Microsoft i FBI u borbi protiv Citadel botneta

Microsoft i FBI razbili su prije nekoliko dana komunikaciju Citadel botneta s milijunima zaraženih računala kojom su upravljali kriminalci kako bi se domogli digitalnih identiteta korisnika. Kriminalci su s bankarskih računa ukrali gotovo 500 milijuna dolara.

Citadel botnet s dva milijuna kontroliranih računala zaraženih virusima i drugim malicioznim softverom funkcionirao je zahvaljujući piratskim verzijama Windowsa, koje su korisnici skidali s mreže ne znajući da sadrže trojance. Citadel botnet već je prozvan vodećim svjetskim sigurnosnim problemom, jer ima mogućnost bilježenja korisnikova rada na tipkovnici što predstavlja najjednostavniji način dolaska do podataka potrebnih za pristup korisničkim imenima i zaporkama bankarskih računa.

Koordinirana akcija provedena je u 80 zemalja, a u njoj su sudjelovali policija, tehnološke tvrtke i banke kako bi pomogle da se operacija uspješno završi. Prema podacima FBI-a Citadel je oštetio gotovo pet milijuna korisnika od kojih najviše u SAD-u, Europi, Hong Kongu, Singapuru, Indiji i Australiji.

Iz FBI-a napominju da je glavni haker iza Citadela koji se naziva Aquabox još uvijek na slobodi, te vjerojatno dolazi iz neke od zemalja Istočne Europe. FBI surađuje s Interpolom i policijama brojnih država svijeta kako bi identificirao stotinjak njegovih suradnika.

Uz ostalo, računala zaražena malwareom kriminalci koriste za automatizirano slanje neželjene pošte, širenje virusa, napade na računala i servere i dr. Kako stvar funkcionira? Zaraženo računalo zapravo postaje dio botneta, a da korisnik računala o tome nema nikakva saznanja. Citadel se teško uklanja s računala, jer malware uspješno blokira korisnika računala u nastojanju da posjeti web stranice s antivirusnim programima.

U suradnji s lokalnim CERT-ovima i pružateljima Internet usluga, Microsoft upozorava korisnike zaraženih računala na situaciju, a onima koji sumnjaju da im je računalo zaraženo pomaže savjetima i nudi besplatne alate za uklanjanje malwarea na stranici http://support.microsoft.com/botnets. [1]

pon, 2013-06-24 08:18 - Uredništvo**Vijesti:** Sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1281

Links
[1] ttp://support.microsoft.com/botnets.
[2] https://sysportal.carnet.hr/taxonomy/term/13