Operacija Harkonnen

 Izraelska tvrtka CyberTinel razotkrila je "Operaciju Harkonnen", špijunsku akciju koja je probila informacijsku sigurnost banaka u njemačkom govornom području (Njemačka, Austrija i Švicarska), ali i mnogih tvrtki, istraživačkih instituta i državnih tijela u tim zemljama.

Razmjeri ovog poduhvata pokazuju, s jedne strane, kakvu mogućnost prikupljanja informacija pružaju moderne komunikacijske tehnologije, a s druge strane što su sve zainteresirani s "tamne strane" spremni poduzeti da se dočepaju korisnih informacija.

Organizatori ove operacije potrošili su 150.000 dolara na osnivanje preko 800 fiktivnih tvrtki, zakup servera, izradu web stranica i nabavu SSL certifikata, kako bi se predstavili kao legitimni poslovni partneri i dobili priliku posijati zloćudne programe u banke i tvrtke s kojima su uspostavili odnose. Prijevara je ostala neotkrivena punih dvanaest godina, pa je vjerojatno najdugotrajnija (dosad otkrivena) malware operacija u povijesti.

Za pribavljanje SSL certifikata iskorišteni su dosta labavi propisi na snazi u Velikoj Britaniji, pa su upravo u toj državi otvarane fiktivne tvrtke.

O razmjerima štete može se samo nagađati. Poznajući tajnovitost banaka, koje će radije pretrpjeti štetu nego ugroziti svoju reputaciju objavljivanjem informacija, vrlo je vjerojatno da nikad nećemo saznati čega su se sve kriminalci dočepali. Zapravo se još ne zna (ili nije objavljeno) tko stoji iza ove operacije, pa se samo nagađa da se radi kriminalnom miljeu, a ne o djelatnosti neke vladine obavještajne agencije. Objavljeno je samo da su organizatori operacije iz Njemačke.

Napad je izveden spear phishing taktikom, a korišteni su trojanci izvedeni iz generičke obitelji Trojan.win7.generic!.bt i wmdmps32.exe.

Izraelska tvrtka ovo otkriće spretno koristi za promociju svojih proizvoda, koji su u stanju prepoznati i blokirati ovakve napade. Više detalja o Operaciji Harkonnen možete pronaći u PDF [1]-u koji su objavili na svom webu.

sri, 2014-09-17 06:21 - Aco Dmitrović**Vijesti:** Sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1432

Links
[1] http://cybertinel.com/press-release-harkonnen-operation/
[2] https://sysportal.carnet.hr/taxonomy/term/13