Kompromitiran Linux Mint repozitorij

Prošlog je vikenda maliciozan napadač kompromitirao web stranicu Linux Mint distribucije, preusmjerivši korisnike na ISO datoteke koje sadrže *backdoor* koji bi, ako korisnik instalira distribuciju pomoću zaražene ISO slike, napadaču omogućio kontrolu nad računalom.

Napad se dogodio kroz WordPress, postavljanjem modificirane PHP skripte koja preusmjerava korisnike koji su željeli doći do ISO datoteke na poslužitelj pod kontrolom napadača, na kojem se nalazila zaražena ISO slika. Kako tvrde održavatelji Mint distribucije, zaražena je samo ISO slika 64-bitne verzije Minta 17.3 Cinnamon, iako se na poslužitelju nalazila i 32-bitna verzija koju su maliciozni napadači, pretpostavljaju, namjeravali "doraditi" naknadno.

Backdoor instaliran u zaraženu ISO sliku relativno je jednostavan botnet klijent koji pristupa jednom od četiri hardkodirana IRC poslužitelja, gdje osluškuje zapovjedi C&C centra i izvršava ih. Maliciozni C kod (identificiran kao Linux/Tsunami-A, odnosno Kaiten) pronađen je u direktoriju /var/lib/man.cy, koji se prilikom prvog pokretanja kompajlira u "apt-cache" i izvršava.

Napadači nisu uspjeli promjeniti originalne datoteke niti su bili u mogućnosti promjeniti *checksume*.

Kako je napad otkriven relativno brzo, u opasnosti su samo korisnici koji su ISO datoteku preuzeli ovog vikenda, 20. i 21. veljače. Ako spadate u takve i ako ste sebi ili nekom drugom instalirali Mint 17.3 Cinnamon distribuciju, najbolje rješenje je reinstalacija sustava pomoću ISO datoteke novijeg (ili starijeg) datuma od datuma u kojem se dogodio napad.

Tijekom ovog napada ukradena je i baza podataka Mint foruma, sa svim adresama, korisničkim imenima, (hashiranim te posoljenim) lozinkama i privatnim porukama. Korisnici koji imaju račun na Mint forumu trebali bi odmah promjeniti lozinku.

Kako navodi ZDNet (http://www.zdnet.com/article/hacker-hundreds-were-tricked-into-installing-linux-mint-backdoor/ [1]), identitet napadača je poznat, a napadač tvrdi kako je ovim napadom stvorio botnet od nekoliko stotina zaraženih Linux Mint instalacija. Također, tvrdi i da je dio ukradenih lozinki već razbijen.

Ovaj događaj popratili su relativno uobičajeni intra-geekovski rantovi [2] o tome koja je distribucija tehnički bolja/sigurnija/geekastija, ali i pomalo neuobičajene teorije zavjere [3] na Mint blogu.

Linux je, čini se, zaista postao mainstream.

sri, 2016-02-24 13:16 - Radoslav Dejanović**Vijesti:** Sigurnosni propusti [4]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1617

Links
[1] http://www.zdnet.com/article/hacker-hundreds-were-tricked-into-installing-linux-mint-backdoor/
[2] https://lwn.net/Articles/676664/

[3] http://blog.linuxmint.com/?p=3001
[4] https://sysportal.carnet.hr/taxonomy/term/14