Linux na meti napadača

 Godina na zalazu bila je izuzetno zanimljiva sa stanovišta informacijske sigurnosti. Dogodile su se brojne krađe identiteta, otkrivene ranjivosti nultog dana i malware kojeg sponzoriraju vlade. Kraj godine ne donosi olakšanje: saznali smo da je otkrivena provala u računala koja upravljaju nuklearnim elektranama u Južnoj Koreji. No ovom ćemo se prilikom usredotočiti na vijesti koje se tiču sigurnosnosnih problema s Linuxom.

Nedavno su objavljeni i detalji o malwareu koji inficira Linux računala, a koji je, po svemu sudeći, godinama pritajeno djelovao. Znači li to da je završeno "zlatno doba" korištenja Linuxa, u kojem čak nismo ni morali, ni na servere ni na desktop računala, instalirati antivirusni software, osim radi zaštite naših Windows korisnika, jer virusa za Linux praktički nije ni bilo?

Početkom godine Kaspersky i Symantec otkrili su napast nazvanu Turla, koja je zarazila nekoliko stotina Windows računala u preko 40 zemalja. Pretpostavlja se da malware potiče iz Rusije i da su ga razvili vladini hakeri. Turla je koristila dva zero day exploita, ranjivost Windowsa i Adobe Readera, šireći se pomoću posebno oblikovanih PDF dokumenata, ali i preko "zagađenih" web siteova, posebno odabranih prema interesima ciljanih žrtava. Mete se bile vladine institucije i ustanove od interesa za nacionalnu sigurnost. Navodno su Rusi na računalima u EU tražili dokumente koji se odnose na Ukrajinu.

Kaspersky je nakon toga objavio i otkriće malwarea specijaliziranog za Linux. Nova napast omogućuje skrivenu mrežnu komunikaciju, udaljeno izvršavanje naredbi i udaljeno upravljanje inficiranim Linuxima. Zasniva se na otprije poznatom proof-of-concept backdooru 'cd00r.c', razvijenom kako bi se eliminirala slabost tipičnih backdoora, stalno otvoren port kojeg je moguće otkriti skeniranjem. Razvijen je softver koji radi na principu sniffera: osluškuje mrežni promet i kada otkrije posebno oblikovan paket, otvara socket i povezuje se s udaljenim računalom s kojeg je paket poslan. Na taj način se skriveni servis ne može otkriti dok je u stanju mirovanja.

Poveznica ovog malicioznog softvera s Turlom jest činjenica da uzorak Linux malwarea sadrži kodirane iste CnC domene, na koje se inficirana računala prijavljuju i očekuju daljnje naredbe, što sugerira da potiče iz istog izvora, odnosno da služi istom nalogodavcu.

U ožujku je javno objavljeno postojanje još jedne napasti koja ugrožava Windows korisnike, ali i Unix/Linux administratore. "Operacija Windigo" koristila je Linux web servere za distribuciju malwarea na Windows računala, ali se istodobno presretalo passworde koje koriste administratori. Napad je bio složen i koristio je više komponenti, na primjer Cdorked HTTP backdoor koji je radio na Apacheu, Nginxu i lighthttpdu. Inficirani web serveri obavljali su redirekciju posjetitelja na web stranice koje su korištene za drive-by distribuciju malwarea (na pr. Blackhole, click fraud malware Win32/Boaxxe.G i Win32/Glubteta.M, generički proxy za Windowse). Na Linux serverima instaliran je Ebury rootkit, koji je omogućavao backdoor root ljusku, slanje spama i krađu passworda. Calfbot je Perl modul kojeg je Ebury koristio za slanje spama. Navodno je u jednom danu tako slano po 35.000.000 spamova! Broj inficiranih Linux servera varirao je između 7.700 i 11.100. Ukupno ih je bilo inficirano oko 26.000, najviše u SAD-u. Praćenje ove napasti počelo je u svibnju 2013., a procjenjuje se da je bila aktivna oko dvije godine.

U izvještajima se ne spominju izrijekom stolna Linux računala, pa možemo zaključiti da su napadačima korisniji Linux serveri, koji su stalno dostupni na javnim adresama. Sofisticiranost ovih napada ukazuje na to da ih provode profesionalci, ne samo iz kriminalnog miljea, nego i iz vladinih krugova. Na Internetu se odvija obavještajni rat u koji se aktivno uključuje sve više država koje ne žele biti samo žrtve, pa osnivaju obrambene timove, ali im daju i napadačke zadaće. Reklo bi se da

nitko ne želi zaostati u ovoj utrci. Rusija igra najotvorenije, iz javno objavljenih dokumenata vidi se da razvijaju strategiju informacijskog ratovanja radi zaštite nacionalnih interesa. Zapadne države to isto rade u tišini, ne objavljujući informacije za koje smatraju da mi ometale rad obavještajnih službi. Na primjer, u SAD-u, kolijevci demokracije, predsjednik čak može donijeti zakon (Act) koji ne mora biti javno objavljen.

Popularni guru informacijske sigurnosti Bruce Schneier praktički je optužio antivirusne tvrtke da šuruju s vladama i zadržavaju informacije o botnetima kojima upravljaju državni hakeri. Po njemu, u interesu javnosti bilo bi pravovremeno objavljivanje takvih informacija, što bi ubrzalo i olakšalo obranu od njih, veći broj ljudi bi se uključio u analizu malwarea. Doduše, Schneir im priznaje da su možda kasnili s objavom jer se radi o složem i vrlo sofisticiranom softveru, čija analiza traje duže od analize "običnog" malwarea kriminalnog porijekla. Scriptie kidze, čini se, više nitko i ne spominje.

Što sve to znači za Unix/Linux admine, a ujedno i korisnike stolnih Linux računala? Na prvi pogled moglo bi se zaključiti da su oni samo kolateralne žrtve u ratnim igrama velikih, a tu ćete čuti standardnu argumentaciju da "nismo dovoljno zanimljivi?". Da to i nije baš tako jednostavno, pokazuje činjenica da su meta napadača bili i znanstveni instituti. Ako je neki fakultet uključen u istraživačke projekte za privredu ili vladu, također postaje zanimljiv izvor podataka. Uvijek se vraćamo na činjenicu da akademska mreža ima izgrađenu brzu i kvalitetnu mrežnu infrastrukturu koja napadačima može dobro poslužiti za napade na važnije, veće mete.

U sadašnjoj besparici jedva se održava osnovna funkcionalnost, a ulaganje u sigurnost upravama izgleda kao nepotreban trošak. Da bi sistemci iskamčili neku crkavicu za nabavu vatrozida ili sličnih zaštitnih uređaja, trebalo bi najprije dokazati upravi da je ta potreba stvarna. Za to se može iskoristiti neka provala, otkriće rootkita, zapravo bilo kakav sigurnosni incident. No ako vaše servere poharaju profesionalci, velika je vjerojatnost da to nećete ni primijetiti i da će vas na provalu upozoriti CERT.

Ustanove bi trebale ulagati i u edukaciju svojih informatičara, ali ni to ne prolazi u krizi, kad ni znanstvenici više ne obilaze svoje stručne skupove kao nekada. Štedi se i na literaturi. Dok čekamo bola vremena, svatko treba brinuti "za sebe" kako zna i umije. Uostolom, to je i pitanje časti, zar ne? Mada nemamo podršku uprave, ipak nam nije svejedno da li netko provaljuje na naša računala i napravit ćemo sve što je u našoj moći da to spriječimo. Sistemcima ne preostaje drugo nego da se sami educiraju, prate dostupne informacije, razmjenjuju ih s kolegama i nastoje se zajednički obraniti. Srećom, dosta se toga može napraviti bez velikih materijalnih ulaganja, a obilje sigurnosnog softvera izdanog pod GPL licencom omogućuje da se razina zaštite podigne na prilično visoku razinu.

Veliku većinu napadača to će obeshrabriti dovoljno da se okrenu lakšim metama. No svi dobro znamo da se od profesionalca koji se baš namjerio na nas ne možemo obraniti. Uvijek će postojati neki zero-day exploit za kojeg još ne postoji zakrpa.

uto, 2014-12-30 11:21 - Aco Dmitrović**Vijesti:** Sigurnost [1]
Kategorije: Operacijski sustavi [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1486

Links
[1] https://sysportal.carnet.hr/taxonomy/term/13
[2] https://sysportal.carnet.hr/taxonomy/term/26