RANSOMVER – EVOLUCIJA I ZAŠTITA

RANSOMWARE – EVOLUTION AND PROTECTION

MSc Nataša Simić, MSc Nevena Miladinović, Mr Zoran Živković, dipl.inž.

Towers Net

***Abstrakt**: Rastući trend ransomver napada i sve sofisticiraniji tipovi ransomvera predstavljaju jedan od većih problema pretežno u svetu poslovnih informacija. Preko 30% poslovnih sistema bi, u slučaju ove vrste napada, platili zahtevani otkup kako bi dobili nazad svoje podatke. Ovakav pristup dovodi do novog problema. Naime, plaćanjem otkupa direktno se finansira razvoj novih ransomvera i evolucija postojećih. U ovom radu je dat opis načina funkcionisanja ransomvera na primeru CryptoLocker-a i CryptoWall-a kao i preporuke za prevenciju ransomvera.Takođe, dat je i predlog sistema koji se mogu koristiti kao efikasna odbrana od ransomvera.*

***Ključne reči:** Ransomver, CryptoLocker, CryptoWall*

***Abstract**: Ransomware is a growing trend in the world of business information. Over 30% of business systems would pay the ransom for their files in the case of ransomware. This approach leads towards a new problem. However, by paying the ransom victim is directly financing evolution and development of ransomwares. This paper describes the working principle of ransomware using CryptoLocker and CryptoWall as examples and gives the recommendation for ransomware prevention. Also, it suggests the systems that can be used for effective defence against ransomware attacks.*

***Key words:** Ransomware, CryptoLocker, CryptoWall*

1. UVOD

Ransomver je klasa malvera koja ograničavanjem ili onemogućavanjem korisnika da pristupi podacima na svom računarskom sistemu iznuđuje novac (otkup). Ova vrsta malvera može da zaključa sistem ili da enkriptuje datoteke i dokumenta koja se čuvaju u samom sistemu. Nakon zaključavanja sistema ili enkripcije podataka, ovaj malver prikazuje poruku u kojoj se zahteva otkup (*ransom*). Poruka o otkupu može biti u formi tekstualne datoteke, slike ili se može prikazati kao veb strana. Sam otkup može biti u vidu vaučera za plaćanje, *PayPal* transakcije ili plaćanje pomoću *Bitcoin* elektronske valute. Ransomver se može svrstati i u klasu *scareware* jer zastrašivanjem korisnika pokušava da iznudi novac. [1]

U ranijim verzijama ransomvera korišćena je tehnika zaključavanja sistema dok se kod novijih verzije češće primenjuje tehnika enkriptovanja datoteka. Oba načina omogućuju da korisnik dobije obaveštenje o radnjama koje su se odvile u njegovom sistemu. Nakon enkripcije datoteka malver najčešće sam sebe izbriše a za sobom ostavi samo poruku o otkupu. U poruci o otkupu korisnik dobija detaljne informacije o načinu plaćanja otkupa u cilju dekriptovanja blokiranih datoteka. Neke varijante ransomvera u okviru poruke o otkupu imaju i tajmer koji odbrojava vreme za plaćanje otkupa. Kod poruka sa tajmerom napadač često preti da će izbrisati sve datoteke pri isteku vremena ili će uvećati iznos otkupa. [2]

Ransomver može dospeti u sistem preko zaraženih veb strana, kao deo nekog drugog malvera ili preko *phishing* kampanja. Kreatori ransomvera su veoma inovatnivni i neprekidno smišljaju nove taktike napada. Radi boljeg razumevanja načina rada ransomvera potrebno je znati i evoluciju ovog tipa malvera. U nastavku rada biće dat pregled evolucije ransomvera sa posebnim akcentom na CryptoLocker i CryptoWall kao i preporuke za prevenciju ove vrste napada.

2. KRATKA ISTORIJA RANSOMVERA

Prvi slučajevi ransomvera zabeleženi su u periodu 2005.-2006. godine u Rusiji. Ovaj ransomver (TROJ_CRYZIP.A) je koristio tehniku zipovanja sa lozinkom da onemogući korisnika da pristupi svojm datotekama. Naime, ransomver bi određene datoteke grupisao u jednu zipovanu datoteku koja bi bila zaštićena loznkom. Osim toga, u sistemu bi se kreirala i tekstulana datoteka sa porukom u kojoj se zahteva otkup u iznosu od 300$. U početku ransomver je korišćen za enkripciju samo određenih vrsta datoteka (pr. DOC, EXE, DLL, XL).

Prvi SMS ransomver (TROJ_RANSOM.QOWA) se pojavio 2011. godine. Ovaj ransomver, nakon inficiranja sistema, takođe je generisao poruku o otkupu koja se pojavljivala sve dok korisnik ne plati otkup. Naziv SMS ransomver potiče od tehnike koja se koristila za naplatu otkupa. Naime, korisnik bi dobio broj premium SMS servisa koji je trebao da nazove kako bi platio otkup i dobio svoje datoteke nazad.

U ovom periodu pojavila se još jedna vrsta ransomvera čija je meta bila Master Boot Record (MBR) ranjivog sistema. Napadom na MBR ransomver ubacuje svoj maliciozni kod u boot sektor i automatski restartuje računar. Nakon restarta sistema na ekranu bi se ispisala poruka o otkupu na ruskom.

Prvih nekoliko godina ransomver je bio pojava vezana isključivo za područje Rusije, ali već 2012. ovi napadi počinju da se događaju širom sveta. U martu 2012. godine primećeno je masovno širenje ransomver napada u Evropi, SAD-u i Kanadi. Osim širenja napada na druge regione, došlo je do promena u tehnikama za propagaciju napada. Ransomver napadi su emitovani u vidu *watering-hole* napada, odnosno, usmeravani su na kompanije ili organizacije. Kod ove taktike napadač inficira veb stranu za koju je članovi ciljane ogranizacije često posećuju kako bi došlo do masovnog širenja ransomvera čak i kod organizacija koje su otporne na *phishing* napade. [3]

Reveton ransomver se pojavio 2012. godine i spade u grupu ransomver Trojan. Ovaj ransomver je poznat i pod imenom policijski ransomver jer se, u svojoj poruci o otkupu, predstavlja kao lokalna policijska služba. U poruci o otkupu navodi se da je računar korišćen za ilegalne aktivnosti kao što su piraterija ili dečja pornografija i da korisnik mora da plati kaznu. U poruci se navodi i IP adresa računara ili snimak sa kamere kako bi se žrtva uverila u autentičnost poruke. Napadači su prilagođavali poruke o otkupu na osnovnu geografske lokacije žrtve, koristili službeni jezik tog područja pa čak i lažne digitalne sertifikate.

U septembru 2013. godine se pojavila nova vrsta ransomvera koja je osim zaključavanja sistema koristila i tehniku enkriptovanja datoteka. Zbog tehnike koju koristi ovaj ransomver je nazvan CryptoLocker. [3]

3. CRYPTOLOCKER

CryptoLocker se prvi put javlja u spetembru 2013. godine. Ovaj ransomver je dizajniran za napad na sisteme koji rade na Windows operativnom sistemu. Za razliku od ranijih vrsta ransomvera, CryptoLocker enkriptuje datoteke koje se nalaze u zaraženom sistemu.

Za propagaciju CryptoLockera korišćene su e-mail poruke i bot mreža. Naime, meta napada dobije e-mail sa prilogom koji je u zipovanom formatu. Ove e-mail poruke su takve sadržine da na prvi pogled deluju kao da dolaze iz legitimnog izvora. U direktorijumu iz priloga se nalazi izvršna datoteka prikrivena pdf ikonicom. Ukoliko korisnik otvori tu datoteku malver će se instalirati u *user*

direktorijum korisnikovog računara i dodati ključ u registar. Zatim, malver će pokušati da se konektuje sa jednim od komandnih servera bot mreže. Nakon povezivanja sa komandnim serverom, server će generisati 2048-bitni RSA par ključeva (javni i privatni) i onda će javni ključ poslati nazad ka zaraženom računaru. Komunikacija između komandnog servera i zaraženog računara se preusmerava preko više različitih tačaka kako bi se onemogućilo praćenje i otkrivanje lokacije servera. Nakon dobijanja javnog ključa, malver će enkriptovati datoteke i upisaće logove svih enkriptovanih datoteka u registar ključeva.

CryptoLocker enkriptuje samo datoteke sa određenom ekstenzijom odnosno dokumente (MS Office, Open Office...), formate slika i AutoCad formate.

Nakon enkripcije datoteka, na ekranu korisnika se pojavljuje poruka u kojoj se traži otkup u vrednosti od 400$ u *bitcoin*-ima ili preko pre-paid vaučera. Ovaj otkup treba da se plati u određenom vremenskom roku (tipično 72-100 sati) ili će ključ za dekripciju biti uništen. Nakon plaćanja otkupa, korisnik dobija program za dekripciju sa upisanim odgovarajućim ključem za dekripciju.

Neke od žratava ovog ransomvera su tvrdile da i nakon plaćanja otkupa nisu dobili program za dekripciju pa su kreatori CryptoLocker-a kreirali online servis za dekripciju. Ovaj servis je pružao mogućnost dekripcije datoteka nakon kupovine ključa za dekripciju kao i kupovinu ključa nakon isteka predviđenog roka za plaćanje otkupa.

Ovaj ransomver je kreirala i kontrolisala bot net grupa pod nazivom Gameover ZeuS, koja je uhvaćena sredinom 2014. godine u sklopu operacije Tovar. Operacija Tovar je okupila bezbednosne agencije više zemalja, kompanije i stručnjake iz oblasti bezbednosti kao i pojedine univerzitete kako bi otkirli grupu koja stoji iza CryptoLocker ransomvera. Nakon razotkrivanja Gameover ZeuS grupe, bezbednosne kompanije su uspele da dođu do baze podataka ključeva za dekripciju koju je ova grupa pokušala da pošalje na bezbednu lokaciju. Stručnjaci su iskoristili ovu bazu i napravili online portal za dekriptovanje datoteka enkriptovanih CryptoLocker-om. Kao vođa Gameover ZeuS grupe identivikovan je Evgenij Bogačev. On i Gameover Zeus grupa su, širenjem CryptoLocker-a i naplatom otkupa, zaradili oko 3 000 000$.

Nakon izolacije CryptoLocker-a pojavilo se više ransomvera koji rade na istom principu. Neki od njih su: Crypt0L0cker virus, CryptoLocker-v3, Cryptografic Locker, PCLock ransomware, CryptoTorLocker 2015, CryptoWall.

4. DALJI RAZVOJ

Početkom 2014. godine pojavio se novi ransomver iz grupe ransomvera koji koriste tehniku enkripcije datoteka – Crypto Wall. U svom radu koristi AES enkripciju, CHM mehanizam za propagaciju i Tor anonimnu mrežu. Postoji više varijanti Crypt Wall-a i to: Cryptorbit, CryptoDefense, CryptoWall 2.0, 3.0 i 4.0.

Prve verzije CryptoWall-a su najčešće bile distribuirane preko *exploit kit*-a ili e-mail poruka sa malicioznim prilogom. U prilogu ovakve e-mail poruke obično se nalazi .rar direktorijum koji sadrži CHM datoteku. CHM datoteka je interaktivna html datoteka spakovana u CHM kontejner. Nakon pokretanja CHM datoteka preuzima binarnu verziju CryptoWall-a i kopira samu sebe u %temp% direktorijum. Ovo preuzimanje malvera se obavlja u pozadini, odnosno, bez znanja korisnika. E-mail poruke koje se koriste za propagaciju CryptoWall-a najčešće pokušavaju korisnika da ubede da je reč o legitimnom obaveštenju koje šalje banka ili druga finansijska institucija. Još jedna odlika CryptoWall ransomvera je poruka o otkupu na više jezika. Naime, kreatori ovog ransomvera su prilagodili poruku o otkupu geolikaciji napadnutog sistema.

Kod CryptoWall 2.0 ransomvera datoteke su enkriptovane pomoću algoritama enkripcije sa javnim ključem dok se kod verzije 3.0 ovog ransomvera koristi 265-bitni AES ključ za enkripciju. Zatim se ovaj AES ključ enkriptuje novim javnim ključem kako bi se smanjila

mogućnost njegovog otkrivanja. Prilikom enkripcije datoteka, CryptoWall 3.0 prvo kopira datu datoteku sa dodatnim slučajnim karakterom, zatim enkriptuje sadržaj datoteke i upiše ga i na kraju obriše originalnu datoteku. Svaka enkriptovana datoteka počinje sa heširanom vrednošću javnog ključa koji je dobijen od servera a zatim sledi 256-bitni AES ključ koji je enkriptovan pomoću algoritma enkripcije sa javnim ključem. Sva imena dodeljena enkriptovanim datotekama skladište su u registar ključeva "HKCU\Software\<unique Identifier>\". Na osnovu javnog ključa CryptoWall 3.0. generiše jedinstveni ID za svaku zaraženu datoteku dok su starije verzije ovog ransomvera javne ključeve skladištile na komandnom i kontrolnom centru.

Nakon enkripcije datoteka CryptoWall emituje poruku o otkupu u kojoj opisuje svoje akcije i daje instrukcije za plaćanje. U sklopu poruke o otkupu nalaze se i Tor linkovi i jedinstveni ID specijalno generisan za odgovarajućeg korisnika. Ova poruka se može generiše na tri različita načina: kao datoteka za prikaz u veb pregledaču, u tekstualnom formatu i u formatu slike. Zahtevani otkup je najčešće u *Bitcoin*-ima a uplata se vrši preko Tor-a. [4]

U najnovijoj verziji CryptoWall ransomvera, verziji 4 unete su neke značajne promene. Naime, jedna od novina kod ovog ransomvera je što osim datoteka enkriptuje i njihova imena kako bi se otežao process dekripcije bez plaćanja otkupa. Osim toga, sam process instalacije CryptoWall-a 4.0 se sastoji od brojnih komandi koje se izvršavaju kako bi kako bi se zavarao anti-virus program i nesmetano izvršila instalacija ransomvera i enkripcija datoteka. Ova izmena je dovela do znatnog smanjenja detekcije CryptoWall ransomvera. Izmene se primećuju i u poruci o otkupu koja je preimenovana u *'Help your files'* i sadrži i FAQ sekciju za korisnika. [5]

CryptoWall i njegove varijante detektovane su širom sveta. Najveći procenat detekcije je u Severnoj Americi i Kanadi (13%), zatim u Velikoj Britaniji, Holadniji i Nemčkoj (po 7%). Procenjuje se da su napadači, samo pomoću CryptoWall 3.0 iznudili preko 325 000 000 $.

Osim CryptoWall-a veliku rasprostranjenost imaju i:

- TeslaCrypt koji se fokusira na korisnike online igrica,
- SamSam koji prvenstveno napada sektor zdravstva,
- Locky koji je fokusiran uglavnom na region Nemačke i Holandije,
- Petya ransomver koji napada boot sektor sistema,
- KeRanger koji je dizajniran za iOS sisteme kao i
- ransomveri koji napadaju Android sisteme.

5. PREPORUKE I PREDLOG ZAŠTITE

Ransomver napadi se mogu izbeći primenom određenih dnevnih praksi. Korišćenjem legitimnih anti-virus programa i firewall-a sa dobrom reputacijom kao i njihovim redovnim ažuriranjem, zatim kreiranjem rezervne kopije podataka na eksternim memorijama i slično. Preporuke za prevenciju ransomvera ili ublažavanje posledica ransomvera su:

- Redovno kreiranje rezervne kopije podataka. Poželjno je čuvanje rezervne kopije podataka na eksternim medijumima jer postoje tipovi ransomvera koji brišu rezervne kopije iz sistema,
- Sistem treba radovno ažurirati kako bi se smanjio rizik od napada,
- Posećivati samo proverene veb sajtove,
- Preuzimati samo one e-mail priloge koji su poslati sa proverenih adresa,
- Koristiti anti-virus i firewall proverenih vendora,
- Instalirati program za blokiranje *pop-up* programa,
- Onemogućiti *System Restore* opciju,
- Obavestiti nadležne o napadu. [1]

Korišćenje anti-virus programa i *firewall-a* proverenih vendora je dobra praksa u zaštiti od kiber napada ali često nije dovoljna. Šteta koju mogu da nanesu ovi napadi zavisi od tipa i značaja podatka koji se skladište u napadnutom sistemu. Kod rezidencijalnih korisnika materijalna šteta je najčešće simbolična jer enkriptovane datoteke obično sadrže fotografije ili profile za igranje online igara (TeslaCrypt). Kod poslovnih korisnika šteta je znatno veća. Podaci koje ransomver enkriptuje kod poslovnih korisnika mogu da budu poslovni planovi, nacrti, finansijskih podaci, lični podaci, odnosno podaci koji su poverljivi.

Malver za pokretanje instalacije ransomvera najčešće se distribuira e-mail *phishing* kampanjam i to u vidu priloga. Prilozi kod *phishing* e-mailova su obično datoteke u word ili eksel formatu sa ugrađenim aktivnim sadržajem (*macros*) koji se koristi za pokretanje instalacije ransomvera. Efikasan sistem za prevenciju ransomvera trebao bi da uoči ovakav sadržaj i da ga ukloni ili blokira. Jedan od pristupa za pravenciju ransomvera je filtriranje datoteka i blokiranje svih aktivnih sadržaja kao i skrivenih i nedozvoljenih sadržaja. Drugi pristup za prevenciju ransomvera je dubinska analiza sadržaja i uklanjanje potencijalno opasnih sadržaja.

Primer sistema koji koristi tehniku filtriranja datoteka je *Selector IT* proizvođača *YazamTech*. *Selector IT* je sistem za filtriranje različitih tipova datoteka. Rad ovog sistem se bazira na kontroli i filtriranju svih datoteka koje se unose u sistem, bilo preko mreže ili preko medijuma (CD, USB…). Kontrola i filtriranje datoteka se vrše na osnovu:

- ekstenzije – datoteke sa lažnim ekstenzijama se odbacuju,
- pretrage teksta – zahtevane reči, zabranjene reči, skriveni sadržaj,
- zabranjenog sadržaja – uklanjanje aktivnog sadržaja.

Ovaj sistem ima podršku za više od 10 anti-virus programa različitih vendora i u svom radu koristi njihove anti-virus mehanizme. Datoteke koje *Selector IT* može da filtrira su:

- MS office tipovi,
- pdf,
- tekstualni formati,
- audio formati i formati slika,
- formati arhiva (zip, rar…),
- HTML, XML,
- CAD, GIS,
- formati poruka (e-mail, kontakti, kalendari),
- datoteke nepoznatog tipa.[6]

Selector IT je preporučeno rešenje za prevenciju ransomvera zbog načina filtriranja datoteka. Naime, ovaj sistem radi filtriranje na osnovu ekstenzije i odbacuje datoteke sa lažnom ili zabranjenom ekstenzijom. Ovaj način filtriranja onemogućuje malicioznim datotekama da uđu u sistem. Osim toga, filtriranje se vrši i na osnovu aktivnog sadržaja, odnosno, aktivni sadržaj se isključuje. Veliki deo ransomvera u sistem dospeva upravo preko aktivnih sadržaja (*macros*) koji su ugrađeni u tekstualne dokumente. Još jedna prednost korišćenja *Selector IT* sistema i činjenica da su mehanizmi više anti-virus programa različitih vendora ugrađeni u ovaj sistem.

Kao primer rešenja koja koriste tehniku dubinske provere sadržaja radi uočavanja i uklanjanja opasnih i potencijano opasnih sadržaja mogu se navesti rešenja za bezbednu komunikaciju kompanije *Deep Secure*.

Web guard, rešenje kompanije *Deep Secure*, konroliše veb saobraćaj organizacije i vrši odbranu od naprednih pretnji i napada. U svom radu *Web guard*, kao i ostala *Deep Secure* rešenja koriste *Transhipment* tehniku. *Transhipment* tehnika se zasniva na dekompoziciji podataka i njihovoj detaljnoj analizi. Naime, kod ove tehnike na prijemu dolazi do prekidanja dolaznog protokola i potpune dekompozicije podataka. U dekomponovanom stanju podaci prolaze kroz verifikator koji vrši proveru i sve nepotrebne ili potencijalno opasne podatke eliminiše. Svi podaci

koji prođu validaciju bivaju rekonstruisani i, pomoću nove konekcije, se prenose kao odredištu.

Na ovaj način *Web guard* vrši proveru zaglavlja svih HTTP zahteva i odgovora. Ukoliko se u njima nalaze osetljivi podaci (pr.*cookies*) oni bivaju odbačeni a ostatak podataka rekonstruisan i prenet dalje do odredišta. *Web guard* podržava autentifikaciju klijenata preko *Windows Integrated Authentifications* ili digitalnih potpisa i na taj način omogućuje da samo autentifikovani klijenti mogu da vrše komunikaciju u mreži. Osim HTTP protokola, *Web guard* podržava i HTTPS protokol što omogućuje prenos enkriptovanog saobraćaja.

Još jedna od pogodnosti *Web guarda* je mogućnost obaveštavanja administratora o detekciji nedozvoljenog ili sumnjivog sadržaja.

Web guard sistem je efektivna zaštita od ransomvera jer potpuno dekomponuje sve podatke i odbacuje sve osim poslovnih informacija. [7]

Osim *Web guarda* postoje i druga specijalizovana rešenja za zaštitu na aplikativnom nivou kao što je rešenje *Mail guard* za zaštitu e-mail saobraćaja, *File Transfer guard* za bezbedan prenos datoteka, *XML guard* za kontrolu XML saobraćaja, *TransGap Import Export* za kontrolu datoteka koje se uvoze/izvoze na medijume, itd. Kod kompleksih sistema najbolja zaštita od ransomvera ali i drugih kiber napada bi bila kombinacija više rešenja iz domena zaštite na aplikativnom nivou. Za što viši stepen bezbednosti preporučuje se višeslojna zaštita mreže korišćenjem *Web guard-a* kao prvi sloj zaštite celokupne mreže, zatim *Mail guard-a* za zaštitu e-mail saobraćaja, *File Transfer gurad-a* za bezbedan prenos datoteka i *TransGap ImpEx* za bezbedan uvoz/izvoz datoteka sa medijuma. Ukoliko sistem poseduje servis za skladištenje datoteka preporučuje se korišćenje i *TransGap SFS* (*Shared File Store*) za zaštitu podataka u skladištima datoteka.

U uslovima savremenih kiber pretnji kao prvi i obavezan stepen zaštite mreže od kiber napada preporučuje se i kombinacija anti-virus programa, *firewall-a* i sistema za detekciju i prevenciju kiber napada – *Intrusion Detection and Prevention Systems*, skraćeno IDPS. Sve je više izvanrednih softverskih rešenja za detekciju i prevenciju kiber napada koji koriste više unakrsnih metoda za detekciju uključujući i specijalne metode za otkrivanje čak i napada nultog dana – *Zero Day Attacks*, koji sve masovnije zamenjuju tradicionalna serverska (*IPS Server type*) i mrežna rešenja (*IPS Gataway type*) poznatih brendiranih, veoma kompleksnih a samim tim i skupih rešenja. Jedno od izvanrednih rešenja za detekciju i prevenciju kiber napada predstavlja *Towers Net Defender – TND*, potpuno automatski IPDS sistem koji veoma efikasno štiti mrežu, lako i brzo se implementira, prilagođen je za rad na svim operativnim sistemima i hardverskim platformama.

Ovaj sistem nadgleda mrežu, blagovremeno identifikuje maliciozne aktivnosti i blokira ih. Zahteva vrlo malo resursa (memorija, potrošnja) i ne usporava rad sistema. Uspešno blokira DoS i DDoS napade, SYN floods, SQL injections, Brute-force napade, Rootkits, XSS napade, Zero Day napade i malvere za uspostavljanje *backdoor-a*. [8]

Kombinacijom predstavljenih rešenja i pravilnom edukacijom zaposlenih sistem se može zaštititi od bilo kog kiber napada ili kombinacije napada.

6. ZAKLJUČAK

Poslednjih godina zapažen je rastući trend ransomver napada. U današnje vreme postoje i ciljani ransomveri, odnosno ransomveri koji napadaju institucije iz sektora finansija, zdravstvenog sektora, korisnike online igara i slično. Osim toga, kreatori ransomvera koriste sve prefinjenije tehnike zavaravanja korisnika. Neke od tih tehnika su prilagođenje napada geolokaciji korisnika kao što su *phishing* e-mailovi na različitim jezicima i sa oznakama kompanija i institucija u zavisnosti od lokacije ciljanog korisnika. Osim tehnika napada i tehnike blokiranja sistema i enkripcije podaka evoluiraju velikom brzinom. Do ubrzanog razvoja je došlo i kod tipa sistema na kojima može da se izvrši napad pa tako imamo ransomvere prilagođene Windows,

Linux i iOS sistemima ali i Andorid sistemima pa osim računara i servera ransomver napad se može izvršiti i na mobilnim uređajima.

Imajući u vidu da ransomveri mogu da nanesu veliku štetu kako finansijsku tako i štetu po reputaciju kompanija i pojedinaca jako je bitno raditi na edukaciji korisnika. Svaki internet korisnik treba da bude edukovan o načinu propagacije i rada ransomvera i preporukama za bezbednost sistema. Takođe, svaka kompanija bi, u zavisnosti od kompleksnosti svoje mreže, trebala da primeni jedno ili više rešenja za prevenciju kako ransomvera tako i ostalih kiber napada.

REFERENCE

[1] Dr.P.B. Pathak, "A Dangerous Trend of Cybercrime: Ransmoware Growing Challenge", International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), Volume 5 Issue 2, Maharashtra, India, February 2016,

[2] Ransmoware: Past, Present, and Future, Cisco Talos Blog, http://blog.talosintel.com/2016/04/ransomware.html, April 2016,

[3] Ransomware, Trend Micro, http://www.trendmicro.com/vinfo/us/security/definition/ransomware,

[4] J.Wyke, A.Ajjan, "The Current State of Ransomware", SophosLabs technical paper, decembar 2015,

[5] A.Allievi, H.Unterbrink, W. Mercer, "CryptoWall 4.0 the Evolution Continues", Cisco Talos white paper, mart 2016,

[6] Selector IT brošura, http://www.towersnet.rs/wp-content/uploads/2016/03/SelectorIT.pdf

[7] Web Guard brošura, http://www.towersnet.rs/wp-content/uploads/2015/06/Web-Guard-flyer.pdf

[8] Towers Net Defender brošura, http://www.towersnet.rs/wp-content/uploads/2015/06/TND-flajer.pdf