SymbOS Malware Classification Problems

Vesselin Bontchev, anti–virus researcher
FRISK Software International
Postholf 7180, 127 Reykjavik, ICELAND
E–mail: bontchev@complex.is

SymbOS Malware Classification Problems

- Introduction
- The Problems
- Identifying SymbOS Malware
- SymbOS Identification Tools
- Conclusion
- Questions

Introduction

- Millions of Smart Phones
- Symbian Has Roughly 60% of the Market
- Since 2004 SymbOS Malware Numbers Have been Increasing Exponentially
- Still Not a Huge Problem
  - Not clear whether it will become one
- Malware Is Primitive but Causes Peculiar Problems

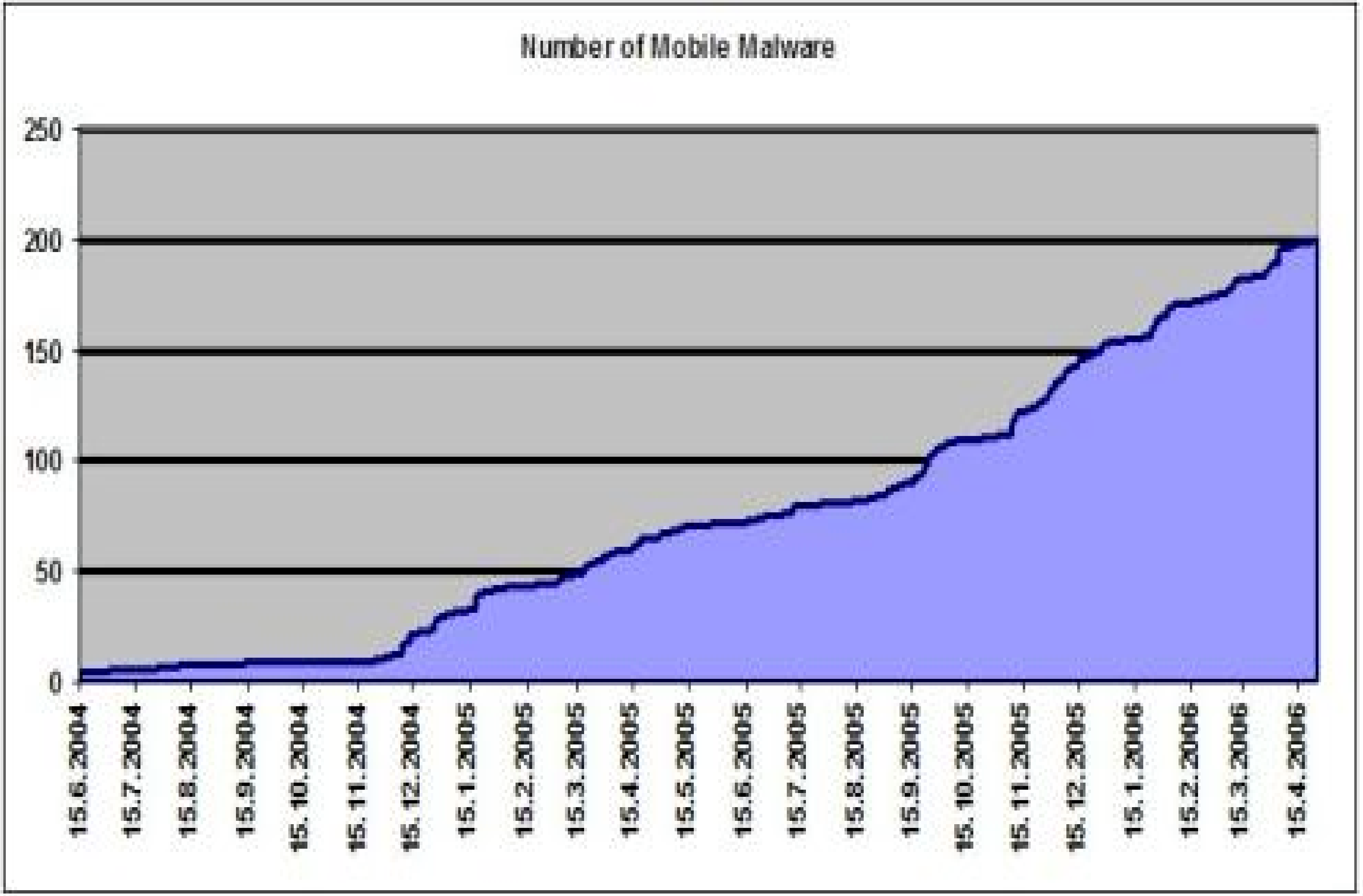

Image Copyright © F-Secure Corporation

The Problems

- The Core of the Problem
  - In Symbian, software is installed *only* as SIS files
  - They are essentially archives
  - The closest analogy is MSI files in Windows
  - Each SIS package contains a set of files
- What Is SymbOS Malware?
  - The set of files in the malicious SIS package
  - Many of them are not executable and/or not directly malicious

The Problems - Continued

- Code Similarity Doesn’t Work Well
  - Sometimes damage is caused by non-executable (icon or font) files
  - Sometimes variants differ only in the non-executable (or non-malicious) files of the sets
- Multi-Droppers
  - Some malicious SIS files just drop a collection of other (known) malicious SIS (or executable) files
  - In which family to classify them?
    - “Multidropper” is lame - contrary to the CARO Naming Scheme and cannot be reported on the infected device

The Problems - Continued

- Multiple Droppers
  - **`SymbOS/Skulls.{O,P,T,U,X,AB,AD,AE,AH,AK,AL,AN,AQ,AW,BA,BB,BC,BD,BE,BF,BG,BK}`** drop the same thing - plus different legitimate files
  - No equivalent in the macro malware world
  - Require different disinfection procedures
  - The CARO Naming Scheme does not support multiple droppers for the same malware variant

The Problems - Continued

- Multiple Ways of Dropping
  - Executable files
    - Recognizers
    - Overwrite popular software
    - Wait for the user to run it
    - Run on install
  - SIS files
  - Automatic installation of SIS files

The Problems - Continued

- Paths Matter
  - Zero-length files can be malicious
  - Valid ROM images can be malicious
  - Fonts can be malicious
- SIS File Infection
  - So, file contents & paths in the SIS package identify the SymbOS variant, huh?
  - Nope - **`Velasco.A`**, **`CommWarrior.Q`**
  - Undistinguishable from Trojanized packages

The Problems - Continued

- Packages Differing Only in Their Pop-Up Messages
  - The pop-up message is a file in the SIS package but doesn’t exist on the device
  - Are they different variants?
    - They have different behavior, so, yes
    - But can’t be distinguished on the infected device

The Problems - Continued

- Different SIS Files Can Install the Same Thing
  - Two archives containing the same files can be different; e.g., if the files are in different order
  - Other differences are also possible
  - Ergo - external identification of SIS files is unreliable
- Malware Combinations
  - 32 possibilities - too many to show here; see the paper
  - In most cases (20) it is not clear in which family to classify the malware

Identifying SymbOS Malware

- Why It Is Important
- SIS File Identification
  - Not reliable - but desirable and necessary
- Identifying as Sets of Files
  - Lengths
  - Paths
  - Checksums
  - Flags
- Identification Problems

Identification Problems

- Mismatch Between the SIS File Contents and the Installed Files
  - Installation messages
  - Localization
  - Drive selection
  - Installing on invalid drives (**`CardTrap.G`**)
- SIS Files Can Drop Only Non-Essential Things – or Nothing
  - Fonts
  - Icons
  - **`SISCONFIG`**
  - Remove files on uninstall

Identification Problems - Cont.

- Corrupted SIS Files
  - **`Drever.C`**
- Large File Sets
  - Very unlike the macro malware case
  - Large sets in the SIS file (**`CardTrap.H`** - 543 files!)
  - Large sets on the device (thousands of files!)
  - Lots of non-malicious files in the malicious SIS package
  - Different algorithms are needed

SymbOS Identification Tools

- SIS Unpacker
  - UnMakeSIS
  - SisView
  - UnSIS
  - Not good enough
- Perl
- DeSIS
- Ident
- SISID

Ident Output - Raw

```
    Name:
    Description:
    Ident:

     55465 6B854F2171CCA50F49D1ACE2D454065A ? Doom_2_wad.sis
     39688 AF018176F6AFEE80666E8ADA7B615198 ? C/ETel.dll
     35288 BC6DDE1954FFC938E5D85237A43B0627 ? C/etelmm.dll
      7332 1AB8AE3F472807EC8BA4A0B720215FE5 ? C/etelpckt.dll
     11952 5770B35E769E08A1CB9BE3B4DC8D313F ? C/etelsat.dll
     27162 BDAE8A51D4F12762B823E42AA6C3FA0A ? Sis components/Commwarrior.B.sis

Comments:
```

Ident Output - Processed

```
Name: trojan://SymbOS/DoomBoot.A
Description: http://www.f-secure.com/v-descs/doomboot_a.shtml
Ident:

 55465 6B854F2171CCA50F49D1ACE2D454065A S Doom_2_wad.sis
 39688 AF018176F6AFEE80666E8ADA7B615198 E C/ETel.dll
 35288 BC6DDE1954FFC938E5D85237A43B0627 E C/etelmm.dll
  7332 1AB8AE3F472807EC8BA4A0B720215FE5 E C/etelpckt.dll
 11952 5770B35E769E08A1CB9BE3B4DC8D313F E C/etelsat.dll
 27162 BDAE8A51D4F12762B823E42AA6C3FA0A E Sis components/Commwarrior.B.sis

Comments:
1) All of these DLL files can cause the phone disabling effect; I don't know
   why McAfee's scanner doesn't detect any of them.
2) The file Commwarrior.B.sis contains the CommWarrior.B virus, to be announced
   later.
```

SISID - Database Format

```
# Droppers:

dropper://SymbOS/Cabir.AB      E1F94DC5557B7D9371D370BF4FDF2393 Comment
dropper://SymbOS/Cabir.B       98F7CFD42DF4A01E2C4F2ED6D38C1AF1
dropper://SymbOS/CommWarrior.C 91C732E3E378B39BADDD9CD1CED7C490

# Garbage:

garbage://SymbOS/Cabir.K       07782CBA4E878EA8BBAF7B7AAF2D46A5

# Trojans:

trojan://SymbOS/AppDisabler.A  A4A60F425128B5C9BC94BABF5ABCBDA6
trojan://SymbOS/AppDisabler.B  DC9F545934281D209C2A4CC88339CF8D
```

SISID - Continued

- Sample output:

```
./CARIBE.SIS       virus://SymbOS/Cabir.A
./Sudoku.SIS       BB4C060C873690840BA3D8D3C859CDF0
./symbian.sis      trojan://SymbOS/AppDisabler.A
```

- Availability:
  - Program:

http://www.people.frisk-software.com/~bontchev/sisid.zip

  - Database:

http://www.people.frisk-software.com/~bontchev/sisid.dat

Other Tools

- Work in Progress
  - Combine the different tools into a single one
- MBM -> BMP Convertor
- IDA Pro disassembler
- Still Looking for:
  - AIF and RSC viewer
  - Emulator/Simulator
  - Debugger

Conclusion

- Questions?