Ransomver – evolucija i zaštita

N. Simić, Z. Živković, N. Miladinović

TOWERS NET
IT & Telecommunications Innovations

Ransomver

- Ransomver je klasa malvera koja ograničavanjem ili onemogućavanjem korisnika da pristupim svom računarskom sistemu iznuđuje novac – otkup.

- U starijim verzijama korišćene su metode zaključavanja sistema dok se kod novijih verzija ransomvera koristi tehnika enkriptovanja datoteka.

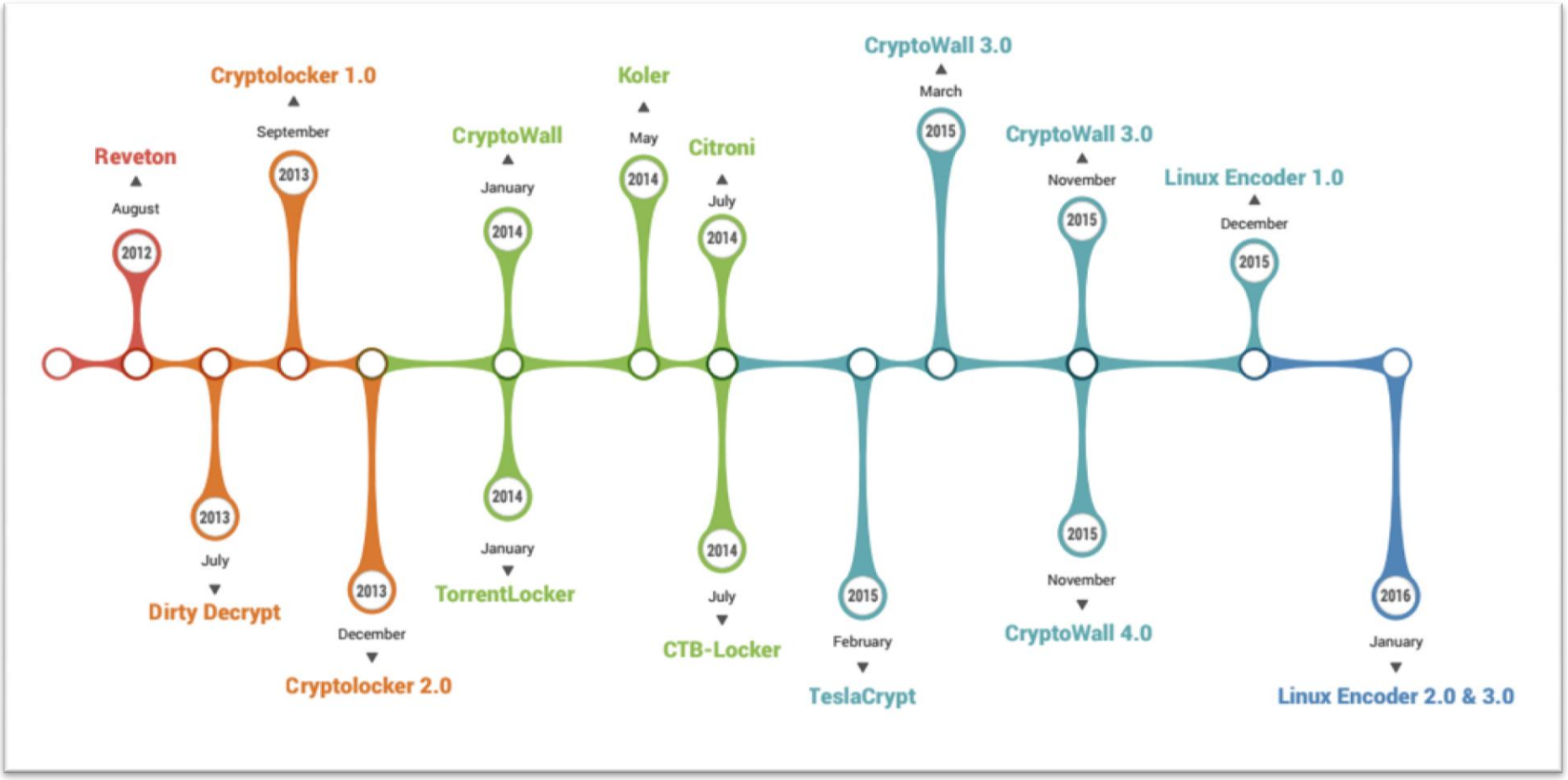
Opis napada

- Nakon zaključavanja sistema i/ili enkripcije datoteka, na ekranu se prikazuje poruka o otkupu.
- U poruci o otkupu je dat opis ransomver napada i uputstva za plaćanje.
- Najčešće se zahteva isplata u *Bitcoin* elektronskoj valuti i to preko Tor pretraživača.

Istorijat

- Prvi slučajevi ransomvera zabeleženi su u periodu 2005.- 2006. godine u Rusiji.
- Ovaj ransomver je koristio tehniku zipovanja sa lozinkom.
- Prvih nekoliko godina ransomver napadi su delovali samo na području Rusije ali već 2012. godine se šire na Evropu, Kanadu i SAD.

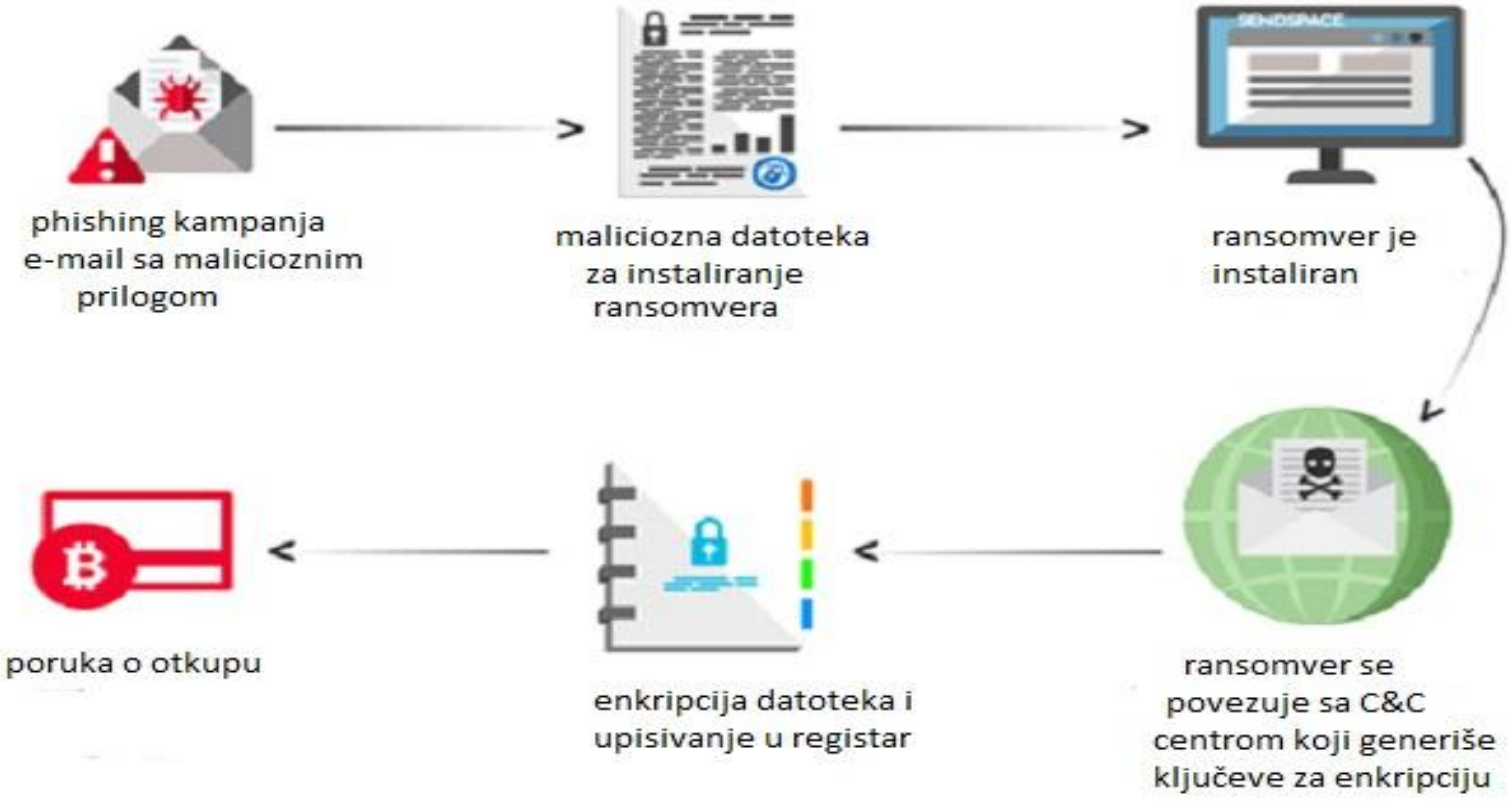
Istorijat



CryptoLocker

- Prvi ransomver koji enkriptuje datoteke.
- Propagacija phishing kampanjama.
- Koristi RSA algoritam.
- Enkriptuje MS Office formate, AutoCad i formate slika.

CryptoLocker

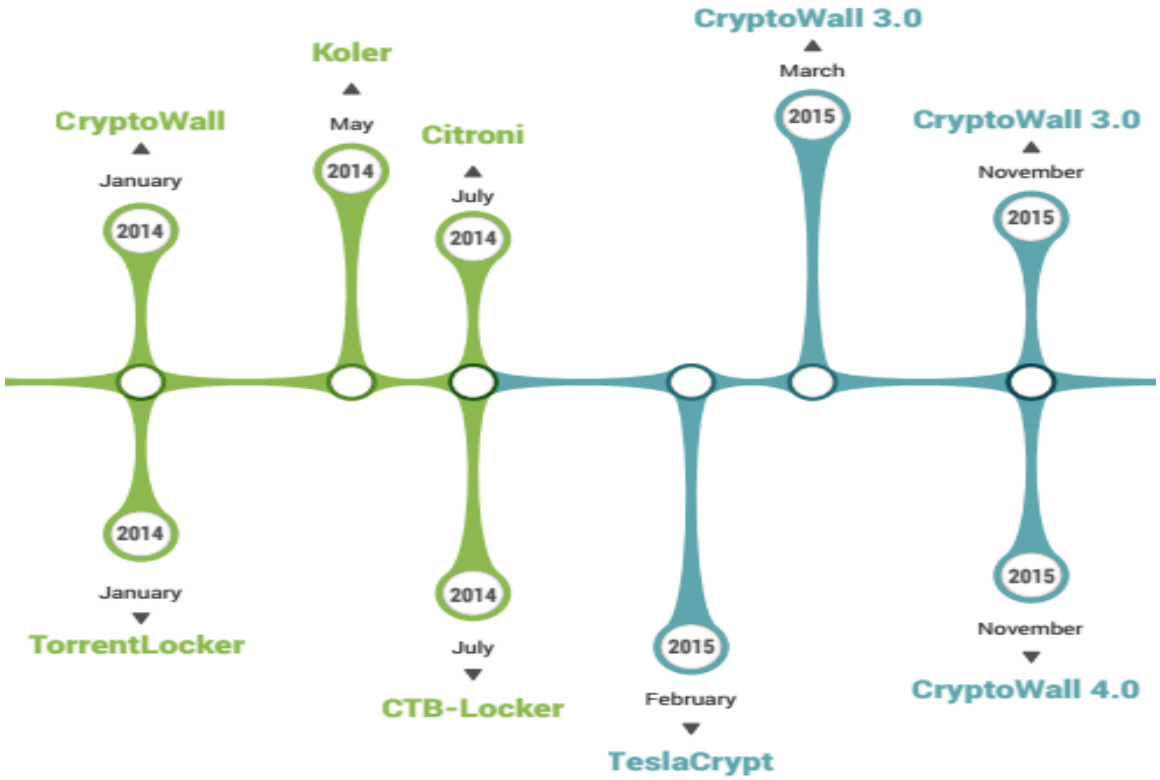


Zahteva isplatu u vrednosti od 400$ u *Bitcoin-ima* ili preko pre-paid vaučera.

CryptoLocker

- CryptoLocker je kreirala i kontrolisala grupa pod nazivom Gameover ZeuS.
- Sredinom 2014. godine ova grupa je uhvaćena u okviru akcije Tovar.
- Stručnjaci su, na osnovu baze podataka ključeva za dekripciju, kreirali *online* portal za dekripciju.
- Širenjem *CryptoLocker* ransomvera naplaćeno je oko 3 000 000 $ otkupa.

Dalji razvoj



Nakon izolacije *CryptoLocker-a* pojavilo se više ransomvera koji koriste tehniku enkripcije od kojih je najpoznatiji *CryptoWall*

Crypto Wall

- Propagacija pomoću *exploit kit-a* ili putem *phishing* kampanja.
- Poruka o otkupu prilagođena geolokaciji napadnutog sistema.
- *Crypto Wall* 2.0 za enkripciju koristi algoritam sa javnim ključem dok se kod verzije 3.0 koristi AES algoritam.

Crypto Wall

- U verziji 4.0 ovog ransomvera uvedene su mnoge komande čija je namena zavaravanje anti-virus programa kako bi se nesmetano izvršila instalacija *Crypto Wall-a*.

- *Crypto Wall* i njegove varijante detektovani su širom sveta, najviše na području SAD-a i Kanade.

- Samo pomoću *Crypto Wall* 3.0 verzije iznuđeno je preko 325 000 000 $ širom sveta.

Preporuke

- Kreiranje rezervne kopije datoteka i čuvanje na eksternim medijumima.
- Redovno ažuriranje sistema,
- Posećivati samo proverene veb sajtove,
- Pažljivo rukovanje prilozima kod e-mail poruka,
- Primena anti-virusa i *firewall-a* proverenih vendora,
- Primena programa za blokiranje *pop-up* programa,
- Onemogućiti *System Restore* opciju,
- Ukoliko dođe do napada obavestiti nadležne.

Predlog zaštite

- Sistem koji, osim malvera, ima mogućnost detekcije i blokiranja i potencijalno opasnog sadržaja kao što je aktivni sadržaj ugrađen u *word* ili *excel* datotekama.

- Jedan od potencijalnih pristupa je korišćenje sistema za filtriranje sadržaja datoteka.

- Alternativno, korišćenje sistema čiji se rad zasniva na dubinskoj analizi saobraćaja i uklanjanju potencijalno opasnih sadržaja.

Sistemi za filtriranje

- Filtriranje datoteka na osnovu ekstenzija, pretrage teksta (zahtevane reči, zabranjene reči) i zabranjenog sadržaja.
- Kontrola i filtriranje datoteka koje se unose u sistem, bez obzira na način unošenja (e-mail, USB, CD...).
- Primena na veliki broj tipova datoteka.
- Uočavanje i blokiranje skrivenog sadržaja.

Selektor IT

- Filtriranje na osnovu ekstenzije,
- Odbacivanje datoteka sa lažnim ili zabranjenim ekstenzijama,
- Blokiranje aktivnog sadržaja,
- Podržava rad sa preko 60 tipova datoteka,
- Podrška za veliki broj anti-virus programa i korišćenje njihovih mehanizama pri filtriranju.

Sistemi dubinske analize

- Dekompozicija podataka i njihova detaljna analiza,
- Uklanjanje opasnih i potencijalno opasnih sadržaja,
- Uklanjanje osetljivih sadržaja,
- Mogućnost obaveštavanja administratora o detekciji nedozvoljenog sadržaja.

Web Guard

- *Transhipment* tehnika za dubinsku analizu saobraćaja,
- Provera zaglavlja i uklanjanje osetljivih sadržaja (pr.*cookies*),
- Podržava rad sa HTTPS protokolom,
- Obaveštenje za administratora o detekciji nedozvoljenog ili potencijalno opasnog sadržaja.

Druga rešenja

- *Mail Guard* – zaštita e-mail saobraćaja,
- *File Transfer Guard* – bezbedan prenos datoteka,
- *TransGap Import Export* – aplikacija za bezbedno korišćenje potrošnih medijuma,
- *TransGap Shared File Store* – aplikacija za bezbedno korišćenje *file store-a*.

HVALA NA PAŽNJI!

Mr Zoran Živković dipl.inž
z.zivkovic@towersnet.rs

TOWERS NET
IT & Telecommunications Innovations