Shvaća li Google neozbiljno sigurnost Androida?

Jedna od temeljnih higijenskih navika korisnika računala svakako je sigurnost. U vrijeme kada neumreženo računalo smatramo informatičkim poluproizvodom, u okruženju u kojem veliki broj ljudi živi uz svoje (stolno, prijenosno ili telefonsko) računalo od buđenje do odlaska na spavanje, pitanje zaštite podataka postalo je još važnije.

Čudi, stoga, nedavna izjava [1] Sundara Pichaia kako je Android zamišljen da primarno bude otvorena platforma, a tek zatim siguran. Ova zbunjujuća izjava prije svega je netočna: ne postoji nikakav razlog zašto neka platforma ne bi bila istovremeno i otvorena i sigurna. Dapače, sam Android zasnovan je na Linux kernelu koji je (uz BSD i još neke) primjer otvorenog sustava koji pritom ima i pristojnu razinu sigurnosti.

Činjenica je da Android pokušava – i uspjeva – ponoviti uspjeh IBM PC računala kojem je otvorenost, tj. mogućnost nadogradnje od strane korisnika i proizvođača hardvera značajno pomogla u ostvarivanju dominacije na tržištu i istiskivanja gotovo sve konkurencije (pa tako umalo i Apple-a) s tržišta. Naravno, bila su to druga vremena i sigurnost PC računala i instaliranih operacijskih sustava evoluirala je zajedno sa napretkom tehnologije. No Android nema tu privilegiju: on mora biti vrlo siguran odmah, jer je nastao u umreženom svijetu, divljem zapadu gdje iz svakog saloona vire oči gladne informacija o nama, o našim navikama i o brojevima naših kreditnih kartica.

Nažalost, čini se da gore navedena izjava ima svoju težinu, jer nedavna objava vrlo nezgodnog modula [2] za Metasploit koji iskorištava sigurnosni propust u ugrađenoj WebView komponenti Androida nije naišla na ozbiljniji Googleov odgovor.

Riječ je o sigurnosnom problemu koji je tipičan za mobilne platforme i, možemo reći, prije njih nije postojao. Naime, uobičajeni način rada web browsera (što WebView komponenta jest) na "običnim" računalima ograničen je u svojim mogućnostima: maliciozni JavaScript kod u ranim je danima pretraživača mogao i načiniti neku štetu, ali osvještavanjem o potrebama sigurnosti browseri su dobili sposobnost zatvaranja koda u ograničeno okruženje u kojem nije moguće komunicirati s drugim skriptama ili pristupiti datotečnom sustavu i sl.

Problem sa Androidovim sigurnosnim propustom mnogo je širi od same činjenice da maliciozni kod može dobiti prava pristupa koja ima preglednik: za razliku od "običnih" računala, browseri na Androidu često imaju pravo pristupa većini funkcija telefona: telefonskom imeniku, kameri, SD kartici... Kad maliciozni kod jednom zavlada WebView procesom postaju mu dostupne gotovo sve funkcije telefona, uključujući i ljusku [3]. Sol na ranu dodat ćemo podsjećanjem da je, osim Jave, druga dominantna platforma za izradu aplikacija na Android uređajima HTML5 koji radi upravo na nesigurnom WebView modulu, što znači da je potencijalno (pažnja, eufemizam!) opasna svaka HTML5 aplikacija koja koristi ranjivi modul; a autori aplikacija ne mogu učiniti baš ništa, jer je modul pod kontrolom Google-a.

A Google je taj problem ispravio u verziji 4.2 Androida i, čini se, nema namjeru popravljati starije verzije – što ostavlja ogroman broj uređaja osjetljivim na napad. Nažalost, notorna je činjenica da proizvođači telefona ne vole kupcima nuditi update za već kupljene uređaje, već ih svojom inertnošću nastoje "nagovoriti" da kupe novi uređaj, pa je malo vjerojatno da će mnogi vlasnici Android telefona vidjeti zakrpu za ovaj ozbiljan [4] sigurnosni propust.

Posjedujete li uređaj sa Androidom 4.1 ili starijim niste u zavidnom položaju, jer ni Google ni proizvođači (barem zasad) nemaju namjeru ispraviti ovaj sigurnosni propust.

Od njega se možete barem dijelom zaštititi tako da na svoj Android uređaj instalirate Chrome, Firefox ili neki treći browser koji ne koristi WebView (tj. koji nije samo lijep front-end za u Android ugrađen web browser). Time ćete izbjeći većinu potencijalnih napada, ali ne zaboravite da su sve aplikacije koje u sebi koriste WebView i dalje podložne napadu.

Rješenje? Prema Google-u i proizvođačima telefona, nabavka novog uređaja sa novim Androidom. No, postoje i iPhone telefoni, te Windows Phone telefoni.

Ovakve igre proizvođača sasvim sigurno će prestati u nekoj budućnosti, ali valja nam do tad izdržati. Ne bih ovo nazvao dječjim bolestima – sva tri igrača (Apple, Google, Microsoft) dovoljno su dugo na tržištu da im mora biti jasno koliko je pitanje sigurnosti vezano uz IT. Tu činjenicu ne mogu promjeniti niti neoprezne izjave čelnih ljudi tvrtke.

pet, 2014-02-28 07:06 - Radoslav Dejanović**Vijesti:** Sigurnosni propusti [5]
Kategorije: Preglednici [6]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1361?page=0

Links
[1] http://www.networkworld.com/community/blog/google-android-chief-sundar-pichai-says-android-not-designed-be-safe
[2] http://www.rapid7.com/db/modules/exploit/android/browser/webview_addjavascriptinterface
[3] https://docs.google.com/file/d/0B3_TQgTE2uPcMkdBOExKNjh0N28/edit
[4] http://arstechnica.com/security/2014/02/e-z-2-use-attack-code-exploits-critical-bug-in-majority-of-android-phones/
[5] https://sysportal.carnet.hr/taxonomy/term/14
[6] https://sysportal.carnet.hr/taxonomy/term/27