Kibernapadačima Hrvatska je laka meta

Zbog niske svijesti o opasnostima kiberkriminala Hrvatska je proljetos dva mjeseca bila među pet najčešćih meta kibernapadača u svijetu. Problem je i u tome što su tradicionalni IT sustavi dizajnirani za obranu od onih prijetnji koje više nisu aktualne

piše **EDIS FELIĆ**
edis.felic@liderpress.hr

Hrvatska je u travnju i svibnju bila među pet najčešćih meta kibernapadača. Ta pomalo iznenađujuća informacija objavljena u SC Magazineu, svjetski poznatom časopisu za IT sigurnost, otvara ne samo pitanje zašto baš Hrvatska nego i to koliko su u našoj zemlji poslovna zajednica i državne institucije svjesne ranjivosti svojih sustava.

Ranjivost računala Treba reći da institucije nisu bile meta kibernapadača, u što nas uvjerava **Maja Petrušić**, direktorica prodaje i poslovnog razvoja u tvrtki CS Computer Systems, napominjući da moramo razlikovati napade na točno određenu žrtvu i one koji su dio neke masovne kampanje. Upravo je masovna kampanja uzrok ovih posljednjih napada na Hrvatsku, a Petrušić navodi više razloga.

– Neko su vrijeme bili kompromitirani određeni web-servisi kojima su se koristili i neki hrvatski web-portali. Masovni napadi funkcioniraju prema načelu sličnom ribarskim mrežama. Nastoje pokriti što šire područje i onda gledaju što se uhvatilo. Stoga će se zemlje žrtve često mijenjati ovisno o tome gdje je trenutačno najviše 'bačenih' mreža – kaže i dodaje da na te napade nisu imune ni druge zemlje, pa ni one najrazvijenije. Dodaje da je veoma velik broj tvrtki u zemlji koje još nisu svjesne tog problema iako stručnjaci godinama o tome govore.

Nedavno je **Dean Coza**, potpredsjednik tvrtke FireEye, jedne od vodećih u svijetu u otkrivanju i sprečavanju naprednih kiberprijetnji, upozorio da su one stvarnije nego ikada dosad te da na njih nisu imune državne tvrtke, agencije i realni sektor nigdje u svijetu. Mnogi nisu svjesni napada i krađe podataka, a problem je u tome, smatra, što su tradicionalni IT sustavi dizajnirani za obranu od onih prijetnji koje nisu više aktualne. Zbog toga je prosječno vrijeme otkrivanja napadača 205 dana od napada. U CS Computer Systems, koja je domaći partner tvrtke FireEye, kažu da su najčešće mete napada financijska industrija, javni sektor, ali i mnoge manje tvrtke koje ne ulažu dovoljno u sigurnost.

Napada je sve više, sve su kompleksniji i teže ih je otkriti, dodaje Petrušić. Ističe da su u posljednje vrijeme bili svjedoci napada s kojima se teško nose i najkompleksnija rješenja. Najčešći su alati napadača ransomware i crypto-locker čiji je način rada jednostavan. Naime, žrtvu se najčešće namami da dođe na kompromitiranu web-stranicu koja može biti čak i legalna, ali vlasnik stranice nema pojma da se na njoj nalazi tzv. zloćudni kod.

– Nakon toga, iskoristivši ranjivost na 'žrtvinu' računalu, a najčešće je to aktivni sadržaj kao Adobe Flash ili Java, zloćudni kod se instalira i počinje s aktivnostima. U slučaju crypto-lockera podaci na računalu bivaju enkriptirani, dakle potpuno nečitljivi korisniku. Nakon toga korisniku zaraženog računala dolazi obavijest da treba uplatiti neki iznos, u pravilu u bitcoinima, uz obećanje da će mu se nakon uplate podaci otključati. Vidjeli smo više slučajeva u kojima su ljudi u strahu zaista i uplatili različite iznose. Često bi im podaci i nakon toga ostali zaključani. Tada preostaje jedino vraćanje podataka s pričuvne kopije (backup) jer bi pokušaj razbijanja šifre kojom su enkriptirani podaci bio predug i preskup proces – kaže Petrušić.

Niska svijest o opasnosti Unatoč tomu što potencijalne žrtve do sada nisu, općenito gledajući, pridavale posebnu pozornost takvim opasnostima, upravo je širenje crypto-lockera kao najvidljivijeg oblika napada, navode u CS-u, znatno povećao svijest o tome. Dodaje kako su alati za zaštitu infrastrukture, kao i sama infrastruktura, vrlo kompleksni upravo zbog toga što su najsofisticiraniji do sada i zahtijevaju angažiranje stručnjaka.

foto Ratko Mavar

MAJA PETRUŠIĆ,
CS COMPUTER SYSTEMS:
– Nova generacija sustava za obranu od naprednih prijetnji na hrvatsko je tržište stigla prije dvije godine. Sada je instalirano deset takvih sustava

– Nova generacija sustava za obranu od naprednih prijetnji na hrvatsko je tržište stigla prije dvije godine. Prvi smo uveli ovakav sustav obrane i trenutačno je instalirano ili se testira više od 10 ovakvih sustava – kaže Petrušić. Upravo zbog takvog stanja stručnjaci predviđaju da će u sljedećih pet godina unutar EU tržište kibersigurnosti rasti između sedam i 12 posto godišnje. Napomenimo i to da je možda upravo zbog male svijesti o opasnosti od kiberkriminala Hrvatska bila najnapadanija zemlja jedno vrijeme ove godine. U prilog tome ide i činjenica da su uz Hrvatsku najnapadaniji bili Alžir, Rusija, Tunis i Kazahstan. Jezikom lavova, napadaš upravo najslabije u krdu.