

Mobile Threat War Room

Ollie Whitehouse
NCC Group

Agenda

- Big Trends
- Some Technical Details
- Real Case Studies
- Predictions for 2013

Big Trends



Mobile Malware... Finally

- Everybody has been predicting mobile malware for five years
 - Finally easy with mobile crimeware kits
- Real events:
 - All Trojans...
 - ... premium rate SMS the money machine
- On Android, automated repackaging is a huge issue
 - You need to keep a constant watch on the Android market
 - Disparate market places (i.e. non Google)
- Demonstration of off-device payloads on iOS and Android
 - Although not on a mass scale...

Messy Android Ecosystem

- Early decisions are coming back to haunt Google
 - OEM patching
 - Loose CTS
 - Open market
- Not all phones are created equal
 - Tier-1 “Google Experience” Devices provide the only trustworthy Android choice
- Google is trying to put the genie back in the bottle
 - We’re trying to help carriers/OEM, but it is an uphill battle

Everybody Goes Employee Liabile

- Increasingly our clients support iOS, with less supporting Android
- RIM's dominance of the FSTE 100 is over
- Varied levels of support:
 - Open ActiveSync  Not Recommended
 - Provisioned ActiveSync 
 - VPN->ActiveSync
 - Secure Container

Death of Network Trust

- GSM is totally toast
 - A5/3 showing massive weakness
 - A5/1 is good enough for 99% of situations
- No longer theoretical
 - We had a high-net-worth client spot an IMEI catcher across the street
- CA system completely failed in 2011
 - DigiNotar, Comodo
 - 1500 ICAs and climbing



Widespread Government Monitoring

- Arab Spring powered, countered by mobile
 - Tunisia is a cyber-warfare power?
- More advanced than you might think
 - JavaScript Injection
 - User-agent, referrer, IP spoofing
- Enabled by Western equipment, utilizing mixture of government and mercenary talent
- Sites with less than 100% HTTPS might be automatically caught up
- ActiveSync CANNOT be used overseas



Secure Containers Get Real

- Many many clients are deploying secure containers for mobile mail and documents
- Very helpful for:
 - More secure provisioning and wiping
 - Avoiding exposure of AD creds
 - Protecting against CA attacks
- Not so helpful against:
 - Jailbroken devices
 - On-device malware
 - Lost phones

SYBASE®



Board Papers®

Mobile Forensics Gets Better..

- ... for 7K GBP
- That can bypass lock screens
 - ... on some devices
- That can do raw sector copies
 - ... which impacts device not fully encrypted
- Becoming incredibly easy to use



Mobile Two-Factor Authentication

- Increasingly clients looking to mobiles for two-factor
- SMS
- Mobile Apps
- Phone call
- Reducing the token cross...



Researchers

- Still successful
 - going lower (cellular baseband)
 - going sideways (NFC)
 - ... these are not theoretical attacks
 - ... but they're also uncommon
- Criminals still not having to invest
 - easy attacks still working
 - but research out there..



Interesting Details

iOS Changed this Year

- iCloud complicates DLP situation
- MDM much improved
 - TLS, iCloud, SMIME
- Upgrade of KeyChain to defeat forensics
 - Didn't work, see ElcomSoft
- Fixes to file privacy settings
- Slight anti-exploit improvements
 - Didn't work, see PDF jailbreak
- Still missing:
 - Real full-device encryption
 - Useful Safari Sandbox



iOS Changing in iOS6

- Guided access
 - Loan a device without fear
- Supervised mode
- Geo fencing notifications
- Global proxy settings – enabling content filtering
- Lock down profiles / certificates
- ... enterprise management gets real!
- or becomes as much fun as a BlackBerry
- ... and 197 security patches, including 4 for the lock screen

Android Changes this Year

- Anti-exploit improvements
- Local MDM API improvements
- Significant fixes to permission regressions
- Configurable CA root store (ICS)
- Real data-partition encryption (ICS)

- Still missing:
 - Kernel syscall sandbox
 - 3LM Technologies
 - Market anti-spoofing analytics



Top iOS App Mistakes

1. SQLite queries not parameterized
2. Bad entropy
3. Data stored insecurely
4. Not controlling iTunes backups
5. Static analyzer results not reviewed
6. General C issues (*malloc()*, and *str**)
7. Format strings not declared
8. Incoming data from user not sanitized/encoded



Top Android App Mistakes

1. Exporting components accidentally
2. Silly custom permissions
3. Intent Reflection (use PendingIntents)
4. Unauthenticated services
5. WebView caching
6. Native Code Bugs
7. Poor HTTPS use
8. Too much local storage



Microsoft bring their game

- Windows 8
 - ... but on a mobile phone
- Ahead of security arms race
 - ... but on a mobile phone
- Without the legacy
 - ... which has been the Achilles of the MS eco system
- Everything we know and love
 - Secure boot
 - BitLocker
 - MDM
 - Etc..



Real Case Study

RSACONFERENCE

eFRAUD GLOBAL FORUM

Predictions for 2013

Disclosed compromise of
cellular carrier

Mobile Phishing
gains traction

Citizen repression tech
Used for Industrial Espionage

Public disclosure of
GSM eavesdropping

Mobile APT DOESN'T
happen

Continued mistakes by handset
OEMs



Continued improvements in
Mobile OS security

Mobile patch management
becomes hot topic