Eestis levib krüpteeriva pahavara epideemia

11 aastat tagasi - 05.11.2015 Autor: AM

Üks vastikumaid pahavarasid on selline, mis küll ei kustuta sinu tähtsaid faile, kuid jätab võimaluse peale krüpteerimist need "lahti osta". Maksad raha, aga ka siis ei tea, kas oma failid kätte saad. Ühesõnaga - väljapressimine.

F-Secure tugikeskus Soomes hoitab leviva krüptovara eest, mis kannab nime „Freespeechmail“. Pahavara nakatab kasutaja arvuti ning krüpteerib esmalt kõik selle arvutiga seotud võrgukettad ning seejärel arvutis endas olevad failid. Pärast krüpeerimise lõetamist edastatakse kasutaja ekraanile teade, kus palutakse kasutajal krüptovara tootjatega kontakteeruda. Seejärel teatatakse kasutajale summa, mille tasumisel lubatakse failide taastamiseks saata vastavad vahendid ning juhised. Failide taastamine/dekrüpteerimine mistahes muul meetodil ei ole võimalik.

„Krüptovara kasutab arvutisse sisenemisel ära arvutikasutaja hooletust. Kasutajale saadetakse e-post, milles sisaldub link viitab pahavarale või milles sisalduv manus on juba nakatatud“. Sõnas F-Secure tugikeskuse juht Raido Orumets.“ Antud juhul on tegemist tõeliselt vastiku pahavaraga, millest lahti ei ole võimalik saada – tegelikuses polegi ju tegemist viirusega või nakatunud failidega, vaid failid on krüpteeritud. Ilma võtit teadmata pole võimalik faile taastada. Failide taastamine on võimalik vaid varundamise või lunaraha maksmise teel.“ lisas ta.

Tööjaamapõhine viirusetõrje on vaid üks paljudest kihtidest, mis püüab kasutajat kaitsta, kuid ei tee seda lõpuni. Seetõttu on alati omal kohal soovitused omada varundust, hoida oma arvuti programmid uuendatuna ning kasutada Internetti „vastutustundlikult“. Lisaks soovitab Orumets vaadata üle oma viirusetõrjetarkvara seaded. Kindlasti tasuks sisse lülitada täiendavad kaitsemoodulid, mis tihtipeale ressursi kokkuhoiu mõttes võivad olla vaikimisi väljas.

Üks levinumaid sotsiaalse manipulatsiooni viise, kuidas küberkurjategijad oma ohvreid leiavad, on petukirja abil sundida kasutajat klikkima lingile, mis siis juba omakorda laeb arvutisse pahavara või suunab kasutaja nakkust levitavale veebilehele.

10 erinevat omadust, mis viitavad petukirjale:

1. Saatja emaili aadress tundub küll tuttav, kuid tegelikult ettevõttet ei eksisteeri.

2. Saatja emaili aadress ja nimi ei kattu omavahel

3. Kiri on saadetud üldaadressile või aadressile, mida ei kasutata, kuid tekst viitab nagu teataks täpselt kellele kiri suunatud on.

4. Kirja pealkirjas kutsutakse kiirele tegutsemisele.

5. Nimed ja pöördumised on ebakorrektsed.

6. Kirja sisus esineb tõlke- või kirjavigu.

7. E-kirjas olev link viitab mujale kui lingi pealkiri seda ütleb.

8. E-kirja manus on parooliga kaitstud – seda kasutavad kurjategijad tihtipeale meilisüsteemi kaitsetest läbi murdmiseks.

9. Kirjas kutsutakse kiirele tegutsemisele

10. Kiri sisaldab manust

Mida pahalaste vastu teha?

Kui midagi tundub liiga hea, et olla tõsi, siis see ongi nii ehk pole tõsi. Ära usu kiiret rikastumist lubavatesse skeemidesse ja ära usu reklaame, mis kinnitavad, et sinu arvutis on juba pahavara või mis lubavad kiiremat internetti või rohkem mälu.

Kontrolli iga e-kirja, pakkumise vms õigsust, kasutades muid vahendeid - telefoni või otsekontakti.

Ja muidugi enne mõtle ja siis kliki!

- Uudised
- Turvalisus