Stand-by odmor

Ljeto je u punom zamahu. Fakulteti su pusti bez studenata i profesora, na poslu je minimalan broj ljudi, jer ipak netko treba obračunati plaće, zar ne? Sistemci se odmaraju, prepustivši servere, mrežu i korisnike da se sami brinu o sebi. Doduše, sistemci su uvijek u *stand-by* poziciji, navikli da ih zovu i na zasluženom odmoru. Ostatak svijeta se ne obazire na Akademiju, radi se punom parom, pa se tako i u svijetu informacijske sigurnosti svakodnevno nešto događa. Pozabavit ćemo se novostima u "revijalnom tonu", kako priliči *ferragostu*, da vidimo što se sve događalo dok smo se mi odmarali.

Hakeri su aktivni i ljeti, kako oni etički, tako i oni s "crnim šeširima". I jedni i drugi se zabavljaju otkrivajući "Kako stvari rade". Pa su tako proučavali ključeve za automobile, kojima se auti zaključavaju i otključavaju na daljinu. Za primjer su uzeli koncern VW. Snimali su signale koje šalju daljinski i otkrili algoritam koji generira kodove. Demonstriralii su kako se malom spravicom kućne izrade mogu otvoriti automobili marke VW, Audi, Škoda, Seat. Uz to su otkrili i "master" kodove pomoću kojih se otvaraju vozila u slučaju gubitka daljinskog. S obzirom da su etički hakeri, obavijestili su VW, koji "radi na otklanjanju problema". Znači li to da će svim vozilima mijenjati brave? Sjećamo se starih golfova kojima su mangupi otvarali vrata uz pomoć teniske loptice! Zarezali bi lopticu, stavili je na bravu i udarcem upumpali zrak u bravu, nakon čega bi se vrata otljučala. To l*ow tech* rješenje je zastarjelo, ali ispada da i novija tehnologija nije jako napredna. Vijest je dostupna ovdje [1].

Vjerojatno je najbombastičnije odjeknula vijest da je 900.000 Android telefona ranjivo na QuadRooter [2] napad. Radi se o skupu od četiri ranjivosti Qualcomm chipseta koji pogađaju Androide do uključivo Marshmallow verzije. Većina tih uređaja nikad neće biti "zakrpana", iako su zakrpe napravljene. Ranjivosti su otkrili u CheckPointu i obznanili ih na DefConu u Las Vegasu. Nude i besplatnu aplikaciju [3] s kojom možete provjeriti da li je vaš mobitel ranjiv.

Saznali smo i kako se na jednostavan način može preuzeti nečiji Facebook račun. Dovoljno je znati broj mobitela vlasnika računa. Evo kako je to jednostavno: pri pokušaju ulogiravanja na tuđi račun klikne se na link *Forgot account?* FB zatraži broj mobitela, pa tu treba upisati broj mobitela vlasnika računa. Zatim se iskoristi ranjivost protokola SS7 koji koriste telekomi, kako bi se poruka s novom zaporkom preusmjerila na napadačev mobitel. Ispada da je taj protokol maltene dizajniran tako da bi se omogućilo prisluškivanje i preusmjeravanje poziva. Ako ne vjerujete, pročitajte ovaj članak [4].

Nedavno smo naučili da je, kao dio nove Microsoftove politike "ljubavi prema Linuxu", u suradnji s Cannonicalom *Linux shell* postao dio Windowsa 10. Sve je još u fazi isptivanja, dotjerivanja. Alex Ionescu iz tvrke Crowdstrike malo se poigrao s tim softverom. Linux se ne vrti u hipervizoru, kao virtualna mašina na vlastitom kernelu, nego ima pristup funkcijama Windows jezgre kao i nativne Windows aplikacije. I obrnuto! Ionesku je otkrio da Win aplikacije mogu ubacivati kod, pisati po memoriji i ugrožavati rad Linux aplikacija. Otkrića je javio Microsoftu, ponešto je popravljeno, ali nove ranjivosti se pojavljuju i dalje. Radoznalci mogu pročitati članak u eWEEKu [5]. Ukratko, Linux aplikacije su manje sigurne na Windowsima nego na samom LInuxu.

Kad već spominjemo "glavne" ključeve koji otvaraju sve brave, ovih se dana u medijima spominje još jedan, kojeg su Microsoftovi marketinški majstori nazvali "zlatni ključ". Pomoću njega se zaobilazi zaštita koju nudi *Secure boot*. *Secure boot* djeluje na razini *firmwarea*, omogućavajući da se na računalu pokreću samo operativni sustavi ovjereni Microsoftovim certifikatom. Na većini osobnih

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

računala može se isključiti u BIOS-u, kako bi mogli instalirati na pr. Linux. No na brojnim tabletima i pametnim telefonima to nije moguće, čime su ti uređaji praktički zaključani. Zlatni ključ je, čini se, isprva bio razvojni alat za debagiranje i testiranje. No sada u igru moramo uvesti nove jake igrače. Sjećate se kako je FBI zahtijevao da mu Apple omogući otključavanje iPhona da bi se mogao provjeriti što s njime rade osobe osumnjičene za terorizam? Je li to možda pravi razlog Microsoftova uvođenja zlatnog ključa?

Naime, stvari su se nedavno zakomplicirale kada su istraživači pronašli zlatni ključ "zaboravljen" na nekim uređajima, koji su kao nehotice otišli na tržište sa softverom za debagiranje. Zlatni ključ je sad objavljen i dostupan na webu. Od sada će svatko tko ga ima moći zaobići *secure boot*, *rootati* Microsoftove proizvode, ili instalirati izmijenjenu verziju Windowsa.

Microsoft je nakon tog otkrića izdao zakrpe koje bi trebale riješiti problem, no teško da je moguća njihova uspješna primjena na svim uređajima. Radi se o zakrpama MS16-094 i MS16-100, a najavljuje se još jedna. Čini se da ćemo morati živjeti s potencijalnim *back doorom.*

U ovom kontekstu zanimljiva je i poučna izjava kojom je Apple CEO Tim Cook obrazložio nevoljkost da udovolji zahtjevima FBI (citiramo):

"Uvažavamo i poštujemo profesionalce koji rade za FBI i vjerujemo da su njihove namjere časne. Do sada smo činili sve što je u našoj moći i unutar zakonskih ograničenja da im pomognemo. Ali sada vlada SAD od nas traži nešto što nemamo i za što smatramo da je suviše opasno da bismo to napravili. Traže od nas da napravimo *backdoor* za iPhone.

Preciznije, FBI želi da izradimo novu verziju operativnog sustava za iPhone, zaobilazeći nekoliko važnih sigurnosnih zaštita i instaliramo ga na iPhone u sklopu istrage. U pogrešnim rukama, taj softver, koji još ne postoji, imao bi potencijal da otključa svaki iPhone kojem netko ima fizički pristup.

FBI može koristiti druge riječi da bi opisao ovaj alat, ali nemojmo se zavaravati: izradom verzije iOS-a koja omogućuje zaobilaženje sigurnosti na takav način nedvojbeno bi napravili *backdoor*. I mada vlada može tvrditi da će njegovo korištenje bilo ograničeno na ovaj slučaj, ni na koji način ne može garantirati kontrolu (nad njegovim korištenjem)."

Ovaj citat pokazuje nelagodnu situaciju u kojoj se nalaze komercijalne tvrtke. Kupci ne bi kupovali komunikacijske uređaje koji im ugrožavaju privatnost. Udovoljavanje zahtjevima vlasti moglo bi ugroziti budućnost tvrtke. Bez želje da sad previše relativiziramo stvari, svjesni smo da naši pamenti telefoni ionako već omogućuju da nas se prati i nadzire. Neki dan mi je moj Android ponudio dogradnju nekoliko aplikacija. Redovito odbijam dogradnju aplikacija koje ne koristim, ali sam pokrenuo instalaciju jedne (nije važno koje), jer mi povremeno zatreba. No najprije treba toj aplikaciji dati neke dodatne dozvole: želi pratiti moju lokaciju i moje *on-line* kupovine! E pa nećemo tako! Dobra mi je i stara verzija, sve dok bude radila! A ljuti me i činjenica da ne mogu deinstalirati aplikacije koje ne koristim a dolaze predinstalirane.

Hoće li sad još i FBI preuzeti kontrolu nad našim telefonima? Nije dovoljno što je već imaju Google, Apple ili Microsoft, a i telekomi.. Tehnologija omogućuje mnogo toga što potrošači ne bi trebali prihvatiti, no za sada je očigledno većina spremna preuzeti rizik, smatrajući da je dobrobit veća od cijene. Spremni su koristiti besplatne aplikacije i plaćati na druge načine, osobnim podacima. No negdje treba postaviti granice, iii će običan čovjek postati posve bespomoćan pred vladama i velikim kompanijama. To je izazov novog postindustrijskog doba koji ćemo svi zajedno morati riješiti, i zakonodavci i građani i kompanije. Po meni, za početak bi bilo dovoljno da svaki korisnik sam određuje gdje će postaviti granicu, a zakonodavac bi mu trebao dati pravo na to da uz osnovnu zaštitu, koja vrijedi za sve, sam može uključiti dodatnu zaštitu, a da ga se radi toga ne sumnjiči za terorizam.

Ah, možda je bolje da ne pratimo vijesti dok smo na odmoru? Problemi će nas ionako dočekati za koji dan, kad se vratimo na posao.

sub, 2016-08-13 19:53 - Aco Dmitrović**Kategorije:** Kolumna [6]
Vote: 0

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

No votes yet

Source URL: https://sysportal.carnet.hr/node/1670

Links
[1] https://blichr.wordpress.com/2016/08/13/jednostavan-hack-otkljucava-vecinu-volkswagena/
[2] http://thehackernews.com/2016/08/hack-android-phone.html
[3] https://play.google.com/store/apps/details?id=com.checkpoint.quadrooter
[4] http://thehackernews.com/2016/06/hack-facebook-account.html
[5] http://www.eweek.com/security/risk-from-linux-kernel-hidden-in-windows-10-exposed-at-black-hat.html
[6] https://sysportal.carnet.hr/taxonomy/term/71

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr