Tko je vlasnik naših računala?

Danas je ponovo petak trinaesti, već drugi mjesec za redom. Trenutak je pogodan da se još jednom osvrnemo na problematiku informacijske sigurnosti u umreženom društvu. Prošli [1] smo mjesec započeli priču o tome kako je globalno prisluškivanje pripremna faza za buduće ratove, koje će dobiti strana koja je bolje informirana o protivnikovim slabostima. Današnja računalna i komunikacijska tehnologija, uza sve dobrobiti koje nam je donijela, lako se da iskoristiti u vojne i obavještajne svrhe.

Prosječan čovjek, zaposlen, oženjen, zaokupljen plaćanjem računa, školovanjem djece i vraćanjem kredita, nakon dolaska s posla baš i nema snage i volje za ozbiljne teme. Gledanje utakmice uz pivo i TV sapunice uspavat će ga, da se može odmoriti za naredni dan. No ako ga goni intelektualna radoznalost na Internetu se može informirati o stvarima o kojima neće čuti u svakodnevnom okruženju. Tako mi je nedavno kolega skrenuo pažnju na snimku predavanja koje je Jacob Appelbaum održao u Hamburgu. Naslov prezentacije je "To Protect and Infect, The Militarization of the Internet [2]". Snimka je (još) dostupna na Youtubeu.

Appelbauma nazivaju hakerom, etičkim zanesenjakom, zagovornikom slobodnog softvera, nezavisnim istraživačem računalne sigurnosti (dio je tima koji razvija Tor) i Snowdenovim glasnogovornikom, jer je prezentirao njegova otkrića o tome kako NSA pretvara iPhone u uređaje za prisluškivanje i razvija uređaje koji mogu prikupljati informacije s računala koja nisu online. Iako nije završio studij zaposlilo ga je Washingtonsko sveučilište radi njegovih znanja i vještina. Danas živi u Berlinu, kamo se vjerojatno sklonio od maltretiranja u SAD, gdje su ga zadržavali na aerodromima, plijenili mu računala i mobitele.

Nema smisla ovdje prepričavati sadržaj prezentacije. Bit će dovoljno ukratko spomenuti samo neke od brojnih iznesenih informacija, što će vas, sigurni smo, potaknuti da poslušate cijelo izlaganje. Evo: NSA presreće poštanske pošiljke i u računala i komunikacijsku opremu ugrađuje svoje implantate. To može biti softver, spominje se izmijenjeni BIOS računala i tvrdih diskova, ali i hardver, pa se daju

primjeri dodataka koji se ugrađuju u kućišta računala i praktički su nevidljivi laiku koji ne zna što treba tražiti. Na primjer, čipovi koji mogu radio valovima emitirati sadržaj ekrana ili umetati TCP pakete u ethernet promet. Razvijen je softver koji pasivno prikuplja mrežni promet, i drugi koji aktivno napada umrežene uređaje, koji se zatim mogu koristiti prema potrebi. Na primjer, vaš kućni routerčić može, a da vi o tome nemate pojma, obavljati posao za NSA. Ako možete upravljati routerima, promet se može preusmjeravati na uređaje koji će glumiti ciljna računala i koristiti se za "man in the middle" napade.

Kada se iz pasivno prikupljenog prometa profiltriraju podaci, mogu se na primjer izdvojiti ljudi koji posjećuju muslimanske sadržaje, nakon čega će agresivni alati provjeriti da li su njihova računala i mrežna oprema ranjivi, pa ih rutinski, onako usput, inficirati. Ti se napadi nazivaju ciljanim, ali teško da je svatko tko otvori stranicu s muslimanskim sadržajima ekstremist i prijetnja nacionalnoj sigurnosti.

Reklo bi se, iako za to nema dokaza, da neki od proizvođača surađuju s obavještajnom zajednicom. Ako vas zanima, u prezentaciji su pobrojane neke od tih tvrki, na primjer proizvođači tvrdih diskova čiji BIOS sadrži "špijunske dodatke". Jedna od posljedica ovog otkrića može biti svjesno bojkotiranje tih proizvođača, pa NSA može naškoditi američkom izvozu. No ne treba biti naivan, i drugi proizvođači rade za svoje vlade, pa nećete biti sigurni ni ako kupujete kinesku robu.

Appelbaum navodi da se SIM kartice mogu iskoristiti da se mobitelu šalju naredbe i upravlja njime, ne samo za lociranje korisnika, nego i za prisluškivanje razgovora i kada se ne telefonira.

Prikupljene podatke NSA čuva petnaest godina, podvrgava ih analizama i koreliranju podataka. Čini se da bi NSA mogla sve što poželi, da ih, kako kaže Appelbaum, ne ograničavaju samo financije i vrijeme koje ne mogu trošiti baš na sve mete.

Appelbaum postavlja neka zanimljiva pitanja. Koliko je ovakva praksa zakonita? Ako vlast sebi dozvoljava da čini stvari koje svojim građanima brani, zar to nije tiranija? Appelbaum nije za razgovor o tim pitanjima uspio naći sugovornika među američkim političarima. Čini se da se radi o sivoj zoni i političari nemaju potiličko rješenje za ove probleme, pa ne žele o njima ni razgovarati. U međuvremenu, na mreži cvjeta trgovanje informacijama bez prave zakonske regulacije

Nakon gledanja prezentacije čovjek se zapita tko je zapravo pravi vlasnik naših računala, mobitela, mrežne opreme? Tko je stvarni vlasnik naših privatnih i poslovnih informacija, u krajnjoj liniji naših života? Ako se u vašem računalu nalaze implantati, ne samo da je sav sadržaj koji je na računalu praktički ponuđen na pladnju, već je vidljiv i sav mrežni promet, koje stranice posjećujete, s kim se i o čemu dopisujete. Ne možete se sakriti od Velikog brata. Sva sreća da nas Veliki brat voli, zar ne?

Nakon što odslušate Appelbaumovo predavanje, zapitate se da li ste već samom činjenicom da ste ga pogledali postali sumnjivi i našli se na nečijoj crnoj listi? Sa sumjom ćete gledati u svoje računalo i razmišljati zašto se odjednom usporilo? Poželit ćete formatirati tvrdi disk i nanovo instalirati OS i aplikacije, pa podatke vratiti s backupa. No što ako je spyware u firmwareu?

Ne smatram se paranoičnim niti mislim da sam toliko važan da bi bio meta obavještajih službi. Ali uzimam si za pravo razmišljati o ovim stvarima i iznositi o njima svoje mišljenje. Smatram da obični, mali ljudi nisu primarna meta, ali sam uvjeren da su u najmanju ruku kolateralne žrtve i da je o ugrožavanju privatnosti neophodna javna rasprava. Tko nadzire ljude koji nas nadziru? U njihovim je rukama ogromna moć koja se može zloupotrijebiti na bezbrojne načine.

Dok sam pisao članak dogodila mi se zanimljiva nezgoda. Kad je tekst već bio pri kraju i kad sam se spremao snimiti na ga USB stick kako bi ga kasnije dotjerao i lektorirao, editor je iznenada zgasnuo i tekst je nestao s ekrana. Svi ostali programi nastavili su normalno raditi. Nema problema, pokrenut ću ponovo editor i na popisu nedavnih dokumenata naći članak, pa će barem veći dio biti sačuvan. Međutim nakon restarta editora, teksta nema na popisu nedavnih dokumenata, a nema ga ni na disku. Netragom je nestao! Huh! Kad vam se ovako nešto dogodi nakon slušanja Appelbauma, nije vam svejedno!

Nije mi preostalo drugo nego članak napisati iznova. No cijelo sam vrijeme razmišljao hoće li se

neobična nezgoda ponoviti? Ne samo to, nesvjesno sam počeo sam sebe cenzurirati, pa sam mnoge stvari napisao u blažem, razvodnjenijem obliku. Nisam ni prije nezgode bio spreman donositi konačne zaključke i sudove, već prvenstveno ukazati na teme o kojima se mora raspravljati. Kao na primjer o tome da li su ideje o individualnim slobodama i pravu na privatnost zastarjele, ili se za njih još vrijedi boriti? No sad sam osjećao da su mi misli otežale i odlučnost splasnula.

Na kraju, zaključio sam da je ipak za sve kriv petak trinaesti! Mnogo je veća vjerojatnost da se radi o običnom pehu, nego o ciljanoj intervenciji, zar ne? Teško je povjerovati da je u kodu editora skrivena naredba koja kaže: ako se u tekstu više od tri puta spominje NSA, tekst mora nestati! Dakle nazad pred televizor, brzo treba pronaći sportski kanal i pustiti mozak na pašu. Inače bih počeo razmišljati o tome kako je na čelu Rusije obavještajac, koji sad ima još i političku moć i kontrolu nad medijima. Nedavno je u atentatu, posve slučajno, ubijen njegov politički protivnik. A onda bih mogao pomisliti da će uskoro i kod nas obavještajac pobijediti na izborima... Ne, sve je to ružan san. Petak trinaesti. Sutra će opet sve biti u redu.

pet, 2015-03-13 23:34 - Aco Dmitrović**Vijesti:** Sigurnost [3]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr./node/1530

Links
[1] https://sysportal.carnet.hr./node/1516
[2] https://www.youtube.com/watch?v=dy3-QZLTpbQ
[3] https://sysportal.carnet.hr./taxonomy/term/13