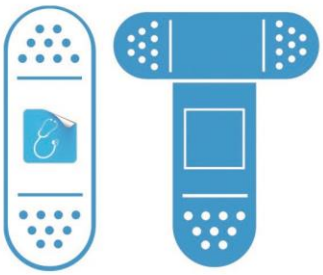


KLINIKA

Specijalisti za IT bezbednost

Ransomware: uvid u unosni kriminalni „poslovni“ model

Najbolji saveti za prevenciju ransomware-a

Powered by

Net++ TECHNOLOGY

www.it-klinika.rs

www.netpp.rs

Kratak pregled

Ransomware, a posebno kriptografski ransomware, je prešao put od beznačajne pretnje do sofisticiranog višemilionskog kriminalnog poduhvata koji cilja kako pojedince, tako i kompanije. Kriminalni „poslovni“ model se pokazao visoko efikasnim u stvaranju prihoda za sajber kriminalce, a pored toga ima ogroman uticaj na poslove organizacija koje pogađa. Gotovo svako preduzeće može postati meta ransomware-a, bilo gde na svetu i u bilo kojoj industriji. Male organizacije, velike organizacije, pojedinci - svi su potencijalna meta. Ransomware u različitim oblicima postoji već decenijama, ali u poslednje 3 godine, sajber kriminalci su doveli do savršenstva ključne komponente napada. Ovo je dovelo do eksplozije novih vrsta malvera koje su učinile tehnike napada efikasnijim i privukle nove maliciozne igrače koji smišljaju i lansiraju ove unosne prevare.

- Finansijski efekat ransomware-a je ogroman. Nekoliko velikih upada u sisteme dovelo je do višemilionskih isplata otkupnine.
- Ransomware je jedan od retkih „poslovnih“ modela sajber kriminala koji može da naškodi i kompaniji iz grupe Fortune 500, lokalnom restoranu i vašoj baki.
- Kripto-valuta Bitkoin je omogućila mehanizam isplate koji podstiče uspeh ovog modela. Mehanizmi isplate na koje su se sajber kriminalci ranije oslanjali su ili ugašeni ili stavljeni pod zakonsku regulativu, dok Bitkoin nema regulatorni mehanizam poput Centralne banke i sl.
- Do skora su napadi uglavnom ciljali sisteme bazirane na Windows-u, ali sada su mete i drugi operativni sistemi, poput Mac OS X.
- Sve dok organizacije širom sveta ne počnu da razmišljaju o preventivi i sve dok ne prestanu da plaćaju otkup kako bi povratili svoje podatke, ovaj kriminalni model će biti pretnja za sve uređaje povezane na internet.

Iako predstavlja narastajuću pretnju, ransomware se može sprečiti kroz adekvatnu obuku, konkretna prilagođavanja postojećem IT okruženju i kroz naprednu endpoint tehnologiju.

Sadržaj

Šta je ransomware?

Napadači moraju da izvrše sledećih 5 koraka kako bi ransomware napad bio uspešan:

1. **Da kompromituju sistem i uspostave kontrolu nad njim.** Najveći broj napada počinje sa spear-phishingom (precizno ciljana phishing email kampanja), kada se pošalje lažni, ali uverljivi imejl koji treba da navede primaoca da preuzme ili otvori zaraženi prilog, koji dalje kompromituje sistem. Ovo može da utiče na jedan računar, mobilni telefon ili na čitavu organizaciju.
2. **Da onemoguće pristup sistemu.** Kada kompromituje sistem, napadač identifikuje i kriptuje određene fajlove koji su od vrednosti za žrtvu napada, kao što su .doc, .xls, .pdf ili zabranjuje pristup čitavom sistemu zaključavanjem ekrana i taktikama zastrašivanja.
3. **Da upozore korisnike uređaja da im je sistem kompromitovan, obaveste o ceni „otkupnine“ i predoče vam korake koje bi trebalo da preduzmete.** Napadači i žrtve često pričaju različitim jezicima i imaju različit nivo tehničkih sposobnosti tako da napadači moraju da objasne žrtvama šta se desilo i koje korake treba da preduzmu kako bi otključali svoje uređaje.
4. **Da prime novac od otkupnine.** Napadač mora da ima pripremljen način da primi novac od otkupnine i da pritom izbegne zakonske peripetije. Zbog toga je jasno zašto se za ovakve transakcije koriste kripto-valute poput bitkoina.
5. **Da obećaju da će nakon što im legne uplata omogućiti žrtvi potpun pristup sistemu.** Ukoliko ovo ne urade, to će smanjiti efektivnost čitavog modela prevare, jer niko neće plaćati otkup bez uverenja da će mu pristup podacima biti omogućen.

Ko je ugrožen?

Organizacije od šireg javnog interesa. Ransomware napadi mogu imati veoma širok uticaj, jer poslovi organizacija koje su žrtve napada mogu biti ozbiljno ugroženi ili čak i prekinuti. Primer za to su nedavni napadi na bolnice širom SAD-a. Kriminalci su shvatili da je ovo veoma unosan posao u koji se lako ulazi, a ransomware postepeno istiskuje druge „poslovne“ modele sajber-kriminala. U budućnosti će napadači biti sve sofisticiraniji u pogledu sposobnosti da odrede vrednost kompromitovanih informacija i procene koliko je žrtvina organizacija spremna da plati, i zahtevaće više otkupnine.

Više platformi. Istorijski posmatrano, napadači su se isključivo fokusirali na Microsoft Windows sisteme. Vremenom su se pojavili i ransomware-i za Android platforme, a kako Palo Alto Networks otkriva, od nedavno i za Mac OS. To znači da praktično nijedan sistem nije imun na ove napade. Gotovo svi računari i uređaji koji su povezani na

Internet su potencijalne žrtve ransomware-a, a to treba još više da nas brine usponom Internet of Things (IoT) i širenjem vrsta uređaja koji su povezani na internet, kao što su kućni aparati i tehnički uređaji koji mogu da se nose poput pametnih satova itd.

Istorija ransomware-a

Prvi zabeleženi slučaj ransomware-a dogodio se 1989. godine. Njegov tvorac je Dr Džozef Pop, biolog i jedan od pionira istraživanja AIDS virusa. On je planirao da distribuira 20.000 flopi diskova u preko 90 zemalja. Na njima su se nalazile informacije o AIDS virusu, a takođe i tzv. AIDS trojanac koji je bio osmišljen tako da se posle 90-og podizanja sistema pojavi sledeća poruka:

On je, dakle, koristeći izmišljenu kompaniju „PC Cyborg Corporation“ pokušao da naplati „licencu za softver“ u iznosu od $189. U to vreme, pre interneta i imejla, nisu ni postojali zakoni koji bi se bavili ovakvim stvarima. Ovaj ransomware je bio osnova za sve buduće. Pažljivo osmišljen, koristio je aktuelnu i osetljivu socijalnu temu, ali je imao neke nedostatke:

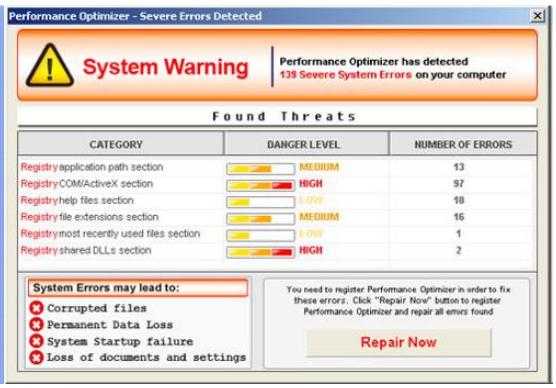
- Sistem nije bio kriptovan u celini, već samo imena fajlova i direktorijuma tako da su svi fajlovi i dalje postojali u nekriptovanom prostoru, ali su bili nedostupni.
- Korišćena je simetrična enkripcija, što znači da je ključ i za enkripciju i za dekripciju isti i sadržan u samom malveru.
- Sistem isplate otkupnine nije bio idealan. Bio je osmišljen tako da se šalje novac ili ček na poštanski fah u Panami uz obećanje da će žrtva dobiti ključ za dekripciju. Sve je to trajalo predugo i žrtve nisu imale garanciju da će se to i desiti, a u međuvremenu su stručnjaci napravili 2 alata za vraćanje fajlova. Međutim,

AIDS trojanac je napravio dosta štete. Jedan italijanski naučni institut je izgubio podatke koje je skupljao tokom 10 godina istraživanja.

Posle ovog slučaja, dolazi do razvoja asimetrične kriptografije, koja će povećati efikasnost budućih ransomware napada.

Razvoj ransomware-a

Od 2005. godine, ransomware malver se razvija u 2 pravca – kao scareware i kao kriptografski ransomware. Scareware je malver koji koristi taktike zastrašivanja i agresivne notifikacije koje upozoravaju na navodne probleme u sistemu koji mogu lako da se reše uz uplatu $30-90. Scareware su često bili programi niskog nivoa sofistikacije, a često nisu ni bili programi. Autori scareware-a su koristili sve moguće taktike da iznude novac – od jednostavnih alata koji su delovali kao legitimni sistemski alati, preko reklama na banerima, slika i jednostavnih pop-up-a. U to vreme, sa početkom razvoja interneta, ljudi nisu bili upućeni, a ni oprezni, pa se scareware širio mrežom. Vremenom je scareware postao više napast nego realna pretnja, s obzirom na to da nije kriptovao fajlove ili zabranjivao pristup nekim delovima sistema. Pritom, način plaćanja otkupnine nije bio dobro osmišljen i razvijen.



Istovremeno, sredinom 2005. Pojavljuje se nova vrsta crypto ransomware-a – „GPCode“ ili „PGPCoder“. Pojavio se u Rusiji i ciljao je ruske organizacije. Prva verzija je imala brojne slabosti, ali je autor nastavio da je razvija i unapređuje u narednih 5 godina i napravio je verziju koja je postala prototip modernog crypto ransomware-a. U početku, malo njih je pratilo ovaj pravac razvoja ransomware-a. Umesto toga, pojavila se nova verzija scareware-a – lažni antivirus (eng. FakeAV) koji je bio najrašireniji malver 2008. i 2009. godine. Zakonske mere, koje je, između ostalih, preduzeo i Majkrosoft, zadale su veliki udarac scareware malverima, a poslednji veliki talas scareware-a se desio 2011. i 2012. godine kada se pojavio „locker“ ransomware. Najpoznatiji „locker“ ransomware je Reveton.

Nakon ovoga, maliciozni hakeri smišljaju kako bi mogli da povećaju efikasnost iznuda. Odgovor se javlja 2013. u vidu CryptoLocker-a.

CryptoLocker

Krajem 2013. godine, stižu prvi izveštaji o malveru koji enkriptuje fajlove u Windows operativnim sistemima. Ispostaviće se da je reč o CryptoLocker-u koji je prethodnica stvaranja multimilionske crypto ransomware industrije.

CryptoLocker je jedinstven zbog toga što je razvijen tako što su njegovi tvorci pažljivo proučavali nedostatke i propuste prethodnih ransomware-a. Dolazi do promene taktike u odnosu na scareware-a koji nije pravio stvarnu štetu u sistemu. CryptoLocker je distribuiran na sličan način kao i scareware i njegovi autori su se oslanjali na phishing napade sa prenosnim izvršnim atačmentima. Autori su se prevashodno oslanjali na neobaveštenost žrtava i koristili su razne tehnike socijalnog inženjeringa kako bi lansirali malver.

Kako CryptoLocker funkcioniše? Najpre, instalira se u folder profila korisnika (user's profile folder). Dalje, dodaje „registry key“ koji se pokreće pri podizanju sistema. Onda, započinje pokušaje komunikacije sa komandnim i kontrolnim serverom kako bi generisao RSA-2048 par ključeva i poslao javni ključ nazad na server mete napada. Asimetrični enkripcijski model se pokazao jako efikasnim pošto je svaki par ključeva jedinstven i nema načina da se dobije privatni ključ zbog toga što se nalazi u komandnom i kontrolnom centru. Nakon što se napravi jedinstveni par ključeva, enkripcija počinje da deluje tako što cilja poslovne fajlove, a ne ceo sistem. Onda sledi obaveštenje korisniku da će privatni ključ biti uništen ukoliko se ne isplati otkupnina u roku od 72h. Plaćanje se vršilo preko MoneyPak i Bitcoin-a. Rastuća popularnost Bitkoina i same karakteristike ove valute su vrlo privlačne napadačima. To je relativno jednostavan, pouzdan i delimično anoniman način plaćanja i nije vezan ni za jednu vladu ili organizaciju koja bi mogla da je ugasi ili konfiskuje sredstva. Kada se CryptoLocker pojavio, autori su zaradili oko 42.000 Bitcoina, što je oko $27 miliona. U ovoj fazi razvoja ransomware-a, napadači više nisu blefirali svoje žrtve već su imali realno oružje u svojim rukama (zaključavanje fajlova).

Ipak, CryptoLocker je ispoljio i neke mane. Prvo, do enkripcije nije dolazilo ukoliko dođe do prekida komunikacije između komandnog i kontrolnog centra ili ako se komunikacija uopšte ne uspostavi. Dalje, rane verzije CryptoLocker-a omogućavale su žrtvama da urade oporavak sistem u Windows-u i vraćanje u pređašnje stanje. Konačno, čak i kad se

napravi par ključeva za enkripciju i CryptoLocker krene da deluje, postoji određeni vremenski okvir u kome se kriptovanje može prekinuti.

Akcijom američkog ministarstva odbrane, 2014. je srušen Gameover Zeus botnet što je uticalo na infrastrukturu CryptoLocker-a. Srećom po žrtve napada, firma Fox-IT je uspela da uđe u privatnu bazu CryptoLocker-a i poništi asimetričnu enkripciju tako što je sve privatne ključeve javno objavila. Ova akcija je okončala operacije CryptoLocker-a, ali nije zaustavila druge sajber-kriminalce i tako smo ušli u doba Crypto Ransomware-a.

Ransomware danas

Ransomware je postao jedna od najvećih pretnji velikim i malim organizacijama današnjice. Tim koji se u Palo Alto Networks-u bavi ovim pitanjima trenutno prati 30 različitih vrsta crypto ransomware-a. Razlike između njih su u detaljima. Neki od njih su CryptoWall, Locky, SamSa, TeslaCrypt. U odnosu na CryptoLocker, autori ovih malvera su uneli brojna unapređenja. Jedno od njih je korišćenje anonimnih mreža poput TOR ili I2P. Zatim korišćenje CAPTCHA prilikom plaćanja. Mnoge varijante ovih crypto ransomware-a danas nude opcije poput live chat-a za tehničku pomoć ili prevod instrukcija na jezik kojim žrtva govori. Sajber-kriminalci su shvatili da je ransomware unosan posao u koji se relativno lako ulazi, usavršili su svih 5 koraka potrebnih za uspeh ovog kriminalnog „poslovnog“ modela, počeli su da napadaju i druge platforme pored Windows-a, poput Androida i Mac OS X sistema. U martu 2016. godine, otkriven je malver KeRanger, koji predstavlja prvi dokumentovani ransomware napad na Mac OS X sisteme. KeRanger je distribuiran tako što je u popularni BitTorrent klijent po imenu Transmission ubačen trojanac.

Budućnost Ransomware-a

S obzirom na činjenicu da se ransomware pokazao izuzetno isplativim kriminalnim poslom, u budućnosti možemo očekivati sledeće:

- **Više platformi:** Nijedan operativni sistem više nije imun na napade i svaki uređaj može biti meta napada.
- **Viši iznosi otkupnina:** Otkupnina u većini slučajeva kada je napadnut jedan sistem iznosi od $200 do $500. Međutim, kada napadači znaju da su kriptovali vredne informacije i kada su svesni da je organizacija spremna da plati veću sumu novca, onda podižu iznos otkupnine. To se dogodilo ove godine u napadu na bolnice kada su plaćani otkupi viši od $10.000.
- **Ciljani ransomware napadi:** Ciljani upad u mrežu je od višestrukog značaja za napadača. Kada upadnu u mrežu, napadači onda mogu identifikovati fajlove

visoke vrednosti, baze podataka i backup sisteme i zatim kriptovati sve podatke istovremeno. Ovakvi napadi preko SamSa malvera već su se pokazali kao izuzetno unosni.

Odbrana od ransomware-a

Kako bi se odbranili od ransomware-a, potrebno je biti svestan pretnje i napraviti plan za njeno sprečavanje. Odbrana se može raščlaniti na 3 dela: priprema, prevencija i odgovor (reakcija).

Priprema

- **Backup i Recovery:** Jedan od najboljih načina odbrane od ransomware-a je kroz backup i recovery proces. Ako možete da vratite kriptovane podatke iz backup sistema, onda možete da se oporavite od uspešnog ransomware napada uz malo ili nimalo pričinjene štete. Backup mora da bude na lokaciji kojoj ransomware nema pristup. Poznato je da su napadači ciljali backup kao deo plana da kriptuju sve vredne fajlove. Testiranje procesa vraćanja fajlova iz backup sistema je skoro podjednako važno kao i sam backup. Ako ovo nikada niste testirali, moguće je da je vaš backup podataka ranjiv.
- **Kontrola pristupa zajedničkom prostoru na mreži**: Mrežni diskovi koji su priključeni na više sistema i sadrže zajedničke podatke su posebno podložni ransomware napadima. Ako je sistem ili korisnik koji ima dozvolu da piše na disku zaražen ransomware-om, svi fajlovi koji se nalaze na zajedničkom disku mogu postati zaraženi, tj. kriptovani. Organizacije moraju da vode računa o tome ko ima pristup pisanju na disku i moraju da svedu broj tih pojedinaca i sistema na najmanju moguću meru. Najveći broj ransomware napada se događa dok korisnici surfuju internetom ili dok čitaju imejl, stoga se o ovome mora voditi posebna briga.

Prevencija

Pošto ransomware deluje brzo (u pitanju su minuti od trenutka prodora u sistem), ključ je u sprečavanju malvera da uopšte uđe u sistem i kriptuje važne podatke.

- **Kontrola imejla i izvršnih fajlova:** Ransomware napadi najčešće počinju imejl porukom u kojoj je sadržan izvršni fajl (eng. executable) ili kada korisnik klikne na link preko kojeg sa preuzima izvršni fajl. Firewall nove generacije može identifikovati ove pretnje i blokirati ih ili staviti u karantin. Ovo neće sprečiti sve ransomware napade, ali mnoge hoće i to je dobar prvi korak u prevenciji.

- **Prevencija nepoznatih malvera:** Pristup detekcije koja se zasniva na potpisima se pokazao nepouzdanim kada su u pitanju novi malveri. Organizacije moraju da imaju način da identifikuju do sada nepoznate malvere (koji se brzo menjaju i razvijaju). Takvi sistemi koriste karantin analizu (eng. sandbox) kako bi identifikovali maliciozno ponašanje, kroz statičku i dinamičku analizu u virtuelnom okruženju, a koriste i globalni obaveštajni sistem o pretnjama.
- **Endpoint kontrola:** Firewall nekada ne reaguje na napade, naročito na one koji se oslanjaju na SSL enkripciju i sl. U ovim slučajevima, najbolja odbrana je kontrola koja se nalazi u endpoint-u i koja sprečava izvršenje malicioznih fajlova pre nego što se aktiviraju.

Odgovor (reakcija)

Ako prevencija nije urodila plodom i ako ste postali žrtva ransomware napada, važno je da imate spremljen plan kao odgovor na napad. On će vam pomoći da u što kraćem roku i uz najmanje štete po organizaciju vratite svoje podatke.

- **Razumite pretnju:** Danas postoji najmanje 30 različitih ransomware-a, a lista se povećava iz dana u dan, tako da je važno da znate sa kojim tačno malverom imate posla. Većina novih vrsta ransomware-a koristi jaku kriptografiju koju je teško savladati, ali u nekim slučajevima stručnjaci su uspeli da dekriptuju fajlove bez plaćanja otkupnine. Jedini način da znate da li je ovo moguće i u vašem slučaju jeste da identifikujete vrstu ransomware malvera. Neke od njih možete identifikovati koristeći informacije iz poruke koju napadači ostavljaju u vašem sistemu. Drugi način je da koristite analizu malvera ili neki informacioni sistem koji je osposobljen za to.
- **Budite spremni na najgore:** Plaćanje otkupnine treba da bude poslednja opcija. Isplate podstiču sajber kriminalce da nastave sa ovim aktivnostima i ohrabruju nove napadače. Čak iako nemate bekapovane podatke, razmotrite sledeće opcije pre plaćanja otkupnine:
  1) Da li možete da vratite ukradene fajlove?
  2) Da li imate stariju verziju fajlova koju možete ažurirati novim informacijama?
  3) Da li podaci postoje na nekom drugom mestu, npr. na drugoj lokaciji koja nije pogođena napadom?

Ako ništa ne urodi plodom i odlučite da platite otkupninu, morate biti spremni da izvršite plaćanje u određenom vremenskom okviru. Skoro svi napadači zahtevaju isplatu u Bitcoin kripto-valuti, ali može biti problematično da u kratkom vremenskom roku pribavite dovoljno novca za kupovinu Bitcoin-a. Plan odgovora na ransomware trebalo bi da sadrži detalje o tome kako izvršiti plaćanje ukoliko dođe do najgoreg scenarija.

Najbolji saveti za minimiziranje uticaja ransomware

1. **Napravite i sprovedite plan za upoznavanje krajnjih korisnika sa problemom**
   - Može biti problematično dobiti dozvolu da se redovno šalju sigurnosni podsetnici u čitavoj kompaniji, ali što su krajnji korisnici upućeniji, to će ransomware incidenata biti manje.

2. **Revidirajte/validirajte procese bekapovanja servera**
   - Neke organizacije nisu svesne da su im bekapovani podaci kompromitovani ili da nisu odgovarajuće konfigurisani, dok ne bude prekasno. Redovno proveravajte stanje i podešavanja.
   - Počnite od vaših fajl servera na kojima su network share-ovi za ključne sektore.

3. **Revidirajte odobrenja mrežnog diska kako bi minimizirali uticaj koji pojedinačni korisnik može da ima**

   Pregled ovlašćenja za krajnje korisnike
   - Zadužite menadžera projekta da pregleda odobrenja koje korisnici imaju u mapiranim mrežnim diskovima. Uvedite princip minimalnog odobrenja kako bi minimizirali uticaj koji pojedinačni korisnik može imati na deljenim mrežnim diskovima organizacije.
   - U zavisnosti od veličine organizacije, ovo može biti zahtevan i kompleksan poduhvat i stoga počnite od lokacija mrežnih diskova koje koriste ključni sektori.

   Pregled ovlašćenja za administratore
   - Revidirajte privilegovane funkcija korisnika koji su zaduženi za server, bekap i mrežu, kako biste adekvatno odredili prava pristupa.
   - Uverite se da administratori imaju svoje naloge sa uobičajenim ograničenjima koji su odvojeni od njihovih naloga sa visokim ovlašćenjima.
   - Zahtevajte od administratora da koriste naloge sa visokim ovlašćenjima samo kada su im potrebni.
   - Uklonite automatska mapiranja mrežnog diska iz administrativnih naloga gde god je to moguće.
   - Onemogućite administrativne naloge da primaju mejlove.

4. **Dokumentujte plan za reagovanje na ransomware incident**
   - Verovatno već imate načelni plan za reagovanje na incidente, ali morate biti posebno spremni za ransomware jer on zahteva veoma specifičan proces oporavka sistema koji se razlikuje od ostalih malware incidenata.
   - U slučajevima kada su kriptovani svi podaci na čitavom disku jednog sektora, čitav proces može postati jako složen jer zahteva koordinisan rad više timova – bekap tima, file-server tima, endpoint, directory tima i drugih. Što više isplanirate sada, brže ćete reagovati u budućnosti.

Najbolji saveti za sprečavanje ransomware-a

1. **Onemogućite macro skripte iz MS Office datoteka pomoću AD Group Policy**
   - Prema podacima Majkrosofta, 98% pretnji koje ciljaju Office koriste macro. Onemogućavanje macro skripti iz MS Office datoteka sprečavaju ransomware, kao što je npr. Locky.
   - Nisu svima u organizaciji potrebni Office macro-i, ali nekima jesu. Dozvolite macro-e samo kao izuzetke za neke sektore.
   - Office 2016 ima novu funkciju koja omogućava administratorima da blokiraju macro-e u Word, Excel i Power Point dokumentima koji dolaze sa interneta. Ako ste u mogućnosti, ažurirajte Office i omogućite ovu funkciju.

2. **Preispitajte svoje mesečne procese upravljanja bezbednosnim ažuriranjima**
   - Mnoge organizacije imaju problema da izvrše bezbednosna ažuriranja sistema u roku od 30 dana od kada Majkrosoft izbaci mesečna ažuriranja.
   - Pregledajte vaše procese bezbednosnog ažuriranja i potražite prilike da uklonite prepreke.
   - Razmotrite opciju da primenite napredni endpoint proizvod koji sprečava iskorišćavanje ranjivosti sistema zbog nedostajućih ažuriranja ili malvera.

3. **Preispitajte zaštitu od spama i malvera**
   - Postarajte se da dolazna pošta bude blokirana prema preporukama vašeg imejl server vendora.

4. **Primenite firewall nove generacije kako biste zaštitili mrežu**

- Postarajte se da vaš firewall automatski blokira poznate pretnje na osnovu liste pretnji koja se stalno ažurira.
- Postarajte se da vaš firewall ima opciju karantina kako bi se mogle stopirati nepoznate pretnje (URL-ovi i izvršne datoteke) pre nego što stignu do krajnje tačke (korisnika). Karantin (eng. Sandboxing) je najbolji način da se detektuju nove varijante ransomware-a koje se stalno pojavljuju.
- Konfigurišite firewall/proxy koji će zahtevati interakciju korisnika za krajnje korisnike koji komuniciraju sa veb sajtovima koji imaju oznaku „nekategorizovani“ (Npr. kliknite „Proceed“). Mnogi nekategorizovani sajtovi se koriste u ciljanim phishing kampanjama kako bi se raširio malver. Ovaj proces od dva koraka sprečava neke vrste ransomware-a da obave eksterni poziv komandnom i kontrolnom serveru. Ako se to ne dogodi, vaša datoteka možda nije kriptovana.

5. **Primenite naprednu endpoint zaštitu kako biste zaštitili krajnju tačku sistema**
   - Tradicionalni antivirus nije efikasan u borbi protiv naprednih malvera, poput ransomware-a, koji se konstantno menja kako bi izbegao detekciju. Vaša krajnja tačka sistema zahteva naprednu zaštitu koja je sposobna da detektuje malver i tehnike iskorišćavanja slabosti sistema (npr. HEAP spray, DEP obmana), a ne samo individualne poznate zaražene datoteke.
   - Bele liste mogu biti od koristi malim, jednostavnijim organizacijama, ali za rastuće organizacije sa puno aplikacija i složenih aktivnosti, upravljanje takvom listom nije jednostavno. Detekcija malvera koja se zasniva na tehnici napada je veoma efikasna u detekciji ransomware-a.

Reference

https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/ransomware-report (datum: 31.05.2016)

https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/ransomware-report (datum: 31.05.2016)

Net++ technology d.o.o.

Bulevar vojvode Mišića 39a | Beograd | Srbija

tel +381 (11) 36-999-67, 4053-516, 4053-519 | fax +381 (11) 4053-447

website | newsletter | map