Najveća krađa osobnih podataka u povijesti

Ovaj kolovoz ostat će zapamćen po mnogočemu, pa i po najvećoj krađi korisničkih imena i lozinki koju su izveli ruski hakeri. Riječ je o ukupno 1,2 milijarde korisničkih imena prikupljenih s više od 420.000 web stranica. U strahu od novih napada i zbog povjerljivosti podataka, sigurnosni stručnjaci u nadležnim službama nisu objavili o kojim je točno siteovima riječ, premda među njima ima globalno poznatih stranica. Da kriminalci nisu lokal patrioti pokazuje podatak da su napadali i stranice iz Rusije.

Alex Holden, osnivač kompanije Hold Security medijima je pojasnio kako ovoj skupini kiminalaca meta nisu bile samo američke kompanije, već bilo koja tvrtka sa Fortune liste 500 najvećih svjetskih kompanija.

Nadležne službe za sada raspolažu informacijom kako kriminalci nisu uspjeli prodati ukradene podatke. Skupina hakera navodno je bila smještena u malom gradu u središnjoj Rusiji, blizu granice s Kazahstanom i Mongolijom. Riječ je o desetak osoba starih 20 ili tek nešto više godina, koji se svi znaju osobno, ne samo virtualno, a serveri su im također negdje u Rusiji.

Navodi da su započeli kao spameri amateri prije tri godine. Tada su na crnom tržištu počeli kupovati ukradene lozinke i korisnička imena. Nekoliko mjeseci kasnije odlučili su se bolje organizirati, pa su ušli u partnerstvo s jednom zasad nepoznatom grupacijom s kojom su navodno podijelili znanja u zamjenu za tehniku.

Formirali su mrežu botneta putem kojih su masovno počeli krasti tuđe podatke i do srpnja ove godine su prikupili čak 4,5 milijardi korisničkih podataka. Budući da se mnogo podataka preklapa, u Hold Securityju su izračunali da je riječ o otprilike 1,2 milijarde jedinstvenih korisnika.

Sistem rada bio je sljedeći - hakeri su upadali na internetska i FTP sjedišta pomoću automatiziranih skripti koje iskorištavaju ranjivosti softvera, a koje su slali sa zaraženih računala. Alex Holden je otkrio kako su hakeri primjerice slali spamove s lažnim proizvodima poput tableta za mršavljenje preko koje su onda skupljali vrijedne podatke.

Zaražena računala najvjerojatnije su kupljena na ruskim underground forumima, odnosno na crnom tržištu. Navedena ranjivost im je omogućila da dođu do cijele baze podataka koja je na napadnutoj stranici. U toj bazi su pronalazili privatne podatke kao što su e-mailovi, korisnička imena te lozinke.

Kada su došli do lozinki, u velikom broju slučajeva zapravo su došli i do velikog broja privatnih informacija s obzirom da većina korisnika ima lošu naviku da koriste istu lozinku za sve usluge na Internetu.

Ova krađa pokazala je još jednu banalost - lozinke na popularnim stranicama i društvenim mrežama bile su jednostavne i nije ih bilo teško provaliti. Stručnjaci za sigurnost stoga predlažu bolju zaštitu, a to je korištenje autentikacije s dva faktora kad god je to moguće prilikom prijava za online usluge.

sub, 2014-08-30 07:23 - Uredništvo**Vijesti:** Sigurnost [1]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1426

Links
[1] https://sysportal.carnet.hr/taxonomy/term/13