(Ne)sigurnost 3G/4G USB stickova

Korisnici koji žele neprestano biti "on-line" koriste pametne telefone, tablete ili modeme na USB sticku koje su dobili od svog telekoma, a koji im omogućavaju bežično spajanje na Mrežu sve dok su na teritoriju koji pokriva njihov operater.

Barem neki od korisnika vjerojatno su se zapitali koliko su sigurni dok koriste bežični pristup Intenetu? Sada će imati o čemu razmišljati. Dvojica ruskih istraživača, Nikita Tarakanov i Oleg Kupreev, na ovogodišnjoj konferenciji Black Hat Europe održali su prezentaciju o rezultatima testiranja 3G/4G stickova koje korisnicima dijele ruski telekomi. Uglavnom se radi o proizvodima kineskih tvrtki Huawei i ZTE, na koje operateri stavljaju svoje logotipe.

Nisu uspjeli obaviti sve testove koje su zamislili, jer u Rusiji nije dozvoljeno uspostaviti vlastitu baznu stanicu, pa najavljuju da će istraživanje nastaviti negdje na zapadu. Zasada su obavili testiranje softvera instaliranog na stickovima i pronašli nekoliko načina njegove zloupotrebe.

Prije svega, moguće je napraviti presliku datotečnog sustava, unijeti izmjene i vratiti ga nazad na stick. Za to Huawey nudi vlastiti softver koji je namijenjen izradi backupa, ali se na Mreži nude i besplatni alati koji istu funkciju obavljaju za stickove različitih proizvođača. Tako modificiran modem nakon toga može inficirati računala na kojima se koristi.

Na sticku je aplikacija koja na računalo instalira softver i drivere za različite OS-ove. Konfiguracija je u običnim tekstualnim datotekama, pa ju je lako izmijeniti. Tu je zapisano koji se DNS serveri koriste, što ovisi o operateru. Ako netko zlonamjeran zamijeni adrese DNS servera, korisnike može usmjeravati server kojeg kontroliraju loši dečki. Sam instaler je potpisana aplikacija pa ga se ne može samo tako mijenjati, no može se iskoristiti mogućnost instalacije antivirusnog softvera, pa se umjesto antivirusa instalira neki posebno pripremljen zlonamjeran program.

Aplikacija koja omogućava rad USB modema periodički traži da li postoje nove verzije softvera na update serverima čije su adrese upisane u konfiguraciji. Zamjenom tih adresa moguća je masovna zaraza računala na kojima se koristi stick.

Istraživači se još nisu pozabavili provjerama drivera, ali očekuju da će i tu pronaći ranjivosti. Poručuju nam da imamo razloga za zabrinutost, jer se danas 3G/4G modemi ugrađuju i izravno u prijenosna računala, a ne samo u pametne telefone i tablete.

Aplikacija za dogradnju softvera krije ranjivost koja omogućava dobijanje većih privilegija na Windowsima. Neposredno prije prezentacije istraživač Stefan Esser poslao je tweet u kojem tvrdi da instalacija komponente za instalaciju novih verzija softvera na Mac OS X-u omogućava pun pristup direktoriju /usr/local, čime se omogućuje ubacivanje inficiranog softvera u OS. Njegova je tvrdnja u zadnji čas ubačena u ranije pripremljenu prezentaciju.

Site h-online [1] izvještava da je iz prvog reda prezentaciju pratio predstavnik Huaweia, koji je tabletom snimao slajdove i marljivo bilježio sve što predavač govori. Nakon prezentacije obećao je da će njegova tvrtka učiniti sve da se otkrivene ranjivosti što prije otklone.

čet, 2013-04-04 14:08 - Aco Dmitrović**Vijesti:** Sigurnosni propusti [2]
Kategorije: Sigurnost [3]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1242

Links
[1] http://www.h-online.com/security/news/item/Huawei-3G-4G-USB-sticks-put-users-security-at-risk-1823894.html
[2] https://sysportal.carnet.hr/taxonomy/term/14
[3] https://sysportal.carnet.hr/taxonomy/term/30