CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Ransomware – plati za svoje podatke

NCERT-PUBDOC-2017-2-346

Nacionalni CERT

Sadržaj

1 Sažetak

U ovom je dokumentu dan kratak pregled *ransomwarea*, povijest njegovog razvoja, najčešći načini njegovog funkcioniranja, ukratko su opisane njegove vrste i njegove specifičnosti te načini zaštite i akcije koje se preporučuju u slučaju zaraze računala. Na kraju je dokumenta ukratko prikazan ekonomski aspekt ransomwarea u kontekstu cyber-kriminala.

2 Uvod

Ransomware je vrsta malicioznog računalnog kôda koji u većoj ili manjoj mjeri ograničava pristup zaraženom računalu. Kako bi se ograničenje uklonilo, traži se od korisnika da plati otkupninu kriminalcima koji upravljaju *ransomwareom*.

Ransomware se najčešće širi kao *trojan*, vrsta prikrivenog malvera. Najčešće se širi privitkom elektroničke pošte, ali sve češće i kao dio web stranica, tako da se računalo zarazi odabirom neke poveznice (često reklame), ali i samim posjetom web stranici.

Nakon što je računalo zaraženo, *ransomware* može djelovati na nekoliko načina:

- lažnim upozoravanjem korisnika da na računalu ima nelegalan softver ili da koristi računalo u ilegalne svrhe (primjerice, radi širenja dječje pornografije). Takva upozorenja vrlo često izgledaju kao da stvarno dolaze od nadležnih institucija poput MUP-a;
- puno opasniji *ransomware* šifriranjem podataka ograničava pristup datotekama ili samom operativnom sustavu, pa čak i mrežnim ili vanjskim diskovima.

U oba slučaja krajnji je cilj plaćanje otkupnine, najčešće u virtualnoj valuti Bitcoin, kako bi se uklonilo upozorenje, odnosno otkupio ključ za dešifriranje podataka.

Uz ova dva najčešća načina, *ransomware* može djelovati i tako da, ukoliko se ne plati otkupnina, djelomično ili potpuno uništi podatke, kopira podatke te korisniku prijeti njihovom objavom na internetu, uspori operativni sustav tako da korištenje računala doslovno postaje nemoguće, ukratko, nastoji se učiniti što veća šteta.

Napadi *ransomwareom* uspješniji su ukoliko se ne koriste efikasne protumjere. Sustavi za informatičku sigurnost najčešće detektiraju anomalije u sustavu, poput pokušaja manipulacije podacima, neuobičajenog prometa i sličnog. Postoji niz aplikacija koje uspješno detektiraju *ransomware* na temelju poznatih korištenih aktivnosti ili načina funkcioniranja, slično kao i kod ostalih vrsta malvera. Tvrtke koje se bave sigurnošću konstantno razvijaju i objavljuju *anti-ransomware* aplikacije i alate za dešifriranje podataka.

Ne postoji općeniti postupak u slučaju napada. Većina isporučitelja sigurnosnih aplikacija savjetuje da se ne plaća „otkupnina“ već da se sredstva ulože u prevenciju i zaštitu. Takav koncept funkcionira sve dok neopreznošću korisnik ne omogući kompromitaciju cijelog sustava zbog, primjerice, otvaranja elektroničke poruke. Tada su tvrtka ili korisnik suočeni s vrlo teškom odlukom – platiti „otkupninu“ ne znajući

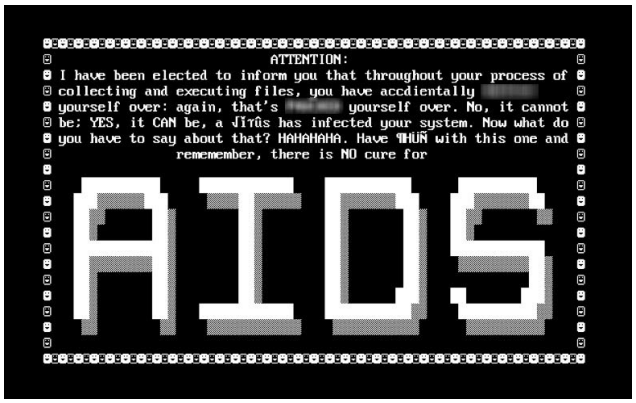
kome su je platili, hoće li dobiti potreban ključ za dešifriranje, što se sve dodatno može dogoditi s podacima itd., ili ne platiti otkupninu i ostati bez svih podataka koji su šifrirani.

Nadalje, policija najčešće nema resurse i nije im „interesantno“ baviti se slučajevima *ransomwarea*, pogotovo ako se radi o napadu na pojedinca, jer je riječ o relativno malim iznosima od nekoliko stotina američkih dolara.

Zaključno, za *ransomware* se također može reći da je to u manjoj mjeri tehnički sofisticiran način cyber-kriminala, a više iskorištavanje ljudskog faktora jer kriminalci računaju na paniku i neracionalno razmišljanje žrtve koja je pod pritiskom zbog vremenskog ograničenja za plaćanje „otkupnine“ i suočavanja s mogućnošću gubitka podataka.

3 Povijest *ransomwarea*

3.1. 1989. godina - AIDS trojan



Prvi slučaj *ransomwarea*, AIDS trojan, pojavio se 1989. godine, a njegov autor bio je biolog Joseph Popp. Na konferenciji Svjetske zdravstvene organizacije (WHO) o AIDS-u, Popp je proširio 20 000 zaraženih floppy diskova među sudionicima. Na sreću, u to je vrijeme bilo relativno malo korisnika osobnih računala pa zaraza nije imala veće razmjere, no imala je sve karakteristike modernog *ransomwarea* – na kompromitiranim računalima pojavila se poruka da žrtve trebaju platiti 189 američkih dolara na poštanski pretinac korporacije PC Cyborg u Panami kako bi se riješile AIDS trojana. AIDS trojan imao je brojač koji je brojao koliko se puta računalo ponovno pokrenulo. Kad bi broj dosegao 90, malver bi sakrio direktorije na C particiji tvrdog diska, a zatim ili zaključao ili šifrirao datoteke na C disku.

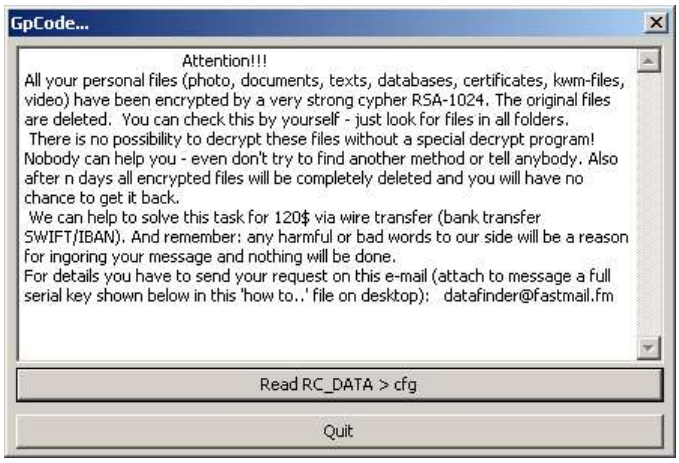
U konačnici je AIDS trojan bio neuspješan iz nekoliko razloga – mogao je zaraziti relativno mali broj računala i algoritam dešifriranja datoteka je vrlo brzo razvijen.

Međutim, kao posljedica su proizašle dvije izvedenice *ransomwarea* kakav je danas poznat i koriste se gotovo isti principi: *crypto ransomware* (*ransomware* koji šifrira korisničke podatke) i *locker ransomware* (*ransomware* koji ograničava pristup računalu). Začuđujuća je i činjenica da se ni iznos „otkupnine“ nije previše promijenio od 1989. godine.

Nakon AIDS trojana kriminalci su počeli češće ciljati korisnike računala u ekonomski razvijenijim zemljama, gdje se korisnici i organizacije više oslanjaju na tehnologiju, čime su šanse za širenje postale veće.

3.2. Početak tisućljeća

Ransomware se ponovno pojavljuje oko 2005. godine u obliku lažnih aplikacija, *spyware* alata, primjerice Spysheriffa, ili malicioznih aplikacija koje su se lažno predstavljale kao „optimizatori performanci“ računala, poput PerformanceOptimizera ili RegistryCarea. Ovim putem najčešće su ciljani korisnici Windows i Macintosh sustava. Upozorenja o oštećenim datotekama i neispravnim unosima u sistemskom registru korištena su kako bi se proširila panika među korisnicima te ih se navelo da plate od 30 do 90 američkih dolara za razne licence i/ili alate kojima bi, navodno, ispravili pogreške u sustavu i poboljšali rad računala, dok bi u stvari takvi alati bili potpuno beskorisni.



2006. godine pojavljuje se Trojan.Gpcoder, prethodnik današnjeg modernog *ransomwarea*. Gpcoder je koristio jednostavan algoritam šifriranja podataka koji je jednostavno dešifriran. No, bez obzira na to, od 2006. i ostali kriminalci uviđaju potencijal u oponašanju Gpcodera. Tada nastaju Trojan.Cryzip i Trojan.Archiveus. Cryzip je neutraliziran nakon što su stručnjaci otkrili da je lozinka za otključavanje arhiva sadržana u samom kôdu malvera.

Archiveus je oponašao Cryzip, osim što je od žrtava tražio da kupuju lijekove u jednoj online ljekarni, a kao dokaz je tražio potvrdu kupnje umjesto uplate „otkupnine“. Stručnjaci vjeruju da su kriminalci dobivali proviziju od ljekarne.

4 Moderni *ransomware*

Oko 2008. godine korisnici počinju shvaćati veličinu prijetnji i važnost sigurnosnog softvera poput vatrozida i antivirusnih programa. Kao odgovor, kriminalci počinju koristiti lažne antivirusne programe koji su se pretvarali da provjeravaju sustav i koji su tvrdili da su detektirali veći broj sigurnosnih propusta. Od žrtava je tada traženo da plate od 40 do 100 američkih dolara za pretplatu ili licencu za lažne antivirusne programe koji će „ispraviti pronađene propuste“. Kako je rasla svijest o postojanju lažnih antivirusnih programa, korisnici su ih prestali preuzimati s interneta te su ih uklonili sa svojih računala. Međutim, taktika koju su kriminalci koristili pokazala se zanimljivom – oslanjanjali su se na sklonosti korisnika da preuzmu aplikaciju s interneta ili da reagiraju na razne oglase. S druge strane, problem kriminalaca bio je u tome što nisu imali dodatnih načina da namame žrtve na plaćanje.

Krajem 2008. godine pojavljuje se prvi *locker ransomware*, trojan Ransom.C. Ova vrsta *ransomwarea* onemogućavala je pristup korisničkom sučelju zaraženog računala, najčešće onemogučavajući korisniku korištenje miša, cijele tipkovnice ili njezinih dijelova te drugih komponenti računala. Ransom.C se najčešće širio putem malicioznih poruka elektroničke pošte ili aplikacija preuzetih s interneta. Nakon aktivacije, Ransom.C bi omeo rad Windows Security Centera (dijela Windows OS-a zaduženog za sigurnost rada računala) i zaključao računalo, te ostavio poruku žrtvi da nazove skupu telefonsku liniju kako bi dobila licencu za reaktivaciju Windows Security Centera. Žrtve su tad morale uplatiti iznos kako bi dobile broj *vouchera* s kojim bi otključale računalo, ili su morale čekati da proizvođači sigurnosnog softvera pronađu rješenje. Potrebno je imati na umu činjenicu da mobilni uređaji u to vrijeme nisu imali mogućnosti kao danas i korisnici većinom nisu imali dodatnu mogućnost pristupa internetu kako bi potražili eventualno objavljeno rješenje, kao ni potrebna znanja kako bi samostalno otključali svoje računalo. Kriminalci su to također prepoznali te podigli cijenu „otkupnine“ u rasponu od 200 do 300 %, odnosno na 150 do 200 američkih dolara po računalu.

S 2013. godinom *locker ransomware* više ne koristi lažne aplikacije jer više nije potrebna svjesna korisnička akcija kako bi se zarazilo računalo. *Locker ransomware* kampanje postaju sve bezobzirnije – korisnici dobivaju obavijest o infekciji i nemogućnosti korištenja računala te ih se traži uplata u nekoj od virtualnih valuta poput Bitcoina. Istovremeno, napadači primjenjuju razne tehnike socijalnog inženjeringa kako bi izazvali što više panike i stresa među žrtvama, s ciljem umanjenja njihove sposobnosti da reagiraju racionalno. Napadači se često predstavljaju kao policija ili druge ustanove koje provode zakon, koristeći sučelja koja su vjerne kopije originalnih sučelja stvarnih organizacija, tvrdeći da žrtva posjeduje piratske kopije glazbe, filmova, ilegalne kopije softvera ili razne zabranjene sadržaje

poput dječje pornografije, sadržaje povezane s trgovinom ljudima i sl. Uspješnost i profitabilnost ovakvih kampanja pada između 2012. i 2014. godine zbog uloženog napora institucija i sigurnosnih stručnjaka u informiranje javnosti i podizanje svijesti o ovim prijevarama, a ujedno se razvijaju aplikativna rješenja koja sprečavaju ovakve napade. Kao rezultat, kriminalci se umjesto prihvaćanja novih taktika u ovoj vrsti prijevare sve više okreću *crypto ransomwareu*.

Od 2013. godine napadači sve više koriste *crypto ransomware* koji je vrlo sličan originalnom Poppovom AIDS trojanu i Ransomware.C trojanu, s jednom bitnom razlikom – koriste se vrlo snažni algoritmi za šifriranje. Evolucija *crypto ransomwarea* ubrzava se posljednjih nekoliko godina jer se kriminalci međusobno oponašaju te sve više analiziraju uspješne i neuspješne strategije. Uspješni kriminalci sve se više oslanjaju na industrijske standarde za šifriranje podataka, poput RSA, 3-DES (engl. *Triple Data Encryption*) ili AES (engl. *Advanced Data Encryption*). Kako *ransomware* postaje sve sofisticiraniji i sve kompliciraniji, tako je i njegov razvoj sve skuplji, a ujedno ga je i teže ukloniti s računala. Iz tog razloga napadači traže i veću „otkupninu“, koja dostiže 300 američkih dolara po računalu, dok je za poslovne i važne sustave taj iznos značajno viši. Od 2016. godine se *ransomware* ponovno mijenja, postaje još štetniji i manje predvidljiv nego prije, a ta tranzicija je mogući rezultat pojave sve vještijih i okrutnijih kriminalaca koji se koriste Advanced Persistent Threat metodama.

5 Vrste *ransomwarea*

U osnovi, kao što je u tekstu već prikazano, razlikuju se dvije vrste *ransomwarea* – *crypto* i *locker*. Za sada hibridni tipovi *ransomwarea* još nisu popularni, iako je *ransomware* sve složeniji, međutim, razvoj hibridnog *ransomwarea* je samo pitanje vremena.

5.1. Locker ransomware

Ova vrsta *ransomwarea* najčešće se širi korištenjem socijalnog inženjeringa i prikupljanjem korisničkih podataka preko lažnih web sjedišta (engl. *phishing*). Prema Symantecu, u oko 36 % slučajeva tijekom 2014. i 2015. godine radilo se o *locker ransomwareu*. *Locker* korisniku na neki od načina onemogućava pristup računalu, ili zaključavanjem korisničkog sučelja ili onemogućavanjem pristupa ostalim računalnim resursima. *Locker* najčešće ne oštećuje sistemske datoteke, već „samo“ onemogućava pristup računalu. U tom se slučaju *locker ransomware* relativno jednostavno uklanja s računala korištenjem sigurnosne kopije sustava u slučaju njezinog postojanja ili korištenjem dostupnih komercijalnih ili besplatnih alata.

Zbog činjenice da *locker ransomware* može biti uklonjen s računala bez dodatne štete za vrijedne korisničke podatke, strategija napadača uvelike ovisi o izazvanoj panici i iracionalnom ponašanju žrtve.

Naprednije verzije u većoj mjeri koriste socijalni inženjering u svojim prijevarama kako bi prisilile žrtve da plate „kaznu“. Ovakva taktika iskorištava žrtvino povjerenje u policiju i institucije koje provode zakon, žrtvinu sklonost poštivanju zakona i strahu od posljedica, na način da se žrtvu optužuje da je napravila nešto protuzakonito. Poznat je slučaj da se žrtvi na ekranu prikaže poruka kojom se tvrdi da je MUP zaključao računalo jer se na računalu nalazi nelegalni softver, piratizirani filmovi ili dječja pornografija. Poruka sadrži upute o načinu plaćanja kazne i načinu obavještavanja napadača, za kojeg žrtva misli da se stvarno radi o MUP-u.

Ukoliko su pak žrtve stvarno sudjelovale u nekim nedozvoljenim aktivnostima, primjerice posjeduju nelegalan softver ili se na neki način mogu povezati s prijetnjom u zahtjevu za otkupninom, povećava se mogućnost da će platiti traženi iznos iako možda i sumnjaju da se radi o prijevari. Budući da se žrtve osjećaju krivima ili posramljenima, vrlo je vjerojatno da će rezonirati racionalno i zatražiti pomoć. Na taj način kriminalci iskorištavaju ljudsku prirodu svojih žrtava kako bi ostvarili željeni profit. Međutim, kako svjesnost o postojanju *ransomware* prijevara raste, tako se broj žrtava i uspješnost prijevara smanjuju.

Iako u posljednje vrijeme napadači napuštaju *locker ransomware* i sve češće koriste robusniju verziju, *crypto ransomware*, *locker ransomware* se još uvijek razvija, ali u manjoj mjeri. Pa ipak, neki stručnjaci očekuju povratak *locker ransomwarea* na scenu zbog toga što ga je moguće uspješno koristiti s tehnologijama koje se razvijaju, poput pametnih mobilnih uređaja, pametnih satova, televizora, hladnjaka i ostalih uređaja koji su povezani internetom. Za razliku od osobnih računala, ovim uređajima može nedostajati mogućnost izrade sigurnosnih kopija sustava. Korisniku preostaje malo mogućnosti: platiti otkupninu, platiti alat za uklanjanje *ransomwarea* te uložiti vrijeme i trud kako bi se naučilo uspješno primijeniti kupljeni alat ili vratiti uređaj na tvorničke postavke (ukoliko takva mogućnost nije zaključana *ransomwareom*).

5.2. Crypto ransomware

Umjesto ograničavanja korisničke interakcije s uređajem onemogućavanjem korištenja sučelja, cilj *crypto ransomwarea* su korisnički podaci i napad na njih, dok samo funkcioniranje uređaja i sistemske datoteke uglavnom ostaju netaknute. Žrtva može i dalje koristiti svoje računalo, osim što nema pristup šifriranim podacima. *Crypto ransomware* često uključuje i vremensko ograničenje unutar kojeg žrtva mora platiti otkupninu, te, ako to ne učini, ključ za dešifriranje bit će izbrisan, čime se korisniku trajno onemogućava pristup podacima. Napadači ponovno igraju na psihologiju korisnika jer pod vremenskim pritiskom žrtve ne razmišljaju racionalno. Žrtve su pod stresom jer znaju da im vrijeme ističe, boje se posljedica donošenja krive odluke te spoznaje da bi podatke mogli zauvijek izgubiti.

Prema Symantecu, u razdoblju od 2014. do 2015. godine u 64 % slučajeva radilo se o *crypto ransomwareu*. Napadači su obično tražili približno 300 američkih dolara u virtualnoj valuti Bitcoin kako bi otključali podatke žrtvama. Za razliku od *lockera*, *crypto ransomware* ostavlja mogućnost pristupa internetu kako bi žrtva mogla kupiti

kriptovalutu poput Bitcoina, a neke inačice čak upućuju žrtve na stranice gdje mogu nabaviti kriptovalutu.

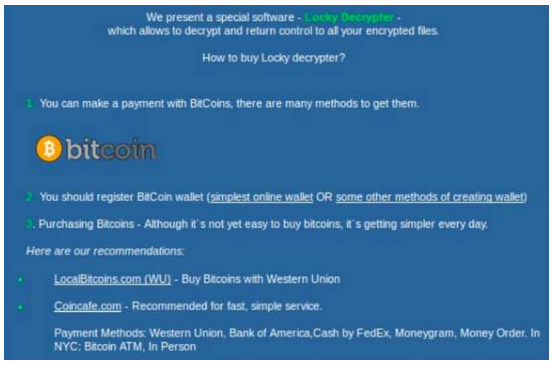
Crypto ransomware nije bio popularan do 2013. jer napadači nisu uočili da uspješan napad *ransomwareom* ovisi o jakom enkripcijskom algoritmu i odgovarajućem upravljanju pripadajućim ključevima za dešifriranje. Starije verzije su bile manje profitabilne od *locker ransomwarea* jer su napadači pohranjivali ključeve na računala žrtava ili su oni bili sadržani u samom kôdu *ransomwarea*, što je omogućavalo njihovo pronalaženje i dešifriranje podataka. Budući da su u nekim inačicama korišteni isti ključevi kod svih žrtava, čim bi netko uspio otključati svoje podatke, mogao je javno objaviti ključ i omogućiti otključavanje ostalim žrtvama.

U svrhu zadržavanja vlastite anonimnosti, programeri *ransomwarea* često se koriste proxy poslužiteljima, alatom Tor (engl. *The Onion Router*) i kriptovalutama poput Bitcoina.

U današnje digitalno doba, većina ljudi svoje osobne i poslovne podatke čuva u digitalnom obliku. Samo mali postotak korisnika radi redovite sigurnosne kopije svojih podataka ili sigurnosne kopije sistemskih podataka. Kako bi žrtvama onemogućio pristup podacima, *Cypto ransomware* koristi snažne kriptografske algoritme. Nakon što se kompromitira korisničko računalo, malver identificira i šifrira korisničke podatke, što korisnik ne primjećuje. Tek nakon što je cijeli postupak dovršen, od žrtve se traži plaćanje otkupnine. Bez ključa za dešifriranje koji je u posjedu napadača ili adekvatnog rješenja za dešifriranje, korisnici gube pristup podacima. U slučajevima kada je korisniku potreban stalan i neprekinut pristup podacima (npr. bolnici ili financijskoj instituciji), čak ni sigurnosne kopije podataka nisu dovoljne. Različitim korisnicima bitne su različite vrste podataka (dokumenti, fotografije, servisi), a kako su i algoritmi šifriranja različiti, mogućnosti *crypto ransomwarea* vrlo su široke.

5.3. Primjeri aktivnih *ransomwarea*

5.3.1. Locky



Ransomware Locky prvi se put pojavio 5. veljače 2016. kad su se medicinski sustavi u bolnici Hollywood Presbyterian Medical Center njime zarazili. Zdravstveni podaci o pacijentima ostali su netaknuti, ali je bio onemogućen pristup raznim laboratorijskim i dijagnostičkim uređajima. Slanje elektroničke pošte također je bilo onemogućeno, ali nije jasno je li servis namjerno ugašen kako bi se sačuvali tragovi napada ili je ugašen kao rezultat napada. Mediji su nagađali o otkupnini od 9 000 Bitcoina, dok je glavni izvršni direktor Allen Stefanek opovrgnuo taj podatak. Nakon gotovo dva tjedna, usprkos znatnoj pomoći FBI-a i policije, bolnica je platila otkupninu u vrijednosti od 40 Bitcoina kako bi ponovno mogla koristiti svoje uređaje jer je smatrala da je plaćanje otkupnine najbrži i najučinkovitiji način vraćanja kontrole nad svojim sustavima. Stefanek je smatrao da bolnica nije bila namjeran cilj, već da je napad rezultat otvaranja maliciozne elektroničke poruke. U suprotnosti s tom tvrdnjom, napadači nisu zahtijevali uobičajenu otkupninu u iznosu od 210 do 420 američkih dolara, već je zahtjev bio mnogo veći.

Locky šifrira datoteke algoritmima RSA-2048 i AES-128, što znatno otežava otključavanje datoteka. Žrtve se obično upućuju na stranice preko kojih dobivaju upute o instalaciji Tora i mogućnostima uplate otkupnine. Tvrtka Proofpoint tvrdi da je Locky razvila i proširila kriminalna organizacija Dridex koja se najčešće povezuje sa širenjem malvera koji za cilj ima napade na banke. Locky se najčešće širi putem elektroničkih poruka koje u privitku imaju MS Word dokumente. Svaka binarna datoteka je jedinstvena, tako da je detekcija bazirana na ključu gotovo nemoguća. Nakon inficiranja računala, malver prvo briše sigurnosne kopije operativnog sustava, ukoliko one postoje, te preimenuje šifrirane datoteke dodavanjem ekstenzije .locky.

5.3.2. TeslaCrypt/EccKrypt

TeslaCrypt inficira sustave koristeći alat Angler koji se oslanja na ranjivosti Adobe Flasha. Silverlight i Internet Explorer također se mogu koristiti za napade. Angler se ubacuje putem *iframea* na kompromitiranom web-sjedištu, a žrtva se zatim preusmjerava na stranice gdje se provjeravaju zaštitne postavke napadnutog računala. Ako su sve provjere uspješne, koristi se Flash kako bi se preuzeo *ransomware* koji se smješta u žrtvin privremeni direktorij. Korištenjem algoritma Xtea preuzeti algoritam se dekodira i zapisuje na disk.

Malver se kopira u %appdata% gdje ujedno pohranjuje SHA 256 ključ (key.dat) te u log datoteku zapisuje podatke o pronađenim i šifriranim datotekama. Šifriranim datotekama dodaju se ekstenzije .encrypted, .ecc, .ezz, .exx, a u posljednje vrijeme i .mp3. Malver zatim djeluje u nekoliko zasebnih procesa: proces kojim se šifriraju datoteke, proces kojim se nadziru i terminiraju procesi .exe, .msconfig, .regedit, .procexp, i .taskmgr, proces kojim se brišu sigurnosne kopije koristeći vssadmin.exe i proces kojim se vrši komunikacija s kontrolnim poslužiteljem (engl. *Command and Control* – C&C). Iako podsjeća na Cryptolocker po dizajnu i izgledu, TeslaCrypt ne koristi isti izvorni kod. Nakon infekcije žrtvi se otvara iskočni prozor kojim se obavještava da su datoteke šifrirane i preusmjeravaju se na TeslaCrypt web sjedište, direktno ili putem Tor2 web proxyja.

U početku je TeslaCrypt koristio simetričnu enkripciju, međutim, nakon što su stručnjaci iz Ciscove Talos Group objavili alat za dešifriranje (Talos TeslaCrypt Decryption Tool), autori su ga izmijenili tako da koristi asimetričnu enkripciju. Krajem 2015. Kaspersky Lab izdao je novi alat, TeslaCrypt Decoder. U siječnju 2016. autori ponovno otklanjaju nedostatke u malveru i šifriranim datotekama dodaju ekstenziju .mp3.

TeslaCrypt je napadao 185 vrsti datoteka povezanih s računalnim igrama (Call of Duty, Skyrim, Minecraft itd.) na Windows operacijskom sustavu. Novije varijante šifriraju .doc, .pdf i .jpg datoteke. Od žrtava se traži da plate otkupninu u vrijednosti 500 američkih dolara (u nekoj od virtualnih valuta), a u znak dobre volje daje im se mogućnost dešifriranja jedne datoteke.

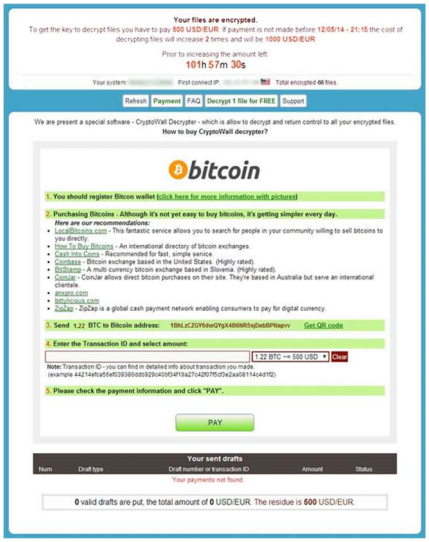
5.3.3. Cryptolocker

Cryptolocker je *crypto ransomware* kojim su se inficirala računala koja koriste Windows operacijski sustav, a njegova pojava otkrivena je u rujnu 2013. putem botneta Gameover ZeuS. Podaci na zaraženom računalu šifrirani su korištenjem RSA enkripcije. Privatni ključevi nužni za dešifriranje pohranjeni su na poslužiteljima koji upravljaju tim malverom. *Ransomware* se širio i putem malicioznih elektroničkih poruka sa .zip datotekom u privitku, koja je sadržavala izvršnu datoteku s PDF ikonom. Cryptolocker se instalira u direktoriju kojim se koristi korisnički profil i dodaje ključ u sistemski registar, tako da se automatski pokreće prilikom pokretanja računala. Zatim se povezuje s jednim od C&C poslužitelja i generira 2048-bitni RSA par ključeva, pohranjuje privatni ključ na poslužitelju, a javni ključ šalje nazad na korisničko računalo. Malver zatim šifrira dokumente, slike i CAD datoteke na lokalnom disku, kao i mapirane mrežne diskove te zapisuje dnevničke zapise o svakoj šifriranoj datoteci u sistemski registar.

Velika većina žrtava bila je iz SAD-a ili Velike Britanije, a od njih je traženo da izvrše uplatu u periodu od 72 do 100 sati ili će privatni ključevi biti izbrisani što će onemogućiti dešifriranje podataka. Događali su se slučajevi u kojima ni nakon uplate otkupnine napadači ne bi dešifrirali datoteke. Cryptolocker je moguće ukloniti sa zaraženog računala, ali datoteke nije moguće dešifrirati bez privatnog ključa.

Cryptolocker i botnet ZeuS na koji se Cryptolocker oslanjao ugašeni su u svibnju 2014. u tzv. Operaciji Tovar. Nakon toga su privatni ključevi pohranjeni na poslužiteljima iskorišteni u online alatu za povrat datoteka. Smatra se da su u šest mjeseci korištenja napadači izvukli oko 3 milijuna američkih dolara od svojih žrtava, iako je procjena da je samo od 1,3 do 3 % žrtava platilo otkupninu. Kao rezultat ovog uspjeha, brojne inačice pojavljuju se na crnom tržištu.

5.3.4. Cryptowall/CryptoDefense/CryptorBit



Vrsta *ransomwarea* Cryptowall prvi se put pojavljuje početkom 2014. godine i postaje popularnom nakon što je ugašena mreža kojom se širio Cryptolocker. Cryptolocker se širio koristeći niz alata, primjerice, kroz neželjenu elektroničku poštu (s .rar datotekom u privitku koja je sadržavala .chm datoteku) ili putem kompromitiranih web-stranica. Nakon što bi na bilo koji način malver bio isporučen na žrtvino računalo, binarna datoteka kopirala bi se u %temp% direktorij. Nakon tog pokrenula bi novu instancu procesa explorer.exe, ubacila bi binarnu datoteku Cryptowall i izvršila kod. Malver koristi alat vssadmin.exe kako bi obrisao sigurnosne kopije, a zatim pokreće proces svchost.exe s korisničkim privilegijama te ubacuje i izvršava kôd u tom procesu. Nakon toga pokušava

se povezati s I2P proxy poslužiteljima kako bi se omogućila komunikacija s C&C poslužiteljima. Nakon što se uspostavi komunikacija, poslužitelj vraća javni ključ i obavještava žrtvu porukom.

Trenutne inačice malvera (poput Cryptowalla 3.0) koriste I2P proxy poslužitelje za komunikaciju s C&C infrastrukturom, te se koristi Tor mreža za prikupljanje uplata u Bitcoin valuti. Početne inačice koristile su RSA algoritam, međutim, malver (Cryptowall 3.0) sad koristi AES 256 algoritam. Nadalje, AES ključevi nužni za dešifriranje čuvaju se na C&C poslužiteljima. Malver dešifrira nekoliko nasumično odabranih datoteka kako bi se žrtvi pokazalo da je moguć povrat podataka ako se plati otkupnina (obično 1 Bitcoin). Za razliku od Cryptolockera, Cryptowall je korišten za napade na računala s Windows operacijskim sustavom diljem svijeta, iako je najviše napada zabilježeno u SAD-u, Velikoj Britaniji, Nizozemskoj i Njemačkoj.

5.3.5. CTB-Locker

„Curve-Tor-Bitcoin-Locker“, CTB-Locker, trojan je baziran na PHP-u čija je analiza objavljena sredinom 2014. godine. CTB-Locker u osnovi je „*ransomware as a service*“ (RaaS), gdje napadač prepušta posao širenja malvera početnicima (tzv. *script kiddies*) i botnet operatorima (često se za njih koristi termin „podružnice“) u zamjenu za udio u ostvarenoj dobiti od otkupnina. U modelu CTB-Locker „podružnice“ plaćaju operaterima mjesečnu naknadu za korištenje malvera, dok u drugim modelima začetnici malvera uzimaju mali postotak od svake otkupnine.

Kroz model „podružnica“, CTB-Locker koristi svaki mogući vektor za širenje. Napadači najčešće koriste alate (Rig, Nuclear i sl.) i kampanje u kojima šalju maliciozne elektroničke poruke. U samim kampanjama često se koriste *downloaderi* Dalexis ili Elenoocka za širenje malvera. Dalexis je autoizvršna datoteka koja se šalje u privitku elektroničke pošte kao .cab datoteka, dok je Elenoocka autoizvršna datoteka skrivena u .zip ili .rar arhivama.

Downloaderima se CTB-Locker smješta u privremeni direktorij i kreira se zadatak koji se izvršava u određeno vrijeme (tzv. *scheduled task*). Zatim se vrši pretraživanje cjelokupnog datotečnog sustava i označavaju se sve datoteke čiji se tipovi nalaze na listi CTB-Lockera te se označene datoteke šifriraju. Zatim se žrtvu obavještava da mora platiti otkupninu u roku od tipično 96 sati (rok određuje „podružnica“) te da će svaki pokušaj uklanjanja malvera rezultirati uništenjem ključa za dešifriranje.

CTB-Locker koristi kombinaciju simetričnih i asimetričnih algoritama. Umjesto korištenja RSA algoritma, koji se često koristi u *ransomwareu*, CTB-Locker koristi AES u kombinaciji s ECC (engl. *Elliptic Curve Cryptography*) algoritmom. ECC može ostvariti jednaku snagu enkripcije kao i RSA, ali s puno manjim ključem. Primjerice, ECC enkripcija s 256-bitnim ključem ekvivalentna je RSA enkripciji s 3072-bitnim ključem. Malver koristi AES algoritam za šifriranje datoteka, a sam način dešifriranja podataka šifriran je ECC javnim ključem. Kao rezultat, isključivo napadač koji posjeduje ECC privatni ključ može dešifrirati žrtvine podatke.

Posebnost CTB-Lockera je u tome da nije potrebna internetska veza niti komunikacija s C&C infrastrukturom kako bi se započeo proces šifriranja žrtvinih podataka. Mrežna povezanost nije nužna sve dok žrtva ne želi dešifrirati svoje podatke. Plaćanje se vrši, kao i kod većine *ransomwarea*, putem Tor alata, a nakon što je otkupnina plaćena, blok za dešifriranje šalje se žrtvi putem C&C poslužitelja.

U veljači 2016. napadači su počeli koristiti CTB-Locker za šifriranje web sjedišta koja koriste WordPress. Ova inačica poznata je pod nazivom Critroni. Napadači su hakirali nezaštićene stranice i zamijenili originalnu index.php ili index.html datoteku s datotekama koje su šifrirale cijelo web sjedište AES-256 algoritmom. Nakon toga se poruka o otkupnini prikazivala kao početna web stranica s uputama za kupnju valute Bitcoin i izvršenje plaćanja otkupnine. U prvom tjednu kampanje zaraženo je oko stotinu web sjedišta, a žrtve su često koristile stare verzije WordPressa ili ranjive dodatke. Iako nisu zaražena veća web sjedišta, kampanja je pokazala mogućnosti ovakvog napada. Critroni je možda bio samo eksperiment ili inovativni pokušaj napada početnika na web sjedišta. Iako je svaki posjetitelj vidio istu poruku o *ransomwareu* kao i administrator web sjedišta, zabrinjavajuća je mogućnost korištenja posjete zaraženoj stranici za širenje *ransomwarea*. Na taj način posljedice i sama isplativost *ransomwarea* značajno bi porasle.

5.4. Hibridni *ransomware*

Jedna od rasprostranjenih strategija za obranu od malvera je tzv. *layered depth*. Ona pretpostavlja da će napadači početi koristiti napade „po razinama“. Ovakav način već se pojavio u APT kampanji i nekim napadima *ransomwareom,* gdje su napadači pokrenuli DDoS napad paralelno s puno ozbiljnijim napadima. Bit će zanimljivo vidjeti hoće li doći do ponovne popularizacije *lockera* kod kojeg se *crypto ransomware* izvršava u pozadini. Slojevitost modela možda se trenutno čini nepotrebnom jer žrtve često plaćaju otkupninu i zato što ni stručnjaci za sigurnost ni policija ne mogu probiti jake metode šifriranja. Međutim, ukoliko se jedna od ove dvije postavke promijeni, tada se *locker ransomware*, koji sprečava većinu korisničkih akcija na računalu, može vratiti s nekim kontrolama preuzetim od *crypto ransomwarea*.

6 Načini distribucije

6.1. Sistem distribucije prometa (Traffic Distribution System – TDS)

TDS sustavi preusmjeravaju promet na maliciozna web sjedišta. Često se, primjerice, promet povlači s web stranica sa sadržajem za odrasle, servisa za *streaming* video sadržaja ili piratskih web stranica. Neke grupe, posebice kriminalci koji su kupili malver, a nisu ga razvijali sami, mogu unajmiti TDS za širenje *ransomwarea*.

6.2. Malvertisement

Jednako kao i kod TDS-a, malicioznim oglašavanjem mogu se preusmjeravati korisnici s legitimnih stranica na maliciozne stranice. *Malvertisement* može izgledati

potpuno stvarno i legitimno te čak postojati na provjerenim web-stranicama ukoliko je, primjerice, administrator prevaren i prihvatio je oglašavača ili je web sjedište kompromitirano.

6.3. Phishing elektroničke poruke

Kao i u većini malver kampanja, *phishing* i neželjene poruke elektroničke pošte primarni su načini rasprostiranja malicioznog sadržaja zbog toga što korisnici neoprezno otvaraju privitke ili odabiru poveznice u porukama. Unatoč treninzima i programima kojima se ukazuje na ove probleme, 15 % zaposlenika ciljanih organizacija još uvijek nasjeda na *phishing* prevare. Napadaču treba jedan jedini korisnik u cijeloj organizaciji da odabirom poveznice proširi maliciozni kod po lokalnoj mreži i time je kompromitira. Što su organizacije veće, to je veći rizik proširenja zaraze putem malicioznih elektroničkih poruka.

7 Najčešći ciljevi

Ciljevi napadača koji koriste *ransomware* nisu pojedinci, već određene grupacije društva za koje napadači vjeruju da će platiti otkupninu. Napadi *ransomwareom* najčešće se vrše masovno, pri čemu se napadači nadaju kako će veći postotak napada imati uspjeha. Sam *ransomware*, bilo da ga napadač sam razvija ili ga je kupio, relativno je jeftin, pogotovo u slučaju kada napadač uopće nema namjeru otključati sustav nakon plaćene otkupnine što isključuje potrebu za ulaganjem u dodatne resurse. Mali tim može upravljati kampanjom kojom je moguće napasti milijune sustava, a ako samo maleni dio žrtava plati otkupninu, kampanje će biti profitabilne.

7.1. Pojedinačni korisnici

Korisnici su u cijelom procesu najslabija karika, a ujedno ih je mnogo i k tome su najosjetljiviji na napade. Pojedini korisnici na koje je lako vršiti pritisak ili nisu upoznati s tehničkim rješenjima vezanim uz *ransomware* su najpoželjnije mete. U tom slučaju napadači nastoje izazvati što veću paniku kako bi žrtva pod stresom odlučila platiti otkupninu. Dodatni pritisak žrtvi napadači stvaraju nametanjem vremenskog ograničenja nakon čijeg isteka povrat podataka ili sustava nije moguć. Žrtve često pod pritiskom donose iracionalne odluke i pristaju platiti traženi iznos.

U današnje digitalno doba većina našeg znanja, posla ili osobno vrijednih podataka (poput slika, glazbe i sl.) pohranjena je na uređaje koji su povezani internetom. Velika većina korisnika nema naviku izrade sigurnosnih kopija ili ih ne radi redovito, kao što nema ni naviku provođenja osnovne „cyber higijene“ kako bi se spriječio napad ili smanjila šteta ukoliko do napada dođe. Prema Symantecu, 25 % individualnih korisnika ne radi nikakve sigurnosne kopije, a 55 % njih ima sigurnosne kopije nekih datoteka. Što se tiče učestalosti izrade sigurnosnih kopija, samo 25 % korisnika izrađuje ih na tjednoj bazi, a ostatak jednom mjesečno ili rjeđe. Uspješnost napada *ransomwareom* ovisi o tome da se napad izvrši između izrade dvije sigurnosne kopije. Ako je interval izrade samo jedan dan, u tom danu korisnik može izgubiti vrlo

vrijedne poslovne podatke. Nadalje, kompleksnije varijante *ransomwarea* mogu obrisati lokalne sigurnosne kopije i proširiti se na mrežne diskove gdje se one čuvaju.

7.2. Poslovni sustavi

Moderna ekonomija doslovno je sagrađena na nematerijalnim vrijednostima i uslugama kao što su znanja i informacije. Veliki ili mali poslovni subjekti ovise o svojim sustavima i informacijama koje su na njima pohranjene kako bi izvršavali svoje dnevne rutine. Poslovni subjekti među glavnim su ciljevima napadača *ransomwareom* jer su na njihovim sustavima baze podataka i ostali servisi koji čuvaju ili koriste vrijedne informacije, dokumente i podatke važne za poslovanje, a ujedno su takvi sustavi često slabo zaštićeni. Nadalje, nemogućnost pružanja usluga za mnoge tvrtke znači direktan gubitak prihoda i ugleda. Posljedično, u slučaju uspješnog napada, vrlo će se vjerojatno odlučiti na plaćanje otkupnine kako bi što prije nastavile s poslovanjem. Velik broj tvrtki ima redundantne sustave i *backup* poslužitelje u slučaju da napad uspije, međutim, jednak ili veći broj tvrtki to nema. Nije realno očekivati da male ili srednje tvrtke imaju jednako kvalitetnu infrastrukturu kao veće tvrtke jer jednostavno nemaju sredstava. No, iako napadnuta organizacija ima kvalitetnu infrastrukturu, za nju se razvija poseban *crypto ransomware* kako bi se nosio s kompleksnim mrežama. Kao rezultat i redundantni sustavi mogu biti kompromitirani. Čak ni velike tvrtke ne mogu ignorirati to da pola njihovog sustava ne radi. U slučaju uspješnog napada, tvrtke mogu reagirati oporavkom sustava, plaćanjem otkupnine ili pristajanjem na trajni gubitak podataka. Mnoge tvrtke ne bi preživjele trajni gubitak podataka, pogotovo ako u pitanje dolaze i podaci njihovih korisnika. Takve tvrtke izuzetno su osjetljive na napade. Ponekad je dovoljno da se kompromitira samo jedan korisnik, nakon čega se *ransomware* širi po cijeloj korporativnoj mreži.

7.3. Financijski sektor

Bankovni i financijski sektor česta je meta botnet napada, poput botneta Dyre, Dridex i Ramnit. *Ransomware* se često širi upravo putem navedenih botneta. Za *ransomware* Locky vjeruje se da ga je razvila grupa Dridex. Kao posljedica, financijske ustanove i dalje će biti jedna od najčešćih meta kriminalaca. Prema dostupnim informacijama, najčešći napadi su u Velikoj Britaniji i SAD-u.

7.4. Državne institucije

Državne institucije, prvenstveno one koje se bave provođenjem zakona, poput policije i državnog odvjetništva, mogu postati žrtve napada kao odgovor kriminalaca na njihovu borbu protiv cyber kriminala. U SAD-u je početkom 2016. godine zabilježen niz napada na policijske postaje u kojima su ili bile nedostupne razne informacije ili su onemogućeni sustavi za internu komunikaciju policijskih djelatnika. Ukoliko se radilo o kritičnim sustavima, za njih je plaćena otkupnina.

7.5. Hitne službe

Zabilježen je porast broja napada na hitne službe poput vatrogasaca, policije, hitne pomoći i ostalih službi. Takve službe, čija bi nemogućnost djelovanja mogla ugroziti živote ljudi, izrazito su zanimljivi kriminalcima.

7.6. Zdravstvene organizacije

Zdravstvene organizacije nisu bile uobičajene žrtve napada. Po jednoj teoriji, napadači ne napadaju sustave čijom bi kompromitacijom mogli ugroziti ljudske živote. Nažalost, ta praksa se mijenja, tako da je početkom 2016. zabilježen niz napada na bolnice u SAD-u i Njemačkoj. Bolnički sustavi izuzetno su ranjivi jer nedostupnost podataka o pacijentima direktno ugrožava živote te zbog toga mogu biti vrlo zanimljivi kriminalcima. U slučaju uspješnog napada na takve organizacije, veća je vjerojatnost da će iste odlučiti platiti otkupninu.

7.7. Obrazovne ustanove

Kriminalne organizacije za mete napada mogu odabrati administrativne sustave obrazovnih ustanova. U tim slučajevima češće će odabirati one ustanove za koje procjenjuju da imaju sredstava za plaćanje otkupnine, većinom fakultete i visokoškolske ustanove. Početkom 2016. godine u SAD-u su zabilježeni brojni napadi na obrazovne ustanove.

8 Najčešće napadani sustavi

Svaki sustav koji je vrijedan korisniku, vrijedan je i napadaču. Kako tehnologija postaje sveprisutna, a ovisnost društva o stalnom pristupu informacijama sve veća, tako se povećava i mogućnost napada *ransomwareom*. Prema Symantecu, najčešći ciljevi napada su osobna računala, mobilni uređaji, poslužitelji za baze podataka i ostali poslužitelji. Dodatno, sa sve većom popularnošću IoT uređaja (engl. *Internet of Things*), i takvi uređaji postaju metom. U posljednje vrijeme sve su češće mete i ostali uređaji bez kojih određeni poslovi ne bi funkcionirali, poput PoS uređaja ili medicinskih aparata.

8.1. Osobna računala

Osobna su računala trenutno primarni cilj *ransomware* kampanja zato što ih je velik broj i vrlo se lako kompromitiraju. Obični korisnici imaju loše navike (ne koriste antivirusne programe, ne rade redovite sigurnosne kopije…), a putem socijalnog inženjeringa velik broj korisnika može biti nagovoren da sam kompromitira svoj sustav . Na ovakvim žrtvama kriminalci zarađuju u prosjeku manje novaca po žrtvi, ali je broj žrtava koje će vjerojatno platiti otkupninu znatno veći nego u slučaju tvrtki. Ujedno, sam *ransomware* je znatno jednostavniji od *ransomwarea* koji se koristi prilikom napada na tvrtke. Zbog velikog broja korisnika najčešće se napada

Windows, ali i Linux, Mac i Android operacijske sustave. Do sada je poznata jedna vrsta *ransomwarea* koja je neovisna o operacijskom sustavu – Browlock Trojan.

8.2. Mobilni uređaji

Prema procjenama, do proljeća 2015. oko 43 % svjetskog stanovništva koristilo je neku vrstu mobilnog uređaja. Taj broj je i veći ako se u obzir uzmu tableti, mobilne igraće konzole i ostali uređaji koji imaju mogućnost spajanja na internet. U većini slučajeva na mobilnim uređajima nisu pohranjene veće količine osjetljivih podataka. Sama vrijednost uređaja i nemogućnost pristupa internetu su faktori na koje kriminalci računaju. Budući da danas većina mobilnih uređaja ima mogućnost pohranjivanja podataka u računalnom oblaku, *ransomware* se snažno oslanja na socijalni inženjering i paniku žrtava. U protivnom, korisnici vrlo jednostavno mogu vratiti uređaj na tvorničke postavke i vratiti podatke iz oblaka.

Većina mobilnih uređaja koristi operativni sustav Android ili iOS. Postoje varijante *ransomwarea* za obje vrste uređaja. Budući da Apple ograničava instalaciju aplikacija samo iz Apple Storea, ti su uređaji zaštićeniji, iako se kriminalci i ovdje snalaze tako što uspijevaju certificirati maliciozne aplikacije. No, takav je postupak prilično rizičan i potencijalno neprofitabilan zato što Apple može brzo otkriti i onemogućiti distribuciju takvih aplikacija. Prvi *ransomware* malver za Android zabilježen je 2013., a njihov je broj u stalnom porastu. Napadi su razni – od prijetnji policijom zbog navodnog posjedovanja ilegalnog sadržaja do zaključavanja uređaja promjenom PIN-a.

8.3. Poslužitelji

Poslužitelji i baze podataka ključni su za poslovanje bilo koje tvrtke jer se na njima pohranjuju osjetljive informacije za poslovanje tvrtke. Kompromitacija samo jednog poslužitelja za neku tvrtku može značiti potpuno usporavanje ili čak zaustavljanje poslovanja. Bez obzira na te činjenice, mnoge tvrtke zanemaruju sigurnost te ne održavaju poslužitelje, ne primjenjuju aktualne zakrpe, čime napadačima otvaraju mogućnosti zloporabe ranjivosti. S druge strane, iako tvrtka može imati dobru sigurnosnu politiku i osmišljen plan za nastavak poslovanja u slučaju kvara, za oporavak sustava ili uvođenje redundantnog sustava u pogon potrebno je određeno vrijeme, što može znatno utjecati na poslovanje. U slučaju uspješnih napada kriminalci obično traže otkupninu od 10 do 50 puta veću nego kod individualnih korisnika. Tvrtke su u pravilu spremne platiti jer svaki zastoj za njih znači smanjene prihode.

8.4. IoT uređaji

Kao i kod svih ostalih korisničkih uređaja, i ovdje kriminalci iskorištavaju potrebu društva za stalnim pristupom informacijama. Mnogi će korisnici radije platiti otkupninu nego uložiti vrijeme i napor kako bi sami uklonili problem. Kako je danas sve više uređaja spojeno na internet, tako su mogućnosti zloupotrebe sve veće. Primjerice, nedozvoljeno upravljanje kućnim klimatizacijskim uređajem i postavljanje neodgovarajuće temperature u stanu samo je jedan od mogućih primjera. Prošle godine demonstrirano je bežično hakiranje automobila, čime je samo djelomično

prikazana potencijalna opasnost. *Ransomware* za IoT uređaje može biti prilično jednostavan, a zbog ograničenja samih uređaja, pohrana originalnih nekompromitiranih podataka može biti upitna pa je moguće da žrtve uopće neće moći vratiti prijašnje postavke.

9 Profitabilnost *ransomwarea*

Prema procjenama tvrtke Kaspersky, izrada *phishing* stranice i podešavanje poslužitelja za slanje masovnih spam poruka košta otprilike 150 američkih dolara. Novi *crypto ransomware* prodaje se za otprilike 2000 američkih dolara, dok je Locker nešto jeftiniji. Računica pokazuje da je napadaču dovoljno naplatiti otkupninu (najčešće 300 američkih dolara) od samo osam korisnika kako bi ostvario profit. Symantec procjenjuje da je 2009. godine 2,9 % žrtava platilo otkupninu. Istraživači procjenjuju da je 2014. godine 1,1 % žrtava platilo otkupninu za Cryptowall (u prosjeku 500 američkih dolara). Bez obzira na male postotke, smatra se da je Cryptowall kriminalcima donio zaradu od oko 18 milijuna američkih dolara. Zaključak je da čak i jednostavan *ransomware* s relativno malim brojem žrtava koje će platiti otkupninu može kriminalcima donijeti značajan profit.

10 Kako se zaštititi

Prvo i osnovno pravilo, koje se na žalost vrlo često zanemaruje, jest pametno i odgovorno korištenje računala. Kao prvo, to podrazumijeva da se ne otvaraju elektroničke poruke nepoznatih ili sumnjivih pošiljatelja, a pogotovo da se ne otvaraju privitci tih poruka ili poveznice sadržane u tim porukama. Čak i ako je pošiljatelj poznat, potrebno je biti oprezan prilikom otvaranja sumnjivih poruka jer je moguće da je računalo pošiljatelja kompromitirano. Primjerice, poruka vašeg kolege s posla naslovljena „Invoice for purchase…“ s dokumentom u privitku trebala bi izazvati sumnju kod vas.

Sljedeće je pravilo ne preuzimati softver iz nepouzdanih izvora i računalne programe koji navodno omogućuju lakše i brže preuzimanje softvera s interneta (engl. *downloaders*). Preporuka je ne instalirati ništa na svoje računalo u što niste potpuno sigurni.

Od preuzimanja trojana s web stranica i internetskih portala prilično se teško zaštititi. Poznati su slučajevi da su neki vrlo posjećeni hrvatski portali, ali i drugi domaći i

strani portali, bili korišteni za širenje trojana. Ovi malveri često su bili prikriveni u *banner* oglasima, što se djelomično može spriječiti korištenjem *ad blocking* dodatka u web preglednicima.

Uz odgovorno korištenje računala, preporučuje se korištenje zaštitnog softvera: kvalitetnih antivirusnih programa i vatrozida te redovito ažuriranje operacijskog sustava i svih korištenih aplikacija. Kvalitetni antivirusni softver prepoznat će *ransomware,* osim kada se radi o *zero-day* malveru, dok će vatrozid omogućiti zaštitu na ulazu u vašu mrežu. Također se preporučuje korištenje nekih od specijaliziranih anti-*ransomware* alata poput CryptoPreventa i Crypto-Monitora.

11 Kako vratiti podatke

Nažalost, postoje slučajevi kad ih je gotovo nemoguće povratiti jer se primjerice radi o novom *ransomwareu*.

Prvo i osnovno pravilo – **ne plaćajte otkupninu!** Ako i platite otkupninu, možda nećete dobiti ključ za dešifriranje. Svakako savjetujemo kontaktiranje policije i ostalih institucija kako bi se što prije proširila informacija o *ransomwareu* jer ćete na taj način pomoći zaštiti druge korisnike.

Redovita izrada sigurnosnih kopija najsigurniji je način za sprečavanje gubitka podataka. O načinu izrade treba voditi računa jer su postojali slučajevi u kojima *ransomware* šifrira podatke na mrežnim i vanjskim diskovima, odnosno na svim diskovima na kojima je korisnik imao prava čitanja i pisanja. Dakle, pričuvna kopija trebala bi biti spremljena na disk koji nije u mreži ili vanjski disk koji nije stalno spojen na računalo. Preporučuje se i redovita izrada sistemske sigurnosne kopije koja se vrši po unaprijed određenom postupku i koju ćete čuvati odvojeno od vašeg sustava.

Također postoje razni postupci i alati za spašavanje šifriranih podataka. Više o spašavanju datoteka možete pročitati na stranici Nacionalnog CERT-a http://www.cert.hr/ransomware.

12 Literatura

[1] **The Institute for Critical Infrastructure Technologies (ICIT)** [Mrežno] http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report2.pdf

[2] **Symantec** [Mrežno] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf.

[3] **Kaspersky Lab** [Mrežno]

https://www.kaspersky.com/resource-center/threats/teslacrypt

https://www.kaspersky.com/resource-center/threats/the-rise-of-ransomware-most-glaring-examples-from-2015-2016

[4] **Trend Micro** [Mrežno]

http://www.trendmicro.co.uk/vinfo/uk/security/news/ransomware

[5] **Nacionalni CERT** [Mrežno]

http://www.cert.hr/ransomware