Salt Typhoon betörés: nincs biztonsági hátsó kapu csak „jó fiúknak”

PCLinuxOS Magazine – 2024. november

ÍrtaJoe Mullin and Cindy Cohn
Electronic Frontier Foundation

Az EFF régóta mondja, hogy nem lehet hátsó kaput beépíteni, ami a jókat beengedi és a rosszakat nem. A hétvégén láttunk egy újabb példát erre: a The Wall Street Journal beszámolt egy, az amerikai telekommunikációs rendszert érintő nagy betörésről, a kínai kormány által támogatott Salt Typhoon hacker-csoport részéről

A jelentések szerint a behatolásra a Verizon, az AT&T és a Lumen Technologies (néhai Century Link) által, a rendőrség és a hírszerzés számára, a felhasználók adataihoz hozzáférést biztosító rendszereket használtákki a maguk javára. Így Kína példa nélküli módon hozzáfért az amerikai kormány által, ezektől a nagy telekommunikációs cégektől kért adatokhoz. Máig sem tisztázott, kikre vonatkozó, és mennyi kommunikációhoz, illetve internetes forgalomhoz fért hozzá a Salt Typhoon.

Igen, pontosan: a cégek által a hatóságok számára biztosított hozzáférést a kínai-hátterű hekkerek láthatóan feltörték és használták. A lehetőséget a CALEA-hoz hasonló hibás törvénynek megfelelés érdekében teremtették meg, ami kötelezte a távközlési vállalatokat, hogy könnyítsék meg a „törvényes lehallgatásokat” – más szóval a poloskázást, illetve a bűnüldöző szervek és nemzetbiztonsági ügynökségek egyéb kérései végrehajtását. Noha a felhasználói adatbiztonság, illetve a USA kormány nemzetbiztonsági és bűnüldöző szervei szempontjából ez egy borzalmas fejlemény, de nem meglepő.

Az elv, hogy csak a kormányügynökségek tudják majd használni ezeket a csatornákat a felhasználói adatok elérésére, mindig kockázatos és hibás volt. Láttunk már ilyet: visszatérőn 2004-ben és 2005-ben is, akkor több mint 100 magas rangú görög kormánytisztviselőt figyeltek meg törvénytelenül 10 hónapon keresztül, amikor ismeretlenek betörtek a görög „törvényes hozzáférés” programba. Most, 2024-ben, amikor növekvő számú, jól felkészült, államilag támogatott hekker-csoport működik, szinte elkerülhetetlenek az ilyen romboló betörések. A hozzáférés lehetősége a különleges bűnüldöző szerveknek, ami a „jó fiúknak” van, nem növeli a biztonságunkat; veszélyes biztonsági rést jelent.

Az internetes lehallgatás mindig rossz ötlet

Az 1994-ben kiadott CALEA-törvény a telekommunikációs eszközök ellátóitól megköveteli, hogy tegyék lehetővé a kormányzati lehallgatást. 2004-ben a kormány jelentősen kibővítette a lehallgatások körét, belevették a internetelérést biztosítókat is. Az EFF ellenezte a kiterjesztést és felvázolta az Internet lehallgatásának veszélyeit.

Az Internet kritikus módon más mint a telefonhálózat, amitől sokkal sebezhetőbb. Az Internet nyílt és folyamatosan változik. „Lehallgatásbarát számítógépes hálózatok készítésére használt sok technológia, a hálózatokat használó személyeket sokkal sérülékenyebbé teszi az adataikat, vagy személyes információikat megszerezni akaró támadókkal szemben.” Írta az EFF közel 20 évvel ezelőtt.

Az átláthatóság és biztonság felé

Nem túl vicces, de lehet, hogy arról, kit figyel meg az amerikai kormány, közöttük az USA-ban élő személyeket, a kínai kormány többet tud, mint az amerikaik maguk. A hátsó kapukat törvényesen használó hírszerző és bűnüldöző szervek következetesen titkolóznak, megnehezítve a felügyeletet.

A kommunikációs eszközöket készítő cégeknek és embereknek tisztában kell lenniük ezekkel a hibákkal és amikor csak lehet beállítani az adatvédelmet alapból. A betörés sokkal rosszabb lett volna, ha az EFF és más adatbiztonság mellett kiállók kemény munkával nem érték volna el, hogy a webes forgalom több mint 90%-a HTTPS-en keresztül, titkosítva menjen. Annak a (közel) 10%-nak, akik még nem titkosították a forgalmukat, épp itt az ideje, hogy titkosításra váltsanak, akár Certbot-ot használva, akár olyan szolgáltatókra váltva, akik HTPPS-t adnak alapból.

Mi lehet a következő lépésünk? Igazi adatvédelmet és biztonságot kell követelnünk.

Meg kell cáfolnunk azokat a hangoskodó bűnüldözőket és egyéb szószólókat, akik folyamatosan állítják, hogy lehet hozzáférést biztosítani „csak jó fiúknak”. Egyebek mellett ezt az esetet is felhozhatjuk érvként a tévhit eloszlatására, ami szerint a digitális világban alapvető elvárás, hogy a kormányoknak (és a rosszindulatú hekkereknek) hozzá kell férniük az üzeneteinkhez és fájljainkhoz. Folytatjuk a küzdelmet az EARN IT jellegű amerikai törvények, az EU „Chat Control” fájlszkennelő kezdeményezés és a brit Online Safety Act ellen, amik mind ezen a hibás feltevésen alapulnak.

Ideje, hogy az amerikai politikusok is lépjenek. Ha tartanak attól, hogy Kína és más külföldi államok kémkednek amerikai állampolgárok után, ideje fellépniük az alapbeállítás szerinti titkosításért. Ha nem akarják, hogy rossz emberek ismét kihasználják a választókat, a hazai cégeket, vagy a biztonsági szerveket – álljanak ki az alapból történő titkosítás mellett. A választott hivatalnokok tudják és tették is már korábban. Ahelyett, hogy meghallgatásokon tennék lehetővé az FBI számára a könnyebb lehallgatást, számoltassák el őket a digitális zárak feltörésről, amit már csinálnak.

A leckét addig ismételjük, amíg meg nem tanulják: nincs olyan hátsó kapu, ami csak a jó fiúkat engedi be és a rosszakat kívül tartja. Ideje, hogy mindnyájan felismerjük ezt és tegyünk lépéseket az igazi biztonságunk és adatvédelmünk biztosítására.