Lietuvos Respublikos ryšių reguliavimo tarnybos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) praneša, kad antrą ketvirtį iš eilės daugėja interneto svetainių, kuriose apsilankiusio asmens įrenginio (pvz., kompiuterio) resursai, pačiam asmeniui nežinant, pradedami naudoti kriptovaliutai generuoti.

Kaip tai veikia. Kriptovaliutos gavimas remiasi specialios programos (skripto) veikimu naršyklėje. Skriptas yra nedidelė programa, dažnai parašyta „JavaScript“ programavimo kalba. Asmeniui užėjus į interneto svetainę (pvz., www.svetainės-pavadinimas.lt), kurios programiniame kode yra nuoroda į kriptovaliutos generavimui skirtą skriptą, esantį toje pačioje interneto svetainėje (pvz., www.pavyzdys.lt/skriptas.js) arba kitoje (pvz., www.kriptogeneravimas.com/skriptas.js), interneto naršyklė pradeda skaičiavimus pagal komandas, aprašytas faile skriptas.js. Jei skaičiavimus atlieka didelis kiekis įrenginių (interneto svetainės lankytojų), į tarpininko nustatytą virtualią piniginę „įkrenta“ tam tikras kriptovaliutos (pvz., „Monero“) kiekis. Tarpininkas – svetainės www.kriptogeneravimas.comvaldytojas – pasilieka tarpininkavimo mokestį (pvz., 30 proc.), o likusi dalis atitenka tam, kas į svetainę www.pavyzdys.lt įdėjo minėtą skriptą.

Pagal apytikslius skaičiavimus, norint uždirbti 5 Eur, reikia, kad interneto svetainę aplankytų daugiau kaip 50 000 lankytojų ir kiekvienas jų išbūtų svetainėje bent 100 sekundžių. Tuo metu, kai tokios interneto svetainės lankytojo naršyklėje veikia skriptas, jo naudojamo įrenginio procesoriaus (*angl*. Central Processing Unit CPU) apkrova smarkiai išauga. Dėl to gali padidėti elektros energijos naudojimas, sumažėti naudojamo įrenginio greitaveika, jei įrenginys yra nešiojamas kompiuteris ar išmanusis telefonas – sumažėti akumuliatoriaus turima energija ir pan. Atkreipiame dėmesį, kad anaiptol ne visuomet procesoriaus apkrova reiškia, kad svetainė minėtu būdu išnaudoja lankytojo įrenginį: svetainėje tiesiog gali būti daug animacijos ar pan.

Atvejai, kai interneto svetainėje gali atsirasti kriptovaliutą generuojantis skriptas:

- Svetainė buvo nesaugi (pvz., su pasenusia turinio valdymo sistema), kibernetiniai nusikaltėliai užvaldė ją ir įterpė minėtą skriptą. Tokių atvejų daugėja.
- Skriptą svetainėje įterpia svetainės kūrėjas (programuotojas) ar administratorius ir tą padaro be svetainės savininko žinios.
- Skriptas svetainėje atsiranda su svetainės savininko žinia.

Šiuo metu Lietuvos kibernetinėje erdvėje fiksuojama apie 60 aktyvių tokių svetainių ir jų skaičius auga. Pirmi du atvejai, aprašyti aukščiau, priskiriami prie kenkimo veikos, jie buvo panaudoti 65 proc. visų tokių svetainių.

Atvejus, kai interneto svetainės savininkas sąmoningai įdeda kriptovaliutai generuoti skirtą skriptą ir neinformuoja svetainės lankytojų apie tai, RRT vertina kaip neetišką veiką – procesas vyksta be lankytojo žinios ir išnaudojami jo kompiuteriniai resursai.

RRT, vykdydama nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio CERT (*angl*. Computer Emergency Responce Team) veiklą, toliau reaguos į tokius atvejus ir sieks, kad apie minėtą veiklą būtų informuojami lankytojai ir jiems būtų leidžiama pasirinkti, ar naudoti savo įrenginio resursus skaičiavimams, ar ne.

CERT-LT rekomenduoja

Interneto naudotojams rekomenduojame apsvarstyti įvairių programinių priemonių naudojimą, siekiant apsisaugoti nuo aptartų veikų:

1) Reklamų blokavimas (*angl*. ad blocker). Atkreipiame dėmesį, kad nemaža dalis populiarių svetainių (pvz., naujienų portalai) gali nerodyti turinio, jei nustato, kad lankytojas blokuoja jų reklamjuostes (*angl*. banners).

2) Specialūs naršyklės („Google Chrome“, „Mozilla Firefox“ ir kt.) įskiepiai (*angl*. extensions, add-ons), kurie blokuotų skriptus, generuojančius kriptovaliutą.

3) Antivirusinė programa, „anti-malware“ tipo programa.