

The Monkey Steals the Berries

Mobile Malware – The State of Mobile Security

VERACODE

Presenter Background



Agenda

- Background
- Attacker Motivation
- Case Studies
- Mobile Security Mechanisms
- Potential Effects and Behaviors
- Detecting Malicious Mobile Applications
- Demonstration
- Conclusion



Background

Malicious Mobile Applications

- Modifications to legit programs
- Developer created
- Intentional
- Inadvertent
- Any programming language
- Any operating system

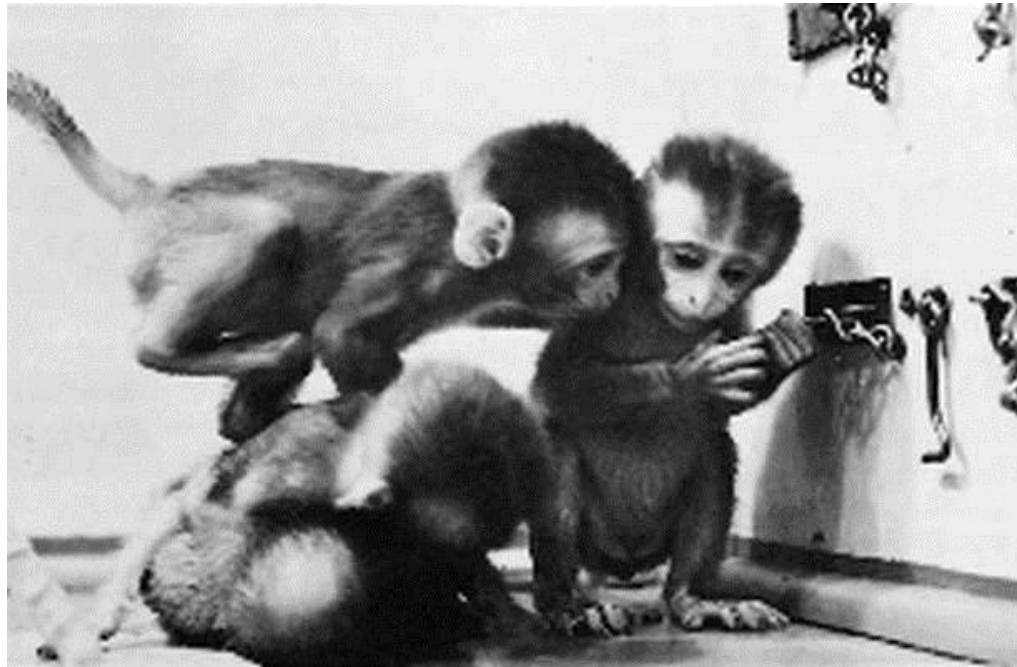




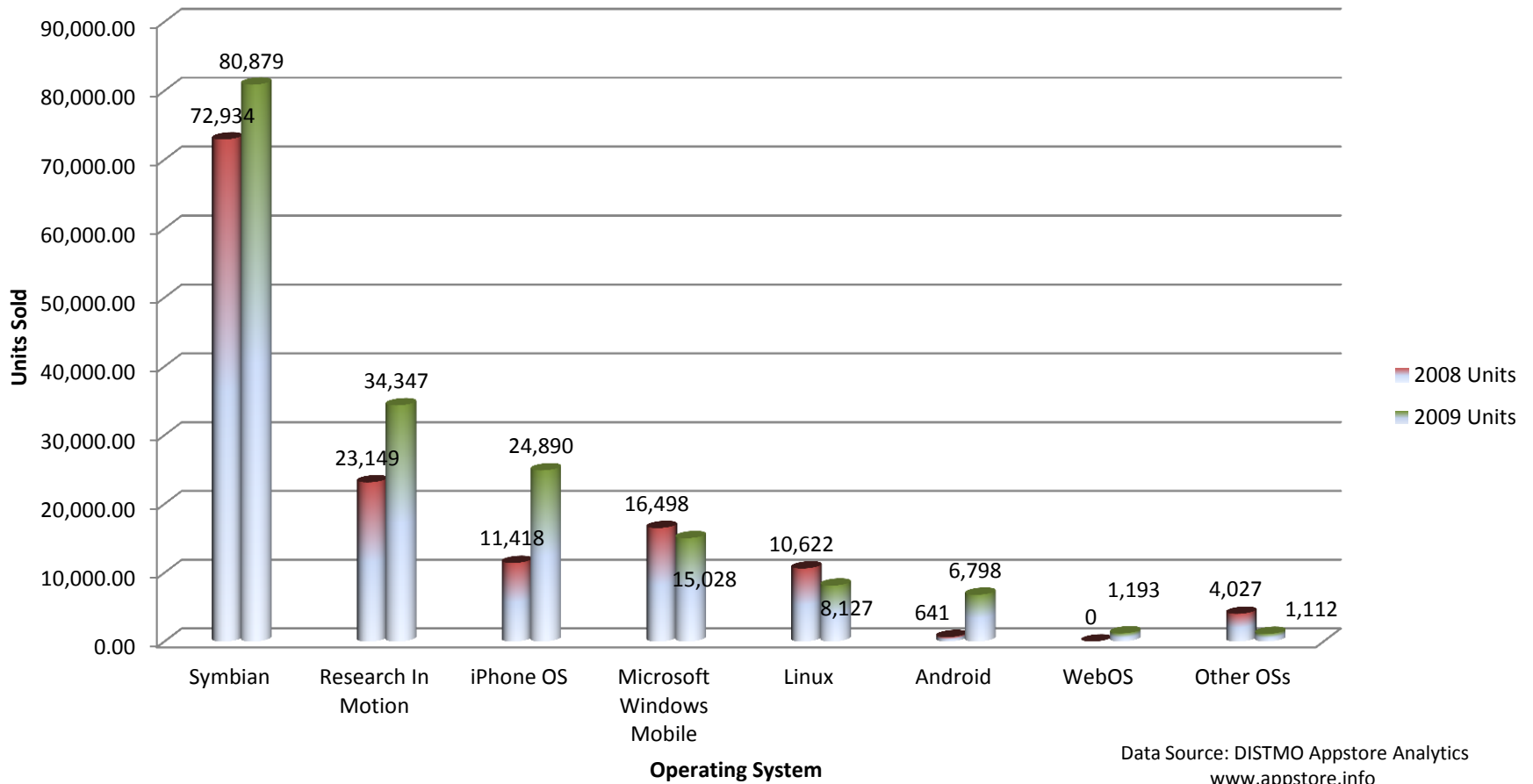
Attacker Motivation

Attacker Motivation

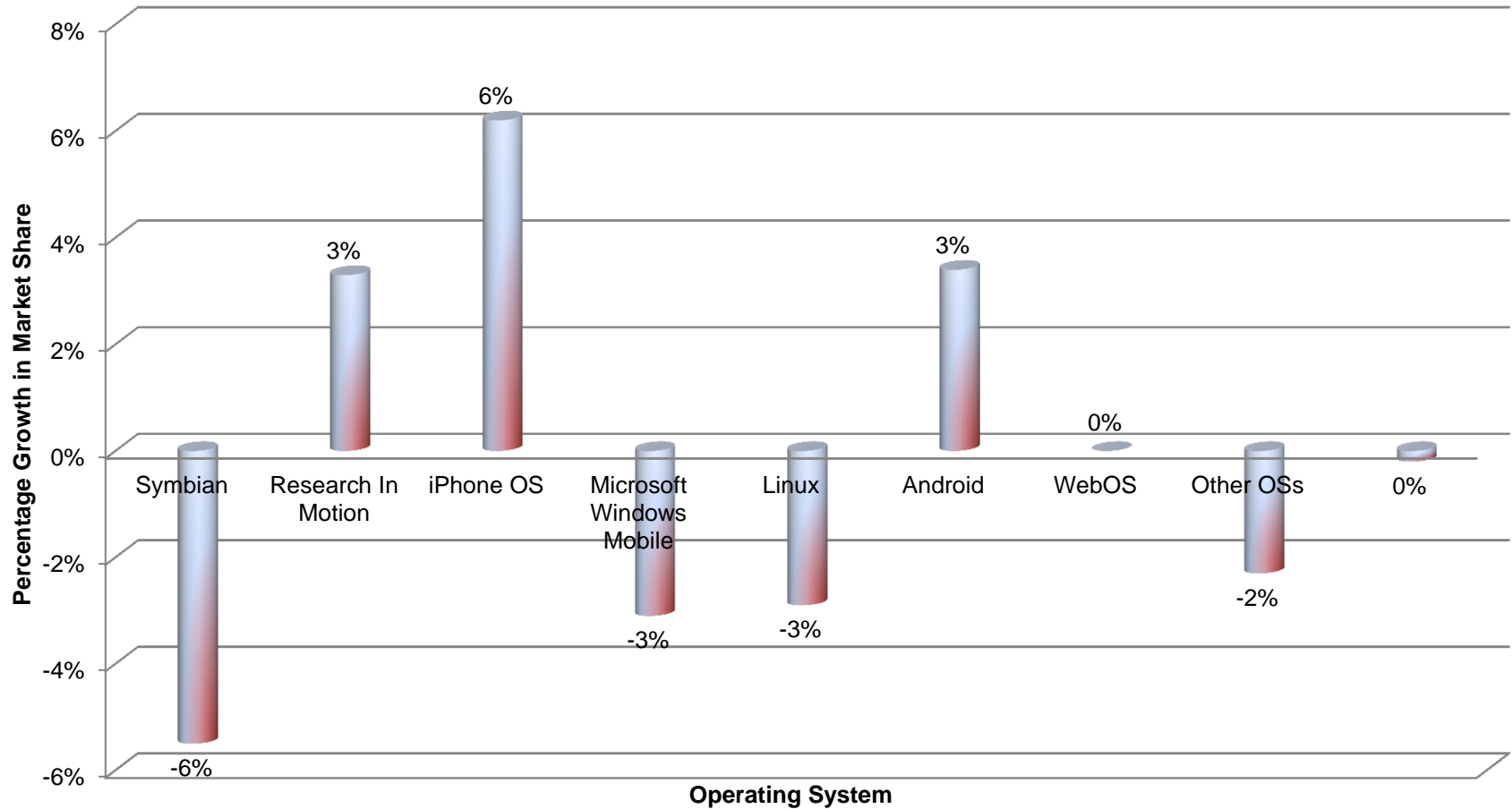
- Practical method of compromise
- Retrieve or manipulate valuable private data
- Cost effective and reliable



Units Sold By Operating System

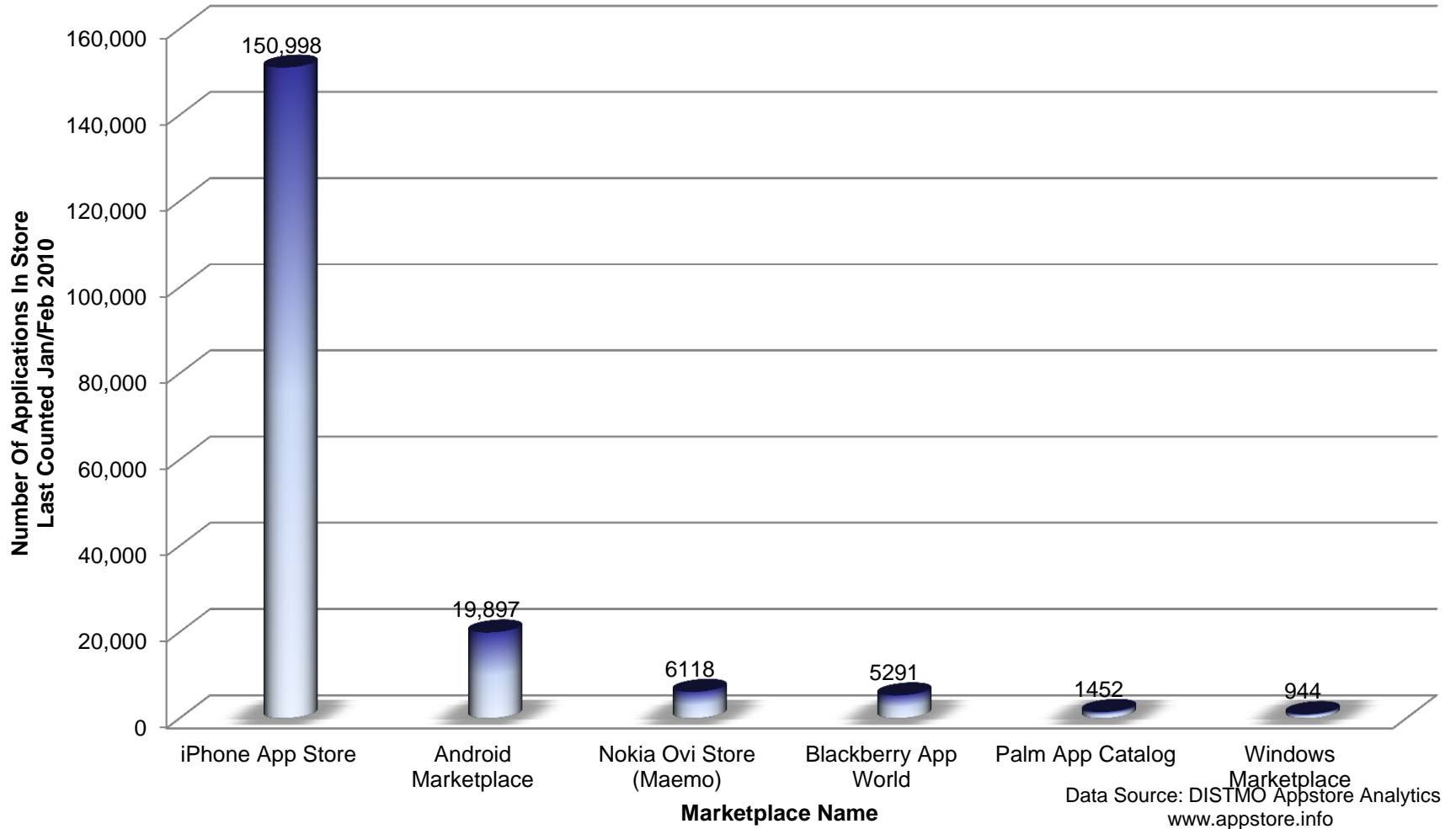


Units Sold Market Growth

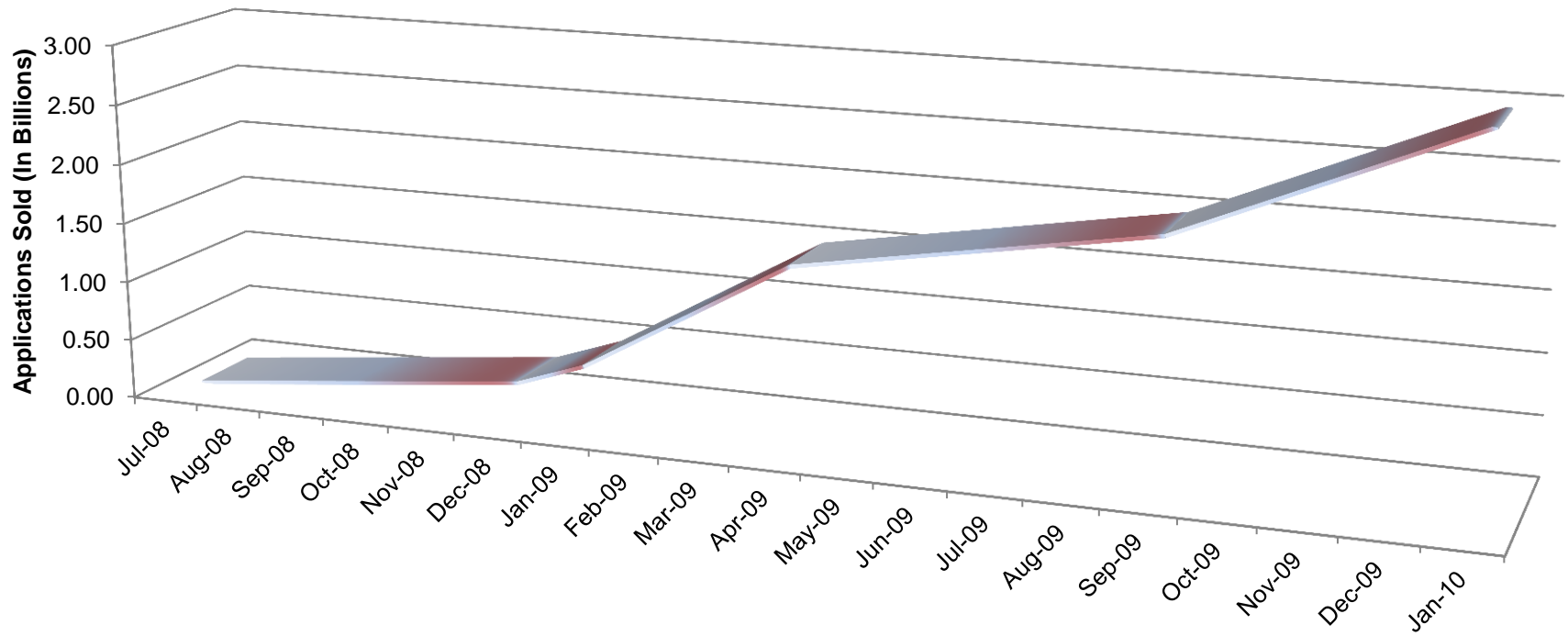


Data Source: DISTMO Appstore Analytics
www.appstore.info

Application Counts



iPhone Applications Sold



Data Source: Gartner, Inc., a research and advisory firm

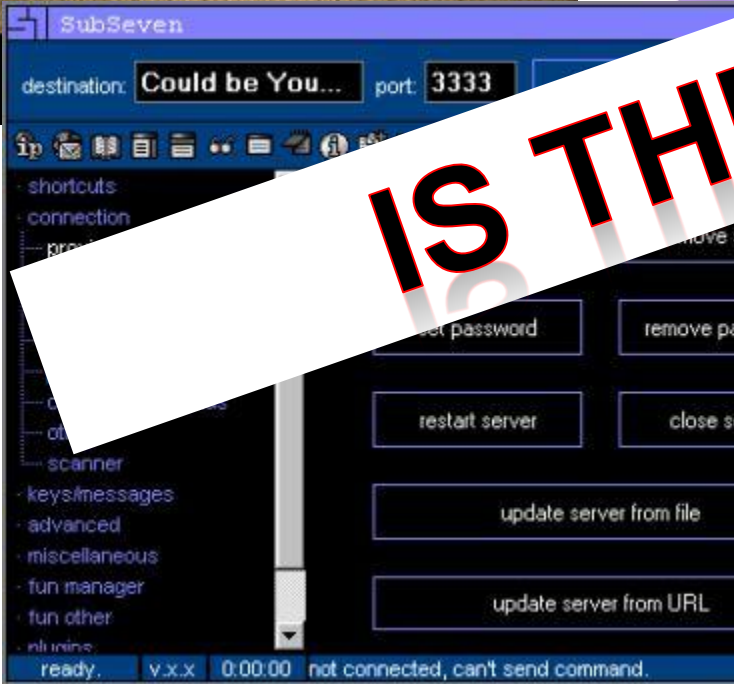
Back To The Future



Back To The Future



IS THIS 1999?!





Case Studies

FlexiSpy

- <http://www.flexispy.com>
- \$149 - \$350 PER YEAR depending on features



FlexiSpy Web Site Quotes

- “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.”
- “F Secure seem to think that its ok for them to interfere with legitimate, legal and accountable software. Who appointed them judge, jury and executioner anyway, and why wont they answer our emails, so we have to ask who is [the real malware](#)? [Here is how to remove FSecure malware from your device](#). Please don't believe the [fsecure fear mongers](#) who simply wish you to buy their products.”

Mobile Spy

- <http://www.mobile-spy.com>
- \$49.97 PER QUARTER or \$99.97 PER YEAR



Mobile Spy Web Site Quotes

- “This high-tech spy software will allow you to see exactly what they do while you are away. Are your kids [texting while driving](#) or using the phone in all hours of the night? Are your employees sending company secrets? Do they erase their phone logs?”
- “Our software is not for use on a phone you do not own or have proper permission to monitor from the user or owner. You must always follow all applicable laws and regulations in your region.”
- “Purchased by more than 30,000 customers in over 150 countries”

eBlaster Mobile

- <http://www.spectorsoft.com>
- \$49.95 a year



eBlaster | mobile
Records Activity on a BlackBerry

REC Text Messages **REC** Email Activity **REC** Voice Call Logs

NEW

Hey Steve! Parents
Let's get together
Sure! I'll try
invite some
Great p
over...

11:00

eBlaster | mobile

eBlaster | mobile

The advertisement features a green background with a white envelope icon at the bottom. On the right, two BlackBerry smartphones are shown, one in the foreground and one slightly behind it. A white banner with the word 'NEW' in red is positioned in the top right corner. The main text is in white and green, and the recording icons are red circles with 'REC' in white.

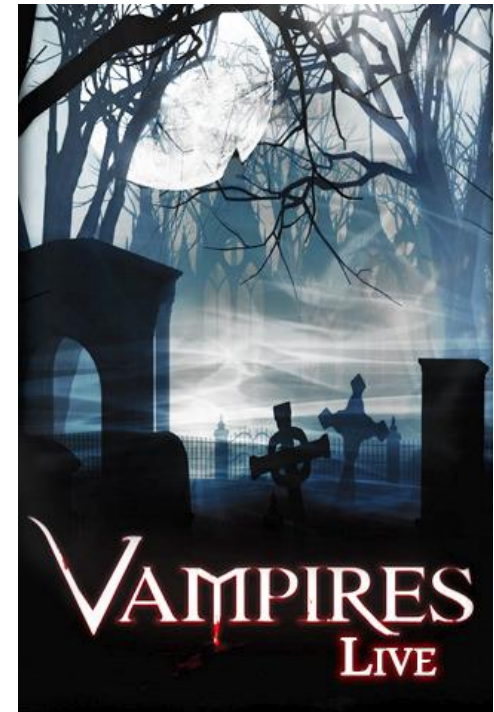
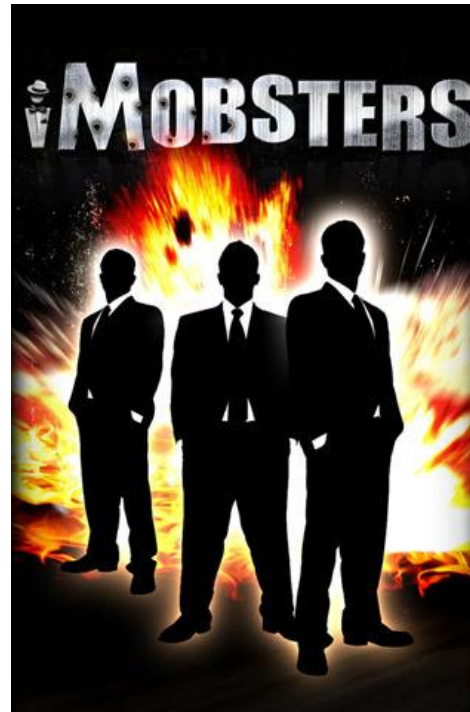
Etisalat (SS8)

- UAE cellular carrier
- ***Distribution: SMS link to patch***
- Command & Control: BB PIN
- Hidden on device
- Data stolen: Email, SMS



Storm8 Phone Number Farming

- iPhone video game maker
- Built into game
- ***Distribution: iTunes***
- Command & Control: None
- Hidden within application
- Data stolen: Phone Number



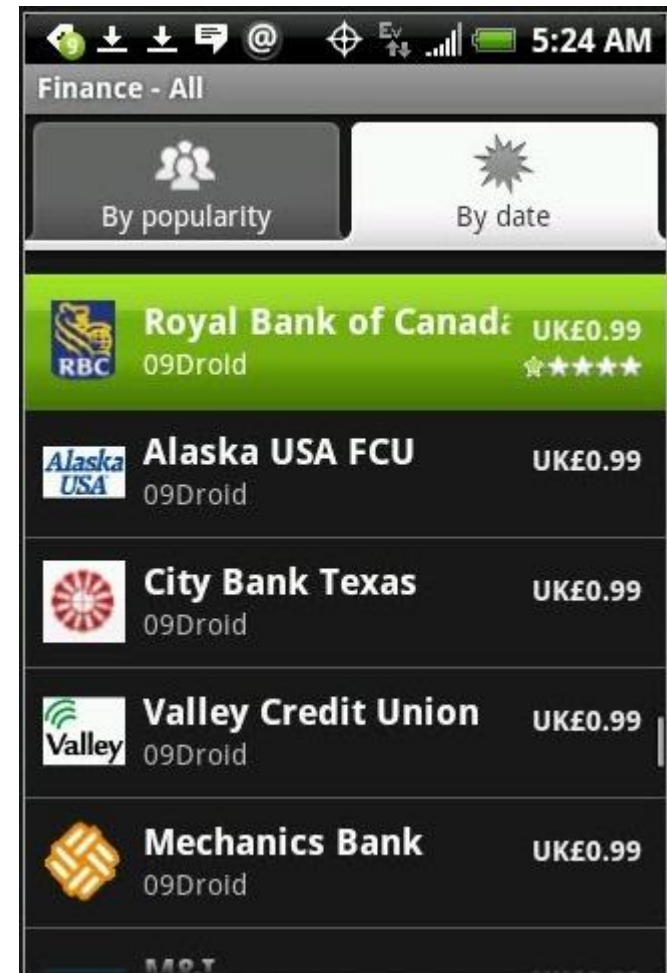
Symbian Sexy Space

- No real facade
- Botnet for Symbian phone
- ***Distribution: Malicious web sites***
- Worm: SPAM contacts
- Data stolen: Phone number, network information
- Signed by Symbian as safe!
 - Anti-virus scan
 - Some manual assessment

The logo for Symbian OS. The word "symbian" is written in a bold, lowercase, sans-serif font. The letter "i" is stylized with a blue vertical bar and a yellow dot above it. Below "symbian", the letters "OS" are written in a large, bold, uppercase, sans-serif font.

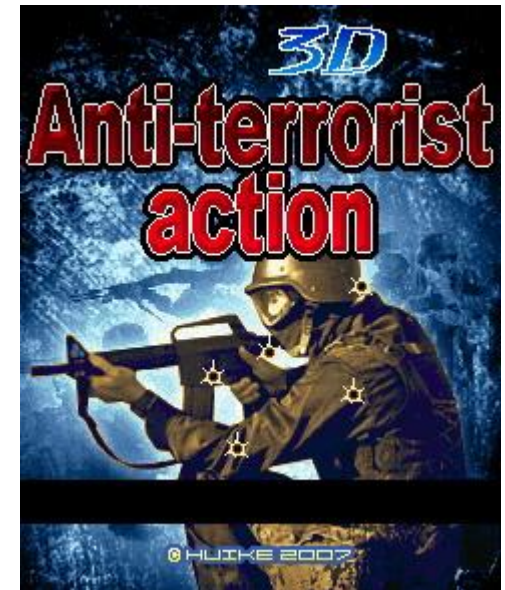
09Droid – Banking Applications Attack

- 09Droid developer
- Web frontends to 50+ banks
- ***Distribution: Android Marketplace***
- Data stolen: Unknown – likely none
- Multiple bank fraud warnings released



3D Anti-Terrorist / PDA Poker Art / Codec Pack WM1.0

- Original author: Huike
- Repackaged in Russia
- Built into game
- Distribution: WM shareware web sites
- Command & Control: None
- Data stolen: Money!





Mobile Security Mechanisms

Does It Really Matter?!

Only 23% of smartphone owners use the security software installed on the devices.

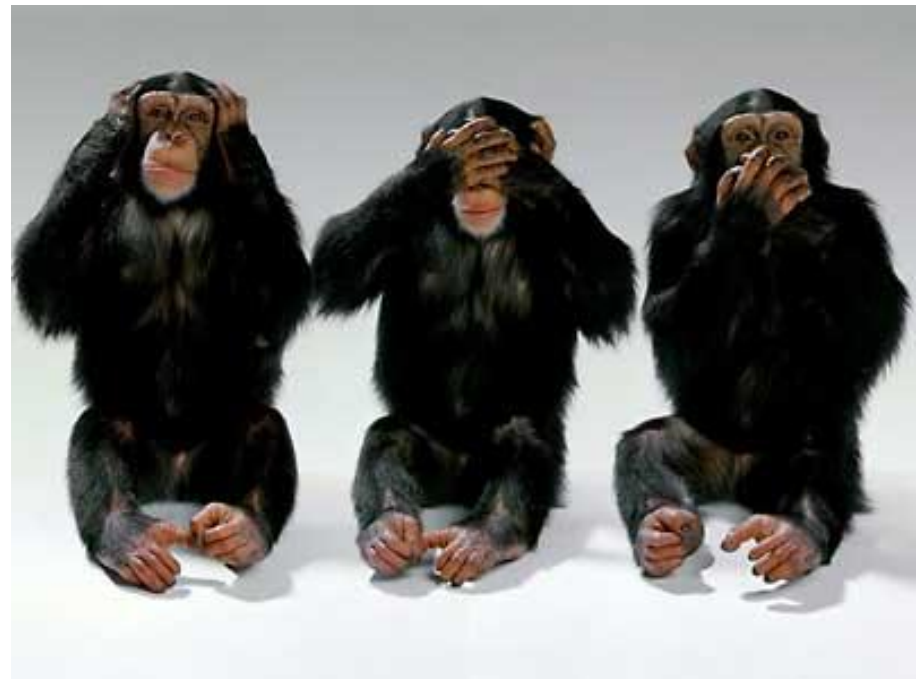
(Source: Trend Micro Inc. survey of 1,016 U.S. smartphone users, June 2009)

13% of organizations currently protect from mobile viruses

(Mobile Security 2009 Survey by Goode Intelligence)

Common Mobile Security Mechanisms

- Corporate level security policies
- Application level security policies
- Mobile anti-virus
- Application marketplace screening
- Code Signing



V5.0.0.328 Trusted 3rd Party Application Permissions

USB Connections	Bluetooth Connections	Phone Connections	Location Data
Server Network	Internet	IPC	Device Settings
Media	Application Management	Themes	Input Simulation
Browser Filtering	Recording	Security Timer Reset	Display Information While Locked
Email Data	Organizer Data	Files	Security Data

V5.0.0.328 Untrusted 3rd Party Application Permissions

USB Connections	Bluetooth Connections	Phone Connections	Location Data
Server Network	Internet	IPC	Device Settings
Media	Application Management	Themes	Input Simulation
Browser Filtering	Recording	Security Timer Reset	Display Information While Locked
Email Data	Organizer Data	Files	Security Data



Potential Effects and Behaviors

Installation Methods

Application Marketplace



- iTunes
- Android Marketplace
- Blackberry App World

Over The Air (OTA)



- Web Sites
- Carrier Pushed

Enterprise Distribution



- Mass Distribution
- Corporate Targets

PC Loader













- User Desktop Push
- With/Without Assistance
- Virus

Technical Methods











- Data Dumpers
- Listeners
- Exfiltration Methods
- Command and Control



Logging and Dumping

	Monitor connected / disconnected calls
	Monitor PIM added / removed / updated
	Monitor inbound SMS
	Monitor outbound SMS
	Real Time track GPS coordinates
	Dump all contacts
	Dump current location
	Dump phone logs
	Dump email
	Dump microphone capture (security prompted)

Exfiltration and C&C Methods

	SMS (No CDMA)
	SMS Datagrams (Supports CDMA)
	Email
	HTTP GET
	HTTP POST
	TCP Socket
	UDP Socket
	DNS Exfiltration
	Default command and control to inbound SMS
	TXSPROTO Bidirectional TCP based command and control



Detecting Malicious Mobile Code

Detecting Malicious Mobile Code

- Signature Based Detection
 - Broken
- Resource Usage Whitelisting
 - Semi-broken
- Sandbox Based Execution Heuristics
 - Semi-broken
- Static Decompilation and Analysis
 - Hard to do, but WORKS!



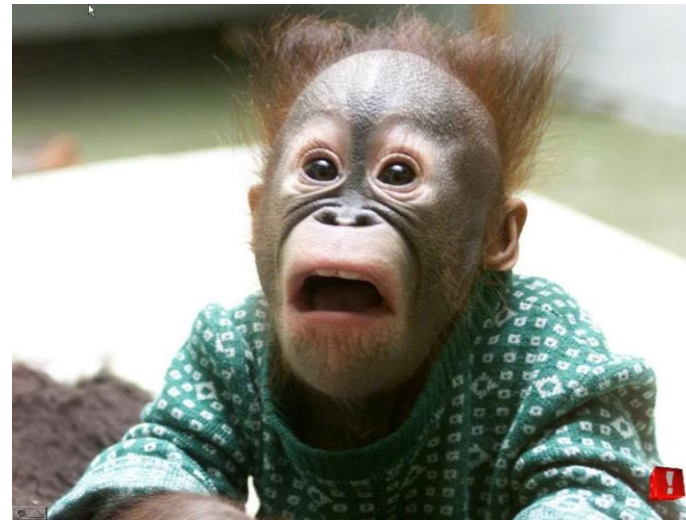
Mobile Malicious Code Detection



Defense in Depth

Do all of the above!

- Implement and enforce strong IT policies
- Implement and enforce additional application policies as required
- Implement a best of breed anti-virus solution
 - If only for thoroughness of deployed options
- Utilize static decompilation and analysis of applications considered for deployment





Demonstration

Conclusion

- We are currently trusting the vendor application store provider for the majority of our mobile device security
- Minimal methods of real time eradication or detection of spyware type activities exists
- When they do exist they are not configured correctly (or at all)
- No easy/automated way to confirm for ourselves what the applications are actually doing
- Automate the decompilation and static analysis of applications that are required for the ongoing functioning of your business



The Monkey Steals the Berries!

Questions?

Questions?

VERACODE