Kako se zaštiti od napada na servere?

Svaki će sistemac prije ili kasnije doživjeti da mu provale na neki od njegovih servera. Većina nerado govori o tome, kao da je to sramota. Počiste sve u tišini i šutke idu dalje. Ali nema tu nikakve sramote. Nema tog umreženog računala na koje se ne može provaliti, pitanje je samo da li su napadači spremni uložiti potrebno vrijeme i resurse. Osim ciljanih napada na vrijedne mete, događaju se automatizirani napadi koji naprosto tuku redom po nekom rasponu IP adresa. Ako nemate vrijedne informacije, napadači će već naći način da iskoriste vaša računala za svoje ciljeve.

Autora ovih redaka možete dodati na listu sistemaca kojima su u prvim danima karijere provalili na server. U to doba je Red Hat dolazio s nekoliko "defaultnih" korisničkih računa koji nisu imali *passworde*! Jedan od njih je bio Gonzo! Bio je to valjda nečiji uvrnuti smisao za humor. Kad bi napadač našao lokalni *exploit*, ulogirao bi se *telnetom* kao Gonzo, pokrenuo *exploit* i dobio veće ovlasti! Jednostavno, zar ne? Bila su to druga vremena, početkom devedesetih, sve je bilo u duhu dijeljenja, uzajamnog pomaganja. Kad bih svratio u CARNet pitali bi me da li sam digao anonimni FTP servis! Da ljudi mogu dijeliti datoteke. Odgovarao sam da na serveru nemam dovoljno diskovnog prostora, što je bilo istina. Danas bih, u duhu sadašnjice, odgovorio drugačije: Ne želim da mi server zatrpaju pornografijom. Onda sam jednog jutra našao mail od *roota*, u kojem mi neki *scriptie kid* s visoka priopćava da on sad posjeduje moj server. Kako znam da se radi o klincu? Profesionalac se ne bi razmetao, trudio bi se da što duže ostane neotkriven. To me natjeralo da se više posvetim informacijskoj sigurnosti. Svakog sam jjutra provjeravao logove, instalirao nove pakete i zakrpe, pratio obavijesti o ranjiovstima. Poslije svake instalacije/upgradea brisao sam Gonza i veselo društvo, dok se oni gore nisu opametili i maknuli ih iz distribucija. U to doba nije bilo paketa za SSH servis, pa sam skidao izvorni kod, kompilirao ga i ručno instalirao kako bi uvijek imao zadnju verziju. Jedva sam čekao da maknem *telnet*, tada standardni protokol za udaljeni rad, da *username* i *password* više ne putuju mrežom kao *plaintext*, bez enkripcije. Gonzo s povećanim privilegijama mogao je snifati sav mrežni promet. Dugo sam morao čekati na to, jer moji korisnici nisu imali SSH klijente, dok je *telnet* bio standardan dio svih verzija Windowsa. Bila su to pionirska vremena!

Tada, početkom devedestih, nisam se imao kome obratiti za pomoć,osim kolegama na Srcu, ali sam rado pomagao drugima, koliko je bilo u mojoj moći. Dijeljenje iskustava odličan je način učenja i prenošenja znanja. Nešto naučiš kolegu, nešto naučiš od njega. Zašto bi se svatko od nas sam nosio s problemima i otkrivao toplu vodu?

Otkad sam kao zaposlenik Srca davnih dana pokrenuo CARNetov portal za sistemce, nastojao sam nagovoriti kolege kojima sam (u svojstvu voditelja sigurnosti) pomagao pri rješavanju incidenata da napišu članak o tome. S minimalnim, bolje rečeno nikakvim uspjehom. Nedavno se kolega Mrki ohrabrio i prenio nam kako su mu provalili na *router*. Bravo Mrki! Dragocjeno iskustvo, mnogi će sada brzo zaštiti svoje Mikrotike.

Na Internetu sam pronašao članak [1] u kojem iskusan i ugledan informatičar opisuje kako se pet dana nosio s automatiziranim napadima na svoja dva bloga. Iskreno je pobrojao svoje greške, ispričao kako se na kraju uspio othrvati napadačima.

Michael Fauscette je voditelj istraživačkog odjela tvrtke G2 Crowd, čiji je proizvod platforma na kojoj zajednica raspravlja o poslovnom softveru. Sami korisnici ocjenjuju softver koji su kupili i koji svakodnevno koriste, nema opasnosti od prikrivenog reklamiranja! Dragocjeno, zar ne? Prije tog posla Fauscette je radio preko 10 godina kao analitičar i istraživač tržišta u izdvačkoj kući IDC. Dakle, radi se o čovjeku kojem IT i informacijska sigurnost nisu strane. Ali ipak moramo reći da nije

"čistokrvni" sistemac, vjerojatno je samo priučen.

Fauscette upravlja kao admin s dva bloga koja rade na WordPressu. Radi se virtualnim serverima iznajmljenim u oblaku. U paketu je dobio srednju razinu sigurnosti, osnovni *firewall* i besplatni antivirus. Podesio je sustav tako da mu se pošalje mail svaki put kad se netko pokuša ulogirati kao admin.

Evo ukratko kronike napada izvedenog uz pomoć botneta. Jedne je večeri, nakon što je već legao, dobio obavijest da se netko ulogirao u njegov admin račun. Sjeo je za notebook, pokušao se ulogirati da vidi o čemu se radi, ali nije uspio jer mu je zaporka već bila promijenjena. Nazvao je hosting kompaniju, koja mu je omogućila pristup. Počistio je sustav (instalirali su plugin koji rudari Bitcoine), promijenio *password*. U međuvremenu je dobio istu obavijest s drugog servera i odradio sve kao na prvom.

Pred jutro iste noći sve se ponovilo. Opet se nije mogao ulogirati bez pomoći hosting tvrke, opet je morao brisati kukavičja jaja. Shvatio je da se mora pobrinuti za bolju zaštitu, ali dok je proučavao sustav ponovo su provalili. Valjda su bili ljuti na njega, ovog su puta pobrisali sadržaj oba bloga, pa je sve morao vraćati iz *backupa* koji mu je osigurala hosting tvrtka.

Uključio je TFA, dvostruku autentikaciju i digao razinu antivirusne zaštite, ali ni to nije zaustavilo napadače u novom naletu. Hosting tvrtka je sa svoje strane povećala sigurnost servera, ali su napadači već ostavili višestruke *backdore* koji su im omogućili povratak. Ovog su puta onemogućili dvostruku autentikaciju, pa Fauscette nakon unosa zaporke više nije dobijao PIN za potvrdu identiteta.

Nakon pet dana i pet uspješnih napada oba bloga su u potpunosti prešla na HTTPS protokol, dakle morao je kupiti certifikate, ali i doplatiti za bolji vatrozid. Na kraju ove priče nude nam tri zaključka:

- **Sve što je spojeno na Internet je ranjivo**
- **Ne nadajte se da ćete otkriti tko vas je napao** (tragovi su vodili do Indonezije, Koreje, Azije, nekoliko istočnoeuropskih zemalja...)
- **Zaštite svoj site** (nabavite IDS ili vatrozid nove generacije, koristite *password manager* koji generira složene zaporke i čuva ih kriptirane u bazi kojoj samo vi imate pristup, neprestano istražujte i učite, a za WordPress ili neku drugu platformu koju koristite nabavite, proučite i primijenite najbolje prakse).

Mnogo posla ako želite izbjeći provalu! Kao i uvijek, prevencija je bolja od kurative. Ipak sistemac ne može biti netko tko to radi usput, uz ostale poslove. A informacijska sigurnost je neizbježna sastavnica našeg posla, još jedan dodatak na sve veću listu zaduženja.

Čitajući o Fauscettovom iskustvu, nameće se zaključak da je rješenje u novcu. Kao da je Fauscette štedio, uzeo minimalan paket usluga, blog bez HTTPS protokola i kupljenih certifikata, s elementarnim vatrozidom. Izvukao se doplatom za bolju uslugu. No iz naše perspektive, mnogo se toga može uraditi bez novca, ako se uloži nešto znanja i truda. Kad se iskoriste sve mogućnosti koje nam nudi slobodni softver, može se posegnuti za novčanikom i uložiti nešto u skupa poboljšanja. No ja govorim o serveru kojeg sistemac ima na ustanovi, s Linuxom, za kojeg ima mnogo dobrih zaštitnih alata, dok je Fauscette u drugačijem okruženju: on naprosto koristi uslugu iz oblaka. Njegovo se administriranje svodi na klikanje (ispričavam se ako sam ciničan). Možda sam zastario, ali na Linux serveru je moja generacija koristila brojne mogućnosti zaštite koje ne koštaju ništa. Na primjer dinamičku listu pristupa: kad s iste adrese stiže više od N zahtjeva za otvaranjem konekcije u sekundi, ta se IP adresa blokira narednih pola sata. Itd, its... Ali više o tome nekom drugom prilikom.

pon, 2018-08-13 21:28 - Aco Dmitrović**Kategorije:** Kolumna [2]
Vote: 0

No votes yet

story_tag: sigurnost [3]
botnet [4]
provala [5]

Source URL: https://sysportal.carnet.hr/node/1819

Links
[1] https://nulltx.com/on-a-mining-mission-to-destroy-what-you-need-to-know/?utm_medium=push&utm_source=onesignal&utm_campaign=traffic%20boost&utm_content=extended%20%traffic%boost
[2] https://sysportal.carnet.hr/taxonomy/term/71
[3] https://sysportal.carnet.hr/taxonomy/term/82
[4] https://sysportal.carnet.hr/taxonomy/term/264
[5] https://sysportal.carnet.hr/taxonomy/term/265