Trojanac Citadel otkriven u neimenovanoj zračnoj luci

Tehnički direktor tvrtke *Trusteer* Amit Klein objavio je na tvrtkinom blogu [1] kako je njegova trtka otkrila da je Trojanac Citadel kompromitirao VPN mrežu poznate zračne luke. Nije otkriveno o kojoj se zračnoj luci radi, niti o kojoj državi. Napad nije išao izravno na VPN, već je trojanac našao najslabiju kariku, a to su korisnička računala, pametni telefoni i tableti, gdje se smjestio kako bi ukrao korisnikov elektronički identitet i poslao ga nalogodavcima.

Time bi napadači dobili pristup u zaštićenu mrežu s ovlastima korisnika čiji su identiteti ukradeni i s pristupom aplikacima s kojima obavljaju svoj posao. Trojanac je izdvojio korisničko ime i password, te napravio slikice ekrana u trenutku kad se korisnik prijavljuje za rad s aplikacijom.

Napad je bio dovoljno ozbiljan da potakne zračnu luku da blokira VPN pristup i pozove upomoć "federalne agencije" (nije li ovime nagoviješteno o kojoj se državi radi?). Citadel je dosada napadao banke, pa se nagađa da ga je ovog puta koristila kriminalna grupa s drugačijim namjerama. Može se samo nagađati da li se radi o pokušaju šverca droge ili nečem drugom.

Trojanac se stalno pojavljuje u novim verzijama, zavaravajući antivirusni softver. U Trusteeru su testirali 40 antivirusnih programa, a samo su četiri otkrila ovu verziju Citadela.

Kako su korisnici pokupili virus? Standardnim metodama koje se danas koriste: otvaranjem inficiranih web stranica, emailom koji nudi download nečeg zanimljivog, ili slijedeći sugestije na društvenim mrežama. Postavlja se pitanje treba li korisnicima na poslu dozvoliti surfanje po sumnjivim siteovima? Dok su u mreži tvrtke, to se još može kontrolirati, ali s obzirom da se sve više za obavljanje posla koriste privatni uređaji zaposlenika, takozvani BYOD (*Bring Your Own Device*), koji se koriste i izvan zaštićene mreže i za privatne potrebe, očigledno je da su potrebne dodatne mjere zaštite. Treba se odreći korištenja statičkih pasworda i pinova, preći na metode višestruke autentikacije, jednokratne zaporke i vremenski ograničene ključeve. Problem je s privatnim korisničkim uređajima to što ih administriraju sami korisici, a na njima često nisu implementirane sve zaštite koje su obavezne na tvrtkinim računalima.

pet, 2012-08-17 12:12 - Aco Dmitrović**Vijesti:** Sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1082

Links
[1] http://www.trusteer.com/blog/citadel-trojan-targets-airport-employees-with-vpn-attack
[2] https://sysportal.carnet.hr/taxonomy/term/13