Mobile App Moolah:
Profit taking with Mobile Malware

Jimmy Shah
Mobile Security Researcher

Contents

- Who we are
- Mobile malware
- Modern for-profit malware
- Examples

Who we are

- Mobile Antivirus Researchers
- My team and I specialize in mobile malware and threat analysis on existing(J2ME, SymbOS,WM, Apple iOS, Android) and upcoming mobile platforms.
- We work with a number of large mobile network operators.

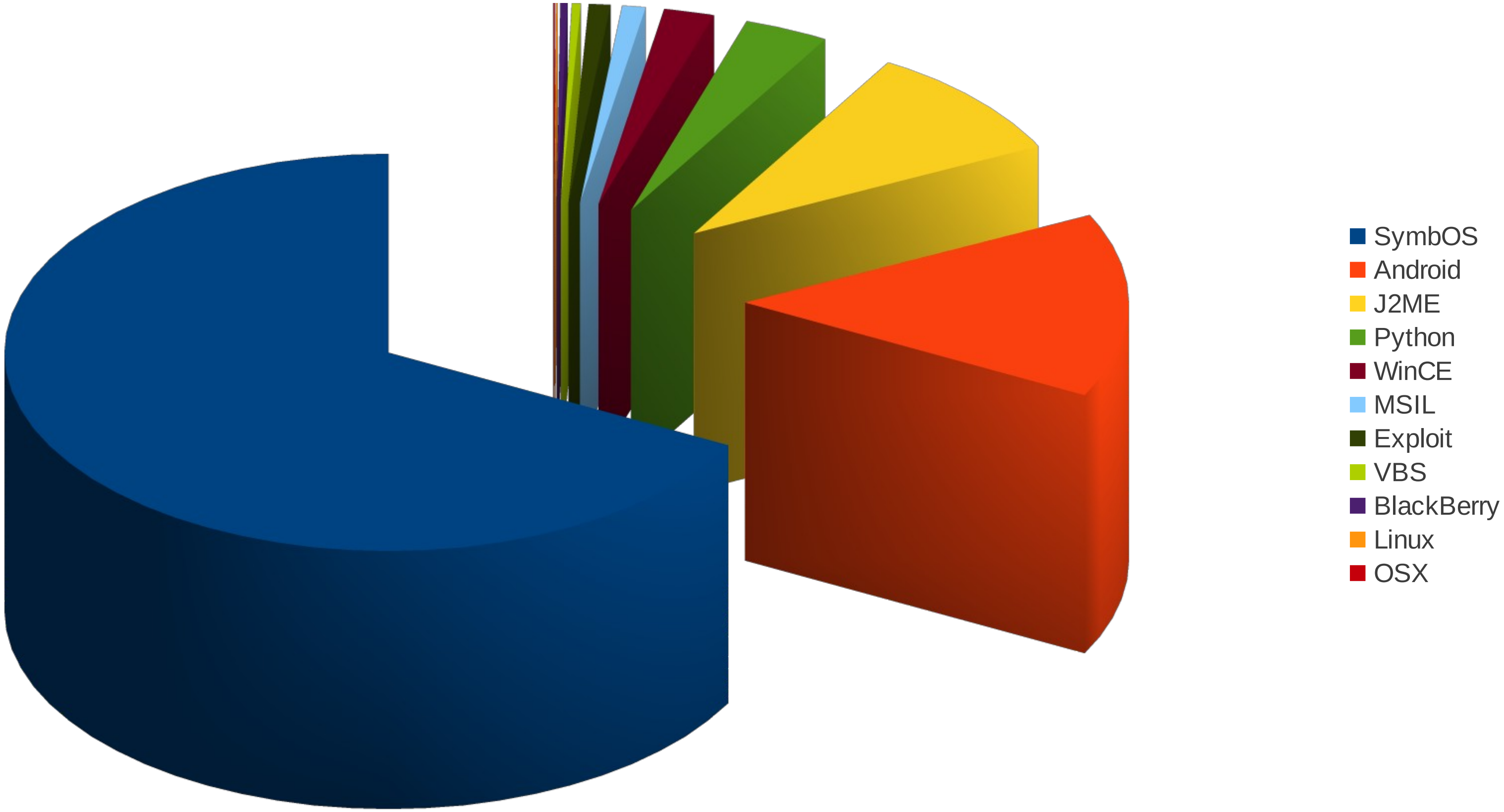
Mobile Malware

In the Wild

Historical For-profit malware

Trends

In the Wild



1300+ variants

Mobile Malware

In the Wild

Historical For-profit malware

Trends

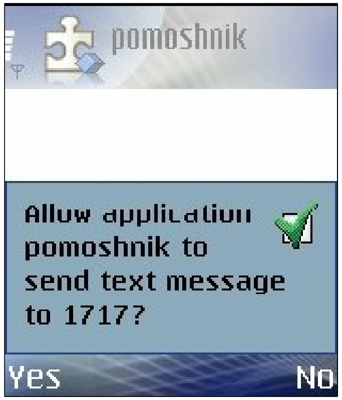
Historical For-profit malware

Simple

Complex

J2ME/Wesber.A

- What it does
  - No GUI, almost pure for-profit J2ME trojan
  - Program that disguises itself as an assistant program
  - It contains two jpg files within itself.
- Profit?
  - Sends SMS to premium rate number to purchase mobile phone games.
  - Presumably written to increase sales for the mobile site



pomoshnik

Allow application pomoshnik to send text message to 1717?

Wesber installation prompt
(Symbian OS, S60 UI)

Jpg files included but not displayed to user.

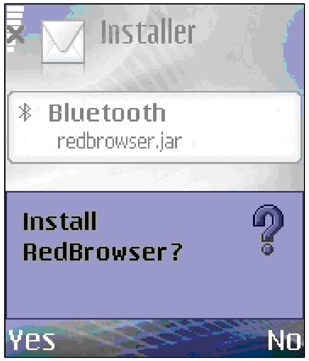
Historical For-profit malware

Simple

Complex

J2ME/Redbrowser.A

- What it does
  - First reported J2ME trojan(2006)
  - Pretends to access WAP web pages via SMS messages
  - Written using the MIDletPascal programming tool
- Profit?
  - In reality, it attempts to send SMS messages to Premium Rate SMS numbers
  - Eventually spawned a large number of J2ME malware/variants



Installer

Bluetooth
redbrowser.jar

Install RedBrowser?

Yes No

RedBrowser installation prompt
(Symbian OS, S60 UI)

> “Carefully read following description of RedBrowser program This program allows viewing WAP pages without GPRS connection. RedBrowser connects to SMS server of your operator (MTS, BEELINE, MEGAFON). Page is loaded by receiving coded SMS. First 5Mb (650 SMS) of traffic are provided free of charge in test mode. ATTENTION!!! Program RedBrowser works ONLY on above mentioned cellular operators.”

description text (original text in Russian)

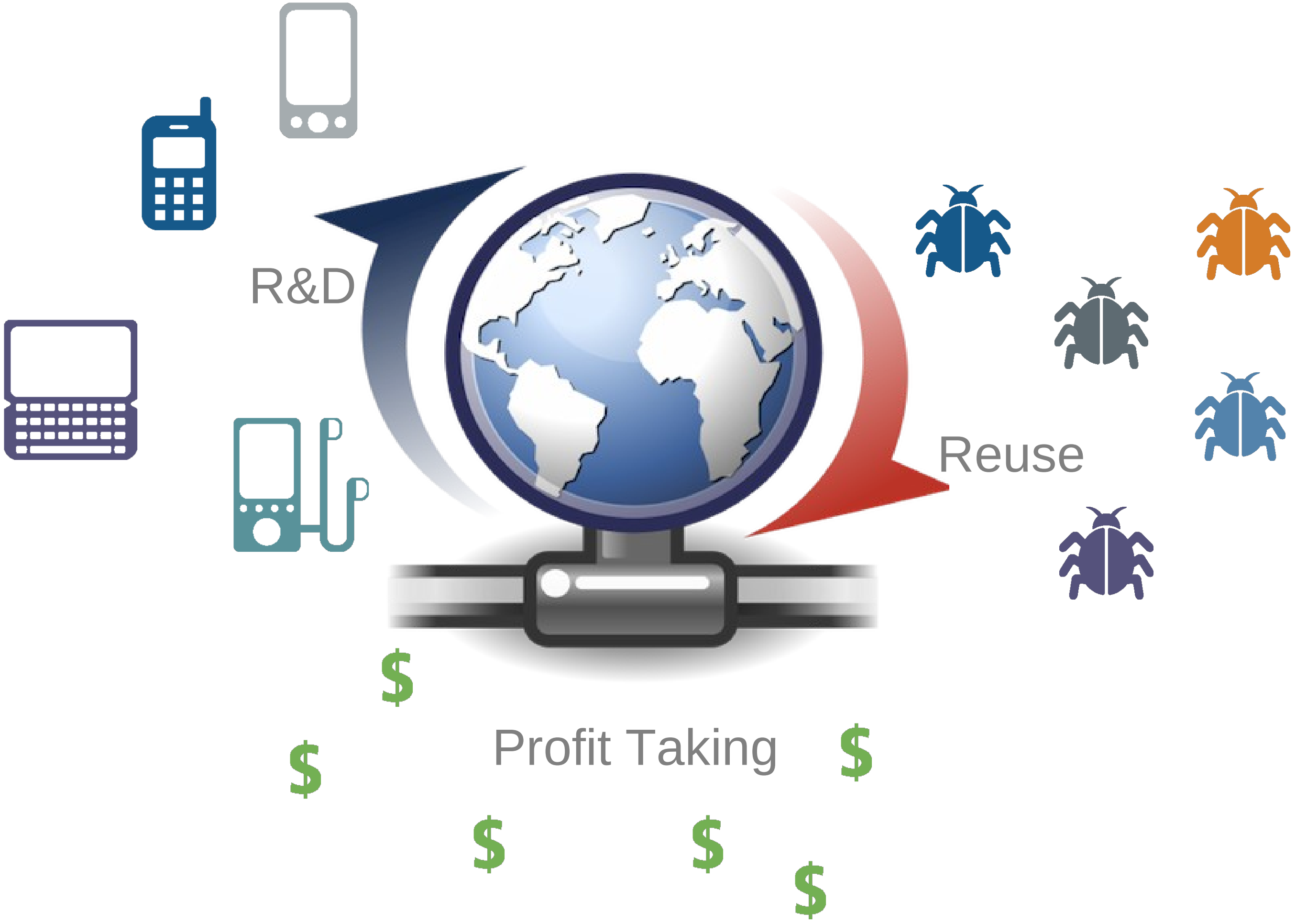
Mobile Malware

In the Wild

Historical For-profit malware

Trends

Trends – Mobile Malware Lifecycle



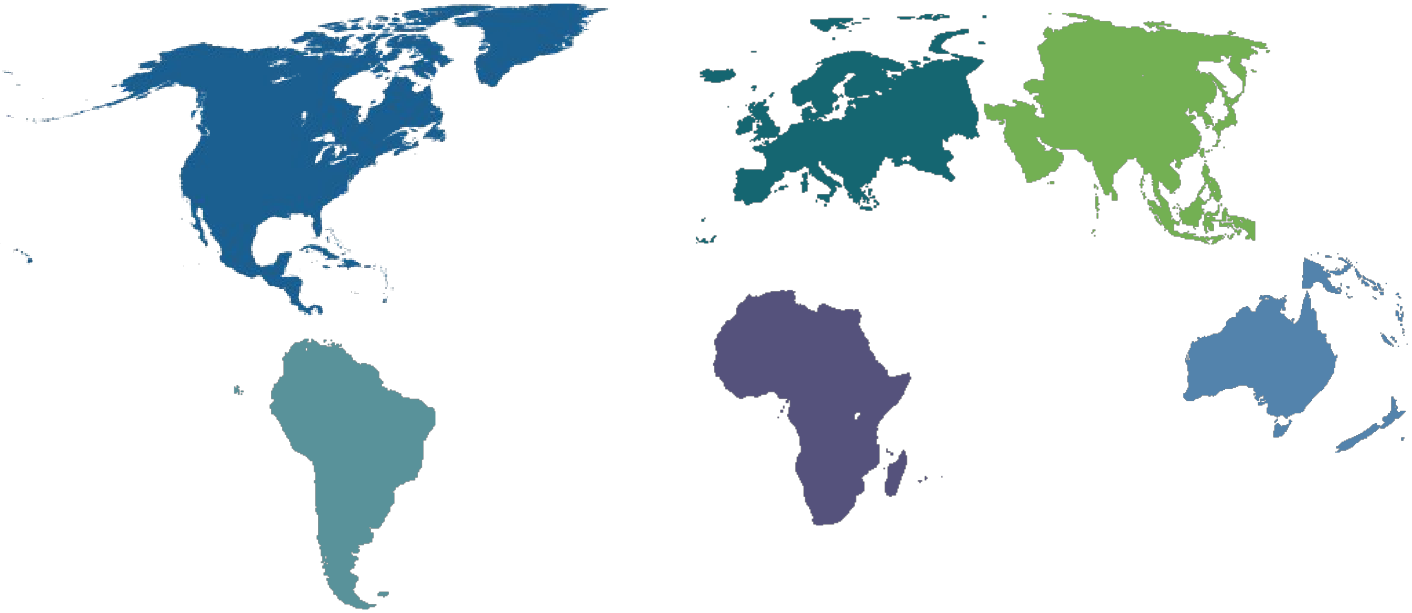
Modern for-profit malware

For-profit malware by geographical region

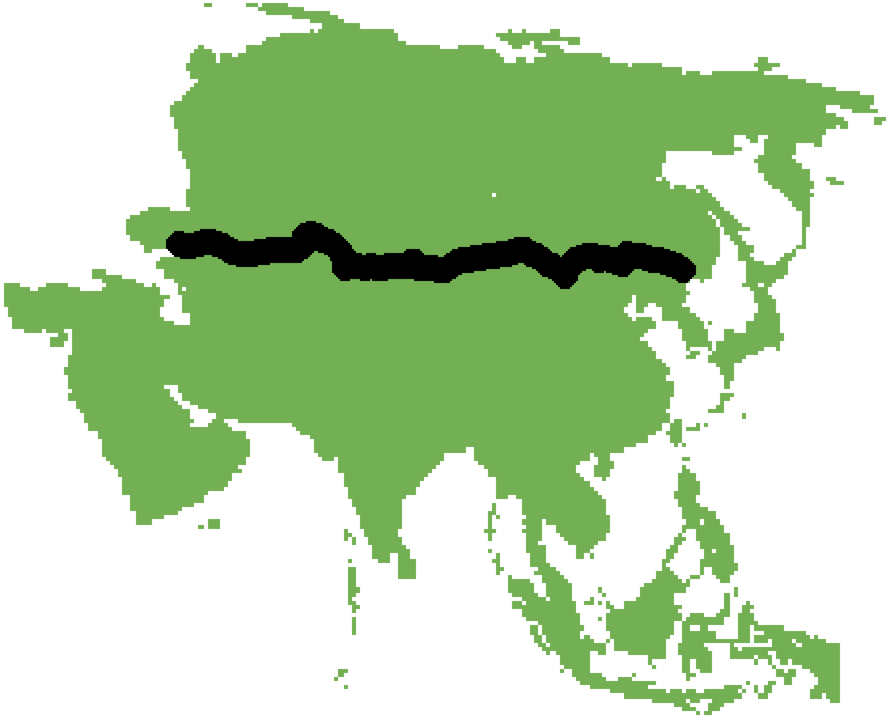
How they Profit

Detection/Analysis Evasion methods

For-profit malware by geographical region



For-profit malware by geographical region



100+ variants

Primarily J2ME w/ Android

SMS sending trojans

200+ variants

J2ME, Symbian, Android

SMS trojans, privacy stealing

Modern for-profit malware

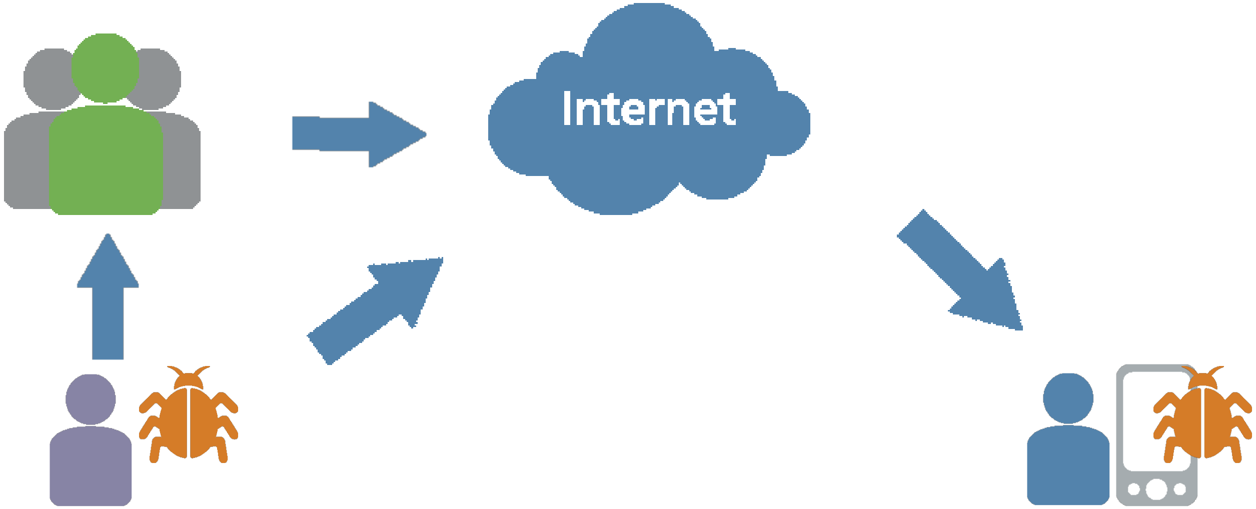
For-profit malware by geographical region

How they Profit

Detection/Analysis Evasion methods

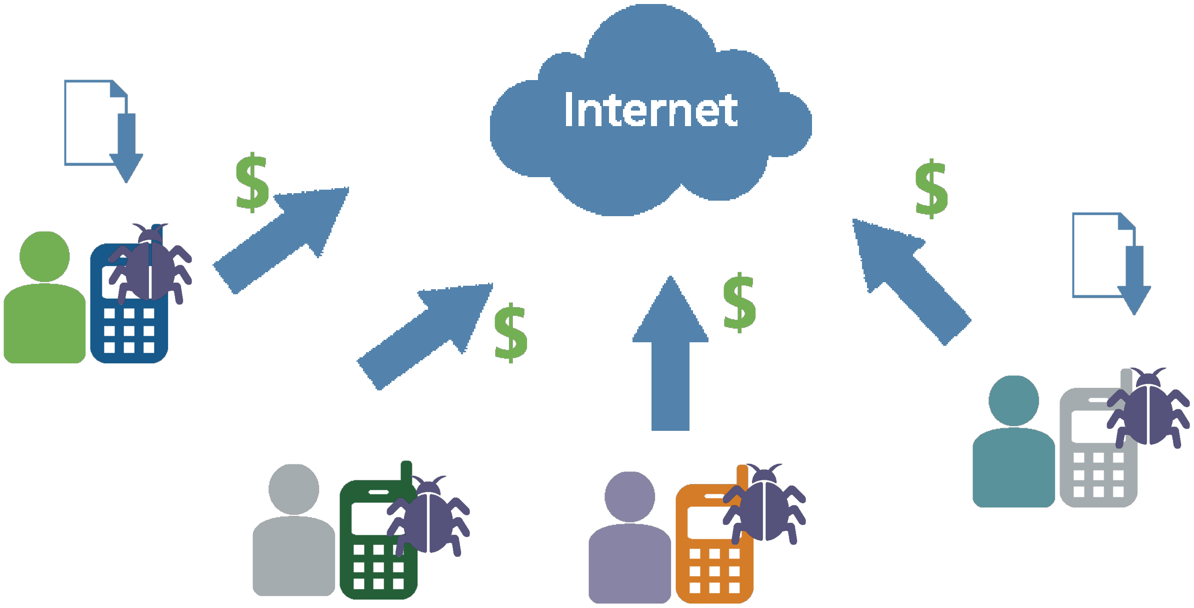
How they profit

- Production
  - Independent malware authors
  - Produce malware for sale
- Distribution
  - Forums, freeware sites, pirated software sites



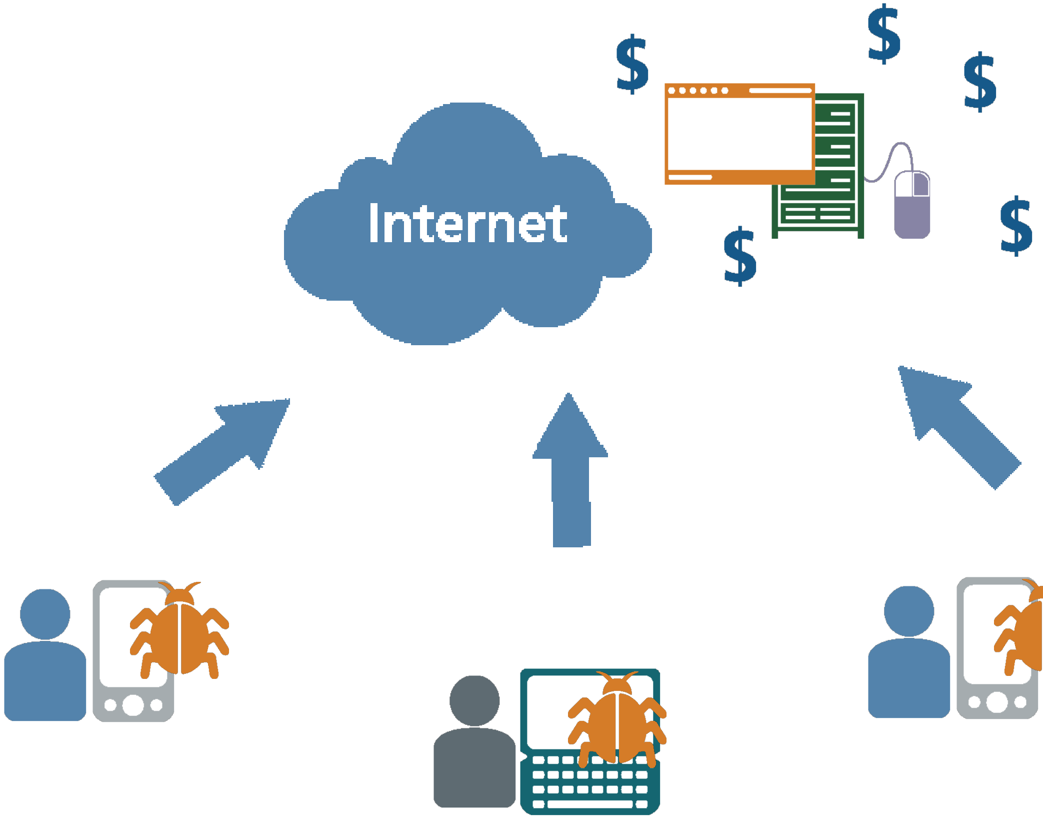
How they profit

- **Where's the money?**
  - Premium Rate numbers
    - Ringtones, downloads, data services/newsfeeds



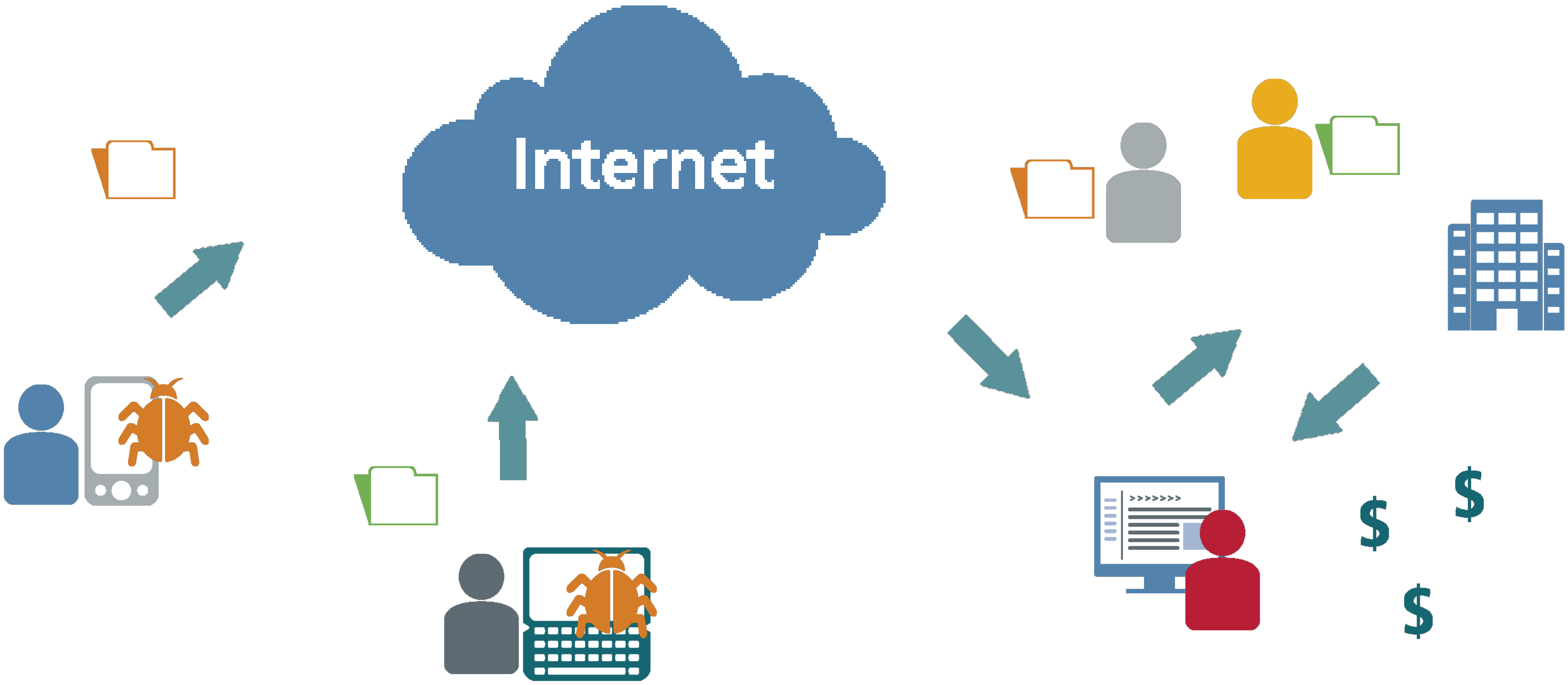
How they profit

- **Where's the money?**
  - Click Fraud, Black Hat SEO
    - Traffic generation, pay-per-click(PPC) ads



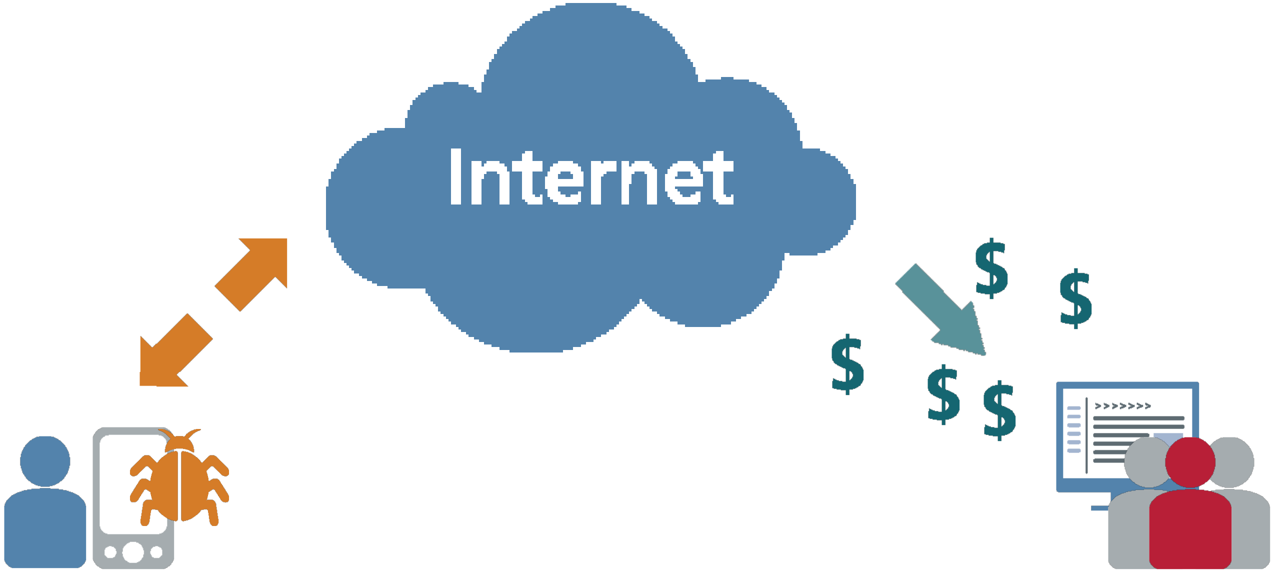
How they profit

- **Where's the money?**
  - Stealing, reselling PII



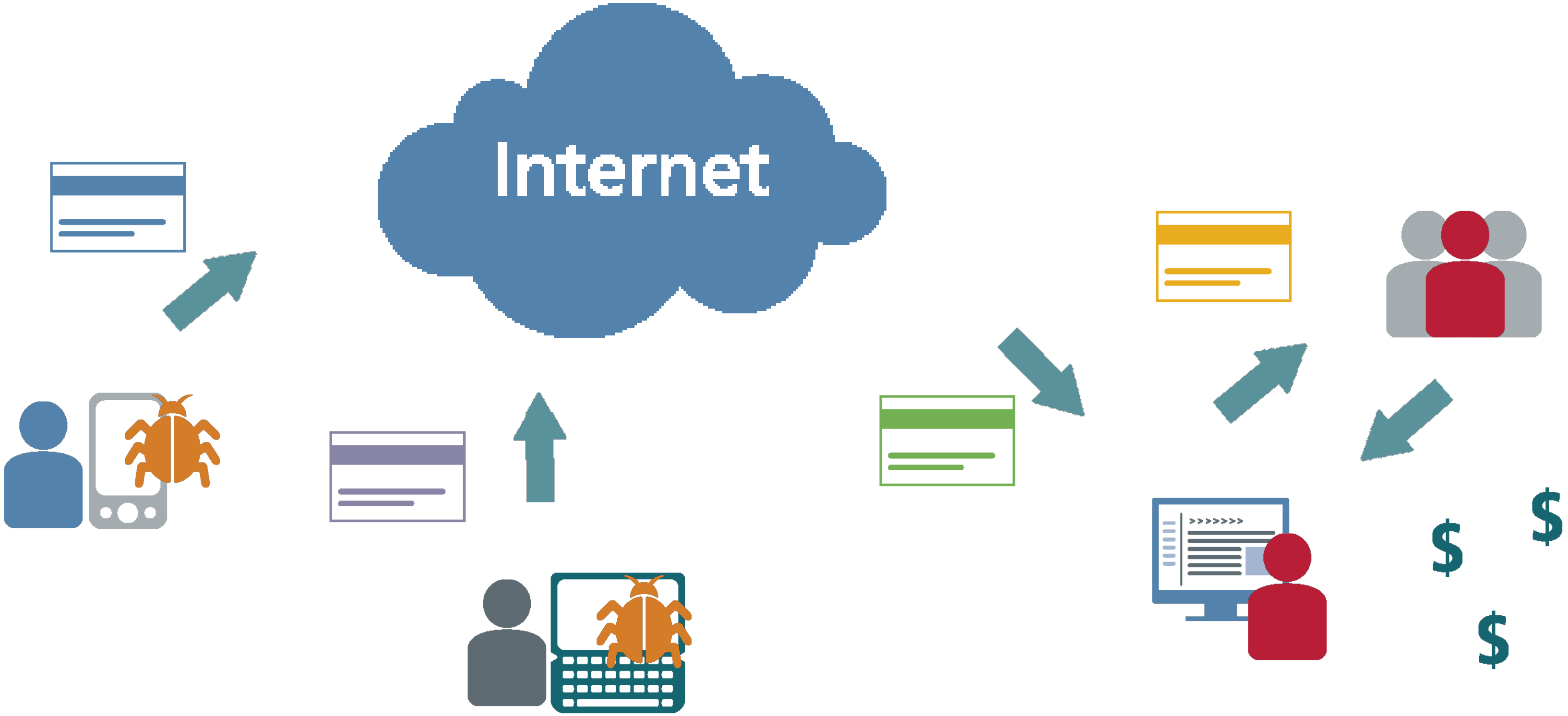
How they profit

- **Where's the money?**
  - SMS phishing, Injecting fake SMS
    - Download malware/adware, Drive traffic



How they profit

- **Where's the money?**
  - Stealing Accounts(Skype, QQ, SIM balances)
    - Using partner businesses to cash out



Modern for-profit malware

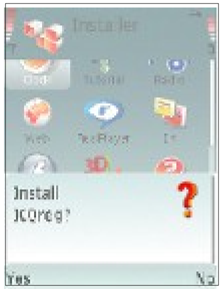
For-profit malware by geographical region

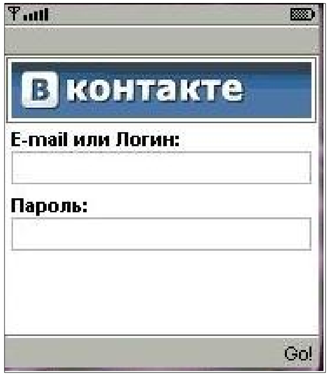
How they Profit

Detection/Analysis Evasion methods

Detection/Analysis Evasion methods

- Infection of/Injection into clean apps
  - J2ME
    - Chat/IM apps
    - Games
    - Adult entertainment
  - Symbian
    - Chat/IM apps
  - Android
    - Games
    - Chat/IM apps





E-mail или Логин:

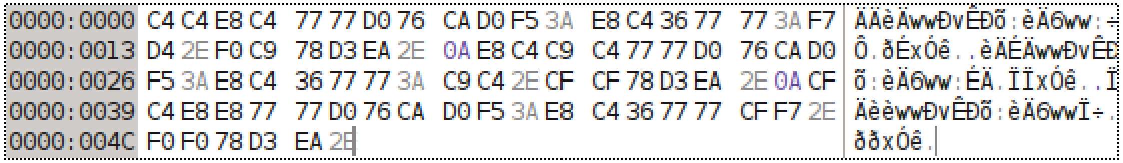
Пароль:

Encryption

- Simple
  - Obfuscations
    - Hiding SMS numbers/message text within plaintext HTML files

```
<link rel="stylesheet" type="text/css" href="/en/shar
ed/core/2/css/css.ashx?sc=/en/us/site.config&amp;pt=cspMscomHomePage&amp;c=cspMscomSiteBrand;cspSearchComponent
;cspMscomFeaturePanel;cspMscomMasterNavigation;[<SMS#>:<MSG>]cspMscomNewsBand;cspVerticalRolloverTab;cspAdControl;cspMscomVe
rticalTab;cspSilverGate" /><script type="text/javascript" src="http//i3.microsoft.com/library/svy/broker.js">
 </script><meta name="SearchTitle" content="Microsoft.com" scheme="" /><meta name="Description" content="Get
product information, support, and news from Microsoft." scheme="" /><meta name="Title" content="Microsoft.c
```

  - Substitution cipher
    - Config file containing encrypted SMS numbers/message text



```
0000:0000 C4 C4 E8 C4  77 77 D0 76  CA D0 F5 3A  E8 C4 36 77  77 3A F7 ÄÄèÄwwÐvÊÐõ:èÄ6ww:÷
0000:0013 D4 2E F0 C9  78 D3 EA 2E  0A E8 C4 C9  C4 77 77 D0  76 CA D0 Ô.ðÉxÓê..èÄÉÄwwÐvÊÐ
0000:0026 F5 3A E8 C4  36 77 77 3A  C9 C4 2E CF  CF 78 D3 EA  2E 0A CF õ:èÄ6ww:ÉÄ.ÏÏxÓê..Ï
0000:0039 C4 E8 E8 77  77 D0 76 CA  D0 F5 3A E8  C4 36 77 77  CF F7 2E ÄèèwwÐvÊÐõ:èÄ6wwÏ÷.
0000:004C F0 F0 78 D3  EA 2E                                           ððxÓê.
```

<SMS#>::**<MSG>**::241.55руб.
<SMS#>::**<MSG>**::173.88руб.
<SMS#>::**<MSG>**::86.00руб.

Encryption

- Complex
  - Symmetric cipher
    - DES

```
byte abyte1[] = k.b;
DESKeySpec deskeyspec = new DESKeySpec(abyte1);
javax.crypto.SecretKey secretkey = SecretKeyFactory.getInstance("DES").generateSecret(deskeyspec);
Cipher cipher = Cipher.getInstance("DES");
b = cipher;
cipher.init(2, secretkey);
```

    - Used by Android/Geinimi to encrypt URL queries and C&C commands
    - Used by Android/DrddreamLite
      - to encrypt/decrypt config file
        - » URLs, next connect time
      - to encrypt/decrypt C&C commands
      - to decrypt root exploits

Reduce security/bypass protection

- Disable Software installation controls
  - WinCE/InfoJack.A turns off the unsigned application prompt, allowing it to perform silent installations

Key	Value
HKEY_LOCAL_MACHINE\Security\Policies\Policies\0000101a	0 = Enable Unsigned Application Prompt 1 = Disable Prompt

- Root vulnerabilities
  - Exploits are used legitimately by users to allow modifying or reflashing new OS versions
  - Android/DrdDream utilizes 2 root exploits to gain a foothold on android devices
  - Android/DrddreamLite uses very similar, 1 identical, root exploits
- Jailbreaking
  - Not In the Wild, used only in PoCs
    - e.g. Eric Monti's modified jailbreak at Toorcon 2010

Examples of for-profit malware

J2ME

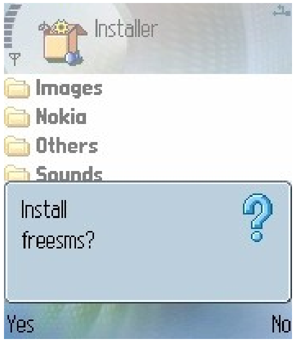
Symbian

Android

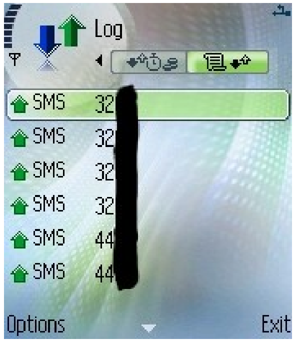
Other

J2ME/SMSFree

- **What it Does**
  - Pretends to be a variety of legitimate apps
    - anonymous SMS sender
    - pornographic app
    - free SMS sender
  - **Profit?**
    - Instead of the user's message it sends to a Premium Rate number
    - Country specific SMS messages are sent
      - Russia (5 SMS)
      - Ukraine (4 SMS)
      - Kazakhstan (4 SMS)



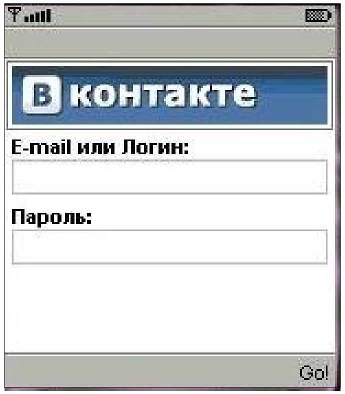
Install freesms?



SMS
SMS
SMS
SMS
SMS
SMS
[redacted]

J2ME/Vkonpass.A

- **What it Does**
  - Pretends to be a mobile client for the VKontakte social network
  - A phishing app, it emails the victim's account details to the attacker



To:	ololoe2010yandex.ru
From:	bork_rulsmail.ru
Subject:	<username>:<password>
Message:	<username>:<password>

- **Profit?**
  - Attackers collect VKontakte user accounts
    - Use trust relationships to spread malware/adware/spyware
    - Resell accounts
    - Blackmail users

Examples of for-profit malware

J2ME

Symbian

Android

Other

Symbian

Simple

Complex

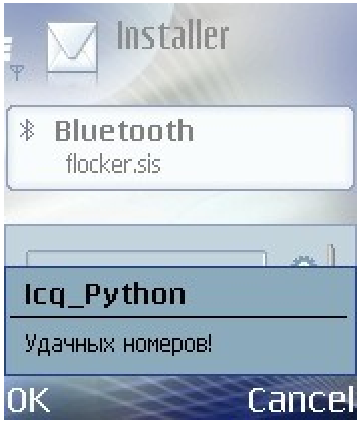
Python/Reclof.A

- **What it Does**
  - Python script designed to run under the S60 Python interpreter
  - Pretends to be a Python client for ICQ
- **Profit?**
  - Sends SMS to premium rate number

```
appswitch.switch_to_fg(u'Phone')#
try:messaging.sms_send('<XXXX>',u'FILES <XXX>')#     ,
except:pass#      ,
```

  - Deletes messages received from the same premium rate number

```
new=sms.sms_messages()#
if len(new)!=0:#
 keypress.simulate_key(63555,63555)#  ← Right button
 keypress.simulate_key(63555,63555)#  ← Right Button
 for id in new:#
  if sms.address(id)==u'<XXXX>':#
   sms.delete(id)#
```


Installer

Bluetooth
flocker.sis

Icq_Python
Удачных номеров!

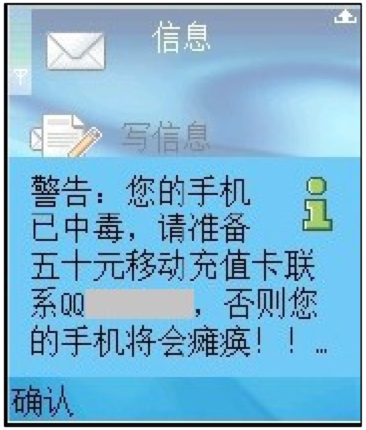
Symbian

Simple

Complex

SymbOS/Kiazha.A

- **What it Does**
  - Distributed as part of a larger collection of malware, SymbOS/MultiDropper.CR
  - Deletes incoming and outgoing SMS messages
- **Profit?**
  - Displays a warning message and attempts to extort money from the user
  - Money is to be transferred as the QQ coin virtual currency



警告：您的手机已中毒，请准备五十元移动充值卡联系QQ[redacted]，否则您的手机将会瘫痪！！…

Warning: Your mobile phone has been infected, please prepare a mobile phone recharge card of 50 Yuan RMB, and contact QQ<*account removed*>, or your phone will be paralyzed!!

SymbOS/SuperFairy.A-B

- **What it does**
  - Adds bookmarks for a smartphone related forum
  - Launches a browser to view the forum
- **Profit?**
  - Generate traffic to the smartphone forum
    - Auto-runs an app that creates the bookmarks

Bookmark title	Translation	URL
<removed> 网 - 手机软件第一站	<removed> Network - the first leg of mobile phone software	http://<removed>.com/?id=<removed>
智能手机大社区	Smart phone community	http://<removed>.com/?id=<removed>
手机主题免费下载	Free downloading mobile phone themes	http://<removed>com/?id=<removed>
手机游戏免费下载	Free downloading mobile phone games	http://<removed>/?id=<removed>

- A second app attempts to download files from the mobile phone forum

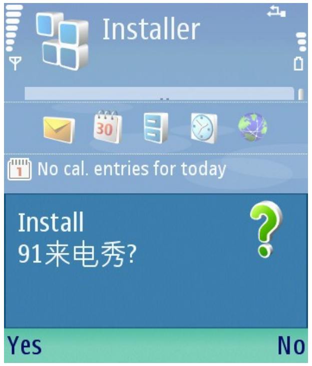
http://<removed>.com:8118/client/symbian/S60v2active.txt

http://<removed>.com:8118/client/symbian/BackgroundUpdata.ini

http://<removed>.com:8118/client/symbian/S60v2StartUpdata.ini

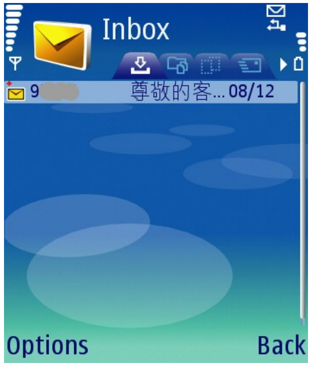
SymbOS/InSpirit.A

- **What it does**
  - Pretends to be “91 calls show”
    - With the “System acceleration patch”
  - Injects a phishing message into the Inbox
  - Text message is spoofed from a Chinese Bank
- **Profit?**
  - Text message directs victim to a mobile banking phishing site
    - “Dear customer, <Bank> reminds you: your account password is entered wrongly for 5 times today. To avoid your fund loss, please login http://<removed>.com for account protection immediately.”

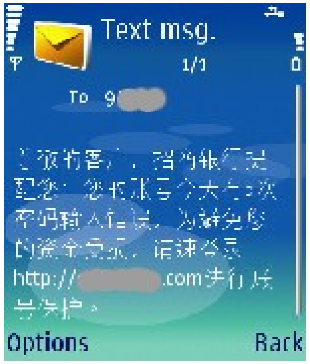

Installer

No cal. entries for today

Install
91来电秀?


Inbox

9[redacted] 尊敬的客...08/12


Text msg.
1/1

To 9[redacted]

尊敬的客户，招商银行提
醒您：您的账号今天有5次
密码输入错误，为避免您
的资金受损，请速登录
http://[redacted].com进行账
号保护。

Examples of for-profit malware

J2ME

Symbian

Android

Other

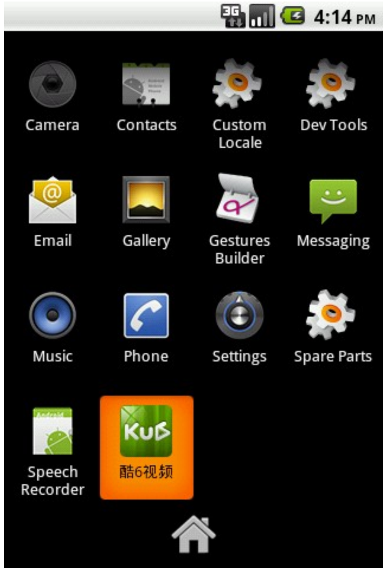
Android

Simple

Complex

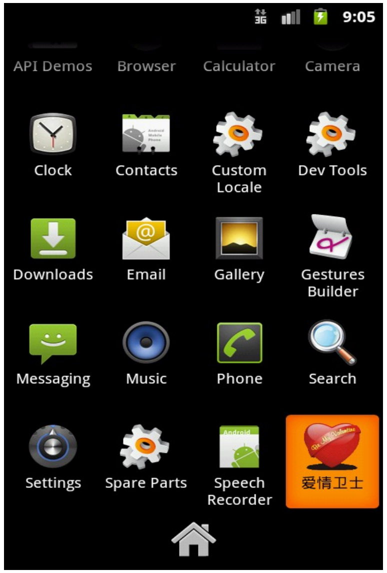
Android/HippoSMS

- **What it does**
  - Malicious code inserted into legitimate app
- **Profit?**
  - Signs up for Premium Rate Services
  - Deletes messages from signed up services
    - No way to know you're subscribed



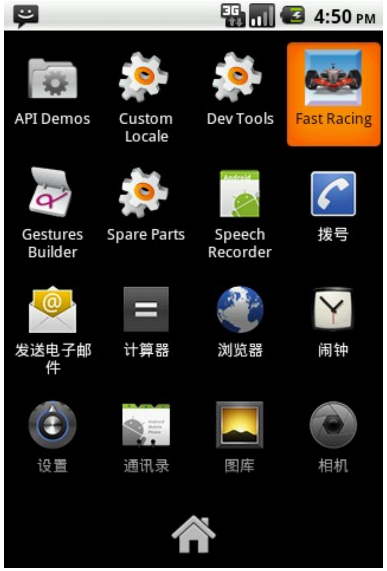
Android/J.SMSHider.A

- **What it does**
  - Malicious code inserted into legitimate app
  - Installs backdoor to listen for commands
  - Sends IMEI, IMSI, GPS coords. to C&C server
- **Profit?**
  - Signs up for Premium Rate Services
  - Deletes messages from signed up services
    - No way to know you're subscribed
  - Installing additional software
    - malware/spyware



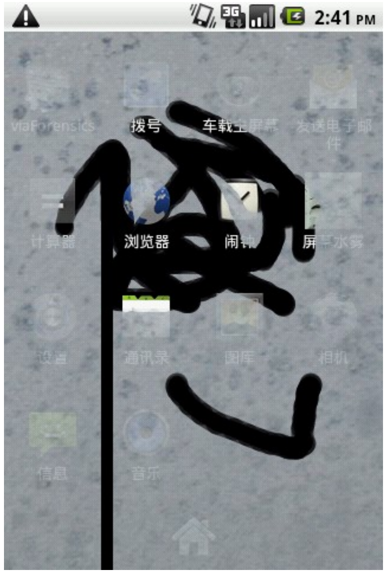
Android/GoldDream

- **What it does**
  - Malicious code inserted into legitimate game
  - Installs backdoor to listen for commands
- **Profit?**
  - Forwards SMS messages
    - Useful for intercepting mTANs
  - Send SMS messages
    - Useful for signing up for Premium Rate Services
  - Installing additional software
    - malware/spyware



Android/SteamyScr.A

- **What it does**
  - Malicious code inserted into legitimate app
  - Requests many additional permissions
  - Sends IMEI, IMSI, and ICCID to C&C server
  - Adds bookmarks for a smartphone related forum
- **Profit?**
  - Generate traffic to a smartphone forum
  - Send SMS messages
    - Useful for signing up for Premium Rate Services
  - Installing additional software
    - malware/spyware
  - Forwarding contacts
    - New targets
  - Traffic generation
    - Loading URLs



Android/Jmsonez.A

- **What it does**
  - Malicious code inserted into legitimate app
  - Requests many additional permissions
- **Profit?**
  - Send SMS messages
    - Useful for signing up for Premium Rate Services
  - Deletes messages from signed up services
    - No way to know you're subscribed

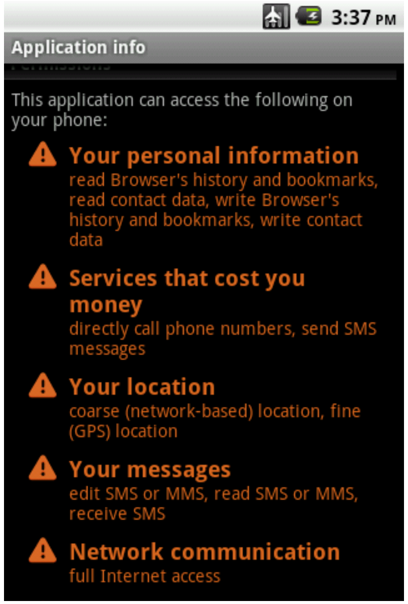
Android

Simple

Complex

Android/Geinimi

- **What it does**
  - Malicious code inserted into legitimate apps/games
    - Most likely inserted manually rather than by a file infector
  - Additional permissions requested
    - Reading/writing SMS, read/write contacts, access GPS, make phone calls, install shortcuts, etc.



3:37 PM

Application info

This application can access the following on your phone:

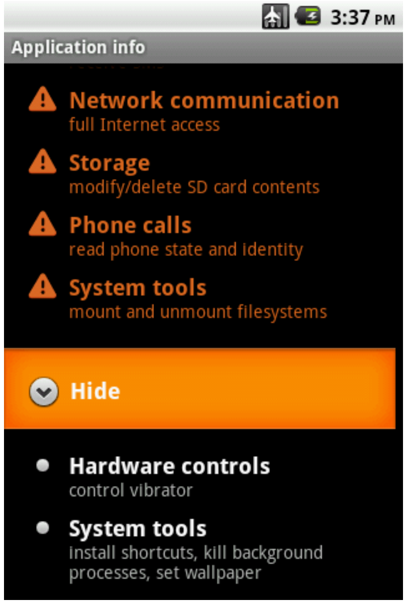
⚠ **Your personal information**
read Browser's history and bookmarks, read contact data, write Browser's history and bookmarks, write contact data

⚠ **Services that cost you money**
directly call phone numbers, send SMS messages

⚠ **Your location**
coarse (network-based) location, fine (GPS) location

⚠ **Your messages**
edit SMS or MMS, read SMS or MMS, receive SMS

⚠ **Network communication**
full Internet access



3:37 PM

Application info

⚠ **Network communication**
full Internet access

⚠ **Storage**
modify/delete SD card contents

⚠ **Phone calls**
read phone state and identity

⚠ **System tools**
mount and unmount filesystems

Hide

● **Hardware controls**
control vibrator

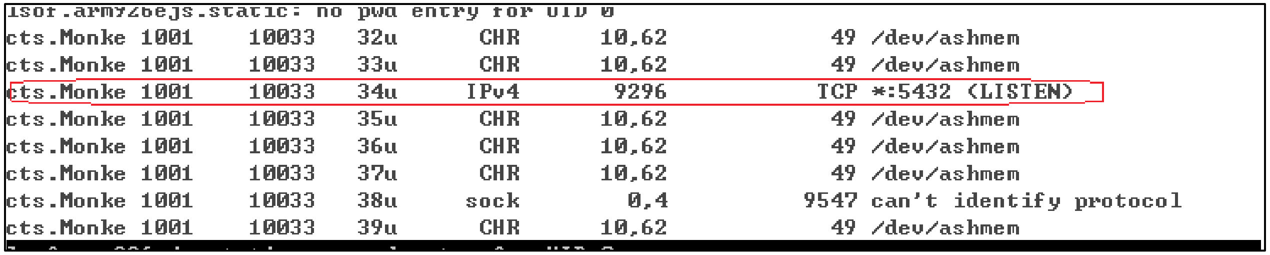
● **System tools**
install shortcuts, kill background processes, set wallpaper

Android/Geinimi, cont.

- **What it does**
  - Encryption
    - backdoor commands, C&C URL queries

```
byte abyte1[] = k.b;
DESKeySpec deskeyspec = new DESKeySpec(abyte1);
javax.crypto.SecretKey secretkey = SecretKeyFactory.getInstance("DES").generateSecret(deskeyspec);
Cipher cipher = Cipher.getInstance("DES");
b = cipher;
cipher.init(2, secretkey);
```

  - Listens on 5432 for handshake, “hi,are you online?”
    - Responds with “yes,I’m online!”
    - Falls back to ports 4501 or 6543
  - Attempts to connect to local backdoor
    - Port 8791



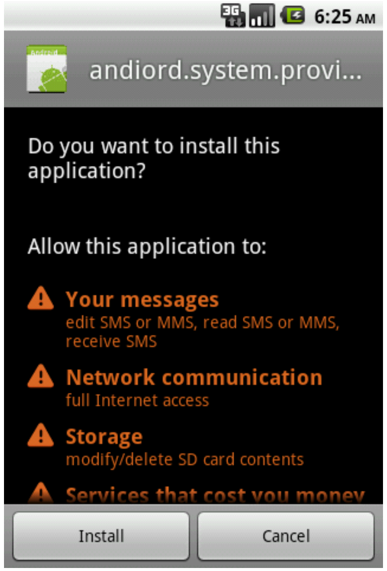
```
lsof.army26ejs.static: no pwd entry for UID 0
cts.Monke 1001     10033    32u       CHR       10,62            49 /dev/ashmem
cts.Monke 1001     10033    33u       CHR       10,62            49 /dev/ashmem
cts.Monke 1001     10033    34u      IPv4        9296           TCP *:5432 (LISTEN)
cts.Monke 1001     10033    35u       CHR       10,62            49 /dev/ashmem
cts.Monke 1001     10033    36u       CHR       10,62            49 /dev/ashmem
cts.Monke 1001     10033    37u       CHR       10,62            49 /dev/ashmem
cts.Monke 1001     10033    38u      sock         0,4          9547 can't identify protocol
cts.Monke 1001     10033    39u       CHR       10,62            49 /dev/ashmem
```

Android/Geinimi, cont.

- **Profit?**
  - Backdoor commands
    - Forwarding SMS to C&C server
    - Installing additional software
      - malware/spyware
    - Forwarding contacts
      - New targets
    - Traffic generation
      - Loading URLs

Android/Tcent.A

- **What it does**
  - Appears to be a system application
  - Sends IMEI and phone number to C&C server
  - Attempts to kill certain security applications
- **Profit?**
  - Signs up for Premium Rate Services
  - Deletes messages from signed up services
    - No way to know you're subscribed



6:25 AM

andiord.system.provi...

Do you want to install this application?

Allow this application to:

Your messages
edit SMS or MMS, read SMS or MMS, receive SMS

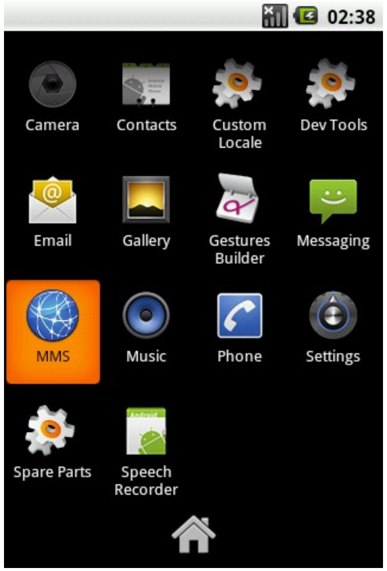
Network communication
full Internet access

Storage
modify/delete SD card contents

Services that cost you money

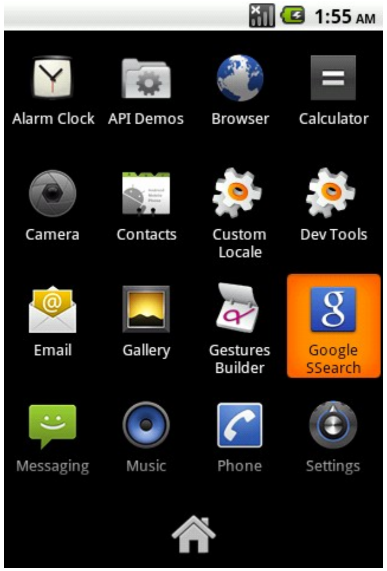
Android/Crusewin.A

- **What it does**
  - Pretends to be an MMS app
  - Sends IMEI and phone number to C&C server
  - Attempts to delete software
- **Profit?**
  - Send SMS messages
    - Useful for signing up for Premium Rate Services



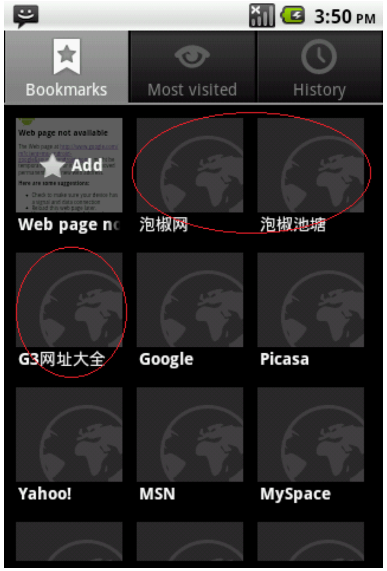
Android/DroidKungfu

- **What it does**
  - Malicious code inserted into legitimate app
  - Installs backdoor to listen for commands
  - Sends IMEI, OS type, Device type, etc. to C&C server
  - Uses two root exploits to install a non-GUI version of the malware
- **Profit?**
  - Installing additional software
    - malware/spyware
  - Traffic generation
    - Loading URLs



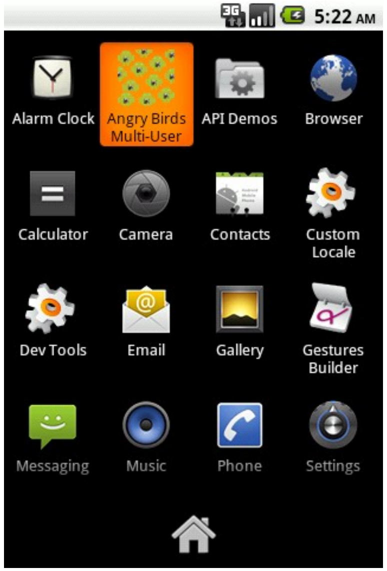
Android/PJApp

- **What it does**
  - Malicious code inserted into legitimate IM app
  - Installs backdoor to listen for commands
  - Sends IMEI, IMSI, SIM serial number, etc. to C&C server
- **Profit?**
  - Send SMS messages
    - Useful for signing up for Premium Rate Services
  - Traffic generation
    - Adding Bookmarks



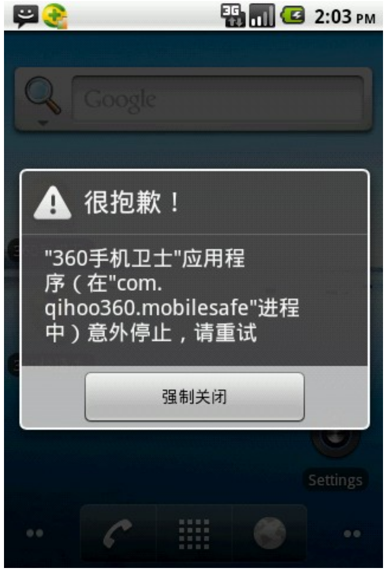
Android/Toplank.A

- **What it does**
  - Trojan pretending to be angry birds update
    - Similar to Oberheide's Twilight preview app
  - Alter/delete browser history
  - Downloads additional APK and loads the code
- **Profit?**
  - Add/delete bookmarks
  - Add/delete shortcuts
  - Display messages
    - phishing



Android/BaseBridge.A

- **What it does**
  - Trojan pretending to be a legitimate app
  - Kills security software
- **Profit?**
  - Send SMS messages
    - Useful for signing up for Premium Rate Services

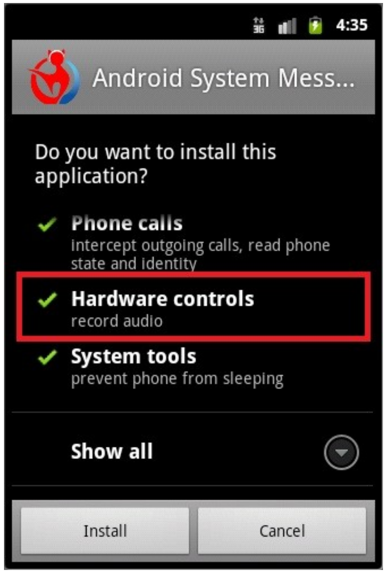


很抱歉！

"360手机卫士"应用程序（在"com.qihoo360.mobilesafe"进程中）意外停止，请重试

Android/Nickispy.A

- **What it does**
  - Records call audio and sends to attacker
- **Profit?**
  - Record sensitive information
    - CC#, SS#, account numbers, PINs
  - Long term attack
    - Attacker waits for opportunity



Android System Mess...

Do you want to install this application?

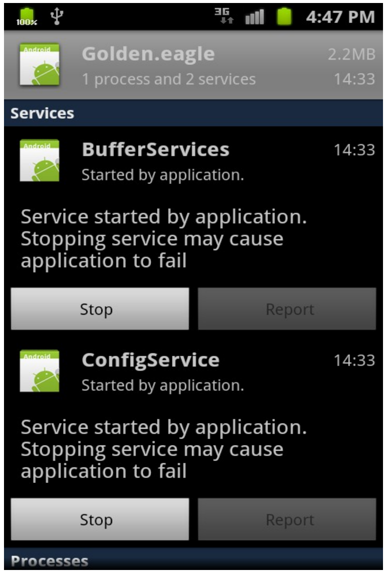
✓ **Phone calls**
intercept outgoing calls, read phone state and identity

✓ **Hardware controls**
record audio

✓ **System tools**
prevent phone from sleeping

Android/GoldenEagle.A

- **What it does**
  - Backdoor trojan
  - Performs commands from C&C
    - Forward SMS, contacts, email
  - Records call audio and sends to attacker
- **Profit?**
  - Send SMS messages
    - Useful for signing up for Premium Rate Services
  - Record sensitive information
    - CC#, SS#, account numbers, PINs
  - Long term attack
    - Attacker waits for opportunity



Golden.eagle 2.2MB
1 process and 2 services 14:33

Services

BufferServices 14:33
Started by application.

Service started by application. Stopping service may cause application to fail

ConfigService 14:33
Started by application.

Service started by application. Stopping service may cause application to fail

Examples of for-profit malware

J2ME

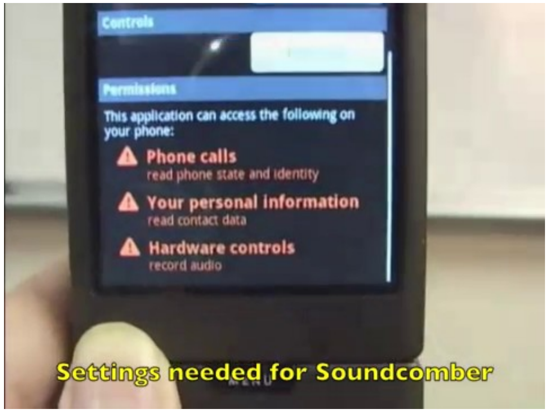
Symbian

Android

Other

Soundcomber

- **What it does**
  - – Set of PoC Android apps
    - Soundcomber
      - – Records phone calls
      - – Identifies relevant portions of IVR
      - – Processes audio for credit card numbers



Controls

Permissions

This application can access the following on your phone:

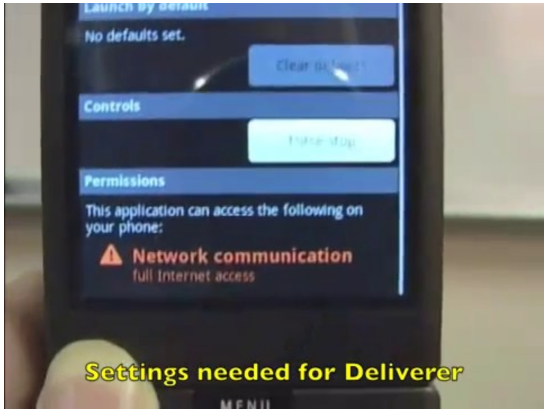
⚠ Phone calls
read phone state and identity

⚠ Your personal information
read contact data

⚠ Hardware controls
record audio

Settings needed for Soundcomber

- Deliverer
  - – Receives extracted information from Soundcomber
  - – Transmits credit card number to attacker



Launch by default

No defaults set.

Clear defaults

Controls

Force stop

Permissions

This application can access the following on your phone:

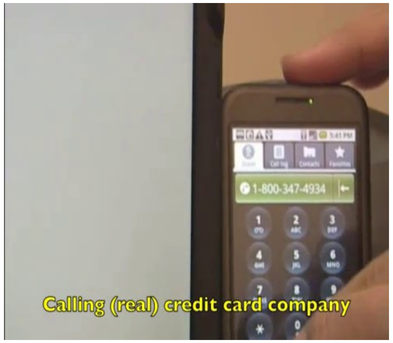
⚠ Network communication
full Internet access

Settings needed for Deliverer

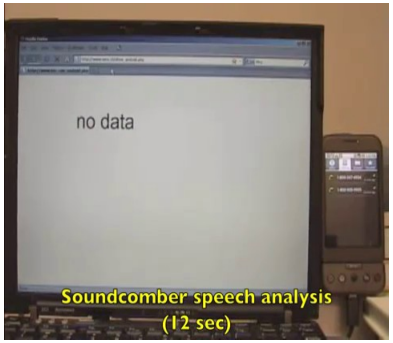
Schlegel, R, Zhang, K, Zhou, X, Intwala, M, Kapadia, A, & Wang, X. (Producer). (2011). Soundcomber demo. [Web]. Retrieved from http://youtu.be/Z8ASb-tQVpU

Soundcomber

- **Profit?**
  - Eavesdrops on voice calls
    - Intercept credit card/account numbers



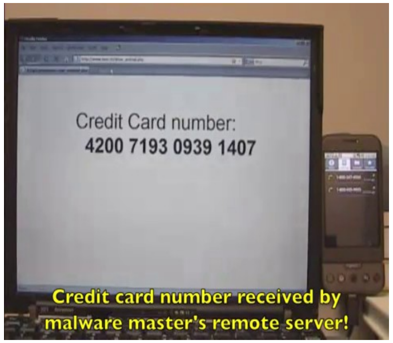
Calling (real) credit card company


no data

Soundcomber speech analysis (12 sec)

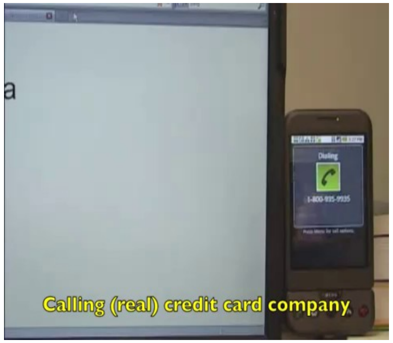
no data

Covert-channel transfer to Deliverer app (3 sec)

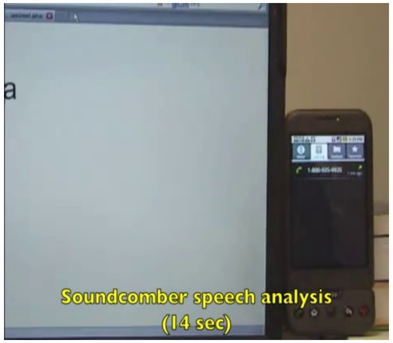

Credit Card number:
4200 7193 0939 1407

Credit card number received by malware master's remote server!

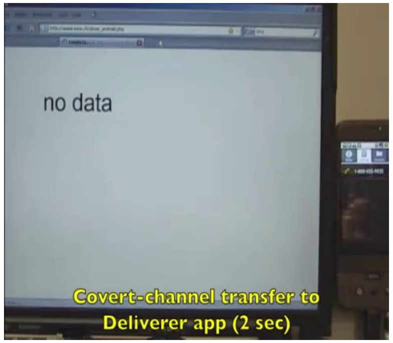
  - Collects DTMF(touch tones)
    - Intercept credit card/account numbers



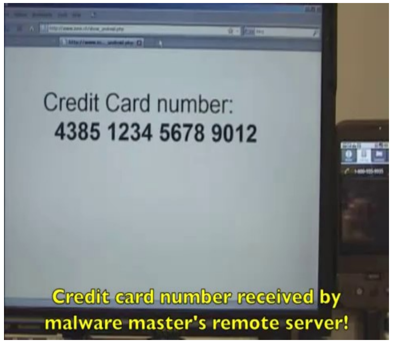
Calling (real) credit card company



Soundcomber speech analysis (14 sec)


no data

Covert-channel transfer to Deliverer app (2 sec)

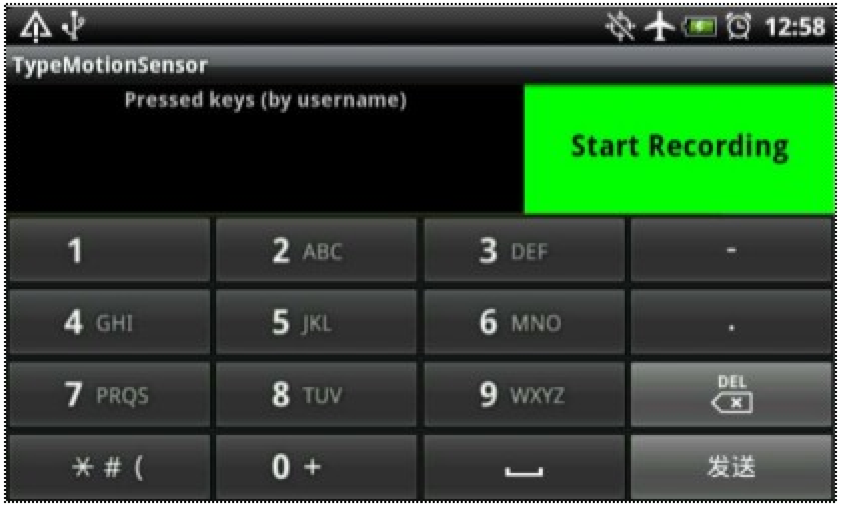

Credit Card number:
4385 1234 5678 9012

Credit card number received by malware master's remote server!

Schlegel, R, Zhang, K, Zhou, X, Intwala, M, Kapadia, A, & Wang, X. (Producer). (2011). Soundcomber demo. [Web]. Retrieved from http://youtu.be/Z8ASb-tQVpU

Touchlogger

- **What it does**
  - Trainer app
    - Detects finger position from accelerometer
    - Digit data used by other app to infer keystrokes


TypeMotionSensor

Pressed keys (by username)

  - Future versions will use other sensors
    - gyroscope
    - Camera
  - Expansion to devices with larger screens

- **Profit?**
  - CC#s, PINs, SS#
    - Other personally identifiable information

TouchLogger: Inferring Keystrokes on Touch Screen from Smartphone Motion
Liang Cai and Hao Chen, University of California, Davis

References

References

- J2ME/RedBrowser.A
  - http://vil.nai.com/vil/content/v_138726.htm
- J2ME/Wesber.A
  - http://vil.nai.com/vil/content/v_140595.htm
- J2ME/SMSFree.A
  - http://vil.nai.com/vil/content/v_145420.htm
- J2ME/Vkonpass.A
  - http://vil.nai.com/vil/content/v_268520.htm
- SymbOS/Kiazha.A
  - http://vil.nai.com/vil/content/v_144207.htm
- Android/Geinimi.A
  - http://vil.nai.com/vil/content/v_342726.htm
- Android/Jmsonez.A
  - http://vil.nai.com/vil/content/v_501748.htm
- Android/Tcent.A
  - http://vil.nai.com/vil/content/v_501599.htm
- Android/Crusewin.A
  - http://vil.nai.com/vil/content/v_501639.htm

References

- Android/DroidKungFu.A
  - http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=522281
- Android/PJApp.A
  - http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=526804
- Android/Toplank.A
  - http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=535360
- Android/BaseBridge.A
  - http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=535367
- Android/J.SMSHider.A
  - http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=527859
- Android/GoldDream.A
  - http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=539671
- Android/HippoSMS.A
  - http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=544065

References

- Roman Schlegel, Kehuan Zhang, Xiaoyong Zhou, Mehool Intwala, Apu Kapadia, and XiaoFeng Wang, "Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones," In Proceedings of the 18th Annual Network & Distributed System Security Symposium (NDSS '11). Retrieved from http://www.cs.indiana.edu/~kapadia/papers/soundcomber-ndss11.pdf
- Roman Schlegel, Kehuan Zhang, Xiaoyong Zhou, Mehool Intwala, Apu Kapadia, and XiaoFeng Wan. (Producer). (2011). Soundcomber demo. [Web]. Retrieved from http://youtu.be/Z8ASb-tQVpU
- Liang Cai and Hao Chen.”TouchLogger: inferring keystrokes on touch screen from smartphone motion.” In Proceedings of the 6th USENIX conference on Hot topics in security (HotSec'11). USENIX Association, Berkeley, CA, USA, 9-9. Retrieved from https://www.usenix.org/events/hotsec11/tech/final_files/Cai.pdf

Acknowledgments

Acknowledgements

- Fyodor Bom of o0o Security Team
- Billy Lee & Tom(潘宣辰) of Antiy Labs
- Roman Schlegel, Kehuan Zhang, Xiaoyong Zhou, Mehool Intwala, Apu Kapadia, and XiaoFeng Wang
- Dr. Xuxian Jiang and his research team at North Carolina State University for their initial discovery of samples of the following malware: Android/DroidKungFu, Android/Toplank.A, Android/GoldDream.A, and Android/HippoSMS.A.
- Zheng Bu of McAfee
- Joey Zhu of Trend Micro

Questions?

McAfee®