REPUBLIKA SRBIJA
RATEL
REGULATORNA AGENCIJA ZA ELEKTRONSKE KOMUNIKACIJE I POŠTANSKE USLUGE

SRB-CERT

PREPORUKE ZA PREVENTIVNU ZAŠTITU OD RANSOMVERA

Ransomver je vrsta zlonamernog softvera ili malvera, koji je osmišljen tako da uskraćuje pristup IKT sistemu ili podacima dok otkupnina ne bude plaćena. Ransomver se obično širi putem fišing poruka elektronske pošte ili nenamerno posećujući zaražene internet stranice.

Ransomver može imati velike posledice kako za individualne korisnike, tako i za kompanije. Svaki korisnik koji čuva važne podatke na računaru ili mreži je u riziku, uključujući javni i privatni sektor, kao i druge subjekte koji predstavljaju kritičnu infrastrukturu. Oporavak može biti težak proces, koji u određenim slučajevima zahteva i korišćenje usluga stručnih lica da bi se otključale inficirane datoteke, a neke žrtve najčešće plaćaju otkupninu, u nadi da će dobiti odgovarajuće ključeve za otključavanje inficiranih datoteka.

Međutim , ne postoji garancija da će se plaćanjem otkupnine dobiti navedeni ključevi.

Nacionalni CERT preporučuje sledeće mere predostrožnosti kako bi zaštitili korisnike od pretnji ransomverom:

- Potrebno je da korisnici redovno ažuriraju operativni sistem, kao i softver i antivirusna rešenja, najnovijim verzijama na uređajima. Aplikacije i operativni sistemi sa zastarelim verzijama su meta većine napada. Redovno krpljenje ranjivog softvera je neophodno da bi se sprečila zloupotreba otkrivene ranjivosti. Razmislite o korišćenju centralizovanog sistema upravljanja zakrpama (eng. centralized patch management system).
- Kreiranje rezervnih kopija na dnevnom nivou ili češće, ukoliko za to postoji potreba. Detaljnije o tome kako kreirati rezervnu kopiju podataka, možete pogledati na stranici Publikacije brošuru pod nazivom Kreiranje rezervnih kopija - Backup. Vraćanje podataka iz sigurne rezervne kopije je najbrži način da se povrati pristup podacima.
- Korisnici ne treba da kliknu na linkove ili otvaraju priloge koji stižu sa nepoznatih i sumnjivih mejl adresa.
- Ne ostavljajte lične podatke kada odgovarate na imejl poštu, neželjeni telefonski poziv ili tekstualnu poruku. Fišing napadači će pokušati da prevare zaposlene i instaliraju zlonamerni softver, ali se mogu i lažno predstaviti tvrdeći da su iz IT-a. Obavezno se obratite svom IT odeljenju ukoliko primite sumnjive poruke ili pozive upućene vama ili kolegama.
- Koristite antivirusni softver i *firewall* poznatih i odobrenih kompanija. Održavanje *firewall*-a i ažuriranje antivirusnog softvera su kritični. Podesite antivirusne i anti-malver programe da redovno skeniranje rade automatski.
- Pridržavajte se sigurne prakse prilikom korišćenja Interneta. *Exploit kits* koji se nalaze na kompromitovanim veb sajtovima se obično koriste za širenje zlonamernog softvera.
- Ako putujete, prethodno obavestite IT odeljenje, posebno ako ćete koristiti javne pristupne tačke za bežični internet (Wi-Fi). Obavezno koristite pouzdanu virtuelnu privatnu mrežu (VPN) kada pristupate javnoj Wi-Fi mreži.

Pored navedenog, Nacionalni CERT takođe preporučuje da kompanije primenjuju sledeće najbolje prakse:

- Sprovesti program podizanja svesti i obuke. Budući da su krajnji korisnici meta napadača zaposleni i pojedinci treba da se upoznaju sa pretnjama od ransomvera, kao i sa načinom na koji se isporučuje i širi kroz mrežu.
- Privilegovane naloge koristite na principu "least privilege" (najmanje privilegije): korisnicima ne bi trebalo dodeljivati administratorski nalog osim ako za to ne postoji izuzetna potreba. Oni korisnici koji poseduju administratorske naloge treba da ih koriste samo onda kada je to potrebno. Prilikom instalacije i pokretanja aplikacija, korisnicima treba uvesti restriktivne mere, odnosno primeniti pomenuti princip "least privilege " za sve sisteme i servise. Ovakav pristup može pomoći kod prevencije pokretanja malvera ili svesti na minimum širenje istog putem mreže.
- Koristite odobrene i proverene aplikacije sa tzv. whitelisting -a, koje omogućavaju sistemima da izvršavaju poznate programe, dozvoljene bezbednosnim politikama.
- Potrebno je koristiti spam filtere, jer na taj način onemogućavate da fišing mejlovi stignu do krajnjih korisnika, kao i potvrdu dolazne imejl pošte koristeći tehnologije poput *Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC)* i *DomainKeys Identified Mail (DKIM)* kako biste sprečili podmetanje pošte (*email spoofing*).
- Radite skeniranje dolazne i odlazne imejl pošte kako biste otkrili potencijalne pretnje i fajlove koji sadrže maliciozni sadržaj i na taj način sprečili da dođe do krajnjih korisnika. Koristite skeniranje i filtriranje sadržaja na serverima imejl pošte. Dolazne imejlove treba skenirati na postojeće pretnje i blokirati sve vrste priloga koji mogu predstavljati pretnju.
- Konfigurišite *firewall* tako da blokira pristup poznatim malicioznim IP adresama.
- Konfigurišite kontrole pristupa - uključujući dozvole za deljenje fajlova, direktorijuma i mreže – koristeći princip "*least privilege*". Ako korisnik treba samo da čita određene fajlove, ne bi trebalo da ima pristup upisa u tim fajlovima, direktorijumima ili deljenim serverima.
- Onemogućite makro skripte iz datoteka koje se prenose putem elektronske pošte. Razmislite o upotrebi *Office Viewer* softvera za otvaranje *Microsoft Office* datoteka koje se prenose putem elektronske pošte umesto potpune aplikacije.
- Primenite *Software Restriction Policies (SRP)* ili druge kontrole da biste sprečili izvršavanje programa sa uobičajenih lokacija koje zahteva ransomver, kao što su privremeni folderi (*temporary folders*) koji podržavaju popularni internet pretraživači ili programe koji služe za kompresiju/dekompresiju, uključujući folder *AppData/LocalAppData*.
- Razmislite o isključivanju *Remote Desktop protocol*-a (*RDP*), ako se ne koristi.
- Izvršne operativne programe ili specifične programe izdvojte u virtuelno okruženje.
- Izvršite podelu baziranu na osnovu organizacione strukture i primenite fizičko i logičko razdvajanje mreže i pristup podacima za različite organizacione jedinice.
- Redovno pravite rezervne kopije podataka. Proverite integritet tih rezervnih kopija i testirajte proces vraćanja podataka, da biste bili sigurni da sve funckioniše na odgovarajući način.
- Sprovesti godišnji test integriteta sistema (*penetration test*) i procenu ranjivosti sistema (*vulnerability assessment*).
- Obezbedite rezervne kopije. Uverite se da rezervne kopije nisu konstatno povezane sa računarima i mrežom za koje se prave rezervne kopije. Primeri za bezbedno čuvanje rezervnih kopija su: oblak (*cloud*) ili fizičko čuvanje rezervnih kopija van mreže (*offline*). Neki

slučajevi ransomvera mogu zaključati rezervne kopije koje se čuvaju u oblaku, kada sistemi neprestano prave rezervne kopije u realnom vremenu, poznato kao konstantna/uporna sinhronizacija (*persistent synchronization*). Rezervne kopije su ključne za oporavak sistema od ransomvera i kao odgovor na pretnju. Ako je sistem kompromitovan, rezervna kopija može biti najbolji način da se povrate kritični podaci.

Ukoliko se ransomver napad uspešno izvede, Nacionalni CERT preporučuje da:

- Ne plaćate otkupninu, jer time ohrabrujete i finansirate zlonamerne napadače. Čak i ako je otkupnina plaćena, nema garancije da ćete povratiti pristup svojim podacima, jer često ključevi koje dobijete za uzvrat, delimično ili uopšte neće otključati inficirane datoteke, odnosno fajlove.
- Prijavite incident nadležnim organima kako bi vam pomogli u rešavanju incidenta, jer postoji mogućnost da je isti tip incidenta prijavljen od strane drugih lica, pa je moguće da postoji dekripcioni ključ kojim možete otključati vaše podatke. Kako možete prijaviti incident, pogledajte na stranici Publikacije brošuru pod nazivom Uputstvo za prijavu incidenta.

Izvor:

CISA: https://www.us-cert.gov/Ransomware
FBI: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view