Uus väljapressimise pahavara krüpteerib veebi ja nõuab omanikult raha

10 aastat tagasi - 10.11.2015 Autor: AM

Alles loetud päevad tagasi kirjutasime krüpteerivast pahavarast Freespeechmail, mis hakkas kiiresti kasutaja kõvaketast ja võrgukettaid krüptima, nõudes andmete tagastamise eest lunaraha.

Nüüd on levimas üks uuem väljapressimise vorm - krüpteeritakse veebiserver ja selleks, et oma kodulehte uuesti näha või e-pood tagasi jalgele saada, tuleb jälle bitcoin väljapressijatele poetada.

Pahavara kannab nime Linux.Encoder.1 ja nagu nimigi ütleb, levib see Linuxiga masinates. See platvorm on levinud ka veebiserverites. Küberturvalisuse ettevõte Doctor Web on registreerinud juba kümneid lukustatud veebiservereid, igaühe eest küsitakse lunaraha 1 bitcoin. Praeguse kursiga on see ligi 470 eurot.

Viirus krüpteerib esimese hooga failid, mis asuvad kataloogides

```
/home
/root
/var/lib/mysql
/var/www
/etc/nginx
/etc/apache2
/var/log
```

Õnneks on väljapressimis-pahavaras tehtud üks viga: võti, millega krüpteeritakse, on äraarvatav. Bitdefender on välja lasknud dekrüpteerimistööriista, mis serveri pahalasest vabastab ning failid nende esialgses olekus taastab. Tööriist uurib krüpteeritud faili, proovib võtmeid ja siis asub taastama. Vaja on tööriist juurkataloogis käivitada.

Laadi skript alla siit: Bitdefender Labs

(loe lähemalt)

- Uudised
- Turvalisus