

# 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



1100+ variants

# Mobile Malware

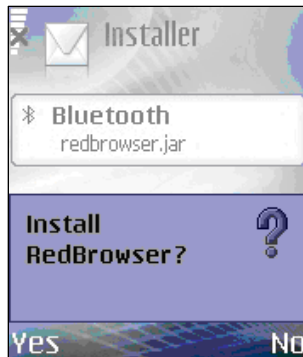


In the Wild

Historical For-profit malware

Trends

- 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

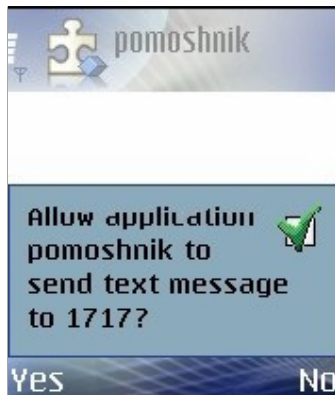


RedBrowser installation prompt  
(Symbian OS, S60 UI)

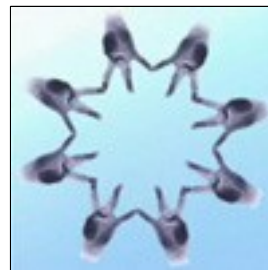
"Carefully read following description of RedBrowser program  
This program allows viewing WAP pages without GPRS connection. RedBrowser connects to SMS server of your operator (MTS, BEELINE, MEGAFON). Page is loaded by receiving coded SMS. First 5Mb (650 SMS) of traffic are provided free of charge in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

description text (original text in Russian)

- 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



Wesber installation prompt  
(Symbian OS, S60 UI)



Jpg files included but not displayed to user.



# Mobile Malware

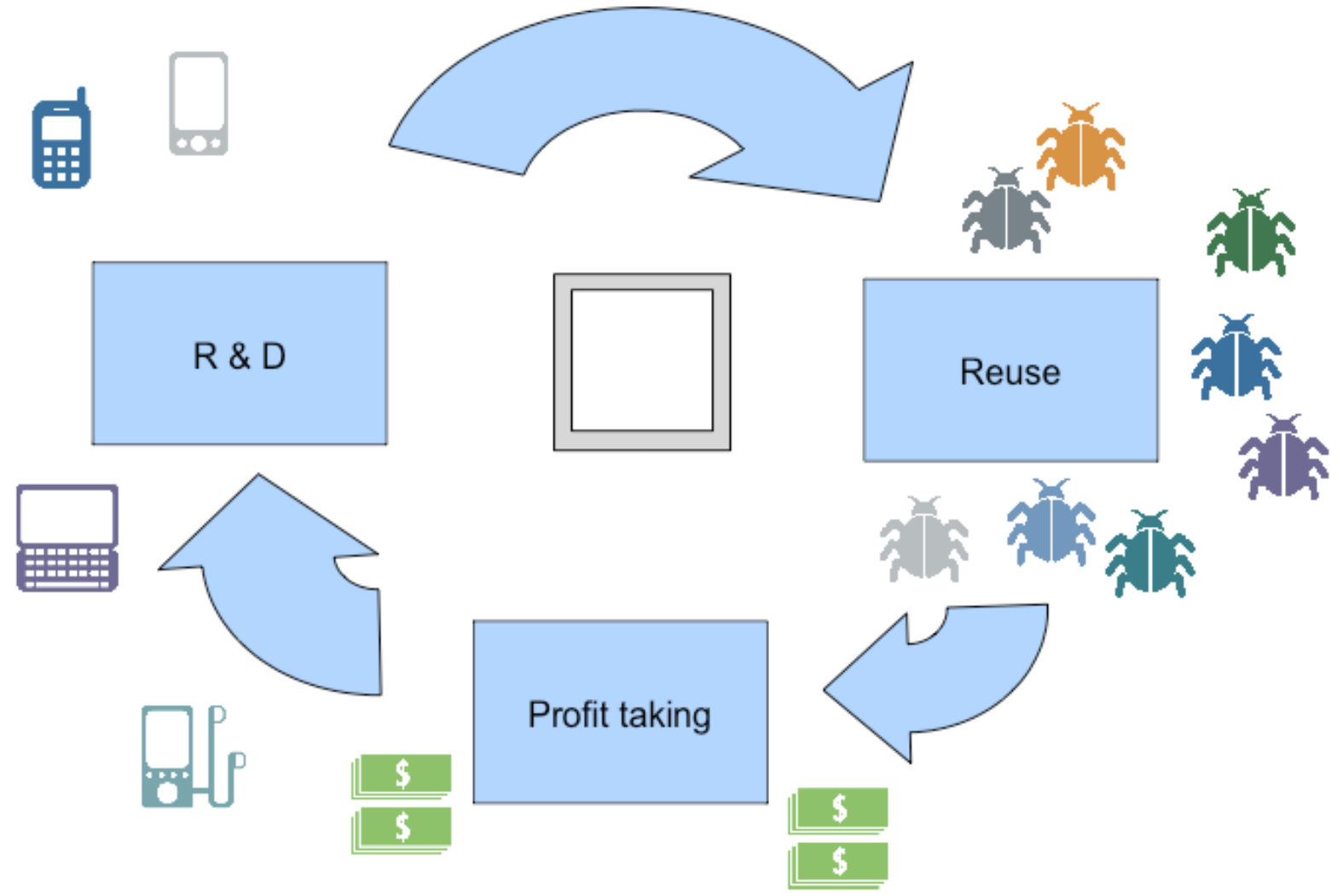


In the Wild

Historical For-profit malware

Trends

# Trends – Mobile Malware Lifecycle



# Modern for-profit malware

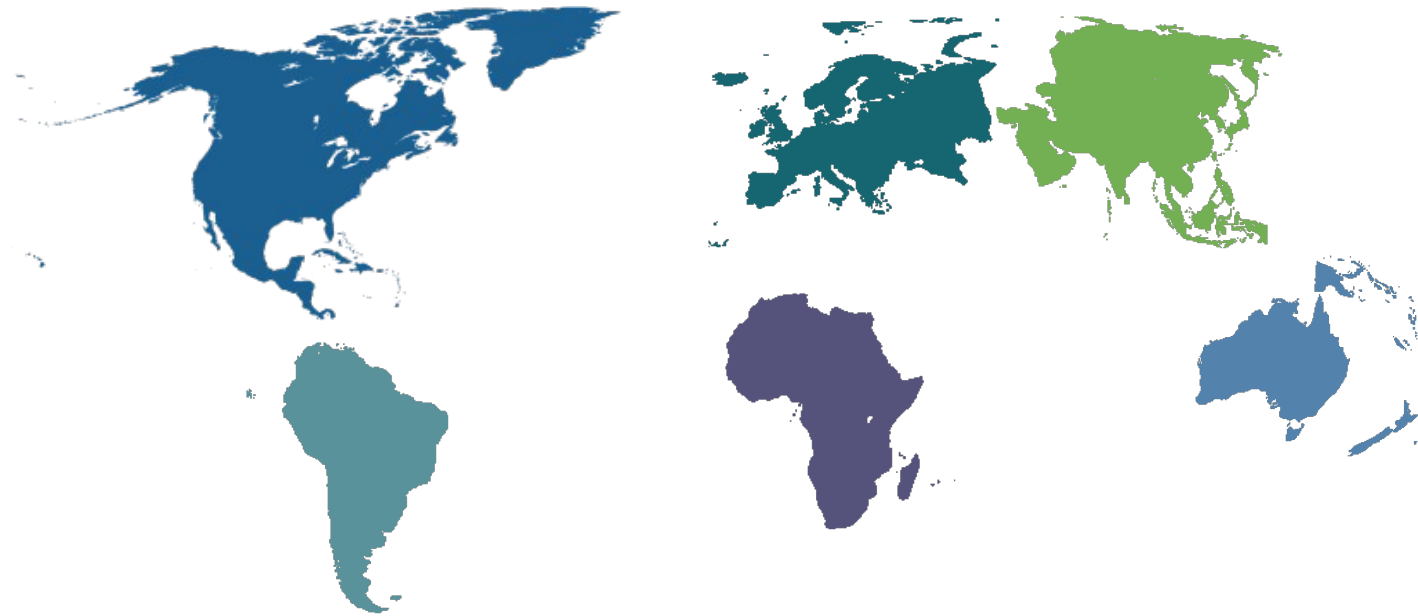


For-profit malware by geographical region

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

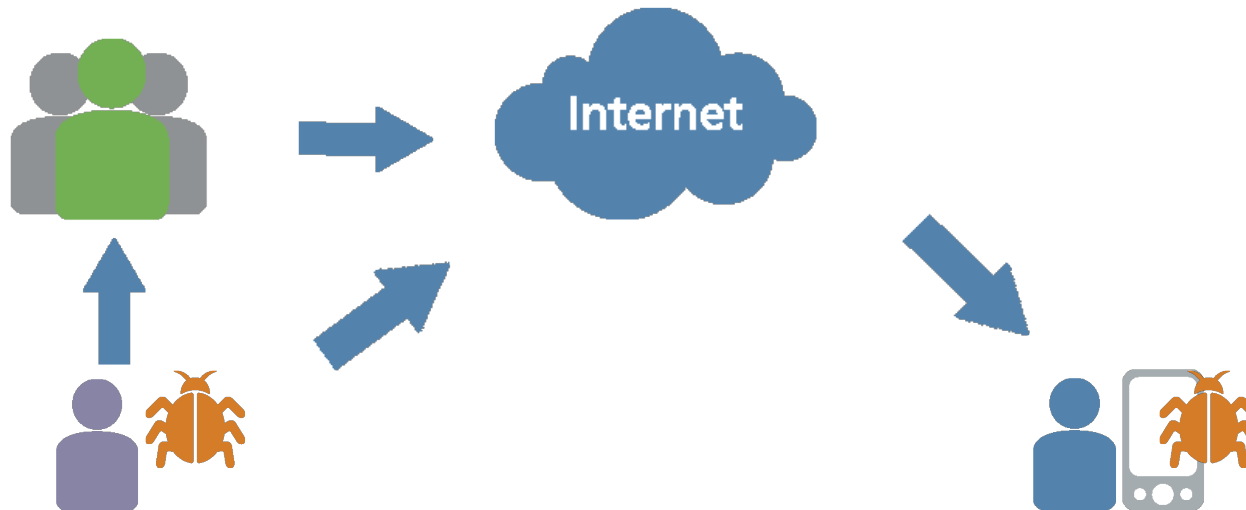
How they Profit

Detection/Analysis Evasion methods

# How they profit

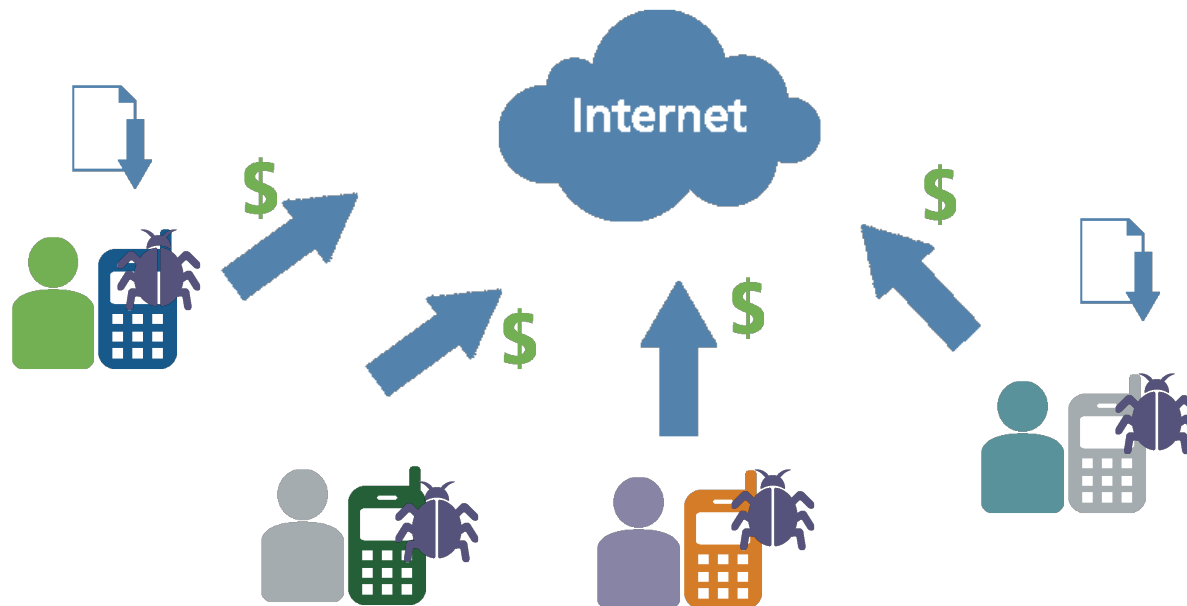


- Production
  - Independent malware authors
  - Produce malware for sale
- Distribution
  - Forums, freeware sites, pirated software sites



# How they profit

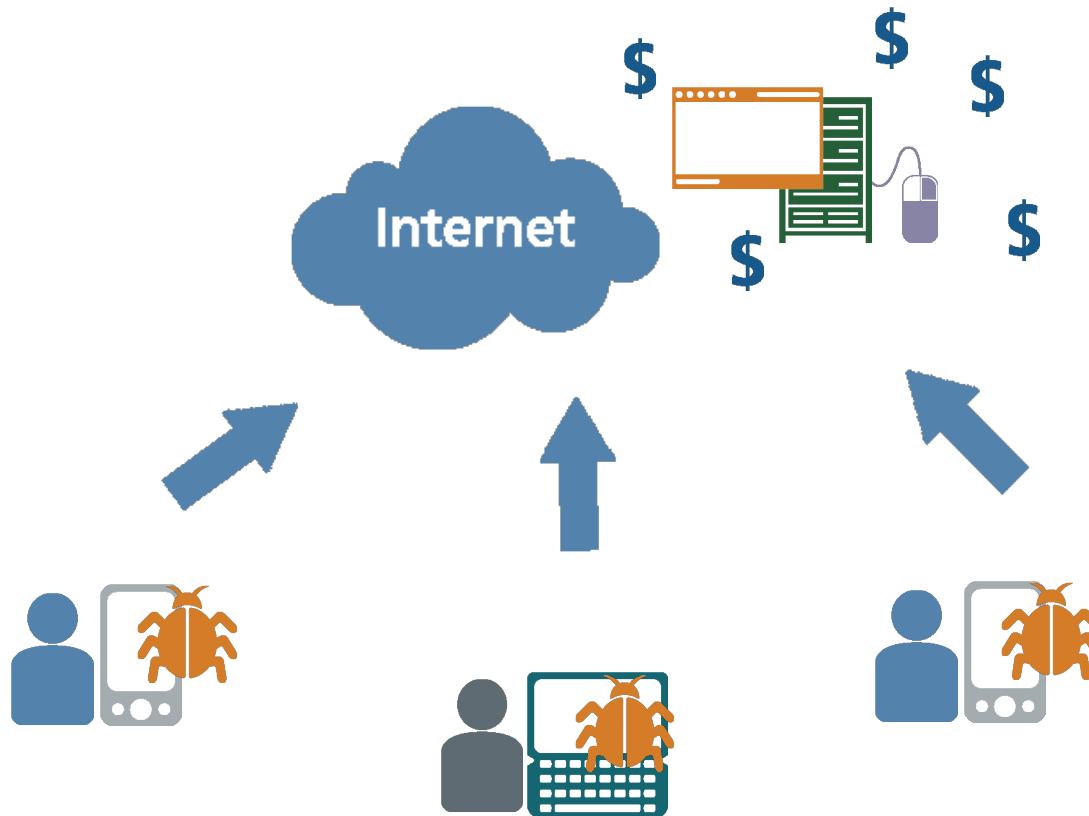
- **Where's the money?**
  - Premium Rate numbers
    - Ringtones, downloads, data services/newsfeeds





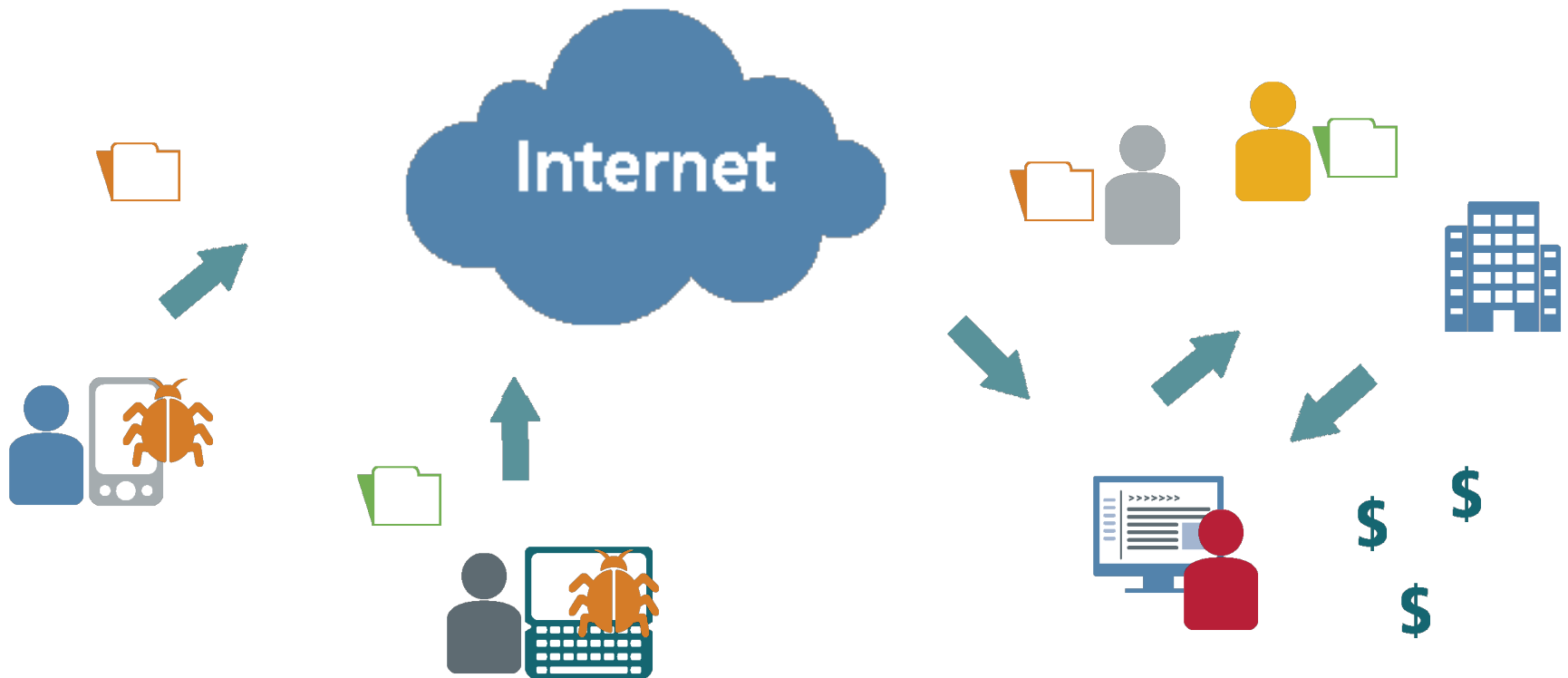
# How they profit

- **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



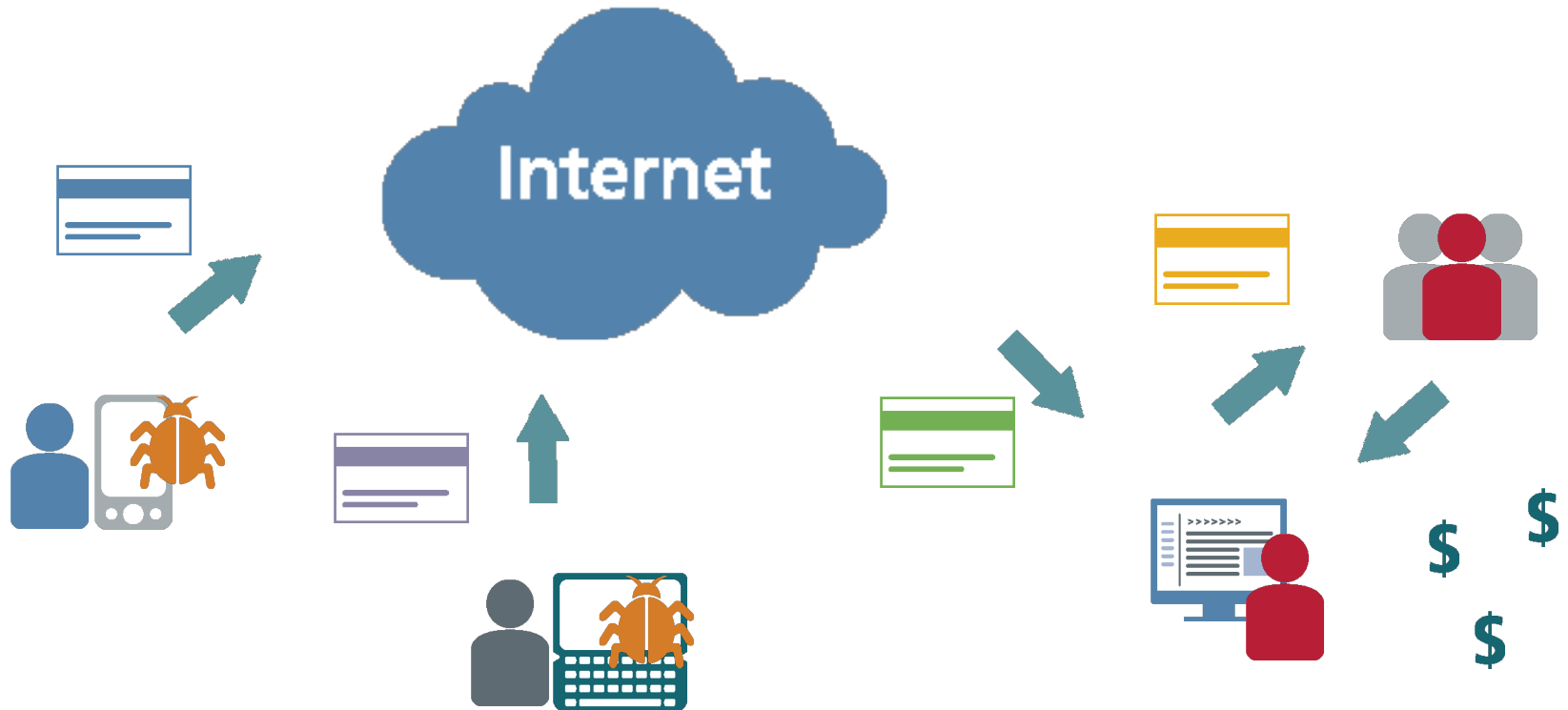
# How they profit

- **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

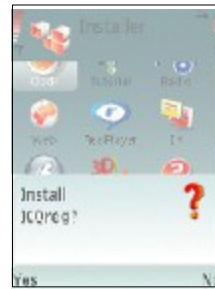
How they Profit

Detection/Analysis Evasion methods

- Infection of/Injection into clean apps

- J2ME

- Chat/IM apps
- Games
- Adult entertainment

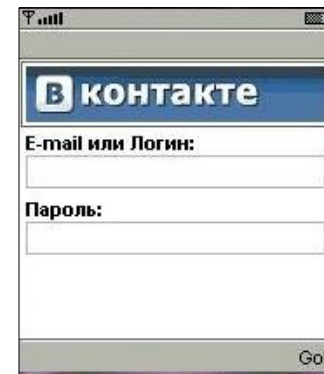


- Symbian

- Chat/IM apps

- Android

- Games
- Chat/IM apps



- 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&pt=cspMscomHomePage&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	ÄÄÄÄwWðvÉDö : èÄ6ww :
0000: 0013	D4 2E F0 C9 78 D3 EA 2E 0A E8 C4 C9 C4 77 77 D0 76 CA D0	Ô. ðÉxÓê. . èÄÉÄwWðvÉÉ
0000: 0026	F5 3A E8 C4 36 77 77 3A C9 C4 2E CF CF 78 D3 EA 2E 0A CF	õ : èÄ6ww : ÉÄ. ÌÏxÓê. . Ì
0000: 0039	C4 E8 E8 77 77 D0 76 CA D0 F5 3A E8 C4 36 77 77 CF F7 2E	ÄèèwWðvÉDö : èÄ6wwÏ-
0000: 004C	F0 F0 78 D3 EA 2E	ððxÓê.



```
<SMS#>::<MSG>::241.55pyб.
<SMS#>::<MSG>::173.88pyб.
<SMS#>::<MSG>::86.00pyб.
```

- 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



# 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
- Jailbreaking
  - Not In the Wild, used only in PoCs
    - e.g. Eric Monti's modified jailbreak at Toorcon 2010

# Examples of for-profit malware



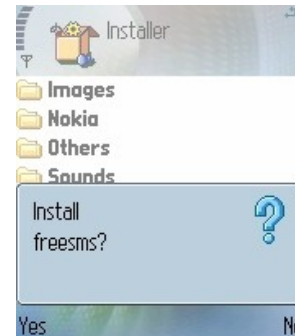
J2ME

Symbian

Android

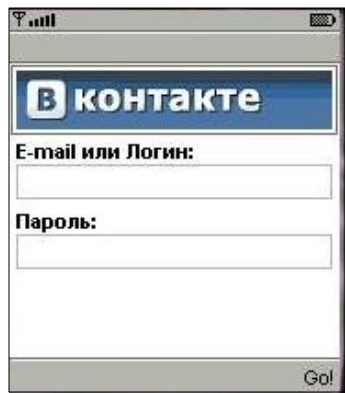
Other

- **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)



- **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



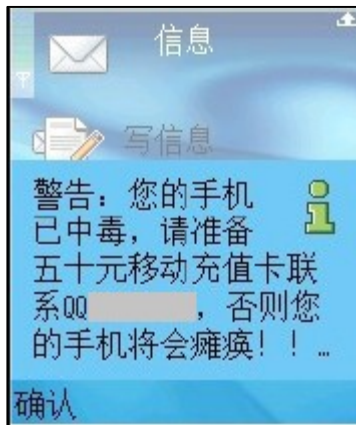
J2ME

Symbian

Android

Other

- **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



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!!

- **What it Does**

- Python script designed to run under the S60 Python interpreter
- Pretends to be a Python client for ICQ

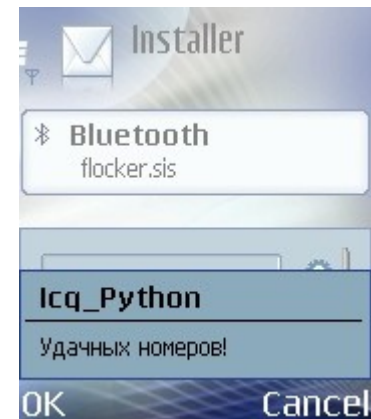
- **Profit?**

- Sends SMS to premium rate number

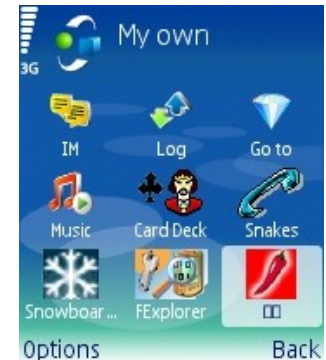
```
appswitch.switch_to_fg(u'Phone')#  
try:messaging.sms_send('<XXXX>',u'FILES <XXX>')#  
except:pass#
```

- 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)#
```



- **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>

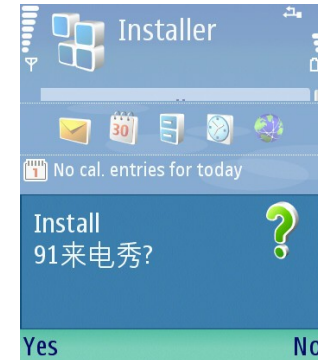
- A second app attempts to download files from the mobile phone forum

```
http://<removed>.com:8118/client/symbian/S60v2active.txt  
http://<removed>.com:8118/client/symbian/BackgroundUpdata.ini  
http://<removed>.com:8118/client/symbian/S60v2StartUpdata.ini
```



- **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.”



# Examples of for-profit malware



J2ME

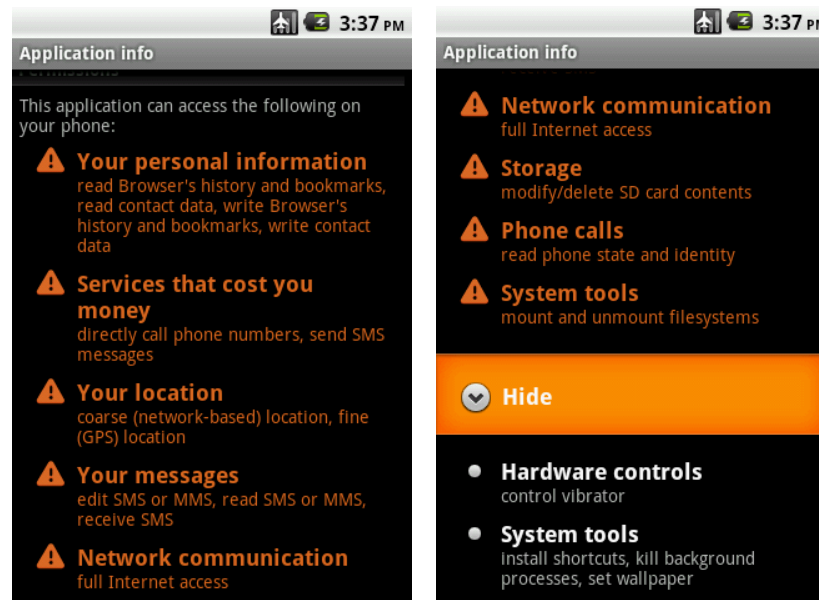
Symbian

Android

Other

- **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.



- **What it does**

- Encryption
  - backdoor commands, C&C URL queries

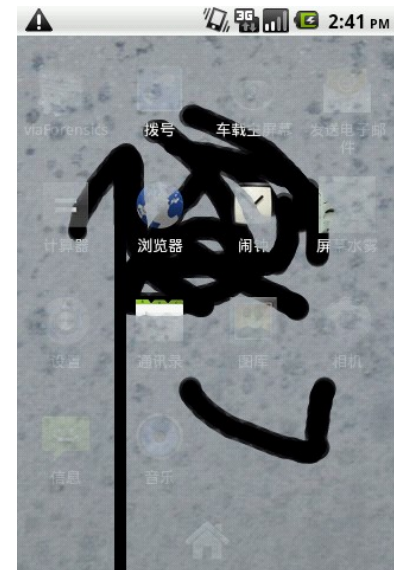
```
byte abyte1[] = k.b;  
DESKeySpec deskeyspec = new DESKeySpec(abyte1);  
javax.crypto.SecretKey secretkey = SecretKeyFactory.getInstance("DES").generateSecret(deskeyspec);  
Cipher cipher = Cipher.getInstance("DES");  
b = cipher;  
cipher.init(2, secretkey);
```

- 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

```
lsor.army7zbejs.static: no pwa 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
```

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

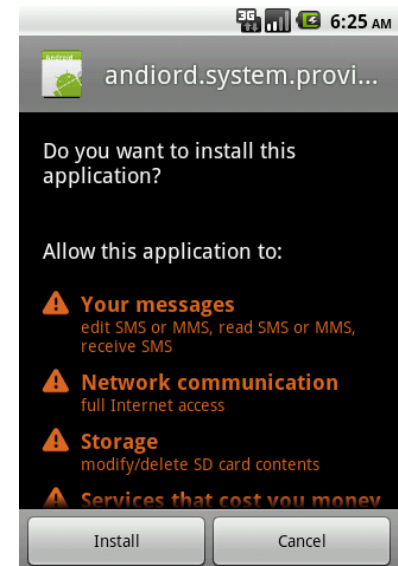
- **What it does**
  - Malicious code inserted into legitimate app
  - Requests many additional permissions
  - Sends IMEI, IMSI, and ICCID to C&C server
  - Adds bookmarks for a smartphone related forum
- **Profit?**
  - Generate traffic to the smartphone forum
  - Send SMS messages
    - Useful for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



- **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

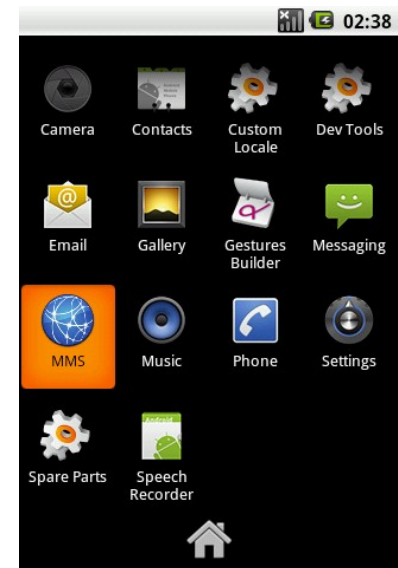


- **What it does**
  - Appears to be a system application
  - Sends IMEI and phone number to C&C server
  - Attempts to kill certain security applications
- **Profit?**
  - Signs up for Premium Rate Services
  - Deletes messages from signed up services
    - No way to know you're subscribed





- **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



# Examples of for-profit malware



J2ME

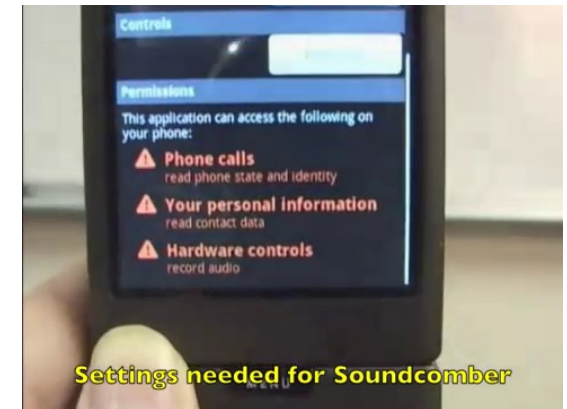
Symbian

Android

Other

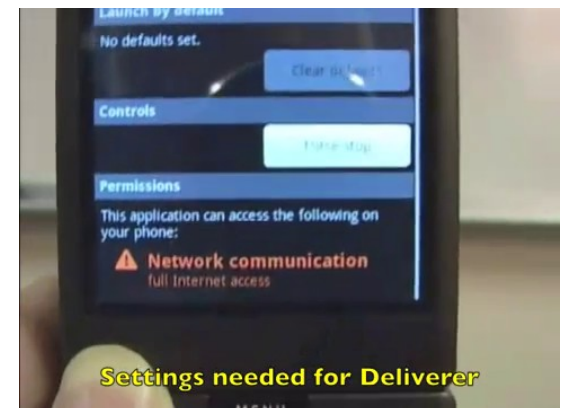
- **What it does**

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



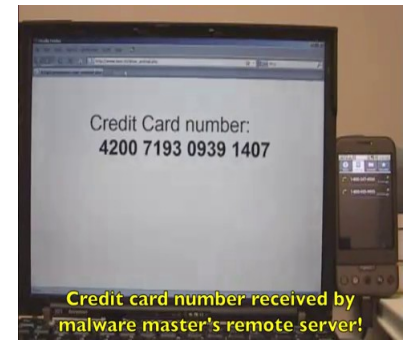
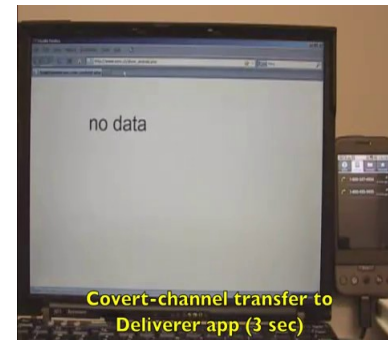
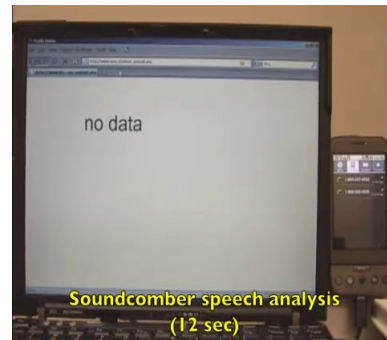
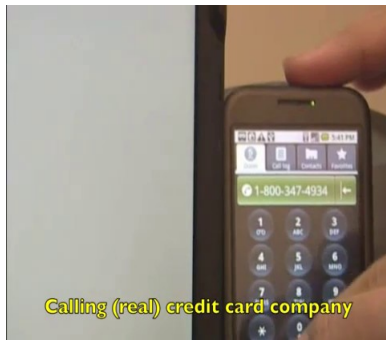
- Deliverer

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

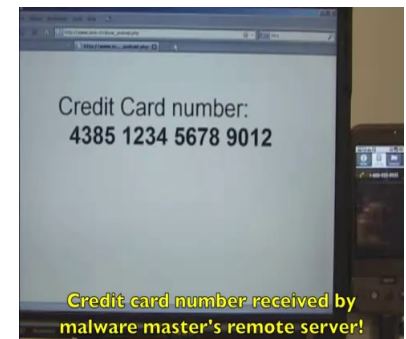
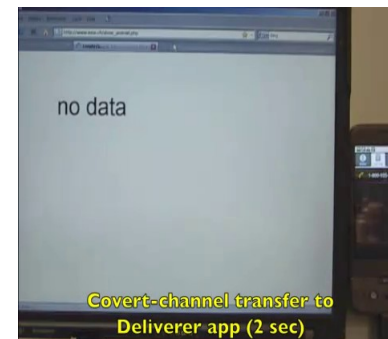
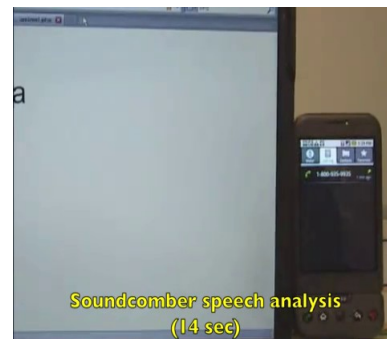
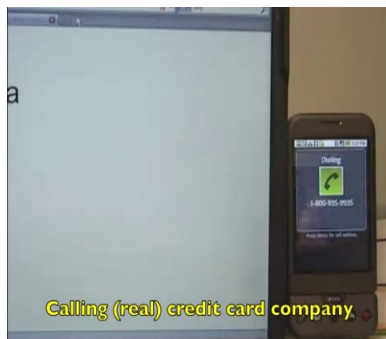


Schlegel, R, Zhang, K, Zhou, X, Intwala, M, Kapadia, A, & Wang, X. (Producer). (2011). Soundcomber demo. [Web]. Retrieved from <http://youtu.be/Z8ASb-tQVpU>

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



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



# References



# References



- J2ME/RedBrowser.A
  - <http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=138726>
- J2ME/Wesber.A
  - <http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=140595>
- J2ME/SMSFree.A
  - <http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=145420>
- J2ME/Vkonpass.A
  - <http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=268520>
- SymbOS/Kiazha.A
  - <http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=144207>
- Android/Geinimi.A
  - <http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=342726>
- Android/Jmsonez.A
  - <http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=501748>
- Android/Tcent.A
  - <http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=501599>
- Android/Crusewin.A
  - <http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=501639>

# 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>

# 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



**McAfee<sup>®</sup>**