Internetti rünnati: DYN, Twitter, Etsy, Github, Soundcloud, Spotify ja teised olid maas

21. oktoober 2016 - 22:40 Autor: Kaido Einama

Täna algas suur DDos-rünnak, mis paisus kiiresti nii suureks, et võttis maha terve rea tuntud veebikeskkondi. Ka Twitter oli mitmeid tunde kättesaamatu. Kuna rünnati üht nö Interneti selgroogu ehk Dyn´i DNS-servereid, ei saanud kasutajad enam ligi sellistele saitidele ja teenustele nagu Twitter, Spotify, SoundCloud, Vox Media, Airbnb, Etsy,Github, Heroku, Shopify, Whatsapp, Paypal jt.

DNS-süsteem on pärit Interneti algusaegadest, kui puudusid küberrünnakud ja suuremad võrguhäkid selle praegusel kujul. Kogu Internet püsib endiselt suures osas sellel algsel süsteemil, kus on hulk olulisi DNS servereid, mis ütlevad, kust aadressilt vajaliku domeeni leiab. Kui seda infot DNS serverist kätte ei saa, siis arvuti ei oska ka õigele aadressile minna.

Dyn´i DNS servereid hakati täna ründama DDoS rünnakuga - see on hajutatult paljudest kohtadest kindlate serverite masspäringutega üleujutamine, kuni serverid ei suuda enam kõiki päringuid teenindada. Dyn DNS-i olekutabelist on näha kolm suuremat katkestust USA idarannikul ja üks Euroopas.

Kes on selle rünnaku taga? Oletusi on mitmeid. Üks esimesi oletusi ja ka mõned säutsud Twitteris kinnitasid, et see rünnak võis olla justnagu kättemaks Wikileaksi lekitajalt Assange´ilt Interneti äravõtmise eest. Kuid on veel kahte tüüpi konspiratsiooniteoreetikuid. Ühed arvavad, et USA tahab Interneti äravõtmisega laiemalt takistada lekkinud Clintoni presidendikampaania e-kirju levimast. Teised teoreetikud pakuvad, et Interneti mahavõtmise taga on Venemaa.

Millega nad ründavad? Brian Krebs seletab uue ajastu küberrünnakud lahti - selliseid massirünnakuid ei saa enam korraldada vaid lohakate kodukasutajate arvutitega neid hõivates ja etteantud servereid päringutega pommitades. Käes on asjade Interneti ajastu ning pisikesed võrku ühendatud seadmed asuvad üle maailma hulga massilisemalt kui koduarvutid ja on tihti hoopis turvamata, nii et nende automatiseeritud ülevõtmine on lihtne. Seda teeb näiteks Mirai, automatiseeritud nutistu ülevõtja. Üks maailma suurimaid 620 Gbit/s DDoS rünnakuid oli just suures osas korraldatud tänu Mirai "orjastatud" võrgusasuvatele nutikatele asjadele (kuid siiski mitte piisavalt nutikatele, et end kaitsta). Muidugi on oma osa ka vähenutikatel kasutajatel. Saksa tootja AVM näiteks, mis pakub mitmeid nutikaid koduseadmeid, tuli välja uue ruuteritarkvaraga, mis uuendab automaatselt ka kõigi koduste nutipistikute, lülitite ja võrgupesade tarkvara. Kasutajad seda niikuinii teha ei viitsi ja ei oska.

Krebs märgib veel, et iga korraga on suured Internetirünnakud muutunud keerukamaks, targemaks ja võimsamaks. Seni on suudetud üldine Interneti kollaps ära hoida.

Illustratsioon: (CC) Kai Stachowiak / Pixabay

- Uudised
- Turvalisus