nije siguran. TSMC, jedna od vodećih tvrtki u svijetu po proizvodnji integriranih krugova, čipova te mikroprocesora napadnuta je u svibnju 2017. godine nakon što je WannaCry *ransomware* nehotice unesen na mrežu kompanije od strane vanjskih suradnika te samo u početnoj fazio zahvatio 10000 terminalnih uređaja kompanije, [33].

4.1.3. Javne i državne službe

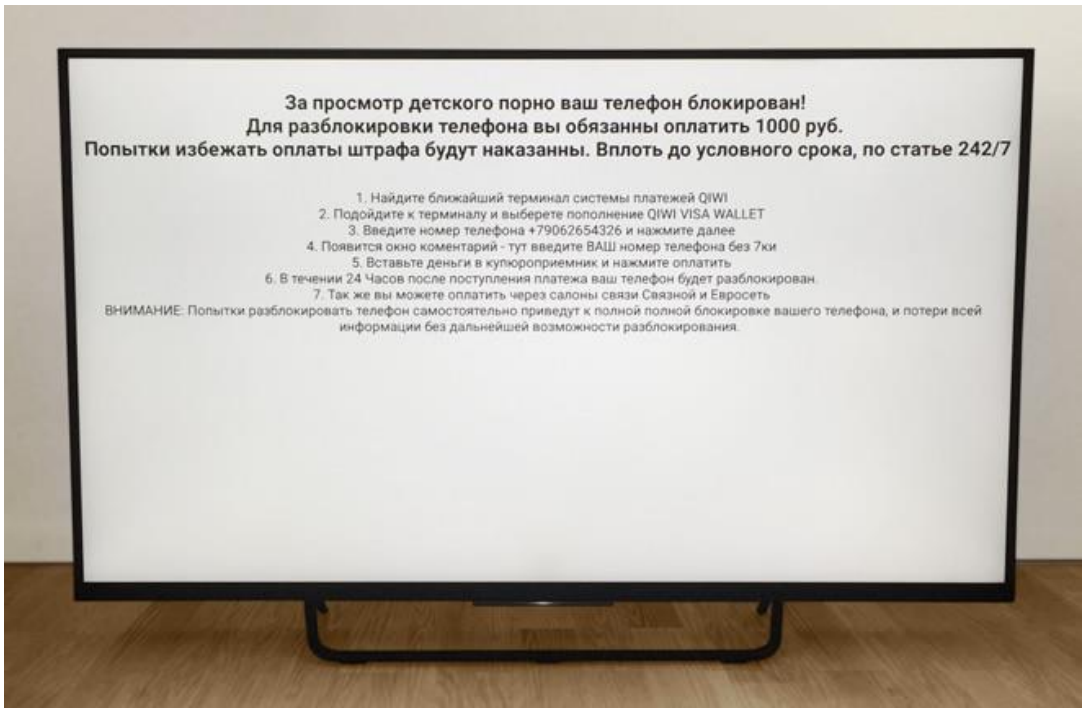
Još jedan od pogođenih sektora spada i u onaj javni. Na meti *cyber* kriminalaca često su policijske i ostale sigurnosne službe koje protiv njih bore. Pokušavajući ući u trag hakerima, policija i ostale službe često se dovedu na samo liniju napada. Hakeri imaju za cilj onesposobiti ih kako bi bezbrižno mogli izvršavati svoje kriminalne aktivnosti. Hitne državne službe i institucije uz policiju poput vatrogasaca,

službe za zaštitu i spašavanje, hitne medicinske pomoći i ostalih čija je zadaća pomoć ljudima u hitnim situacijama znaju se naći na listi hakera jer te ključne institucije ne mogu podnijeti pad svojih sustava i obično uplaćuju željeni iznos otkupnine. Jedan od specifičnih slučajeva su zdravstvene službe i institucije. Bolnice se znale biti napadnute zbog svoje izloženosti podataka o pacijentima koji su vrlo važni za njihovo liječenje te su one iz tog razloga bez pogovora plaćale za otključavanje svojih računala i podataka. Zanimljivo je kako su nakon napada na jednu američku bolnicu koja se je slučajno zarazila ucjenjivačkim softverom (nije bila cilj napada) hakeri dobrovoljno otključali podatke iako se na takve slučajeve organizacije ne oslanjaju jer su vrlo rijetki. Uz navedeno poznati su primjeri napada na policijsku i vatrogasnu postaju u američkom gradu Riversideu u saveznoj državi Ohio iz travnja 2018. godine, gdje su te dvije postaje javnih službi napadnute i zaražene kriptografskim ucjenjivačkim softverom. Postaje su oglasile kako nisu platile otkupninu jer su uspjele spasiti dio podataka sa svojih terminalnih uređaja (putem *backup-a*) ali da su nepovratno izgubili podatke vezane uz rad prethodnih 10 mjeseci, [34]. Također, poznat je i napad na bolnicu Hancock Helath iz američkog grada Greenfielda koja je zaražena kriptografskim *ransomwareom* SamSam u siječnju 2018. godine. SamSam napada poslužiteljska računala te se njima širi dalje na sustav. Bolnica je platila otkupninu u iznosu od 55000 američkih dolara nakon čega su joj podatci i ostali resursi postali dostupni, [35].

Česta meta su i financijske organizacije, banke ali one redovno svoje resurse ulažu u sigurnosne mehanizme i zaštitu infrastrukture te predstavljaju tzv. tvrd orah za hakere. Bankarski sektor u najvećoj mjeri bio je pogođen u Velikoj Britaniji i SAD-u gdje se ucjenjivački softver širio putem tzv. *botnets* mreža. Poznati su slučajevi napada na obrazovne ustanove, fakultete, fakultetske kampuse te škole. Ovakvi napadi su posebno opasni jer osim prodora u mrežu i računala fakulteta, hakeri se mogu infiltrirati i na računala sami korisnika odnosno studenata, profesora i profesora čime se povećava broj žrtava i time nastaje veća šteta. Primjer je napad iz 2015. godine na školskom području New Jerseya s nekoliko osnovnih škola gdje je potraživana otkupnina iznosila 500 Bitcoina čija je tadašnja protuvrijednost iznosila 124000 američkih dolara, [9], [11].

4.2. Ugroženi sustavi

Zlonamjerni hakeri iskorištavaju činjenicu da je korištenje terminalnih uređaja svih vrsti u porastu kao i svakodnevna potražnja za raznim informacijama i podatcima. Društvo je svakim danom sve više digitalizirano i informatizirano pa prema tome svatko tko posjeduje bilo kakav terminalni uređaj može postati žrtva *cyber* kriminalaca. Između tradicionalnih sustava terminalnih uređaja poput osobnih računala, poslužiteljskih računala te pametnih mobilnih uređaja važno je spomenuti i sveprisutne IoT koji sve više plijene pažnju hakera.



Slika 11. Pametni TV inficiran s ucjenjivačkim softverom, [36]

TV uređaji, hladnjaci, klima uređaji, pametne kućne i javna rasvjeta, POS uređaja (engl. *Point Of Sale*), razni medicinski aparati, automatizirani gradski uređaji za regulaciju prometa te na kraju i autonomna vozila mogu se okarakterizirati kao budući izvori prihoda *cyber* kriminalaca. Iako nisu u potpunosti zaživjeli, njihov trend rasta sve je veći a time i problem njihove zaštite koji ne prati paralelno taj rast. Stoga se smatra kako bi napadi u budućnosti mogli ponajviše biti usmjereni takvim uređajima. Primjer takvog napada vidljiv je i sa slike 11 gdje na ruskom jeziku piše: „Ucjenjivački softver funkcionira i na pametnim TV uređajima! Prema licenci Ionut Ilascu, datuma 27. studenog 2015. vaš uređaj je zaključan zbog gledanja sadržaja dječije pornografije. Kako bi otključali Vaš uređaj, uplatite 1000 ruskih rubalja prema niže napisanim uputama. Svaki pokušaj izbjegavanja kazne bit će sankcioniran prema članku zakona 242/7“. Jasan je pokušaj utjecanja socijalnim inženjeringom na samog korisnika tj. žrtvu.

4.2.1. Osobna računala

Osobna računala spadaju u kategoriju uređaja koja je najviše pogođena napadima s ucjenjivačkim softverom. Uz to, većina takvog softvera dizajnirana za infekciju Windows operativnog sustava koji je najšire rasprostranjen. Osobna računala najmanje su osigurana od napada što je prethodno objašnjeno. Razlog se može tražiti u njihovim vlasnicima, rezidencijalni korisnicima nad kojima je iznimno lagano izvršiti napad putem socijalnog inženjeringa. Upravo su različite inačice Windows platforme operativnog sustava zastupljene u 89% svih osobnih računala dok se ostatak dijeli na macOS i Linux operativne sustave. Kako bi hakeri proširili svoj maliciozni softver, koriste greške u programskom kodu tih operacijskih sustava ili mane unutar njihovih aplikacijskih programabilnih sučelja. Navedeno stvara problem hakerima jer pri izradi softvera moraju implementirati takve karakteristične propuste što njih krajnji rezultat čini opasnim za točno određen operativni sustav.

Kako je zastupljenost Windows platforme 89%, to im ne stvara pretjeranu brigu. Unatoč tome, korisnici osobnih računala s macOS i Linux operativnim sustavima nisu u potpunosti sigurni jer njih najviše pogađa ucjenjivački softver pod nazivom Browlock Trojan. On je neovisan o operativno sustavu jer se inficira putem raznih web preglednika koji su interoperabilni među sva tri navedena operativna sustava. Iako su za macOS bili razvijeni posebni ucjenjivački softveri poput Mabouta i KeRangera. Dok je prvotni bio samo koncept za koji je ubrzo Apple izdao zakrpu kroz ažuriranje, drugi je bio ozbiljniji. Distribuiran je putem kompromitiranog BitTorrent klijenta i vršio enkripciju korisničkih podataka uz traženu otkupninu u iznosu od 1 Bitcoina. U svojem programskom kodu, sadržavao je identifikacijski Mac broj čime ga je operativni sustav smatrao pouzdanim te ga nije blokirao ili onemogućavao. Apple je ubrzo uvidio rupu u sustavu i riješio je ažuriranjem, [9], [11], [37].

4.2.2. Poslužiteljska računala

Prvi zabilježeni napadi na kompanije bili su u obliku DDoS napada koji su često uspješno odbijani pa su napadači promijenili taktiku i svoju pažnju usmjerili ka poslužiteljskim računalima. Za razliku od osobnih računala, poslužitelji kompanija sadržavaju puno veću količinu podataka koji ujedno mogu biti ključni za rad i opstanak poslovanja kompanije. Primjeri takvih tipova podataka su:

- Radni dokumenti
- Izvorni kodovi aplikativnih rješenja kompanije
- Tragovi izvršenih transakcija i drugi financijski podatci
- Poslovni tajni dokumenti
- Korisničke baze podataka
- Podatci o korištenoj sigurnosnoj zaštiti i primijenjenim standardima

Ukoliko se samo jedan dio infrastrukture kompanije bude kompromitiran, primjerice njen poslužitelj, napadači će imati sve vitalne informacije o njoj i moći će proizvesti još ozbiljniji i prodorniji napad. Iz tog razloga često su iznosi otkupnina namijenjenih kompanijama i do 10-15 puta veći nego kod napada na osobna računala te takvi iznosi budu i uplaćeni. Iako veće tvrtke brinu o sigurnosti svojih poslužitelja i pripadajućoj opremi, česte su pojave loših sigurnosnih politika te slaba organizacija i implementacija redundantne poslužiteljske infrastrukture.

Drugi obrazac ponašanja vidljiv kod raznih kompanija je posjedovanje kvalitetne sigurnosne politike i infrastrukture u kombinaciji s dobro odrađenim redundantnim poslužiteljima ali uz njihovo neredovito iskorištavanje. Primarno se ovdje misli na zastarjele verzije operacijskih sustava te sigurnosnih alata i rješenja što pruža mogućnost iskorištavanja dobro poznatih propusta u tim programima za infiltraciju i širenje infekcije među tvrtkinom informacijsko-komunikacijskom infrastrukturom. Napadi na poslužiteljska računala se obično izvode instalacijom određenog programskog koda tj. zakrpe na operacijski sustav poslužitelja kako on ne bi mogao biti izmijenjen ili legitimno ažuriran od strane kompanije. Zatim se prelazi na enkripciju podataka koja može trajati vrlo dugo zbog njihove velike količine. Nakon određenog kriptiranja, napadači uklanjanju svojevrsnu zakrpu, te putem poslužitelja na računala tvrtke prikazuju ucjenjivačku poruku, [9], [11].

4.2.3. Pametni mobilni uređaji

U ovu kategoriju spadaju dvije vrste ovakvih pametnih uređaja a to su:

- Pametni mobilni uređaji (tzv. *smartphones*)
- Nosivi uređaji (tzv. *wearables*)

Iako je se trenutno većina napada ucjenjivačkim softverom odnosi na osobna računala, valja napomenuti kako svjetski trendovi pokazuju rapidan rast korištenja pametnih mobilnih uređaja što može nagovijestiti kako će se povećati broj *ransomware* napada na njih u budućnosti. Kada se govori o pametnim mobilnim telefonima u današnje vrijeme većinom se misli na dvije najzastupljenije platforme koje ih pokreću: Android operativni sustav i iOS operativni sustav. Osim zastupljenosti, koja iznosi kako Android drži oko skoro 86% svjetskog tržišta a iOS oko 16%, [38] to nisu jedine razlike. One se očituju u sigurnosnom dijelu.

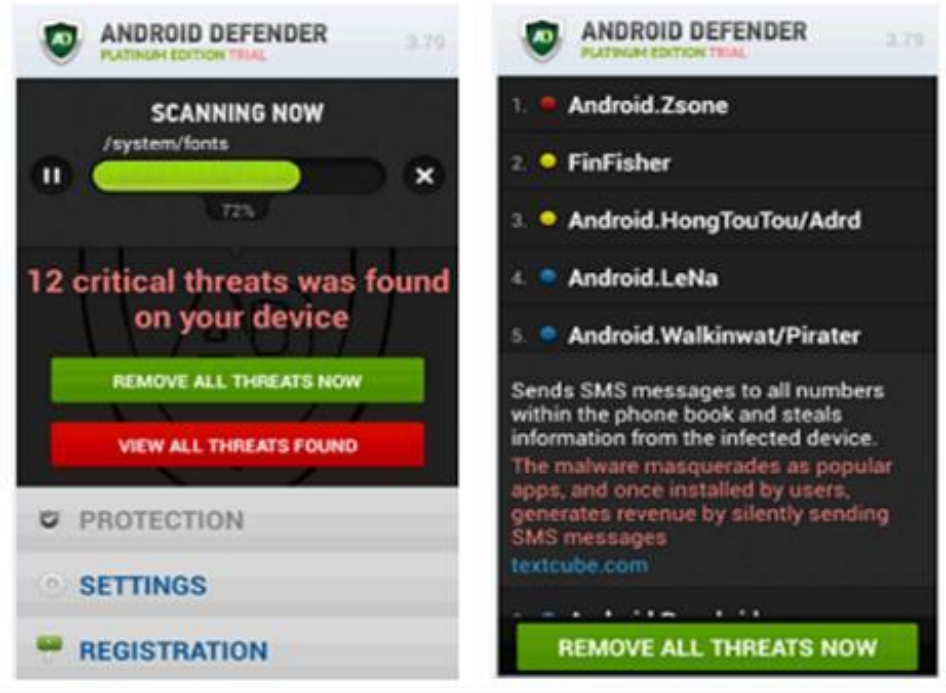
Korisnici iOS uređaja koji nisu samostalno omogućili pristup sustavu (tzv. *jailbreak*) već su koristili tvorničke postavke uređaja i redovito ažurirali sustav bili su jako dobro zaštićeni jer je Apple pazio na sigurnost korisnika svoga prepoznatljivog ekosustava. On je jako ograničen te se korisnicima onemogućava instalacija aplikacija od nepouzdanih trećih strana što se u ovom slučaju pokazalo kao dobar korak prema sigurnosti. Kako bi učinio aplikacije na svojem App Storeu pouzdanima, Apple koristi dodjelu certifikata razvojnih programera. Ako bi se neka hakerska skupina odlučila za napad na iOS operativni sustav, prvo bi za kompromitiranu aplikaciju kojom bi se ucjenjivački softver širio trebala dobiti navedeni certifikat. Uz stroge Appleove kontrole to je takoreći nemoguće te se iz tog razloga napadačima ne isplati ulagati u razvoj ucjenjivačkog softvera za iOS, [9], [11], [37].

S druge strane, Android se oslanja na otvorenost i mogućnost prilagodbe svojeg operativnog sustava od strane korisnika. Mnogi korisnici vole otvorene mogućnosti koje pruža Android, poput instaliranja aplikacija od trećih strana, prilagodbe samog operativnog sustava (putem tzv. *custom rom*-a), njegovog dijela za izradu sigurnosnih kopija (tzv. *custom recoveries*) otključavanja dijela sustava zaduženog za njegovo pokretanje (tzv. *bootloader*) te omogućavanja sustavnog korijenskog pristupa (tzv. *rooting*). Uz sve navedeno, može se zaključiti kako upravo ova platforma pruža priliku hakerima za izvršavanje ucjenjivačkih napada na Android pametne mobilne telefone. Važno je napomenuti kako korisnici uređaja s verzijom Androida starijom od 5.0, moraju biti oprezniji prilikom korištenja uređaja jer su stariji uređaji manje otporniji na maliciozne softvere te im se preporučuje korištenje nekog oblika antivirusne zaštite.

Android.Fakedefender iz 2013. godine jedan je od tipova zaključavajućeg ucjenjivačkog softvera koji lažno djeluje kao antivirusni alat. Nakon skeniranja uređaja javlja kako su pronađene sigurnosne prijetnje u obliku malicioznog softvera ili koda te zaključava radnu površinu onemogućavajući korisniku pokretanje bilo kojih drugih aplikacija te uklanjanje Android.Fakedefendera deinstalacijom. Kako je riječ o tipu ucjenjivačkog softvera koji zaključava radnu površinu, njegovo uklanjanje je

moguće ukoliko korisnik uđe u tzv. *safe mode* te ga ručno ukloni. Android.LockDorid.E je tip kriptografskog ucjenjivačkog softvera iz 2014. godine te dijeli sve karakteristike sa svojim srodnim softverom prilagođenim za osobna računala. On se širi kroz kompromitiranu aplikaciju za gledanje video sadržaja za odrasle kako bi tematski naveo korisnike da ju instaliraju. Nakon instalacije prikazuje korisniku poruku s lažnim upozorenjem policije kako je gledan nedozvoljen sadržaj i porukom za uplatu na iznos kazne od 500 američkih dolara. Još jedan primjer ucjenjivačkog softvera za Android je Android.Simplelocker. On je kriptografskog tipa te je funkcionirao na starijim inačicama softvera na kojima je kriptirao unutarnju i vanjsku pohranu uređaja. Drugi pokušaji napada *ransomwareom* uključivali su softver s mogućnošću postavljanja lozinke za zaključavanje zaslona ukoliko ona nije bila aktivirana.

Kako su ovo uređaji na kojima nije praktično raditi u poslovnim aplikacijama te obavljati produktivne poslovne stvari, hakeri su smanjili pokušaje kriptografskih napada zbog neimanja dovoljno važnih podataka na takvim uređajima. Rastom njihove interne pohrane, kvalitetnijim kamerama, razvojem mobilnog plaćanja te sve manjim smanjivanjem razlike u korisničkom iskustvu između tih uređaja i osobnih računala postoji mogućnost da se navedeno promijeni zbog količine dnevno dostupnih podataka koji će se sve više pohranjivati na njima, [11].



Slika 12. Sučelje Android Fakedefender ucjenjivačkog softvera, [39]

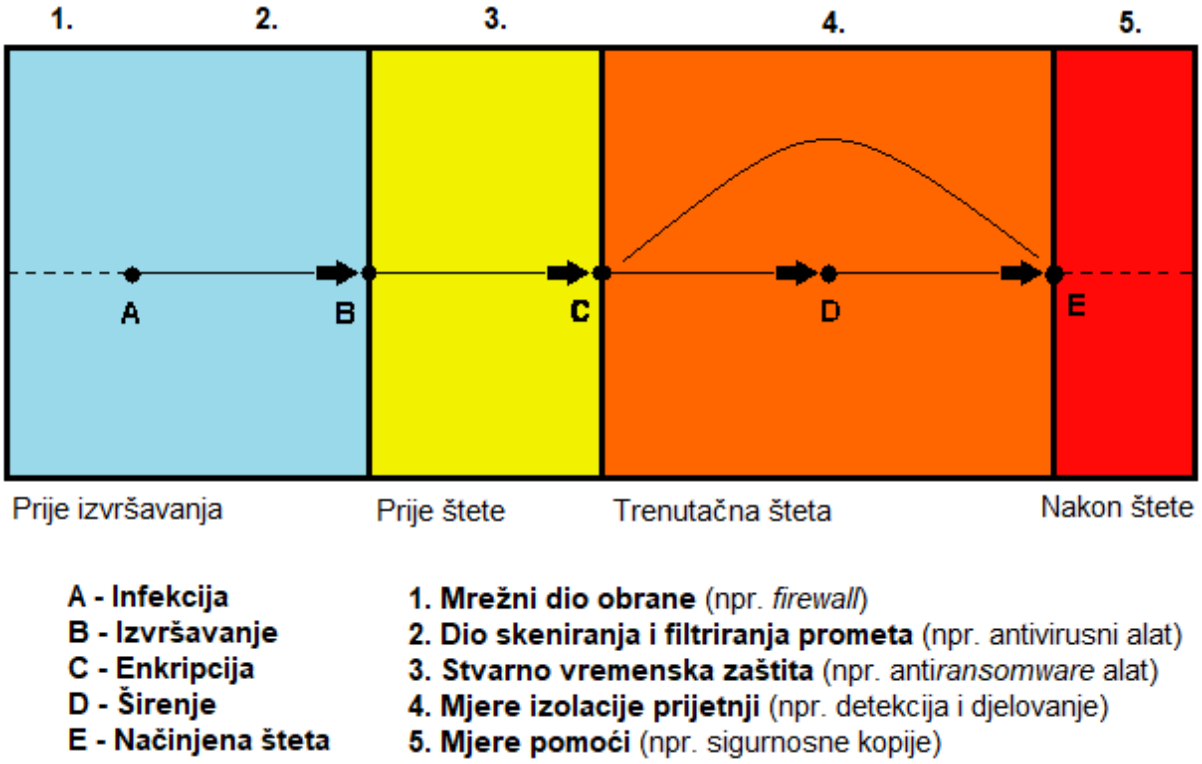
Pod nosive pametne uređaje (tzv. *wearables*) smatramo pametne satove, pametne narukvice, ogrlice, prstenje i sl. modne terminalne uređaje. Na ovom tržištu su također ključna dva operativna sustava, Android Wear za pametne satove i ostale nosive predmete te watchOS kojim je pokretan Appleov pametni sat. Početni trendovi korištenja bili su brzo rastući ali su zadnjih godina usporili. Uz to, cijene

nosivih uređaja pokretanih Android Wear operativnim sustavom značajno su pale pa i dalje postoji određeni tržišni udio. Kako je riječ o uređajima malih dimenzija, ograničenih procesorskih mogućnosti i ograničenim funkcionalnostima korištenja te davanja naredbi putem malih zaslona na dodir i glasovnih naredbi, ovakav tip uređaja nije sklon hakerskim napadima ucjenjivačkim softverom. Teorijski ona postoji ali nije zapažena u tolikoj mjeri. Njihov prostor pohrane izuzetno je beznačajan te se u njega ne pohranjuju važni korisnički dokumenti u suprotnosti s osobnim računalima. Potencijalna opasnost leži u aplikacijama koje se instaliraju na pametni mobilni uređaj a zatim služe za komunikaciju s nosivim uređajem. Putem jedne takve kompromitirane aplikacije noseći uređaj bi mogao biti inficiran. Takve napade korisnik bi lako riješio samostalno potpunim tvorničkim resetiranjem uređaja dok ukoliko bi bila riječ o ozbiljnijem *ransomware* napadu, uređaj bi ostao softverski uništen, neupotrebljiv te bi na taj način korisniku bila načinjena šteta, [11].

5. Mogućnosti zaštite terminalnih uređaja i prevencije ucjenjivačkih prijetnji

Kako bi se zaštitili od raznovrsnih ucjenjivačkih prijetnji važno je poznavati kronološki slijed napada i djelovanja *ransomware* ucjenjivačkog softvera. Slijed se prema [40], može podijeliti na četiri faze:

I. Faza prije izvršavanja ucjenjivačkog softvera
II. Faza prije učinjene štete
III. Faza nastanka štete
IV. Faza oporavka od štete



Slika 13. Vremenska crta slijeda napada ucjenjivačkim softverom,

Izvor: [40]

Nakon razumijevanja kritičnih točki napada, može se početi s implementacijom zaštitnih postupaka. U njih svrstavamo preventivna djelovanja, detekciju i djelovanje u stvarnom vremenu te moguće opcije djelovanja nakon završetka uspješnog napada.

Faza prevencije je najlakši i najjednostavniji način zaštite od ucjenjivačkih napada. Ona prije svega obuhvaća apsolutno sve mjere zaštite te iako niti jedan terminalni uređaj nije 100% siguran od napada, navikama predostrožnosti i općenitom brigom moguće je u velikoj mjeri spriječiti izloženost i izbjeći same napade. Informiranost i edukacija o ucjenjivačkom softveru je polovica obavljenog posla zaštite. Krajnje korisnike treba educirati o ucjenjivačkom softveru, što je on, kakvu prijetnju

predstavlja, objasniti osnovne principe rada i sl. Također, preporučljivo je objasniti korisnicima i ostale *malware* prijetnje jer su one u korelaciji sa samim ucjenjivačkim softverom. Nadalje, korisnici bi trebali steći redovite navike kao što su: ažuriranja operativnog sustava te korištenih programa i aplikacija, izrada standardnih sigurnosnih kopija sustava i vlastitih podataka uz izradu tzv. *shadow copy* sigurnosnih kopija, korištenje komercijalnih ili barem besplatnih antivirusnih programa i aplikacija te ako je moguće dodatnih alata koji se temelje na zaštiti od ucjenjivačkih prijetnji, korištenje hardverski ili softverski temeljenih vatrozida za obranu na dijelu mrežnog sučelja, razumno pretraživanje i procjenjivanje pouzdanosti web stranica te na kraju razumljivo čitanje dobivene elektroničke pošte uz pažnju kod otvaranja sumnjivih poruka i priloga koje je također preporučljivo skenirati antivirusnim alatima.

Kako i uz pridržavanje svih navedenih preporuka, korisnikov terminalni uređaj može biti zahvaćen ucjenjivačkim softverom s primjerice legitimnih web stranica koje su vanjskim napadom kompromitirane. Zadnja linija preventivne obrane temelji se na redundanciji. Poželjno je posjedovati barem jedan uređaj za pohranu (npr. tvrdi disk) koji će sadržavati sve redovno izrađene sigurnosne kopije sustava te korisničkih podataka. On se ne bi trebao stalno nalaziti priključenim na terminalni uređaj i mrežu kako i on ne bi postao kompromitiran. Korištenje ostalih mrežnih pohrana kao usluga pohrana u oblaku (tzv. *cloud*) koje sadrže korisničke podatke i sigurnosne kopije je također preporučljivo. Što je veći broj kopija podataka, sigurnost će biti zajamčena jer i u najgorem scenariju da svi prethodno navedeni mehanizmi zakažu, ucjenjivački program žrtvu, korisnika neće dovesti u očaj već će on moći razumno djelovati primjerice ponovnom instalacijom operativnog sustava, formatiranjem tvrdog diska te implementacijom posjedovanih sigurnosnih kopija.

Korisnici nikako ne bi trebali plaćati otkupninu jer upravo time potiču napadače na dodatne napade koje su upravo oni financirali. Ako se ipak žrtve odluče na uplatu, trebaju biti svjesni činjenice da ne postoji jamstvo kako će njihovi podatci biti vraćeni. Također, jedna od prvih radnji ukoliko dođe do zaraze trebala bi biti informiranje policije i opće javnosti kako bi ostali korisnici mogli pravovremeno reagirati. Najbolji način obrane i zaštite je onaj slojeviti, koji uključuje sve prethodno navedene postupke.

Stadij napada između infekcije i aktiviranja ucjenjivačkog softvera vrlo je teško uočljiv, prilika za djelovanje pruža se tek neposredno nakon aktivacije ucjenjivačkog softvera. U tom trenutku napad se ne može spriječiti, kao niti vratiti učinjena šteta, jedina opcija je zaustavljanje njegovog daljnjeg napredovanja. Na tržištu postoje razni alati koji detektiraju ucjenjivački softver i sprječavaju njegovo širenje unutar sustava. Oni rade na principu blokiranja bilo kojeg softvera koji pokušava izmijeniti određene datoteke sustava te onemogućuju pokretanje datoteka koje je samostalno preuzeo ucjenjivački softver. Ako se primjerice radi o kriptografskog ucjenjivačkom softveru, postoji mogućnost da su neke datoteke kriptirane te da im korisnici neće moći pristupiti ali će daljnje širenje biti zaustavljeno zatvarajući *ransomware* u

karantenu unutar sigurnosnog programa. Upravo ovi postupci omogućit će dovoljno vremena za daljnju reakciju žrtve kako bi spasila ostale datoteke.

Žrtve ucjenjivačkih softvera nakon inicijalnog šoka i panike misle kako im ne ostaje mnogo mogućnosti osim plaćanja otkupnine. To često nije istina, te iako je napad uspješno izvršen, postoje neki postupci koji se preporučuju tom slučaju. Prvotno je važno zaraženi uređaj isključiti iz mreže kako se zaraza ne dalje širila. Ako je riječ o zaraženom poslužitelju također treba isključiti njegovu pohranu, tvrde diskove iz rada, jer se određene verzije ucjenjivačkog softvera šire i putem lokalno podijeljenih datoteka. Zatim je potrebno prepoznati o kojoj je verziji ili barem tipu ucjenjivačkog softvera riječ. Primjerice neke kriptografske prijetnje mijenjaju formate kriptiranih datoteka prema svojem nazivu (1edrh4h.locky) te izrađuju tekstualne datoteke (README.txt) koje sadrže informacije s kakvim softverom je izvršen napad. Prepoznavanje točnog oblika zlonamjernog softvera je ključno je postoje određeni lažni *ransomware* alati koji samo ispišu ucjenjivačku poruku a ustvari ne izvršavaju enkripciju. Za neke starije verzije već postoje sigurnosna rješenja i zakrpe te je iz tog razloga je važno prepoznati sve detalje koji mogu identificirati pojedini ucjenjivački softver. Pronalaženje izvora zaraze, datoteke, e-mail poruke ili web stranice putem kojeg je proširen ucjenjivački softver ili postupka kojim je započeta infekcija isto može poslužiti kao način identifikacije.

Nakon svih prikupljenih dokaza žrtva će biti u stanju potražiti samostalno ili uz pomoć drugih moguća rješenja problema te upozoriti ostale korisnike, potencijalne žrtve ukoliko je riječ o korporativnom okruženju. Nakon neuspješnog pokušaja potrage potencijalno dostupnih sigurnosnih alata, žrtve mogu krenuti na implementaciju redundantnih sigurnosnih kopija (ako ih posjeduju) te ponovnu instalaciju operativnog sustava kao zadnju mjeru kojom se neće uspjeti ništa spasiti ali će terminalni uređaj postati dostupan za korištenje. Nakon svakog napada važno je retrospektivno ga sagledati, pronaći vlastite propuste te ih ispraviti kako se isti ne bi ponovno dogodio, [9], [11], [17], [22], [37], [40].

Zaključak

Ucjenjivački softver predstavlja jednu od vodećih prijetnji današnjice u informatičkom svijetu, uzimajući u obzir i ostali zlonamjerni softver. Nagli razvitak cijele tehnologije, sklopovlja i terminalnih uređaja, a potom i programske podrške (softvera), doveo je do raznih prijetnji usmjerenih prema krajnjim korisnicima. Jedna od takvih novorazvijenih prijetnji je i ucjenjivački softver. On kao glavni cilj ima financijski se okoristiti žrtvom, onemogućavajući joj pristup resursima terminalnog uređaja ili korisničkim podatcima, a zatim potraživati novčana sredstva kako bi žrtva ponovo mogla pristupiti tim resursima. Gledajući iz perspektive društva, takvi napadi i prijetnje izrazito su štetni prvo za pojedinca, a potom i za gospodarstvo općenito.

Činjenice o porastu korištenja različitih terminalnih uređaja u različitim životnim situacijama na dnevnoj bazi, poput internetskog bankarstva i pohrane osjetljivih podataka na terminalnim uređajima, iskoristili su *cyber* kriminalci. Prepoznali su loše obrasce ponašanja korisnika u vidu slabe informatičke zaštite i slabije edukacije te stalno smišljaju nove načine distribucije i nadogradnje svih zlonamjernih softvera pa tako i ucjenjivačkog softvera. Na taj način pokušavaju biti ispred korisnika te infiltrirati ucjenjivački softver na terminalni uređaj i navesti žrtvu na plaćanje otkupnine. Sav ucjenjivački softver, uz navedene aktualne ucjenjivačke prijetnje u ovom radu, predstavlja sve veći problem kako prema korisnicima, tako i prema sigurnosnim stručnjacima zato što je osmišljen na taj način da iskorištava sve više propusta u samom hardveru i softveru terminalnih uređaja. Upravo različite karakteristike ucjenjivačkog softvera usporedno su prikazane u ovom radu kako bi se istaknula njihova potencijalna opasnost i problematika.

Stalnim educiranjem krajnjih korisnika o aktualnim ucjenjivačkim prijetnjama te o načinima zaštite, može se postići najveća sigurnost kroz samu prevenciju napada. Pri tome korisnici moraju promijeniti svoju svijest te kritične oblike ponašanja pri radu s terminalnim uređajima na mreži. Jedino se pravovremenom reakcijom educiranog korisnika te kvalitetnim zaštitama od zlonamjernih softvera tj. sigurnosnim alatima, ucjenjivački napadi mogu prvenstveno prevenirati, a potom i onemogućiti.

Literatura

[1] Subrahmanian, V.S., Ovelgonne, M., Dumitras, T., Prakash, B.A.: *The Global Cyber-Vulnerability Report,* Springer International Publishing, Švicarska, 2015.

[2] Prgomet, M.: *Karakteristike zlonamjernog softvera kao sigurnosne prijetnje mobilnim uređajima*, Završni rad, Sveučilište u zagrebu, Fakultet prometnih znanosti, 2017.

[3] Kaspersky portal. Preuzeto sa: https://www.kaspersky.com/resource-center/threats/adware [Pristupljeno: travanj 2018.]

[4] Kaspersky portal. Preuzeto sa: https://www.kaspersky.com/resource-center/threats/viruses-worms [Pristupljeno: travanj 2018.]

[5] Avast portal. Preuzeto sa: https://www.avast.com/c-keylogger [Pristupljeno: travanj 2018.]

[6] Microsoft portal. Preuzeto sa: https://www.microsoft.com/en-us/wdsi/threats/rootkits [Pristupljeno: travanj 2018.]

[7] Kaspersky portal. Preuzeto sa: https://www.kaspersky.com/resource-center/threats/spyware [Pristupljeno: travanj 2018.]

[8] AlienVault: *Beginner's Guide to Ransomware Prevention & Detection*,2017., Preuzeto sa: https://www.alienvault.com/resource-center/white-papers/ransomware-prevention?utm_medium=Email&utm_source=RENG&utm_content=REC&utm_campaign=Ransomware-BegGuide&utm_term=180108&mkt_tok=eyJpIjoiWXpSaU56QTBOR1E0Tm1NNCIsInQiOiJ5UXZGUnhiVjBHcWdtTGNkWmhPOHpIa1hiZEVyK0VRSnFwdFR5bWV0ZTJUNVVzc2NkVkZvTllGb1NhVG0wRGtEVHF1NHRVZVo0a3p0OWRRTStqQnV4Y2pxQUU2T1FhS29kbnNpa3RhRmVwVCtOU0RiM2l2RG50QjRtTCtRTnFoQyJ9 [Pristupljeno: lipanj 2018.]

[9] Nacionalni CERT, *Ransomware – plati za svoje podatke NCERT-PUBDOC-2017-2-346*, CARNET - Hrvatska akademska i istraživačka mreža, Hrvatska, 2017., Preuzeto sa: https://www.cert.hr/30383/ [Pristupljeno: lipanj 2018.]

[10] Trend Labs: *Ransomware Past, Present, and Future*, Trend Micro, 2017., Preuzeto sa: https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf [Pristupljeno: lipanj 2018.]

[11] Savage, K., Coogan, P., Lau, H., *Security Response The Evolution of Ransomware*, Symantec, California, SAD, 2015., Preuzeto sa: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf [Pristupljeno: lipanj 2018.]

[12] Kaspersky portal. Preuzeto sa: https://www.kaspersky.com/blog/ransomware-faq/13387/ [Pristupljeno: lipanj 2018.]

[13] Keonesoftware portal. Preuzeto sa: https://keonesoftware.com/guides/cryptolocker-2016/ [Pristupljeno: lipanj 2018.]

[14] Threatpost portal. Preuzeto sa: https://threatpost.com/critroni-crypto-ransomware-seen-using-tor-for- command-and-control/107306/ [Pristupljeno: lipanj 2018.]

[15] Srce.hr portal. Preuzeto sa: http://moodle.srce.hr/2016-2017/pluginfile.php/847977/mod_resource/content/3/14_Vje%C5%BEbe_RM_Sigurnost%20u%20ra%C4%8Dunalnim%20mre%C5%BEama_1617.pdf [Pristupljeno: lipanj 2018.]

[16] Microsoft portal. Preuzeto sa: https://cloudblogs.microsoft.com/microsoftsecure/2014/12/17/your-browser-is-not-locked/ [Pristupljeno: lipanj 2018.]

[17] O'Brien, D., *Internet Security Threat Report Ransomware 2017*, Symantec, California, SAD, 2017., Preuzeto sa: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf [Pristupljeno: lipanj 2018.]

[18] Nacionalni CERT, *Analiza WannaCry ransomwarea NCERT-PUBDOC-2018-1-354*, CARNET - Hrvatska akademska i istraživačka mreža, Hrvatska, 2018., Preuzeto sa: https://www.cert.hr/33204/ [Pristupljeno: lipanj 2018.]

[19] Symantec portal. Preuzeto sa: https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper [Pristupljeno: lipanj 2018.]

[20] De Bruycker, M., Petya/NotPetya Malware Report on worldwide infection, Centre for Cybersecurity Belgium, Brussel, Belgija, 2017., Preuzeto sa: https://www.cert.be/files/CERTbe_Petya_NotPetya_Malware_E.pdf [Pristupljeno: lipanj 2018.]

[21] Hansberry, A., Lasse, A., Tarrh, A., *Cryptolocker: 2013's Most Malicious Malware*, Boston University Arts & Sciences Department of Computer Science, Boston, SAD, Preuzeto sa: https://www.cs.bu.edu/~goldbe/teaching/HW55815/cryptolockerEssay.pdf [Pristupljeno: lipanj 2018.]

[22] Cyber Intelligence Team,*Ransomware: What You Need to Know*, Chech Point and Europol, Hague, Nizozemska, 2016., Preuzeto sa: https://www.europol.europa.eu [Pristupljeno: lipanj 2018.]

[23] Tech republic portal. Preuzeto sa: https://www.techrepublic.com/article/cryptowall-what-it-is-and-how-to-protect-your-systems/ [Pristupljeno: lipanj 2018.]

[24] Bleeping computer portal. Preuzeto sa: https://www.bleepingcomputer.com/virus-removal/ctb-locker-ransomware-information#ctb_locker [Pristupljeno: lipanj 2018.]

[25] Antivirus baidu portal. Preuzeto sa: http://antivirus.baidu.com/news/2014-08-01/1407367219.html [Pristupljeno: lipanj 2018.]

[26] News.softpedia portal. Preuzeto sa: https://news.softpedia.com/news/ransomware-hits-website-and-defaces-homepage-500359.shtml [Pristupljeno: lipanj 2018.]

[27] Statista portal. Preuzeto sa: https://www.statista.com/statistics/593093/leading-types-of-encryption-ransomware/ [Pristupljeno: lipanj 2018.]

[28] Statista portal. Preuzeto sa: https://www.statista.com/statistics/701029/number-of-newly-added- ransomware-families-worldwide/ [Pristupljeno: lipanj 2018.]

[29] *ISTR Internet Security Threat Report Volume 23*, Symantec, California, SAD, 2018., Preuzeto sa: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf [Pristupljeno: kolovoz 2018.]

[30] Beazley portal. Preuzeto sa: https://www.beazley.com/documents/Whitepapers/201802-beazley-breach-briefing.pdf [Pristupljeno: kolovoz 2018.]

[31] Kaspersky Lab, *KSN Report: Ransomware and malicious cryptominers 2016-2018*, SAD, 2018., Preuzeto sa: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/06/27125925/KSN-report_Ransomware-and-malicious-cryptominers_2016-2018_ENG.pdf [Pristupljeno: kolovoz 2018.]

[32] Barkly blog portal. Preuzeto sa: https://blog.barkly.com/file-spider-ransomware [Pristupljeno: kolovoz 2018.]

[33] The Hacker News portal. Preuzeto sa: https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+TheHackersNews+(The+Hackers+News+-+Security+Blog)&_m=3n.009a.1802.pa0ao0cjb7.13po [Pristupljeno: kolovoz 2018.]

[34] Bleeping computer portal. Preuzeto sa: https://www.bleepingcomputer.com/news/security/police-dept-loses-10-months-of-work-to-ransomware-gets-infected-a-second-time/ [Pristupljeno: kolovoz 2018.]

[35] ZDNet portal. Preuzeto sa: https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/ [Pristupljeno: kolovoz 2018.]

[36] Security ledger portal. Preuzeto sa: https://securityledger.com/2015/11/ransomware-works-on-smart-tvs-too/ [Pristupljeno: lipanj 2018.]

[37] O'Brien, D., Power, J., Wallace, S., *An ISTR Special Report: Ransomware and Businesses 2016*, Symantec, California, SAD, 2016., Preuzeto sa: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/ransomware-and-businesses-16-en.pdf [Pristupljeno: lipanj 2018.]

[38] Statista portal. Preuzeto sa: https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/ [Pristupljeno: lipanj 2018.]

[39] Quick Heal portal. Preuzeto sa: https://blogs.quickheal.com/they-come-they-hide-and-they-mess-up-android-obad-and-android-fakedefender/ [Pristupljeno: lipanj 2018.]

[40] Barkly portal. Preuzeto sa: https://www.barkly.com/ransomware-protection-and-prevention [Pristupljeno: lipanj 2018.]

Popis kratica

AES	(Advanced Encryption Standard) napredni enkripcijski standard
API	(Application Programming Interface) sučelje za programiranje aplikacija
BTC	(Bitcoin) virtualna kriptovaluta
CAB	(Cabinet file format) format datoteke
CTB	(Curve-Tor-Bitcoin) tip kriptografskog ucjenjivačkog softvera
DDoS	(Distributed Denial of Service) uskraćivanje usluge
DHCP	(Dynamic Host Configuration Protocol) protokol dinamičke dodjele IP adresa
DOC	(Document file format) format datoteke
ECC	(Elliptic Curve Cryptography) algoritam šifre javnog ključa
EXE	(Executable file exstension) imenska ekstenzija izvršne datoteke
HTML	(HyperText Markup Language) prezentacijski jezika za izradu internetskih stranica
IoT	(Internet of Things) Internet stvari
IP	(Internet Protocol) Internet protokol
JPG	(Joint Photographic Experts Group file format) format datoteke
MBR	(Master Boot Record) programski zapisa za učitavanje operativnog sustava
NSA	(National Security Agency) američka sigurnosna agencija
NTFS	(New Technology File System) formatski sistem pohranjenih datoteka
PDF	(Portable Document Format) prenosivi format dokumenta
PHP	(Hypertext Preprocessor) programski jezik za web stranice
POS	(Point Of Sale) sustav praćenja transakcija na mjestu prodaje
PPI	(Pay-Per-Install) model plaćanja po izvedenoj instalaciji
PPT	(Presentation file format) format datoteke
RAR	(Archive file format) format datoteke
RaaS	(Ransomware-as-a-Service) model ucjenjivačkog softvera kao usluge
RDP	(Remote Desktop Protocol) protokol sesije udaljene veze
RSA	(Public-key encryption) algoritam šifre javnog ključa
SMS	(Short Message Service) slanje kratkih tekstualnih poruka
TDS	(Traffic Distribution Systems) mrežni distribucijski sustavi

Tor	(The Onion Router) programski alat za komunikaciju anonimnom mrežom
TXT	(Text file format) format datoteke
USD	(United States Dollar) američki dolar
XLS	(Excel file format) format datoteke
XML	(EXtensible Markup Language) programskih jezik za označavanje podataka
ZIP	(Archive file format) format datoteke

Popis slika

Popis grafikona

Popis tablica