Linux.encoder.1 - magični ransomware za Linux

Tvrdnja kako je Linux (ili bilo koji Unixoid) zbog svoje arhitekture imun na zloćudne programe ne stoji, a argument kako je mali broj poznatih zaraza dokaz toj tvrdnji je promašen. No, činjenica jest kako je u odnosu na druge popularne operacijske sustave Linux značajno manja, rekli bismo i teža meta - ako ni zbog čega drugog, onda zato što su korisnici Linuxa uglavnom tehnički dobro potkovane osobe kojima nije lako podmetnuti trikove u stilu "klikni ovdje za besplatan pornlć".

Sigurnosne tvrtke povremeno izvještavaju korisnike o pronađenim (ili prijavljenim) "komadima" zloćudnog softvera, pa tko prati scenu zna da ona nije beživotna. A ponekad se pojave i priopćenja poput ovog (https://news.drweb.com/show/?i=9686&lng=en&c=5 [1]) - o ransomware zlu koje napada Linux poslužitelje i od webmastera zahtjeva otkupninu od jednog bitcoina.

Istraživači zapravo ne znaju na koji način *malware* zarazi poslužitelj: kalkuliraju sa propustom u Magentu, ali u tom slučaju malware ne bi smio dobiti administratorske privilegije, već one tipične za web poslužitelj (www-data).

S tim pravima malware ne može učiniti sve za što ga se okrivljuje (enkriptirati korisničke datoteke u /home direktoriju, primjerice), pa istraživači na posredan način sugeriraju kako *malware* "magično" dobije administratorske ovlasti (hmm, možda neki sistemaši ipak padaju na trik sa besplatnom pornjavom?).

Objava je pomalo konfuzna, a ne pomaže niti pretpostavka autora da je ovim *ransomware* uratkom zaraženo na... desetke korisnika.

Članak na žalost ne opisuje problematiku dovoljno detaljno pa je teško iz njega izvući konkretne podatke, ali možemo pretpostaviti da je riječ o *ransomware* napadu koji iskorištava propust u Magento CMS-u (ili propust administratora [2] koji zaboravi vratiti dozvole nakon instalacije ekstenzija), ili o nesposobnom administratoru koji je pokrenuo nepoznat program sa administratorskim privilegijama.

Što god bilo, najjednostavnije rješenje je - vratiti podatke iz backupa. *Malware* se čini glup, pa odmah po infekciji zaključa sve što se zaključati da i tako ekspresno obavjesti okolinu o svom postojanju. Srećom po žrtvu, jer to znači da su backup datoteke vjerojatno čiste.

Podatak o iznimno velikom broju žrtava (desetine) govori nam da taj *malware* nije naročito raširen, no nemojte na osnovu toga zaključiti kako je to dokaz da je Linux imun na digitalne gadarije; očito je mala vjerojatnoća da će ova digitalna beštija ikad doći do vaših poslužitelja, ali dobro je tu informaciju imati na umu.

čet, 2015-11-12 09:22 - Radoslav Dejanović**Vijesti:** Sigurnost [3]
Kategorije: Informacijska sigurnost [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1579

Links
[1] https://news.drweb.com/show/?i=9686&lng=en&c=5
[2] http://devdocs.magento.com/guides/m1x/install/installer-privileges_after.html
[3] https://sysportal.carnet.hr/taxonomy/term/13
[4] https://sysportal.carnet.hr/taxonomy/term/32