Domoljubni radio

Portal domoljubnog radija

Što poduzeti ukoliko je vaše računalo zaraženo zlućudnim računalnim programom?

Mario Strinavić · Monday, January 13th, 2020

Na internet poveznicama može se pronaći informacija o tome kako spriječiti ransomware napad

Policija je zaprimila više prijava građana i trgovačkih društava u kojima navode kako su njihovi privatni i poslovni podaci na računalima kriptirani te im više nisu u mogućnosti pristupiti, a na njihove adrese elektroničke pošte dostavljena je ucjenjivačka poruka kojom nepoznate osobe traže uplatu iznosa u virtualnim valutama u zamjenu za pomoć u otključavanju podataka.

Ukoliko je vaše računalo zaraženo zlućudnim računalnim programom koji je kriptirao vaše datoteke i onemogućio pristup vašim podacima, pomoć možete potražiti na internetskoj poveznici https://www.nomoreransom.org/cro/index.html na kojoj se nalazi alat pod nazivom KRIPTO ŠERIF, koji omogućuje da na jednostavan način učitate kriptirane datoteke. To će nam omogućiti provjeru postoji li dostupno rješenje za dekripciju te, ukoliko postoji, dobit ćete upute o načinu na koji možete pristupiti vašim podacima.

Kako spriječiti ransomware napad?

- **Sigurnosna-kopija!** Postavite sustav za vraćanje podataka tako da zaraza ransomwareom ne može trajno uništiti vaše podatke. Najbolje je napraviti dvije sigurnosne kopije: jednu koja je spremljena na cloud aplikaciji (budite sigurni da koristite cloud aplikaciju koja automatski radi sigurnosne kopije) i jednu fizičku kopiju (prijenosni tvrdi disk, usb stick, dodatan laptop, itd.). Isključite ih iz računala nakon završetka rada na njima. Vaše sigurnosne kopije će također biti korisne u slučaju da slučajno izbrišete važnu datoteku ili naiđete na poteškoću sa tvrdim diskom.

- **Koristite kvalitetan antivirusni softver** kako biste zaštitili vaš sistem od ransomware zloćudnog računalnog programa. Nemojte isključiti "funkcije za heuristiku", jer one pomažu rješenju da pronađe primjerke ransomware zloćudnog računalnog programa koji još nisu formalno otkriveni.
- **Redovito ažurirajte softver na vašem računalu.** Kad vaš operativni sustav (OS) ili aplikacije zatraže ažuriranje, odobrite ga. Ako softver nudi mogućnost automatskog ažuriranja, prihvatite ju.
- **Ne vjerujte nikome. Doslovno.** Bilo koji korisnički račun može biti ugrožen, a zloćudne poveznice mogu stići s korisničkih računa prijatelja na društvenim mrežama, kolega, ili partnera na online video igrama. Nikad ne otvarajte priloge u e-mailovima koje ste dobili od ljudi koje ne poznajete. Cyber kriminalci često dijele lažne e-mail poruke koje su vrlo slične e-mail obavijestima internetskih trgovina, banaka, policije, suda, ili porezne službe, te na taj način mame primatelje da kliknu na zloćudnu poveznicu i tako dopuste zloćudnom softveru pristup u njihov sustav.
- **Omogućite "prikaži ekstenziju datoteka" ili "show file extensions" opciju u Windows postavkama vašeg računala.** To će značajno olakšati pronalazak zloćudnih datoteka. Klonite se datoteka sa nastavcima '.exe', '.vbs' i '.scr'. Prevaranti često koriste nekoliko nastavaka kako bi zloćudnu datoteku predstavili kao video, fotografiju, ili dokument (kao što je hot-chics.avi.exe ili doc.scr).
- Ako otkrijete nepoznati ili nekontrolirani proces na vašem uređaju, **odmah prekinite internetsku ili drugu mrežnu vezu (kao što je kućni Wi-Fi)** – to će spriječiti daljnje širenje zaraze.

This entry was posted on Monday, January 13th, 2020 at 9:04 pm and is filed under Nekategorizirano You can follow any responses to this entry through the Comments (RSS) feed. Responses are currently closed, but you can trackback from your own site.