Nemaš se kamo sakriti

Tvrtka VPNpro objavila je rezultate istraživanja aplikacija za Android. Isprva su testirali VPN aplikacije, među njima nekoliko iz Kine, a onda su otkrili da pojedine traže od korisnika da im dodijeli prevelike ovlasti, da bi ih nakon toga zlorabili. Otkrili su da je izvor tih aplikacija tvrtka Shenzhen HAWK, iako su kao autori navedeni različite pravne osobe. Radi se o 24 aplikacije sa skrivenim funkcionalnostima koje je instaliralo preko 380 milijuna korisnika.

Primjera radi, aplikacija pod imenom Weather Forecast šalje podatke o korisnicima na servere u Kinu. Osim krađe osobnih informacija, aplikacija pokreće skriveni browser i prikazuje reklame. K tome još aktivira pretplatu na telefonske brojeve s posebnim uslugama čime korisnicima nabijala račune.

Evo popisa inkriminiranih aplikacija, s brojem preuzimanja u zagradi:

- Sound Recorder (100M)
- Super Cleaner (100M)
- Virus Cleaner 2019 (100M)
- File Manager (50M)
- Joy Launcher (10M)
- Turbo Browser (10M)
- Weather Forecast (10M)
- Candy Selfie Camera (10M)
- Hi VPN, Free VPN (10M)
- Candy Gallery (10M)
- Calendar Lite (5M)
- Super Battery (5M)
- Hi Security 2019 (5M)
- Net Master (5M)
- Puzzle Box (1M)
- Private Browser (500,000)
- Hi VPN Pro (500,000)
- World Zoo (100,000)
- Word Crossy! (100,000)
- Soccer Pinball (10,000)
- Dig it (10,000)
- Laser Break (10,000)
- Music Roam (1,000)
- Word Crush (50)

Ako neku od njih nađete na svom telefonu, deinstalirajte je bez oklijevanja. Objava VPNpro dostupna je online [1].

Da bi ovakve aplikacije mogle funkcionirati od korisnika traže da im da dozvolu za obavljaje poziva, fotografiranje, snimanje zvuka i videa. Možda se pitate kolika je doza naivnosti potrebna da se aplikaciji dodijele tolike ovlasti? Nažalost, velik broj korisnika jednostavno da pristanak, ne provjeravajući ništa i ne čitajući što se traži, samo da se što prije riješe gnjavaže i pokrenu aplikaciju. U nekim situacijama malware nije ni trebalo skidati s mreže jer je bio predinstaliran na mobitelima (spominje se Alcatel). Prisjećamo se da je 2017. Indijska vojska tražila od svojih pripadnika da uklone

aplikaciju Virus Cleaner, jer je otkriveno da je to zapravo spyware.

Google je nakon upozorenja uklonio navedene aplikacije iz svog dućana, uz obrazloženje kako oni ozbiljno shvaćaju narušavanje sigurnosti i privatnosti svojih korisnika. (U napasti smo da ovdje stavimo smješkića :) Iz Kine je ubrzo stigao odgovor kojeg je pripremila služba za odnose s javnošću majčinske tvrtke TCL Corporation. Oni razumiju zašto je Google uklonio aplikacije i aktivno rade s tvrkom Shenzhen kako bi bolje razumjeli uzroke Googlove zabrinutosti. Također planiraju angažirati vanjskog sigurnosnog konzultanta koji će nadzirati svaku njihovu aplikaciju kako bi za svoje kupce osigurali “peace of mind and trust”. Kako to lijepo zvuči, zar ne? Njima je stalo do našeg duševnog mira i uspostave međusobnog povjerenja.

U vijestima ovih dana saznajemo da su Kineski hakeri optuženi za krađu osobnih podataka dvjestotinjak milijuna američkih državljana. Prisjećamo se jednog takvog slučaja o kojem smo pisali, kada su 2017. provaljeni serveri tvrtke Equifax iz Atlante, koja prikuplja osobne podatke američkih građana radi provjere kreditne sposobnosti. Hakeri u kineskim vojnim uniformama prikupili su imena, datume rođenja, brojeve socijalnog osiguranja i kreditnih kartica, a usput su se dočepali i povjerljivih poslovnih podataka. Opsežna istraga slijedila je tragove napadača preko 34 servera u dvadesetak država, da bi došli do izvorišta napada. Podignuta je optužnica protiv četiri člana 54-tog Istraživačkog instituta Kineske armije. Državni tužitelj SAD tvrdi da se radi o "uznemirujućem i neprihvatljivom uzorku upada na računala koja sponzorira kineska država i njeni građani". "Podaci imaju ekonomsku vrijednost, ove krađe mogu doprinjeti razvoju alata umjetne inteligencije, kao i pripremanju ciljanih obavještajnih paketa."

Ne možemo se pohvaliti da razumijemo obavještajni žargon, nije nam baš jasno o kakvim se paketima radi. Ali razumijemo da su kao krivci označeni ne samo državne institucije Kine nego i njeni građani! Zar se tu sugerira kolektivna krivnja? Ne raspolažemo cijelim govorom tužitelja pa je bolje da se uzdržimo od tumačenja. Možda se tu sugerira da nisu svi napadači u državnoj službi, ali se njihov rad tolerira? Samo nam je jasno da građani SAD ne mogu odgovarati za rad njihovih obavještajnih agencija, pa valjda analogija vrijedi i za druge države. No na stranu prepucavanja među nacijama, razmjeri zloupotrebe Interneta su zaista užasavajući, bez obzira na to tko je počinitelj, kriminalci, kompanije ili države. Ostaje činjenica da ih tehnologija omogućava i da smo svi ugroženi, bez obzira u kojoj državi živimo.

Iako se načelno slažem sa stavovima koje iznosi Američki državni tužitelj, ne mogu ne primjetiti da se ljudi zgražaju samo kad su u položaju žrtve, a kad njihova strana to isto radi drugima, onda je to patriotizam. Kad ćemo se izvući iz tih podjela, "mi" kao dobri dečki i "oni" kao loši? Živimo u vremenu sebičnosti nacija, gdje ekonomski i vojno jače države nameću svoju volju slabijima. Tu kolektivističku paradigmu prevladali su rijetki pojedinci.

Jedan od ljudi koji misle da su ljudska prava pojedinca iznad prava nacija i država jest Edward Snowden, čija je knjiga Trajni zapis (*Permanent record*) prevedena i u nas. Zanimljiva priča čovjeka koji je programirao za NSA, sve dok mu se nije smučilo. Odlučio je javnosti ispričati što se događa "iza ogledala". Ukratko, NSA ima izravan pristup serverima Googlea, Facebooka, telekoma, automatski i bez ikakvog biranja snima ukupan promet i pomoću programa, koje je razvijao i sam Snowden, može tu sirovu građu pretraživati i organizirati prema zadanim kriterijima. Ako netko postane "osoba od interesa", softver automatski upozorava na njegove telefonske pozive, mailove, pretraživanja itd. Tako se u realnom vremenu može pratiti što takav čovjek radi. Rukovoditelji NSA svjedočili su pred kongresnom komisijom da se to radi samo kad imaju sudski nalog, dok Snowden otkriva da su lagali. U prikupljanje podataka uključene su i države saveznici SAD, tako da je nadzor globaliziran. Osim nadzora telekomunikacija provodi se i fizički nadzor, iznad kuća američkih građana lete dronovi koji snimaju dolazi, odlazi, također bez sudskog naloga.

Snowden je zaglavio u Rusiji, protiv svoje volje. U razgovorima s Putinom, Oliver Stone postavlja pitanje Putinu da li odobrava to što je napravio Snowden? Ne, odgovara Putin, ako se Snowden nije slagao s time što radi NSA trebao je dati otkaz, kao što je Putin učinio dok je bio ruski obavještajac. Ali nije trebao djelovati protiv svoje domovine. I Putin razmišlja kolektivistički.

Glenn Greenwald, nezavisni novinar kojeg je Snowden odabrao da prenese njegovu priču, izdao je knjigu pod naslovom *No Place to Hide, Edward Snowden, the NSA and the Surveilance State,* u kojoj

iznosi svoje viđenje masovnog nadzora. Saznajemo da je 2001. New York Times objavio kako je Bushova administracija u tajnosti naredila NSA da bez sudskog naloga nadzire elektronsku komunikaciju američkih građana. U trenutku objave takva praksa je trajala već četiri godine. Bila je to demonstracija moći, praksa po kojoj je predsjednik iznad zakona kad se radi o sigurnosti nacije i zaštiti od terorizma. Greenwald je po obrazovanju pravnik, bavio se ustavom i građanskim pravima. Bez ustručavanja je javno iznosio svoj stav da je predsjednik takvom odlukom prekršio zakon i da za to treba odgovarati. Zato ga je Snowden odabrao i donio mu brojne dokumente koji pokazuju masovne razmjere nezakonitog nadzora.

Američki kolonisti u osamnaestom su se stoljeću protivili tome da Britanski službenici po volji ulaze u njihove kuće i preturaju po stvarima. I tada je morala postojati opravdana sumnja. Opći nalog koji bi omogućio da se sve građane redom nadzire i pretražuje bio je nezakonit. O tome govori četvrti amandman, koji garantira zaštitu osobe, kuće, dokumenata i stvari od neopravdanih pretraga i zapljena, traži da se u sudskom nalogu izričito i precizno navede prostor koji se smije pretražiti, stvari koje se smiju zaplijeniti, kao i osobe koje se smiju privesti. Prava pojedinca su iznad moći države, osim u slučaju kada se njihovo ograničenje može opravdati. U to se vrijeme radilo o pretresu kuća, ali s razvojem tehnologije mijenja se i način nadzora. S izgradnjom željeznice i poštanske službe vlast si je prisvajala pravo da otvara poštu, a u dvadesetom stoljeću počeli su prisluškivati telefonske razgovore. Uvijek su na udaru bili marginalci i disidenti. Sve do 21. stoljeća, kada tehnologija omogućuje da se snima i sprema sva elektronička komunikacija.

Kamo to može odvesti? Hoće li se ostvariti Orwellova 1984., ali ne u Sovjetskom savezu, nego u razvijenim demokracijama? Nije teško zamisliti da softver pokupi neke ključne riječi i zaključi da netko potencijalni protivnik režima. Ne vjerujemo da je softver u stanju razumjeti kontekst u kojem je nešto izrečeno, da se radi o ironiji, šali, ili je izrečeno u žaru usijane rasprave kakvih ima dosta na Mreži. Kad je takav pojedinac označen kao "osoba od interesa", nedostaje još samo korak pa da postane "sumnjivo lice" i da nadzorni softver počne aktivirati alareme svaki put kad mu zazvoni telefon.

Ako su građani cijelo vrijeme svjesni da ih se nadzire, to vodi do autocenzure i atmosfere straha, a time se ugrožavaju sami temelji demokracije. Lako je to povezati s Kinom u koju demokracija još nije dospjela, gdje autokratski vlada jedna partija, a građanima se dodjeljuju bodovi u skladu s njihovom lojalnošću državi i vlasti. Ali Amerika je kolijevka demokracije, tamo to nije moguće, zar ne? U 70-tim godinama prošlog stoljeća FBI je prisluškivao razgovore pola miliona građana koji bili označeni kao subverzivni. Na popisu su bili na primjer Martin Luther King, John Lennon, feministice. Kolonijalne sile poput Velike Britanije i Francuske nadzirale su pripadnike antikolonijalnih pokreta. Nedavno smo svjedočili Arapskom proljeću, masovnoj pobuni protiv diktature, kada su režimi na vlasti shvatili da brzo moraju uspostaviti kontrolu nad Internetom. Krenuli su u šoping i nakupovali tehnologiju razvijenih zapadnih, demokratskih zemalja. Na primjer, alate za razbijanje enkripcije Skypea, kako bi mogli prisluškivati razgovore aktivista.

Masovni nadzor daje ogromnu moć onima koji ga provode, a s obzirom na nesavršenu ljudsku prirodu teško je zamisliti da oni tu moć neće zloupotrebljavati, da se održe na vlasti ili da ostvare neku drugu korist za sebe.

U prošlom smo nastavku govorili o tome kako se privatnost narušava iz komercijalnih pobuda, a sada smo dodirnuli društvenu stranu problema, ugrožavanje demokracije. U 21. stoljeću pojedinac se ne može zavući u neku rupu i sakriti, cijeli je svijet premrežen tehnologijom koja se može koristiti protiv njega. Što nam preostaje, osim nastojanja da jačamo demokraciju i ograničimo moć ljudi koji upravljaju tehnologijom. U protivnom, naša formalno zajamčena prava u praksi će biti bezvrijedna. Srećom, demokracija nam daje mogućnost da se pobunimo i izborimo za svoja prava. Sad još samo preostaje da to i učinimo, zar ne?

čet, 2020-02-13 12:59 - Aco Dmitrović**Kategorije:** Kolumna [2]
Vote: 0

No votes yet

story_tag: masovni nadzor [3]
Snowden [4]

Source URL: https://sysportal.carnet.hr/node/1863

Links
[1] https://vpnpro.com/blog/chinese-company-secretly-behind-popular-apps-seeking-dangerous-permissions/
[2] https://sysportal.carnet.hr/taxonomy/term/71
[3] https://sysportal.carnet.hr/taxonomy/term/350
[4] https://sysportal.carnet.hr/taxonomy/term/351