ÞEKKING

Malware in Mobile

Árni Már Harðarson/Öryggisráðgjafi

Agenda

- Facts & figures
- Examples
- Detection
- Mobile Drive-By
- Good Practice
- Conclusion

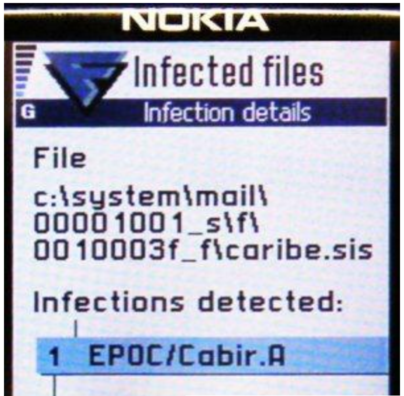
Facts & figures

- Google (Android market) and Apple (App Store)
  - 500K+ apps
  - Billions of downloads
- Juniper Networks research:
  - Mobile payments will triple in value by 2015
    - $670 billion (up from $240 billion last year)
  - Android malware up 400% first six months of 2011

Examples (The old)

- Cabir (2004)
  - First computer worm capable of infecting mobile phones?
  - Was targeted at devices running **Symbian OS**
  - Hijacked the phone’s user interface

- iKee (2009)
  - Targeted “Jail broken” **iPhones**
  - Compromised phones through default SSH password (alpine)
  - Turned the phone into both a bot and a botmaster.
  - Changed the wallpaper to an image of the 80’s singer Rick Astley
  - Written as an experiment



Infected files

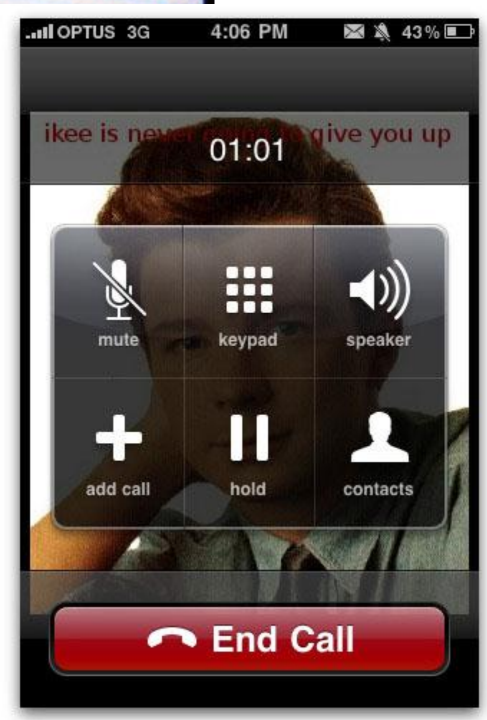
Infection details

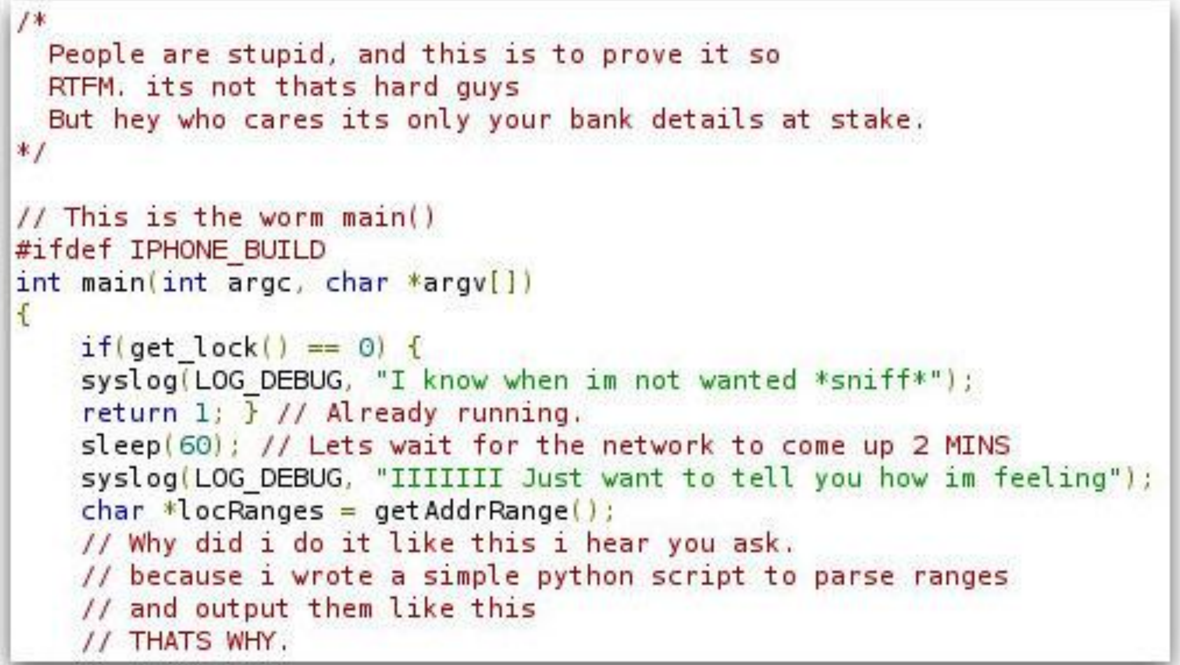
File

c:\system\mail\00001001_s\f\0010003f_f\caribe.sis

Infections detected:

1 EPOC/Cabir.A



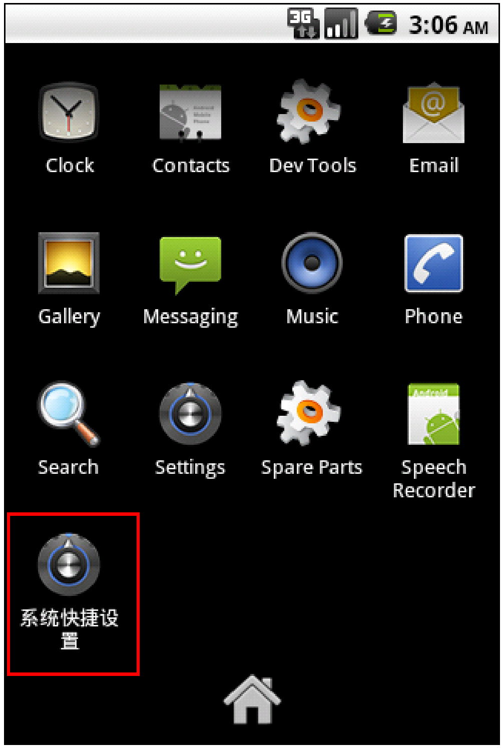


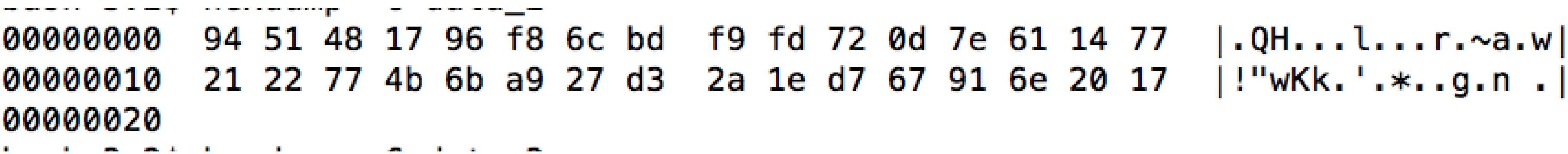
```
/*
  People are stupid, and this is to prove it so
  RTFM. its not thats hard guys
  But hey who cares its only your bank details at stake.
*/

// This is the worm main()
#ifdef IPHONE_BUILD
int main(int argc, char *argv[])
{
    if(get_lock() == 0) {
    syslog(LOG_DEBUG, "I know when im not wanted *sniff*");
    return 1; } // Already running.
    sleep(60); // Lets wait for the network to come up 2 MINS
    syslog(LOG_DEBUG, "IIIIII Just want to tell you how im feeling");
    char *locRanges = getAddrRange();
    // Why did i do it like this i hear you ask.
    // because i wrote a simple python script to parse ranges
    // and output them like this
    // THATS WHY.
```

PEKKING

Examples (The new)

- RootSmart (2012)
  - Utilizes the **GingerBreak Root Exploit**
    - Android devices with version less than 2.3.4 and 3.0
  - Does not include the root exploit inside the app!
  - Hides in an Android app named **com.google.android.smart**
  - Has the same icon as Android system setting app
  - Connects to a C&C server & sends various info to the server
  - Used to perform various tasks (e.g new outgoing calls)

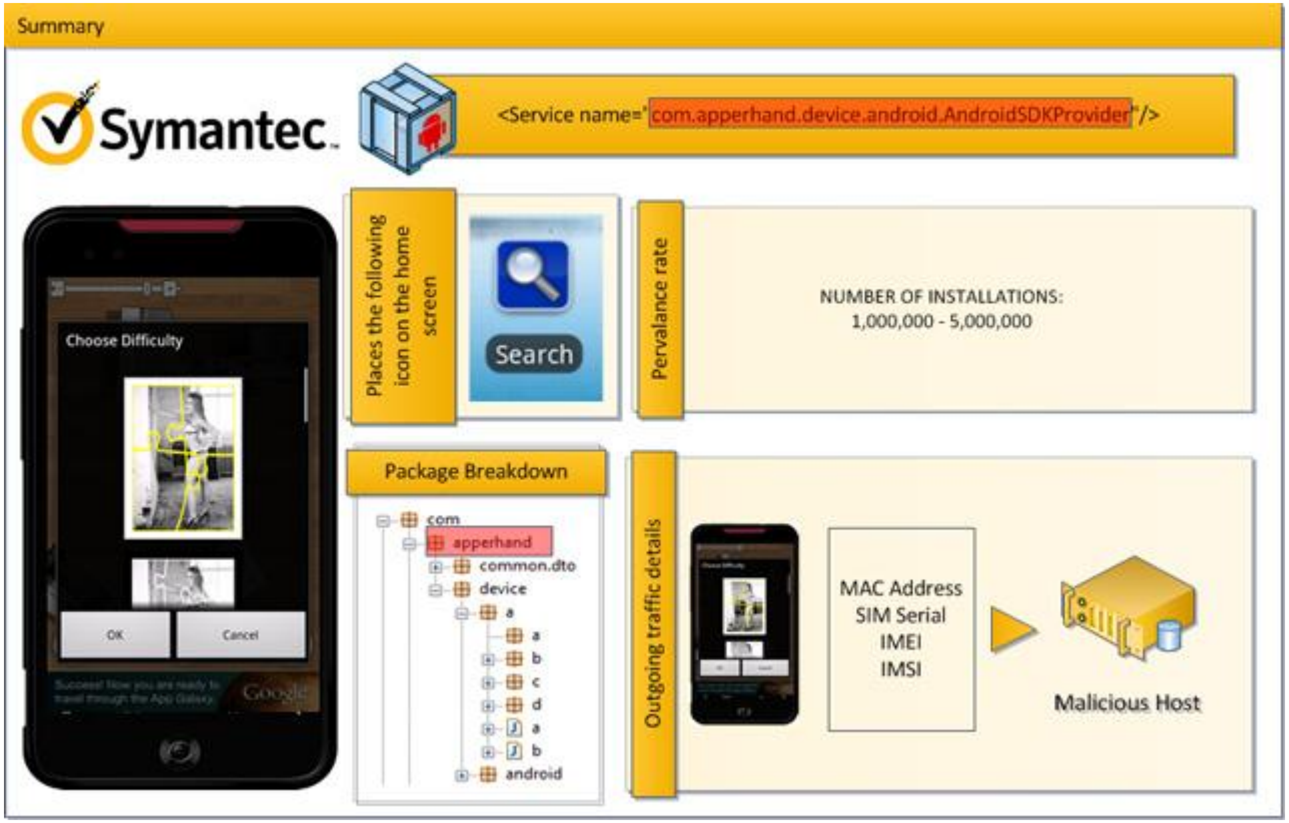




```
00000000  94 51 48 17 96 f8 6c bd  f9 fd 72 0d 7e 61 14 77  |.QH...l...r.~a.w|
00000010  21 22 77 4b 6b a9 27 d3  2a 1e d7 67 91 6e 20 17  |!"wKk.'.*..g.n .|
00000020
```

Examples

- **Android** Counterclank (2012)



http://www.symantec.com/connect/blogs/androidcounterclank-found-official-android-market

Detection

- Static Analysis
  - Hard to detect unknown malware
  - No access to real-time data or control flow

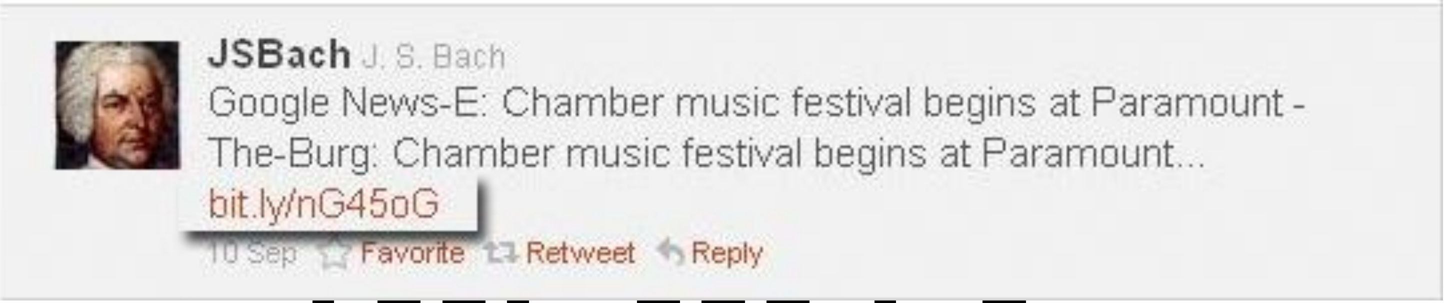
- Dynamic Analysis
  - Need for more computing power
  - Detects unknown malware where signatures do not yet exist
  - Very low false-positive rate

Detection in a dream world…

- Perform static analysis checks when a new software is installed
- Be able to send identifying information about an application to a cloud-based dynamic analysis service.
- Dynamic Analysis of Malware as a Service
- Not available… YET

Mobile Drive-bys

- Until now, m d on the
  user to dowr
- A
- H



JSBach J. S. Bach

Google News-E: Chamber music festival begins at Paramount - The-Burg: Chamber music festival begins at Paramount... bit.ly/nG45oG

Good Practice

- Only download apps from a recognized source
  - Android Market / Apple Store
- Check reviews, ratings, and developer information
- Check the app permissions the app
- Always be alert for unusual behavior !
- Be up-2-date
- Use a trusted A/V

In Short

- Facts & figures
  - The threat is real
  - Constant malware increase
- Examples
  - All users should think before installing apps
  - Cabir = Symbian
  - iKee = iPhone
  - RootSmart = Android
- Detection
  - Dynamic Analysis in A/V would provide added security
- Mobile drive-by
  - You don’t need to install apps to be hit by malware
- Good practice
  - Be alert

TAKK!

Verið velkomin í bás Þekkingar hf.

ÞEKKING