NSA, kriminalci i sveta vodica

Prosječan korisnik vidi Internet kao veliki zabavni park koji nudi brojne usluge, informacije, zabavu, druženje s nepoznatim ljudima i poznatima koji su otišli na drugi kraj svijeta. No istovremeno Mrežom se služe i ljudi koji se ne uklapaju u tu idiličnu predodžbu i imaju skrivene motive. Ova godina bit će zapamćena po posljedicama gubitka alata za provaljivanje na Windows računala kojeg je koristila američka Nacionalna Sigurnosna Agencija, NSA.

Naši mediji uglavnom su se usredotočili na **WannaCry** *ransomware*, upozoravajući gledateljstvo na opasnost i podižući svijest o problemu. Ali taj je *malware* samo vrh ledenog brijega, pozadinska zbivanja ostala su skrivena od očiju javnosti. Praćenjem manje eksponiranih medija i stranica specijaliziranih za informacijsku sigurnost u stanju smo zaviriti ispod površine i otkriti barem dio zakulisnih igara.

Zapravo se prijelomnica dogodila kolovoza 2016-te, kada su zasad još anonimni pojedinci ili grupe koji se kriju iza pseudonima Anna Senpai i ShadowBrokers svojim objavama podigli razinu prijetnje na novu razinu.

Anna-Senpai, tko god to bio, objavio/la je izvorni kod **Mirai** *malwarea*, softvera koji na Linuxu bazirene mrežne uređaje i IP kamere, kojima kronično nedostaju zakrpe, pretvara u robote koji se koriste za DDOS napade.

Inficirani uređaji neprekidno skeniraju Internet tražeći IP adrese *Internet of things* (IoT) uređaja. Mirai sadrži tablicu adresa koje neće inficirati(!), među kojima su adrese alocirane za US poštu i Ministarstvo obrane. Mirai identificira ranjive IoT uređaje, te koristi tabelu s više od 60 tvornički zadanih korisničkih imena i zaporki kako bi ih inficrirao. Ti će uređaji normalno raditi, samo će se povremeno usporiti i povećati potrošnju mrežnog prometa. Ostaju zaraženi dok se ne restartaju. Nakon restarta, ako korisničko ime/zaporka nisu promijenjeni, a najčešće nisu, uređaj će u kratkom vremenu ponovo biti inficiran. Zanimljivo je da nakon infekcije MIral traži drugi *malware* i uklanja konkurenciju te blokira portove koji omogućuju udaljeno administriranje. Kako stotine tisuća IoT uređaja koristi tvorničke postavke, svi su odreda ranjivi. Njima upravlja CNC server koji im šalje adrese ciljeva koje treba napasti. Treba li reći da su odreda ranjivi uređaji koji se isporučuju kao gotovi proizvodi, crne kutije, nitko ih ne održava, ne administrira, ne ažurira softver. Naši ISP-ovi nam isporučuju male kućne rutere s istim postavkama, kako bi im lakše pristupali kad korisnik zatraži pomoć. Čak i ako ne koriste standardne tvorničke postavke, one izmijenjene su jednake za sve korisnike, pa se nije previše teško dočepati admin ovlasti.

Analizu izvornog koda Miraia pogledajte ovdje [1].

Shadow Brokers izašli su iz sjene također u kolovozu 2016. godine kratkom najavom aukcije naprednih kibernetičkih oružja za koja su tvrdili da u ukradeni Equation grupi. Tako su naime dečki iz Kaspersky laba prozvali ekipu koja je navodno dio TAO jedinice (*Tailored Access Operations*) u sastavu NSA. Procurili su exploiti za Ciscovu mrežnu opremu, na primjer EXTRABACON, koji koristi ranjivost nultog dana i JETPLOW, "trajni usadak" (*persistent implant)*. Objava je dočekana sa skepsom i prošla nezapaženo, pa su nakon toga objavili popis servera koje je "navodno" kompromitirala NSA. Kako ni time nisu uspjeli privući pažnju, nakon nekoliko tjedana objavili su snimke s ekrana koje prikazuju dio datotečne strukture sadržaja koji se nudi na aukciji. Na njihovom

Bitcoin računu ni nakon toga nije zabilježen veći promet. Nastala je tišina, koja je prekinuta u travnju 2017-te, kada je objavljeno pismo [2] upućeno predsjedniku SAD Donaldu Trumpu. U njemu se tvrdi da su ShadowBrokers podržavali Trumpa, ali su sada razočarani jer je Trump zaboravio na bazu svojih birača, kojima je dosta republikanaca i demokrata i koji su od Trumpa očekivali da Ameriku opet učini velikom. Pisan je malo čudnim engleskim, sami zaključite je li to namjermo ili se radi o nepoznavanju jezika. Pismo izgleda više kao medijski projekt s ciljem privlačenja pažnje na grupu, nego stvarna poruka predsjedniku SAD.

Tjedan dana nakon toga, 24. travnja 2017. objavili su nekoliko konkretnih zloćudnih proizvoda. Ističe se FUZZBUNCH [3], Komplet alata za provaljivanje, instaliranje usadaka (implants) i udaljenu kontrolu, Radi se o otprilike četiri godine starom proizvodu (vidi se veriziji Pythona koji je korišten), ali se procjenjuje da je to nepatvoreni alat kojeg je pripremila NSA. Tu su *exploiti* za ranjivosti nultog dana koji se koriste godinama, a nikad nisu javno objavljeni. U paketu je i ETHERNALBLUE napad koji je korišten za *ransomware*.

U toj je situaciji zanimljivo pratiti ponašanje Microsofta. Nakon objave ShadowBrokersa da su na prodaju provalnički alati, pripremili su zakrpe i izdali ih u ožujku, mjesec dana prije objave alata korštenih za *ransomware*. Čini se da je Microsft znao za ranjivosti prije nego su javno objavljene, što silno zabavlja pristalice teorija zavjere. Ali te su zakrpe isprva objavljene samo za podržane verzije Windowsa, dok su korisnici koji još imaju instalirane na primjer Windowse XP dobili zakrpe samo ako plaćaju skupu pretplatu! Ispada da je Microsfot istovremeno napravio zakrpe za sve verzije, podržane i nepodržane, ali ih je plasirao samo za podržane inačice Widnowsa. Tek nakon što su veliki korisnici poput britanske ustanove javnog zdravstva NHO imali probleme, pustili su zakrpe svima.

U izjavi medijima Microsoft izražava nezadovoljstvo činjenicom da vladine obavlještajne agencije gomilaju ranjivosti i alate za provaljivanje, jer time ugrožavaju sigurnost njihovih kupaca. Ni riječi o tome da su i oni sami odgovorni za sigurnosne propuste u svojim proizvodima! Nove verzije Windowsa vukle su staru ranjivost radi kompatibilnosti sa prethodnim verzijama SMB protokola.

Zanimljiv način zaštite računala demonstriran je u Rusiji: Moskovski patrijah Kiril, vođa ruske pravoslavne crkve, posjetio je Ministarstvo unutarnjih poslova i tamo škropio računala svetom vodicom [4]kako bi ih zaštitio od WannaCry crva. Time je u informacijski rat uvedena nova, duhovna i metafizička razina!. Prije nego se nadmoćno nasmijete, sjetite se da i našim vijestima povremeno prikazuju svećenike koji posvećuju razne prostore, kad god se lokalni političari požele dodvoriti svojoj izbornoj bazi.

Uopće ne sumnjamo da spomenute objave ne otkrivaju sve slojeve ove zavrzlame i da je mnoštvo informacija i dalje skriveno od nas. Međutim i ovo je dovoljno da sami sebi postavimo nekoliko bitnih pitanja.

Napravio sam brzu anketu među poznanicima. Pitao sam ih: "**Je li ti draže da ti na tvoje računalo provale kriminalci ili NSA?"** Pri tome NSA predstavlja zbirno ime za razne državne obavještajne agencije, bile on iz SAD, Kine, Rusije, Koreje, Hrvatske... svejedno.

Većina je odgovorla da bi željeli da su njihova računala sigurna i da im nitko ne može samo tako provaliti i ugrožavati privatnost.

Jedan manji dio odgovorio je da im je draža NSA, jer će oni to obaviti neprimjetno, a na njihovim uređajima ionako nema informacija koje bi nekoga mogle zanimati. Ti ljudi nisu svjesni vrijednosti svoje privatnosti i kakve se moćne metode profiliranja koriste danas.

Jedan jedini poznanik odgovorio je da bi mu draže bilo da mu provale kriminalci. "Kriminalci žele samo moj novac, a NSA želi moju dušu!"

Ponovo se vraćamo na pitanje o tome tko je stvarni vlasnik uređaja koje kupujemo? Ispada da smo mi vlasnici samo *hardwarea*, bez obzria da li je to računalo, tablet, pametni telefon, kućni ruter, IP kamera ili neki od brzbrojnih IoT uređaja. Iako pri kupovini plaćamo i softver, taj softver pripada

proizvođaču i on ga koristi onako kako njemu odgovara, ne obazirući se na prava korisnika, koji prečesto i sami olako pristaju na uvjete korištenja, samo da bi dobili svoje omiljene igračke.

Podsjećamo se da je LInux slobodan i da ga nitko ne posjeduje, izvorni kod mu je otvoren, pa prema tome nije već u startu uključen u globalne "igre prijestolja". Ali Linux je i dalje izbor (prosvijetljene) manjine.

U kakvom mi to svijetu živomo? U svijetu u kojem smo slobodni biti neslobodni i nadzirani, gdje nam moćni daju kruha i igara, ali nam uzimaju dušu.

uto, 2017-06-13 17:42 - Aco Dmitrović**Kategorije:** Kolumna [5]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

story_tag: informacijska sigurnost [6]

Source URL: https://sysportal.carnet.hr/node/1745

Links
[1] https://medium.com/@cjbarker/mirai-ddos-source-code-review-57269c4a68f
[2] https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1
[3] https://github.com/fuzzbunch/fuzzbunch
[4] https://heatst.com/tech/russias-secret-weapon-against-ransomware-virus-holy-water/
[5] https://sysportal.carnet.hr/taxonomy/term/71
[6] https://sysportal.carnet.hr/taxonomy/term/101