REPUBLIKA SRBIJA
RATEL
REGULATORNA AGENCIJA ZA ELEKTRONSKE KOMUNIKACIJE I POŠTANSKE USLUGE

SRB-CERT

KAKO POSTUPITI UKOLIKO SE REALIZUJE RANSOMVER NAPAD

Priprema

- Potrebno je dobro poznavanje bezbednosnih politika operativnih sistema
- Potrebno je dobro poznavanje uobičajenih politika korisničkih profila
- Uverite se da su *endpoint* bezbednosni uređaji ažurirani (imejl *gateway-i*, proxy keševi)
- Budući da krajnji korisnici najčešće otkriju ovu pretnju, podignite svest o IT podršci u vezi sa ovom pretnjom
- Budite sigurni da imate odgovarajuće i pouzdane kopije podataka lokalnih i mrežnih korisnika

Identifikacija

Opšti znakovi prisustva ransomvera

Nekoliko potencijalnih pretpostavki može nagovestiti da bi sistem mogao da bude ugrožen ransomverom:

- Primaju se neobični profesionalni imejlovi koji sadrže priloge
- Poruka o otkupnini je prikazana na monitoru korisnika i objašnjava da su dokumenti šifrovani i traži se novac za otkup
- Korisnici se žale na to da su njihovi fajlovi na računaru nedostupni ili oštećeni ili da su njihovi fajlovi koji se dele putem mreže sa neobičnim ekstenzijama (.abc, .xyz, .aaa, itd...)
- Mnogo fajlova se menja u veoma kratkom roku na mreži.

Identifikacija kod korisnika

- Pogledajte da li se u profilima korisnika nalaze neuobičajene izvršne binarne datoteke (%ALLUSERSPROFILE% ili %APPDATA%) i %SystemDrive%
- Potražite gore navedene ekstenzije ili poruke o otkupnini
- Pokušajte da vidite zauzetu memoriju kompjutera, ukoliko je to moguće
- Proverite da li ima neuobičajenih procesa
- Potražite u imejl porukama da li ima neuobičajenih imejl priloga
- Proverite da li ima neuobičajenih aktivnosti na mreži ili u internet pretraživačima; posebno obratite pažnju na konekcije ka *Tor* ili *I2P IP*, *Tor gateways* (*tor2web*, itd) ili ka *Bitcoin* veb stranicama za plaćanje

Identifikacija na mreži

- Pogledajte da li ima konekcija ka *Exploit Kits*-ovima
- Pogledajte da li ima konekcija ka ransomveru *C&C* serverima
- Proverite da li ima neuobičajenih aktivnosti na mreži ili u internet pretraživačima; posebno obratite pažnju na konekcije ka *Tor* ili *I2P IP*, *Tor gateways* (*tor2web*, itd) ili ka *Bitcoin* veb stranicama za plaćanje
- Potražite u imejl porukama da li ima neuobičajenih imejl priloga

Sprečavanje daljeg širenja

- Odmah izolujte sve računare koji su ugroženi i isključite ih sa mreže. Zaražene sisteme treba ukloniti sa mreže što je pre moguće kako bi se sprečilo dalje širenje ransomvera i napadne mreža ili deljeni diskovi.
- Izolujte ili isključite pogođene uređaje koji još nisu u potpunosti oštećeni. Ovo vam može pružiti više vremena za čišćenje i obnavljanje podataka, zadržavanje štete i sprečavanje da se uslovi pogoršaju.
- Ako ne možete da izolujete računar, isključite/otkažite (disconnect/cancel) konekcije ka deljenim diskovima (NET USE k:\\unc\path\ /DELETE).
- Odmah obezbedite rezervne kopije podataka ili sistema tako što ćete ih isključiti sa mreže. Potrebno je proveriti da rezervne kopije ne sadrže zlonamerni softver.
- Blokirajte saobraćaj koji je identifikovan kao ransomver *C&C*
- Izbrišite vrednosti i fajlove iz registra, kako biste zaustavili da se program učitava.
- Ako su dostupni, pokušajte da prikupite i obezbedite delove ransomver fajlova koji mogu postojati. Uzorke pošaljite krajnjem provajderu.
- Pošaljite nekategorisani zlonamerni URL, imena domena i IP adrese krajnjem provajderu
- Ako je moguće, promenite sve lozinke za online naloge i mrežne lozinke, nakon isključivanja sistema sa mreže. Pored toga, promenite sve sistemske lozinke nakon uklanjanja zlonamernog softver iz sistema.

Sanacija

- Uklonite binarne datoteke i povezane unose u registre (ako ih ima) iz kompromitovanih profila (% ALLUSERSPROFILE% ili % APPDATA%) i % SistemDrive%
- Ako prethodni korak nije moguć, uradite *reimage* računara prvobitnom instalacijom koja ne sadrži zlonamerne fajlove.

Oporavak

Cilj : Vraćanje sistema u normalno funkcionisanje

- Ažurirajte potpise antivirusne zaštite za identifikovane zlonamerne binarne datoteke koje treba blokirati
- Obezbedite da se mrežni saobraćaj vrati u normalan režim rada
- Vratiti dokumenta korisnika iz rezervnih kopija

Savet je da se prethodne stavke urade korak po korak i uz tehnički nadzor.

Izveštaj

Izveštaj o incidentu treba da bude napisan i dostupan svim zainteresovanim stranama.

Trebalo bi opisati sledeće:

- Kada je incident otkriven
- Akcije koje su preduzete, kao i vremenski rokovi
- Šta je urađeno kako treba
- Kako je došlo do incidenta
- Finansijski gubitak koji je incident pouzrokovao

Zaključak

Na bazi ovog iskustva trebalo bi izvući pouke, tako što će se definisati akcije za poboljšanje procesa detekcije zlonamernih softvera i mreža.

Izvor:

https://github.com/certsocietegenerale/IRM/blob/master/EN/IRM-17-Ransomware.pdf