Android: za inficirane aplikacije spremni! (1/2)

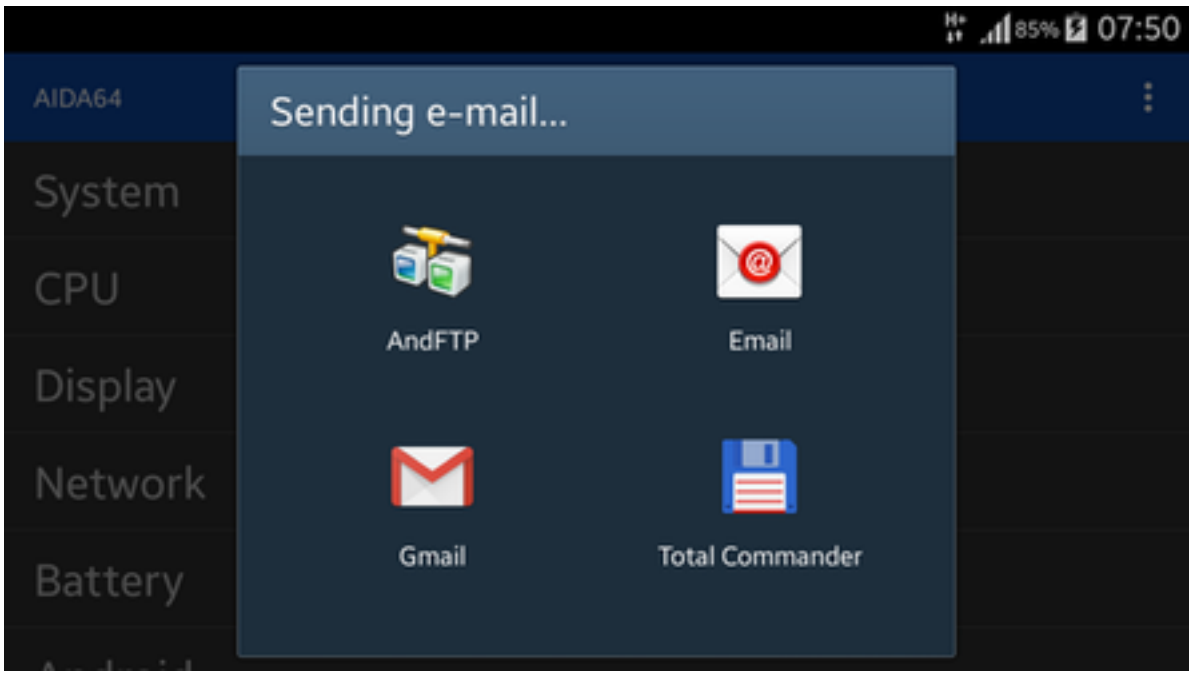
Neugasiva je želja agilnijih, znatiželjnijih korisnika Android uređaja da se barem povremeno odmaknu od Googleovog dućana aplikacija jer korisne ili zabavne aplikacije (i usluge) postoje i u drugim online dućanima, poput **Amazon**ovog, tu su i **ApkMirror**, **Aptoide**, **F-droid**, **Getjar**, **SlideMe**... ma ima ih više od zavoja na Jadranskoj magistrali! Slijepo držanje za Googleove skute najviše šteti nama IT profesionalcima jer nam sužava spoznajne horizonte te, u konačnici, značajno otežava stručno napredovanje u oblasti mobilnih tehnologija.

Nažalost, turobne prognoze upućenih da tek slijede stvarno sofisticirani napadi na Android mobilne uređaje zlorabljenjem ne samo lokalnih ranjivosti već i onih prisutnih u mobilnim mrežama, djeluju poput hladnog tuša i gase istraživački žar. Uistinu, što više čovjek prati sigurnosne peripetije Android smartfona - ranjivosti se ne otkrivaju samo u AOS-u nego i u firmwareu SoC-a, pokrpa se jedna ranjivost a otkriju dvije, "slow motion" princip krpanja i to samo novijih modela, stotine malwareom zaraženih aplikacija otkriveno je i u dokazano najsigurnijem od svih dućana, Googleovom... - to je veća bojazan da ćemo vrludanjem po Webu i instaliravanjem aplikacija "from untrusted sources" izložiti svog dragocjenog digitalnog asistenta svakojakim softverskim opačinama. Budući da isti taj uređaj često rabimo za financijske transakcije, udaljeno administriranja računala firme i slične u osnovi senzitivne poslove, radije ćemo odustati od traganja za novim ili boljim alatima nego se izložiti kompromitaciji i odgovornosti. Nitko neće pokazati previše razumijevanja za naše samoeduciranje ili nastojanje da što učinkovitije izvršavamo svoje radne obveze ako se ustanovi da je sigurnosni incident uzrokovao malware koji čuči u našem smartfonu.

Srećom, uz nešto samokontrole, uparene s niže izloženim postupcima, moguće je zamalo-pa-bezopasno ispitivanje raznih web sadržaja i isprobavanje aplikacija prisutnih u katalozima dućana niže sigurnosne razine od Googleovog. Kako to već biva u oblasti računalne sigurnosti, rizik ne možemo eliminirati ali ga možemo minimizirati.

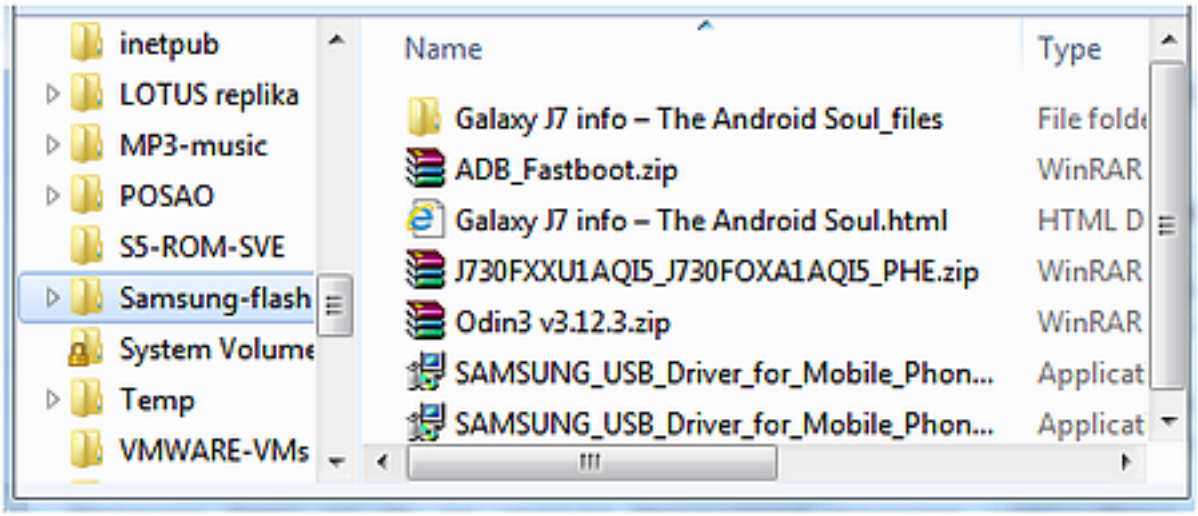
U svim primjerima unutar ovog članka referentni Android OS nam je izvorni (vanilla) Nougat, trenutno je ta verzija „zlatna sredina“ zastupljenijih AOS verzija na tržištu (Marshamallow – Nougat - Oreo).

1. Za smartfon izraditi tzv. baseline snimku stanja, baš kako to radimo za servere neposredno prije puštanja u produkciju ili nakon većih preinaka. Alata vrste "system info" ima napretek, osobno kombiniram AIDA64 i Network Connections. Nažalost, zbog novouvedenih sigurnosnih restrikcija u Sedmici, vrijedni alati poput OS Monitora više nas ne mogu informirati o procesima. Tja, odradit ćemo ono što možemo. Na nižoj slici iz Aide si šaljem izvješće u mailbox, od tamo odlazi u arhivu.



2. Uvjerit ćemo se da je opcija Untrusted sources isključena, eno je u sistemskim postavkama AOS-a pod stavkom Security. Opciju ćemo uključiti neposredno prije instalacije aplikacije, o tome kasnije. Nasuprot ovome, Play Protect funkcionalnost treba biti uključena. Ne rootati smartfon jer time postaje ranjiviji, o tome smo ranije pisali, vidi https://sysportal.carnet.hr/node/1629 [1]. Par odličnih aplikacija spomenutih tijekom obrade ove teme nesmetano radi na nerootanim uređajima.

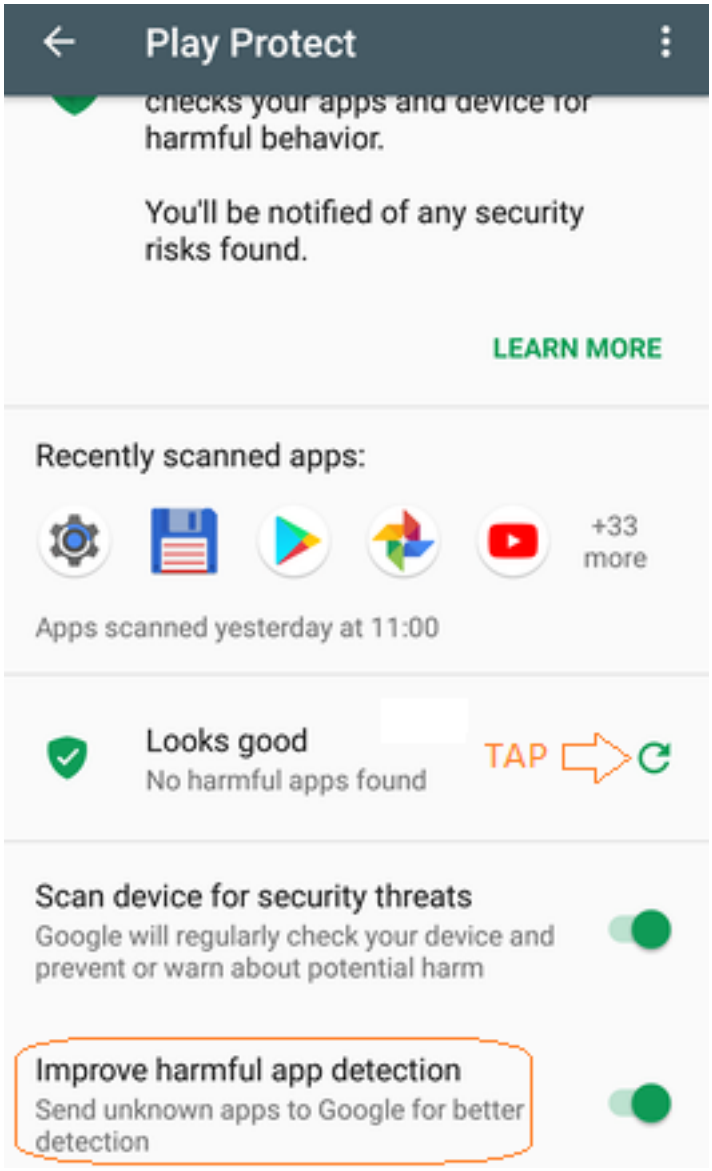
3. Slijedi priprema za brzu i potpunu revitalizaciju smartfona, time se u podjednakoj mjeri osiguravamo od teško uklonjivog malwarea i osobnih lakomislenih postupaka. Dakle, opremit ćemo se s aktualnim službenim ROM-om (stock ROM, official firmware), alatom s uputama kako taj ROM natočiti na smartfon te s driverom za USB konekciju smartfona s računalom. Važna napomena: dođemo li u situaciju da uistinu moramo flashati smartfon, prvo odradimo Factory data reset (kroz Settings AOS-a) ili Wipe data/Factory reset iz Recovery konzole jer moramo počistili Data i Cache particije. Niže je "borbeni komplet" za moj phone.



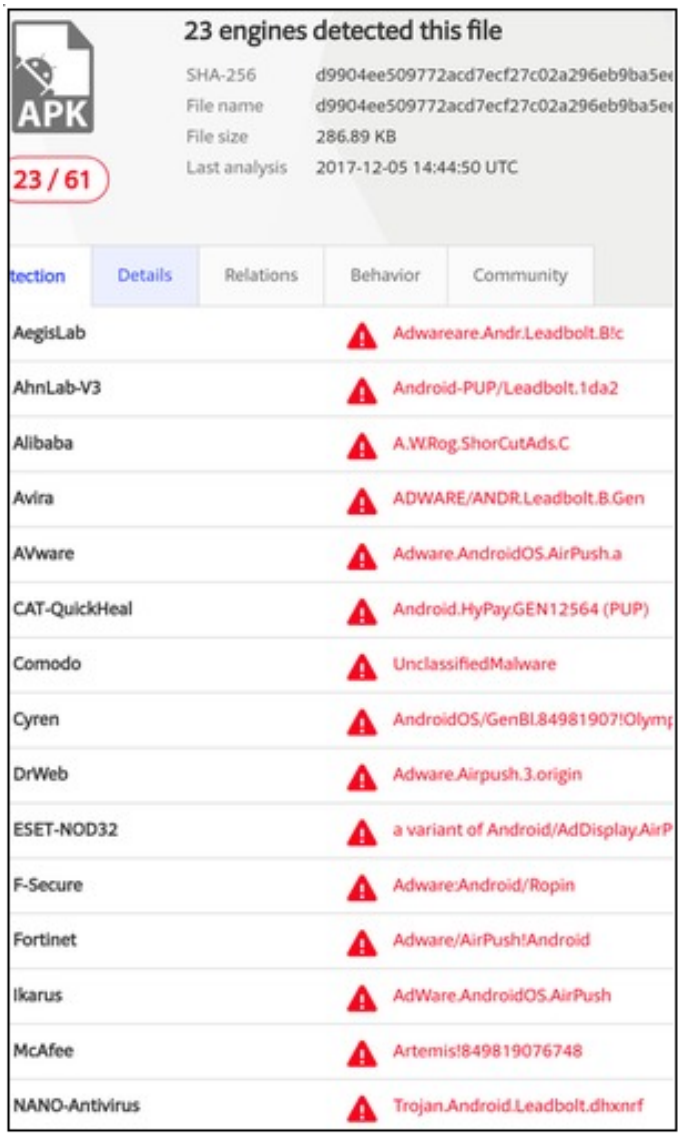
4. Postoji cijela jedna „škola“ koja problematizira korisnost antivirus/antimalware aplikacija na mobilnim Android uređajima, nećemo ulaziti u raspravu, samo skrećemo pozornost da od njihove prisutnosti na uređaju ipak imamo više koristi nego štete. Rečeno se posebno odnosi na situaciju za

koju se pripremamo. Guglanjem ćemo lako pronaći usporedne analize raznih softverskih rješenja ove vrste pa se možemo opredijeliti.

U prilog iznesenom je i to što u AOS integrirana Googleova antimalware usluga Play Protect za sada gubi bitke u komparacijama sa drugim produktima iste namjene. Do daljnjega, znači, nije mudro osloniti se isključivo na zaštitne potencijale Play Protect mašinerije. Zgodno je znati da je opcija Improve harmful app detection defaultno isključena - vjerojatni je razlog minimiziranje trošenja podatkovne kvote od strane samog AOS-a – ali isplati nam se aktivirati ju; nadalje, Play protect možemo i ručno pokretati kad god nam se prohtije.



5. Sad smo spremni za skitaranje po bespućima Weba i skidanje zanimljivih nam aplikacija kako bismo ih isprobali. Evo, napikirali smo jedan sistemski alat, tko zna, možda nam baš on postane glavni za odrađivanje nekih poslića. Skinemo na smartfon .apk paket i sad ga trebamo instalirati, dakle, uključit ćemo maloprije spomenutu opciju Untrusted sources , jel'te.... NE! Postoje online servisi poput **VirusTotal** i **NVISO Apk Scan** koji "češljaju" apk-ove u potrazi za malicioznim kodom, zašto ih ne bismo iskoristili?! Znači, dostavit ćemo skinuti .apk antimalware servisu i saznati što će reći o toj aplikaciji. U prvom dijelu niže slike vidimo mišljenje Virus Totala. Ako se njegov nalaz podudara s nalazom drugog servisa iste namjene - a vidimo da je tako – tu aplikaciju je najpametnije zaboraviti, kolikogod nam se učini "bogomdanom". A opciju Untrusted sources uključit ćemo samo kad nas servisi poput spomenutih izvijeste da je s .apk-om sve u redu, kako bismo instalirali aplikaciju.



Gornja slika ujedno opominje: zaguglajte da biste provjerili status kreatora aplikacije i same aplikacije prije nego što ju uopće skinete na svoj uređaj.

Zašto je dobro opet isključiti Untrusted sources nakon instalacije? Zato jer nam se u pravilu nudi instalacija aplikacije odmah nakon skidanja .apk paketa pa pukom zabunom možemo odobriti instaliranje zloćudnog koda!

Nasuprot raširenom mišljenju, i aplikacije skinute s nezavisnih dućana mogu se automatski ažurirati, naime, postoje aplikacije - spominjemo ApkUpdater - koje upravo tome služe, da provjere postojanje novih verzija instaliranih aplikacija. Obično dućani nude vlastite aplikacije te namjene.

6. Cyber kriminalci imaju nezgodnu navadu plasirati nekoliko čistih verzija aplikacije, onda počnu distribuirati istu aplikaciju "obogaćenu" malwareom. Srećom, nismo nemoćni ali treba znati kontrirati. Budući da ulazimo u pomalo iritantnu "može biti a i ne mora" materiju, bolje nam je točki 6 posvetiti zaseban članak.

(nastavlja se)

čet, 2018-01-11 14:16 - Ratko Žižek**Kuharice:** Android [2]
Kategorije: Operacijski sustavi [3]
Vote: 0

No votes yet

story_tag: Android [4]
zaštita [5]
aplikacije [6]
smartphone [7]

Source URL: https://sysportal.carnet.hr/node/1786

Links
[1] https://sysportal.carnet.hr/node/1629
[2] https://sysportal.carnet.hr/taxonomy/term/64
[3] https://sysportal.carnet.hr/taxonomy/term/26
[4] https://sysportal.carnet.hr/taxonomy/term/183
[5] https://sysportal.carnet.hr/taxonomy/term/204
[6] https://sysportal.carnet.hr/taxonomy/term/205
[7] https://sysportal.carnet.hr/taxonomy/term/185