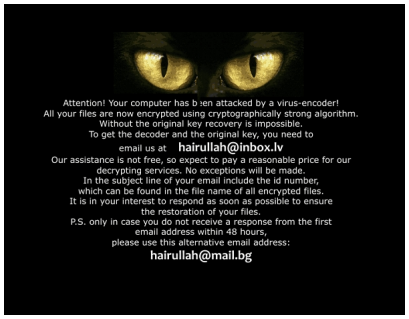
Vis daugiau kreipiasi į mus klientai, praradę duomenis po viruso, kuris šifruoja visus kompiuteryje esančius duomenis ir prašo atlygio už duomenų dešifravimą bitcoinais. Sumokėjus jokios garantijos, kad duomenis bus dešifruoti nėra.

Vos per kelias darbo minutes (kartais užtrunka ilgiau 1-2 val.) Ransomware tipo virusas sugeba užšifruoti visus kompiuteryje pasiekiamus duomenis, ir beveiks visais atvejais duomenys prarandami negrįžtamai. Retais atvejais pavyksta atstatyti didesnį ar mažesnį duomenų kiekį, todėl budrumas ir aiškus žinojimas, ką veikti tokioje situacijoje, padeda išvengti labai nemalonių pasekmių.

Virus-encoder priskiriamas ransomware kenkėjiškų programų grupei https://en.wikipedia.org/wiki/Ransomware_(malware)
.

## Požymiai

1. Pradeda keistis failų pavadinimai: prie failo vardo prisideda .id-XXXXXXXXXX_kazkas@kazkas.xx.
2. Viruso užšifruotus failus operacinė sistema identifikuoja kaip neatpažintus failus. To pasekmėje keičiasi ir failų išvaizda (piktogramos) Windows languose.
3. Grėsmingas (pvz. akys juodame fone) pranešimas darbalaukyje su užrašų Attention! Your computer was attacked by virus-encoder...




4. Sulėtėja darbas kompiuteriu.

## Ką daryti?

Jei turite svarbių duomenų ir pastebėjote požymius, patariame iš karto išjungti kompiuterį, pageidautina "negražiai išjungti", tiesiog iš rozetės ištraukti maitinimo kabelį arba ilgiau palaikyti išjungimo mygtuką įspaustą, ir kreiptis į specialistus, kurie nuskaitys duomenis iki jų šifravimo. Jei neturite svarbių duomenų, suinstaliuokite patikimą antivirusinę sistemą ir nuskenuokite kompiuterį.

## Kaip apsisaugoti?

1. Naudokite patikimą antivirusinę sistemą.
2. Reguliariai tikrinkite ar atsinaujina antivirusinės programos versija ir antivirusinės bazės.
3. Neatidarynėkite el. laiškuose, Skype žinutėse priedus (angl. file attachment), kol neįsitikinsite, kad laiškas atėjo nuo patikimo siuntėjo.
4. El. laiškas, Skype žinutė gali atkeliauti nuo Jums žinomo asmens, tačiau tai gali būti virusinės programos suklastotas laiškas, žinutė. Todėl visada atkreipkite dėmesį į laiško turinį. Jei turinys Jums pasirodys įtartinas ar neįprastas, geriausiai pasitikslint siuntėjo, ar tai jo siųstas laiškas, žinutė.
5. Dažniausiai Interneto naršyklės (Internet Explorer, Chrome, Firefox, Opera...) perspėja dėl galimo pavojaus. Būkite dėmesingi naršyklės klausimams ir neignoruokite jų.
6. Reguliariai darykite rezervines svarbių duomenų, buhalterinių, verslo valdymo ir kt. sistemų duomenų bazių kopijas ir saugokite jas išorinėse laikmenose neprijungtose prie kompiuterių, serverių. Taip pat galite saugoti kopijas debesijos (Cloud) talpyklose.
7. Sistemų administratoriams ir IT žinovams pateikiame JAV Nacionalinio saugumo agentūros rekomendacijas programinės įrangos saugumui užtikrinti. Kai kurie nustatymai labai efektyviai veikia kaip prevencinė priemonė prieš ransomware tipo virusus. Rekomendacijos