

Trebate li RDP pristup tuđim računalima?



Čini se da je istraživačko novinarstvo osvojilo novo zanimljivo i relevanto područje interesa: sigurnost Interneta i prisutnost kriminalnih grupa na globalnoj mreži. Jedan od pionira tog žanra je Brian Krebs, nekadašnji novinar uglednog Washington Posta. Na svome blogu naslovljenom [Krebs on Security](#) [1] nedavno je objavio članak o siteu koji "iznajmljuje" pristup kompromitiranim računalima pomoću Remote Desktop protokola, a neka od tih računala pripadaju uspješnim tvrtkama iz grupe Fortune 500.

Za uslugu se treba pretplatiti, žrtvovati 20 dolara u virtualnoj valuti preko sitea WebMoney, nakon čega kupac dobije pristup listi raspoloživih računala od kojih se neka nalaze u mrežama najuspješnijih tvrtki na svijetu, takozvanih Fortune 500. Tu je i računalo koje pripada Cisco, a koje možete dobiti za 4,55 USD (username Cisco, password Cisco). Nemojte se polakomiti, to je najvjerojatnije takozvani honeypot, računalo ostavljeno na nemilost napadačima, kako bi se proučile metode napada. Cisco je izjavio samo toliko da se radi o "lošem laboratorijskom računalu", bez ulaženja u detalje.

No nisu sva ponuđena računala zamke za napadače. Tvrtka koja prodaje informacije, Dedicatexpress, zapravo samo posreduje, preprodajući "robu" koje su se dočepali zločesti dečki (Krebs kaže hakeri, ali nekako mi je teško tu u osnovi časnu titulu upotrijebiti za odmetnike). Čak su razvili i sustav vrednovanja dobavljača, kako bi potencijalni kupci mogli procijeniti rizik ulaganja. A cijena po kojoj se daje pristup kompromitiranim računalima određuje se prema upotrebljivosti računala, na primjer da li dobijate administratorske ovlasti, može li ga koristiti za on-line kockanje, prijevare na PayPalu itd.

Činjenica da ne prodaju RDP servere na području Rusije Krebsa navodi na zaključak da se ne žele zamjeriti lokalnim vlastima u zemlji iz koje posluju.

Amerikancima je tu zanimljiva činjenica da su dostupna računala Fortune 500 tvrtki. No nama bi bilo zanimljivo otkriti da li su neka od ponuđenih računala u Hrvatskoj. Tko je spreman potrošiti šaku virtualnih dolara, kako bi provjerio koliko je siguran naš djelić Interneta?

Izvor:

[Service Sells Access to Fortune 500 Firms](#) [2]

čet, 2012-11-08 18:20 - Aco Dmitrović **Vijesti:** [Sigurnost](#) [3]

Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/1137>

Links

[1] <https://krebsonsecurity.com>

[2] <https://krebsonsecurity.com/2012/10/service-sells-access-to-fortune-500-firms/>

[3] <https://sysportal.carnet.hr/taxonomy/term/13>