SECTOR 2015
Malware Activity in Mobile Networks
Kevin McNamee (Alcatel-Lucent)
Agenda

• How the data is collected
• Lies, Damn Lies and Statistics
• Windows PC Malware
• Android Malware
• Examples of malware
• Conclusion
Monitoring the Mobile Network

• Monitor GTP-C traffic
  - Maps IMSI, EMEI & MSISDN to IP address
  - Associates infection with a specific device or user

• Monitor GTP-U traffic
  - Malware C&C
  - Exploits
  - DDOS
  - Hacking
Monitoring the Mobile Network

• Analytics Provides
  - Raw security alerts
  - Trigger packets
  - Infection history by device
  - Infection history by malware

• Reports
  - Most active malware
  - Network impact
  - Infection rates

MOBILE NETWORK SECURITY ANALYTICS

Alert Aggregation & Analysis
Malware Detection Sensor

Forensic Analysis

NodeB
RAN
eNodeB

RNC

Alternate Tap (Iu-PS and S1-u)

SGSN

10GE or GE

Recommended Tap (Gn and S5/8)

GGSN/PGW

Internet

Recommended Tap choice (Gi and SGi)

Alternate tap choice (Gi and SGi)

SGW
Detection Rules Development Process

- **MALWARE SAMPLES**
  - 120K+ ANALYZED PER DAY
  - 30M+ Active samples
- **VIRUS VAULT**
- **SANDBOX**
- **MALWARE TRAFFIC LIBRARY**
- **RULES DEVELOPMENT**
- **RULES LIBRARY**
- **TRAFFIC POLICY**
- **ZERO DAY BEHAVIORAL RULES**
- **RULES REPOSITORY**
- **DEPLOYMENT-SPECIFIC RULE SETS**
- **FIELD TESTING IN LIVE NETWORKS**
- **QUALITY TESTING**
- **RULE ACTIVATION**
- **FEEDBACK FROM FIELD TESTS**
Lies, Damn Lies & Statistics
Highlights

- 80% of mobile infections are on Windows PCs
- 10 of the top 25 smartphone infections are spyware
- 14% of homes are infected with malware

Source: https://www.alcatel-lucent.com/solutions/malware-reports
Overall Mobile Infection Rate

- About 0.7% of mobile devices exhibit signs of malware infection.
- Lookout and Google are in the 0.4% - 0.7% range.
- Verizon and Damballa report much less.

Google: “... US English devices have a PHA (potentially harmful app) installed on about 0.4% of devices, which is about 0.2% below the worldwide average.”

Source: Google Report - Android Security 2014 Year in Review
Watch out for bad reporting in the press

Slight change in word order makes a huge difference:

What was said by NQ Mobile:

“31.7% of infected devices are in China”

What was reported in the press:

“31.7% of devices in China are infected”

Source: NQ Mobile (2013)

Mobile Infections by Device Type

- 80% are actually Windows PCs
- 20% are Android devices
- Less than 1% are iPhone, Blackberry, Symbian and Windows Mobile.
Windows Malware impacts mobile networks

• Mainstream Professional Cybercrime

• Types
  - Botnets, Rootkits, SPAM, Identity Theft, Banking Trojans, DDOS, Ad-Click, Bitcoin, FakeAV, Ransomware, Hacktivism, Spyware...
Android is mobile target of choice

- **Mostly trojanized apps** from 3rd party app stores or Google Play
- **Installed** by victim as a result of phishing or social engineering.
- **Types** (varies by region) : Adware, Info Stealers, Spy Phone, SMS Trojans, Banking Trojans, Fake Security Software, Ransomware, Lockers
- **Impact** is low on the network so far but moderate to high on users
Android Malware

- **Lacks Sophistication**
  - C&C servers are hard coded in the source code as URL’s, domain names or IP addresses.
  - The C&C protocol is not robust and can be disrupted by taking out a single server.
  - The malware make no real attempt to conceal itself or avoid detection by anti-virus software.
  - The malware makes no attempt at persistence and can be removed by a simple uninstall.

However it’s getting “better” with time
Why Android?

• **Sideloading**
  - Android apps can be downloaded and installed from anywhere.
  - This provides the malware developer with an easy way to deliver the malware.
  - Some third-party app stores specialize in pirated software with a high malware content.

• **Google Play**
  - Survey of 130k free apps in early 2014 showed 1/700 had some sort of malware content.
  - Google has greatly improved on this since then.
Why Android?

• **App Hijacking is trivial**
  1. Get the APK file for the target app
  2. Open it using “apktool d”
  3. Cut and paste the Trojan “smali” code directories into target app
  4. Edit the onCreate() function in the apps main activity to invoke the Trojan service
  5. Edit manifest to add the Trojan service and any required permissions
  6. Rebuild the app using “apktool b”
  7. Use “jarsigner” to sign the app (any key will do).
  8. Use “zipalign” to complete the process

This of course can be scripted...
Android vs Apple app security

- Signed with self signed certificates that are created by the developer.
- Available from a large number of third party app stores

- Signed with certificates issued by Apple and linked to the developer registration information.
- Only available from Apple.
Examples of Mobile Malware
Mobile Spyware

• Mobile spyware is definitely on the increase. Ten of our top 25 mobile malware are spyware.
• These are apps that are used to spy on the phone’s owner.
• They track the phone’s location, monitor incoming and outgoing calls and text messages, monitor email and track the victim’s web browsing.
• Used by individuals, private investigators and in cyber espionage.
## CELL PHONE SPY SOFTWARE REVIEWS

<table>
<thead>
<tr>
<th>RANK</th>
<th>Excellent</th>
<th>Very Good</th>
<th>Good</th>
<th>Average</th>
<th>Poor</th>
<th>Bad</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MSPY</td>
<td>HIGHERSTE</td>
<td>MOBILE</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>HIGHER</td>
<td>MOBILE</td>
<td>Mobi</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>MOBILE</td>
<td>Mobi</td>
<td>STEA</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>FLEXISPY</td>
<td>SPYERA</td>
<td>MOBILE</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>SPYPHONE</td>
<td>TAP</td>
<td>MOBILE</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>6</td>
<td>MOBILESIA</td>
<td>GENT</td>
<td>THEO</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td>THEESPY</td>
<td>ITPRO</td>
<td>THETR</td>
<td>9</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>THEESP</td>
<td>STEA</td>
<td>ITPRO</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>THEESP</td>
<td>STEA</td>
<td>ITPRO</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>THEESP</td>
<td>STEA</td>
<td>ITPRO</td>
<td>10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Visit Website: GO, GO, GO, GO, GO, GO, GO, GO, GO, GO
Review: READ REVIEW, READ REVIEW, READ REVIEW, READ REVIEW, READ REVIEW, READ REVIEW, READ REVIEW, READ REVIEW, READ REVIEW, READ REVIEW

### FEATURES

<table>
<thead>
<tr>
<th>Feature</th>
<th>MSPY</th>
<th>HIGHERMOBILE</th>
<th>MOBILESTEAM</th>
<th>FLEXISPY</th>
<th>SPYERA</th>
<th>MOBILESPY</th>
<th>SPYPHONE</th>
<th>TAPMOBILE</th>
<th>MOBILESIA</th>
<th>THEOESP</th>
<th>THEITRUESPY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi OS Support</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>SPY on Calls</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>SPY on SMS and MMS</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>SPY on Emails</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Track GPS Location</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Monitor Internet Use</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Access Address Book</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
</tbody>
</table>

[http://www.top10spysoftware.com/]
**Ransomware & Lockers**

- This malware claims to have locked your phone and/or encrypted your data.
- It demands a ransom to restore it.
- Often data is not really encrypted.
Permissions used by Lockers

• SYSTEM_ALERT_WINDOW
  - Allows app to display a window on top of everything else
  - You can’t interact with the phone
  - Usually combined with auto start on BOOT
  - Effectively locks the phone

• Device Administration
  - Provides additional permissions
  - Must be activated by user
  - Can block “Settings” app until user OKs the activation
  - Can’t uninstall an app with the permission
  - Also combined with auto start on BOOT

Solution: Start Phone in “safe mode” and delete the app.
Koler

- Koler is an Android scareware Trojan that claims it has encrypted all the data on your phone and demands a ransom to restore the data.

The victims are usually visitors to Internet-based pornographic sites, who are duped into downloading and installing a “premium access video player.” The malware “lock-screen” is customized depending on the location of the phone. The screen image is from a United States based phone.
Android.Locker.B

- This looks like an Norton AntiVirus app
- Finds problems with your phone
- Asks to activate “device admin”
- Gives you the bad news
- Tells you how to fix it
Android.SLocker.A

- Looks like the Adobe Flash Player
- Immediately asks for Device Admin
- Disappears from APPS screen
- Can’t be stopped or uninstalled
- Has all sorts of permissions
- Communicates with C&C
- Uses “alert window” to:
  - Lock phone
  - Ask for Google Wallet credentials
  - Ask for credit card credentials
- Goal is to get your credit card info
Malware Survives Factory Reset

• An Android factory reset operation does not reset the /system partition.

• So any apps stored in /system/app directory will survive a factory reset.

• Malware can take advantage of this by rooting the phone and installing apps in the /system directory.

• This happened to one our lab phones…
Malware Survives Factory Reset

1. Malware from Chinese app store was run on one of our test phones.
2. It had almost every of permissions possible.
3. It included a library with known root exploits.
4. Over time a number of additional “system” apps appeared in the /system/app directory.
NotCompatible - Overview

- Web Proxy Bot ported from Windows to Android environment.
- Uses same C&C as Windows version.
- Allows remote miscreants to anonymously browse the web through the victim’s phone.
- Consumes lots of bandwidth, for example 165MB in two hours over 300K TCP sessions
NotCompatible - Infection

- Phishing spam is used to lure the victim to an infected web site.
- Web site tells you the browser is “not compatible” and provides an update.
- The user downloads and installs update.apk
- Malware has no icon or user interface. It is automatically started on BOOT.
- You can get rid of the infection by uninstalling the application.
NotCompatible - Operation

• Opens an encrypted configuration file containing the address and port number of the server.

• The bot connects to the server via TCP.

• Sophisticated command and control protocol is then used to multiplex Web proxy services over that connection.

• This provides an anonymous web browsing services to clients.
NotCompatible - Command & Control

- Simple command/response packet format contains both commands and data.
- Channel number can multiplex many connection at once.
- The ping and pong are used as a heartbeat when there is no proxy work to be done.
- Once a proxy request is issued the “raw data” commands are used to transfer the data in either direction.

Packet format:

<table>
<thead>
<tr>
<th>0x04</th>
<th>chan</th>
<th>type</th>
<th>length</th>
<th>...data...</th>
</tr>
</thead>
</table>

0x04 - Protocol Version (1 byte)
chan - Multiplexor Channel number (2 bytes)
type - 0x00:Proxy Data, 0x01:Command (1 byte)
len - Length of the data field (4 bytes)
data - Is either proxy packet data or a command

Commands:

Initial handshake: | 00 | 07000v00 |
Proxy to IP: | 01 | 00 | IP & port |
Proxy to domain name: | 01 | 01 | len | domain name |
Response to proxy: | 02 | nnnn |
End of proxy session: | 03 |
Ping: | 04 |
Pong: | 05 |
Unknown (from victim): | FC | 01 |
Set Timeout: | FD | timeout |
Set Reserve Server: | FE | server IP and port |
Set Primary Server: | FF | server IP and port |
NotCompatible - Uses & Impact

• Uses
  - Anonymous Web Browsing Service
  - Providing Access to Restricted Foreign Content
  - Ad-Click Fraud
  - Web Site Optimization Fraud
  - APT Probing and Exfiltration

• Impact
  - One user from Finland, roaming in the US, used over 165MBytes in less than two hours of airtime.
  - In the lab it averages 100MBytes per hour.
  - Causes huge data bills
  - Caused the battery to run down quickly
  - Who knows what sites your phone is visiting!!!
StageFright

• Vulnerabilities in Android’s media display software provides attacker remote code execution from unsolicited MMS message with a specially crafted media attachment.
• Android automatically opens the attachment and the device is infected without any interaction from the user.
• Over 1 billion devices are estimated to be vulnerable.
• Patches are available, but the real question is how to get them deployed.
• Has forced Google, the phone manufacturers and the mobile carriers to take a serious look at how to improve how Android patches are deployed in the field.
iPhone not immune

• KeyRaider steals over 225,000 Apple accounts
  - Targets jailbroken iOS devices and is distributed through third-party Cydia repositories
  - Steals Apple credentials and uploads them to C&C server
  - Allow attackers to use stolen iPhone credentials for purchases at the Apple store

• xCodeGhost infiltrates Chinese app development
  - Trojanized xCode SDK was used by Chinese app developers
  - Embeds malware in any apps developed using this SDK
  - Apps distributed through official channels
  - Used for billing fraud, password stealing and to install additional malware
  - Infected 39 apps including WeChat, the popular interactive message app.
Conclusion

• Windows PCs & Laptops are still the major focus of Cybercrime.
• Android and iPhone malware lacks sophistication and focuses on things that work well in the mobile environment.
  - Spyphone Apps & Trojans
  - SMS Trojans
  - Scareware
  - Adware
• However we are starting to see:
  - Advanced persistence
  - Stealth
  - Sophisticated C&C
  - Remote exploits
Questions ?