21. maj 2019.

PRIKUPLJANJE DIGITALNIH DOKAZA

Uvod

Napadi u sajber prostoru su svakodnevna pojava, kako u Republici Srbiji, tako i u svetu. U toku jednog dana se dogodi veliki broj pokušaja upada u informacione sisteme, računare ili mobilne uređaje. Zanimljiva je činjenica da su sve češće mete napada i konzole za igru, digitalne kamere, navigacioni sistemi ili Internetom povezane stvari (eng. *IoT*), kao i uređaji za bežični pristup Internetu (eng. *Wi-Fi*). Ciljevi ovih napada mogu biti različiti, od krađe ličnih podataka, zloupotreba naloga na društvenim mrežama, ostvarivanje terorističkih ciljeva, pa sve do špijunaže. Pozadina svih ovih napada najčešće bude sticanje protivpravne koristi za napadača.

Prikupljanje digitalnih dokaza

Kada korisnici informacionih sistema preduzimaju preventivne mere za zaštitu od sajber napada, preporučene od strane Nacionalnog CERT-a, veći deo navedenih tipova napada može biti sprečen. Međutim, određen broj napada se ipak uspešno realizuje i korisnicima bude naneta šteta. Postavlja se pitanje šta korisnici mogu da preduzmu u takvim situacijama, kako bi pričinjena šteta bila svedena na minimum i računar bio ponovo spreman za rad.

Korisnicima koji postanu žrve uspešnog napada hakera, Nacionalni CERT Republike Srbije preporučuje preduzimanje sledećih koraka:

- prekinuti konekciju računara sa Internetom, bilo da je reč o direktnoj konekciji putem kabla, ili Wi-Fi uređaja,
- ukoliko je računar deo određenog informacionog sistema, neophodno je da korisnici iz računara izvuku mrežni kabl, kako ne bi inficirali ostale računare u mreži.

Veoma je važno napomenuti da se ne sme prekidati dovod napajanja računara električnom energijom, niti ponovo pokretati operativni sistem računara (eng. *Restart*). Time se onemogućava kvalitetno prikupljanje digitalnih dokaza, odnosno sprovođenje forenzičke analize od strane Odeljenja za visokotehnološki kriminal pri Ministarstvu unutrašnjih poslova Republike Srbije (vtk@mup.gov.rs), kao i Posebnog tužilaštva za borbu protiv visokotehnološkog kriminala Republike Srbije (http://www.beograd.vtk.jt.rs/).

Za potrebe očuvanja digitalnih dokaza, neophodno je kreiranje identične kopije hard-diska, koja sadrži celokupnu strukturu samog diska, kao i sve podatke, programe, fajlove i foldere koji su bili na računaru u trenutku napada. Postoji nekoliko softverskih rešenja za kreiranje kopije (npr. Symantec Ghost, EaseUS Todo Backup) koje korisnici mogu upotrebiti.

Pored kreiranja kopije hard-diska, korisnici mogu sačuvati i druge podatke, koji mogu biti od velike koristi prilikom sprovođenja istražnih radnji od strane nadležnih organa, kao što su:

- čuvanje logova, koji predstavljaju zabeležen skup podataka o aktivnostima određenog uređaja,
- zaglavlje imejl poruke (eng. *e-mail header*) koji predstavlja skup metapodataka koji mogu sadržati detalje o pošiljaocu maliciozne poruke,
- uznemiravanje putem Interneta (eng. *cyberbullying*) korisnici mogu zabeležiti snimkom određene tekstualne pouke, ili video zapisa koji je postavljen na društvenim mrežama, a predstavlja određeni vid uznemiravanja korisnika putem Interneta.

Po završenom kreiranju rezervne kopije i prikupljanju navedenih podataka, korisnici mogu početi sa oporavljanjem računara, koje uključuje:

- ponovno instaliranje operativnog sistema (npr. *Windows, Linux, macOS*) koje sadrži sve zakrpe (eng. *patch*),
- ponovno instaliranje poslednje dostupne verzije aplikativnih rešenja koja su bila korišćena na inficiranom računaru,
- ponovno instaliranje i pokretanje poslednje dostupne verzije antivirusnog softvera izdate od strane proizvođača.

Ukoliko ima više inficiranih uređaja na mreži, neophodno je za svaki od njih sprovesti sve navedene korake. Nakon oporavka je neophodno ispratiti rad inficiranih računara, kako bismo utvrdili da nema nepravilnosti u njihovom daljem radu.

Zaključak

Svakoga dana se na Internetu pojavi oko 3000 novih malicioznih sadržaja i nije realno očekivati da se korisnici mogu odbraniti od svakog od njih, ali primenom preventivnog pristupa znatno možemo smanjiti verovatnoću uspešnosti hakerskih napada na računare i ostale elektronske uređaje i time omogućiti neometan rad informacionih sistema i prisustvo na Internetu.