IBM hoiatab: küber-oht kolme Eesti panga kohal

15. september 2016 - 23:05 Autor: AM

IBM postitas turvahoiatuse, mis puudutab ka kolme Eestis tegutsevat panka: IBM X-Force Research´i andmetel on Dridex´i pahavara lisaks tuntud suurtele riikidele sihitud spetsiaalselt ka mõnedele kindlatele sihtmärkidele. Viimase kahe kuu jooksul on suunatult rünnatud Leedu, Läti, Eesti, Liibanoni ja Ukraina sihtmärke.

Dridexi ründetarkvara konfifailide andmete põhjal on sihtmärkideks 20 Läti, 3 Eesti ja 3 Leedu panka.

> **Mis on Dridex?**
>
> Dridexon panganduse sihikule võtnud pahavara (sest neil on ju raha), mis jätab Microsoft Office´i dokumentidesse makrod (käivitatavad skriptid), mis nakatavad dokumente avava arvuti ja sellega seotud seadmed. Kui arvuti on nakatunud, näppab Dridex panga-andmeid ja isiklikku infot ning püüab ligi saada kasutaja rahalistele andmetele.
>
> Dridex saabub tavaliselt spämmikirjadega e-posti teel, lisandis troojalasena Microsoft Wordi dokument. Kui kasutaja avab dokumendi, käivitub klassikaline, juba paar aastakümmet kasutusel olnud trikk - Wordi dokumenti peidetud makro nakatab arvuti. Makro laeb masinasse Dridexi panganduse pahavara, mis esmalt üritab leida ja salvestada pankadesse sisselogi mise infot ja hiljem, kui vajalik hulk andmeid kogutud, proovib teha kahtlasi rahaülekandeid kasutaja kontolt.

Miks üritatakse rünnata just Baltimaid? Põhjus on ebaselge, kuid rünnaku objektide järgi (1% Eestist) pole siinseid kasutajaid (ikkagi ID-kaardi või mobiil-ID-ga sisselogimine?) õnnestunud väga palju ära kasutada. Läti on näiteks 20% "turuosaga".

Kuidas kahtlane kiri välja näeb, saab vaadata siit. Viirus üritab ka näidata, nagu oleks kasutajal mõni arve maksmata ja pakub võimalust see ära maksta. Kui makroga arvefail avada, laaditaksegi alla troojalane, mis hakkab nuhkima järgneva pangasessiooni järele. Kergeusklikumad kasutajad võivad ka ise raha kuhugi valesse kohta üle kandma hakata.

Wordi makrodega levisid viirused massiliselt viimati kümme aastat tagasi, kuni 2007. aastal välja tulnud Microsofti uues Office´is oli see vaikimisi ära keelatud. Nüüd kasutavad makrod ära seda, et Word küsib, kas lubada makrosid, et dokumenti näha. Uudishimulik kasutaja peab need ise käsitsi sisse lülitama (ja väga paljud teevadki seda).

- Uudised
- Turvalisus