

The Monkey Steals the Berries

Mobile Malware – The State of Mobile Security

VERACODE

Agenda

- Background
- Attacker Motivation
- Malicious Mobile Applications In The Wild
- Mobile Security Mechanisms
- Potential Effects of Behaviors
- Detecting Malicious Mobile Applications
- Mitigation



Background

Presenter Background

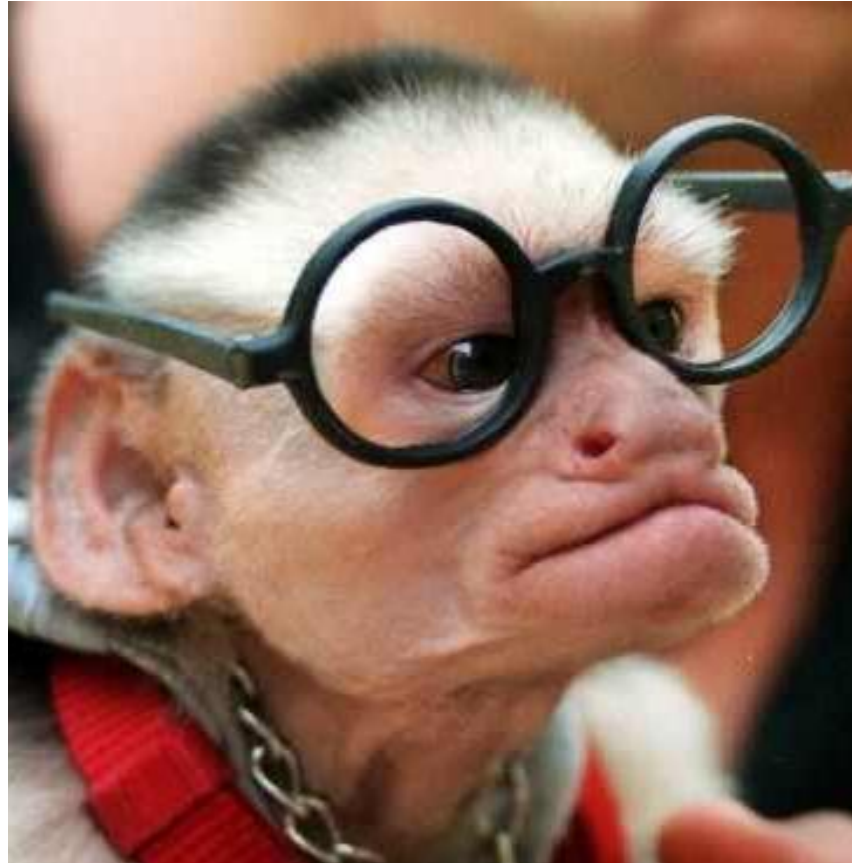
- Currently
 - Sr. Security Researcher, Veracode, Inc.
- Previously
 - Security Consultant - Symantec
 - Security Consultant - @Stake
 - Incident Response and Forensics Handler
- Wishes He Was
 - Infinitely rich
 - Able to leap tall buildings in a single bound
 - Smarter than the average bear



Malicious Mobile Applications

- Often includes modifications to legitimate programs designed to compromise the device or device data
- Often inserted by those who have legitimate access to source code or distribution binaries
- May be intentional or inadvertent
- Not specific to any particular programming language
- Not specific to any particular mobile Operating System



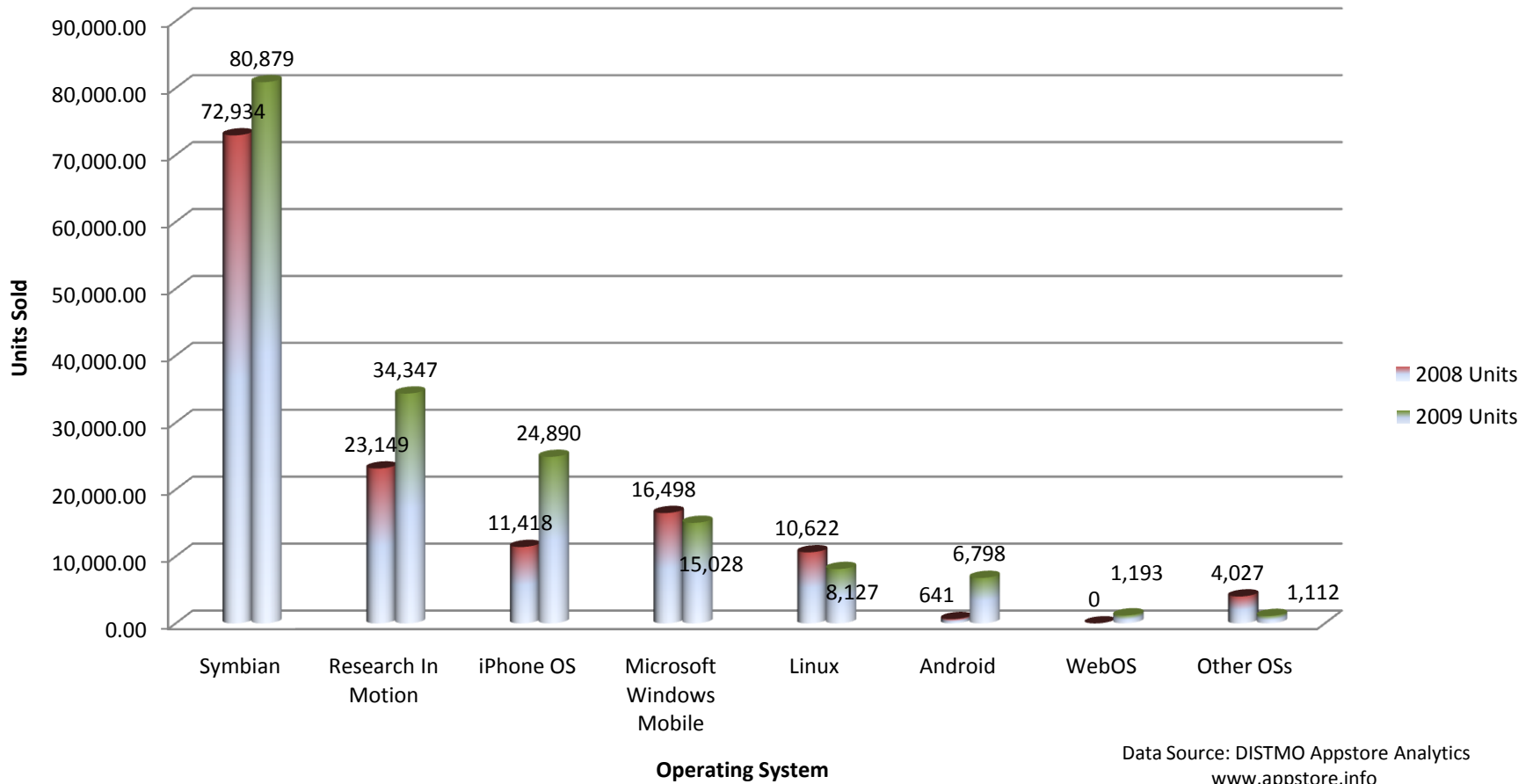


Attacker Motivation

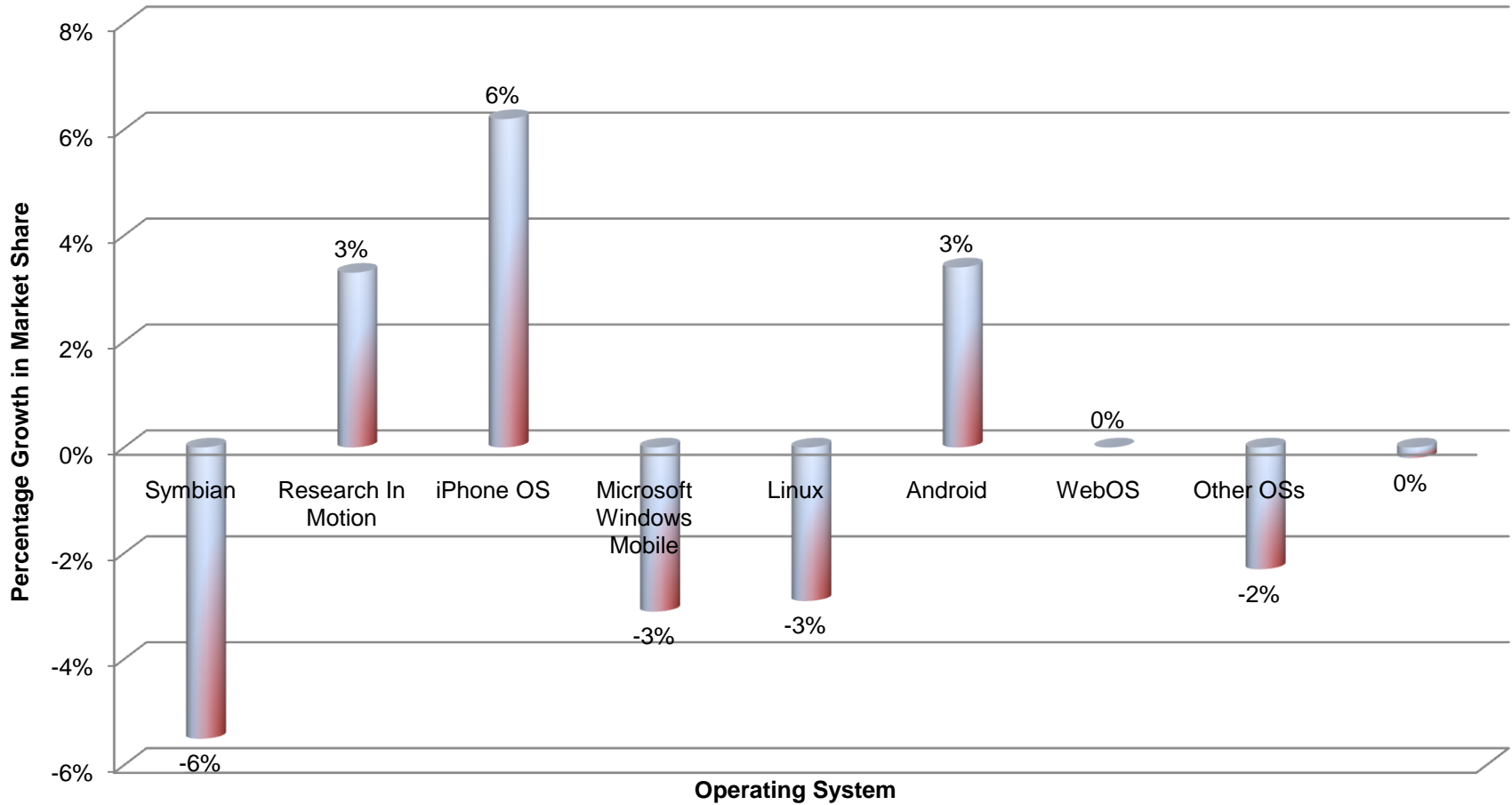
Attacker Motivation

- Practical method of compromise for many systems
 - Let the users install your backdoor on systems you have no access to
 - Looks like legitimate software so may bypass mobile AV
- Retrieve and manipulate valuable private data
 - Looks like legitimate application traffic so little risk of detection
- For high value targets such as financial services and government it becomes cost effective and more reliable
 - High-end attackers will not be content to exploit opportunistic vulnerabilities, which might be fixed and therefore unavailable at a critical juncture. They may seek to implant vulnerability for later exploitation
 - Think “Aurora” for Mobile Devices

Units Sold By Operating System

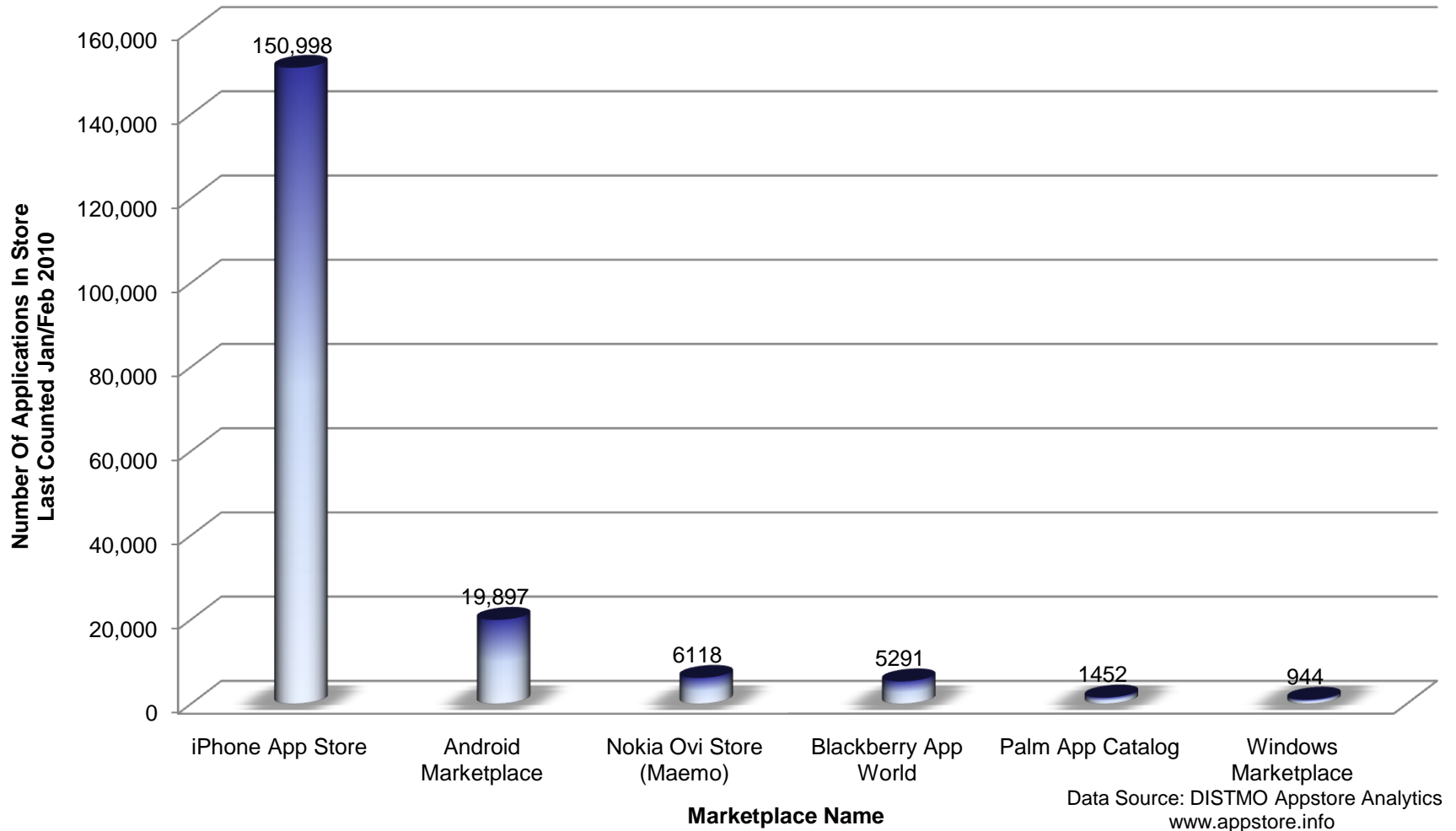


Units Sold Market Growth

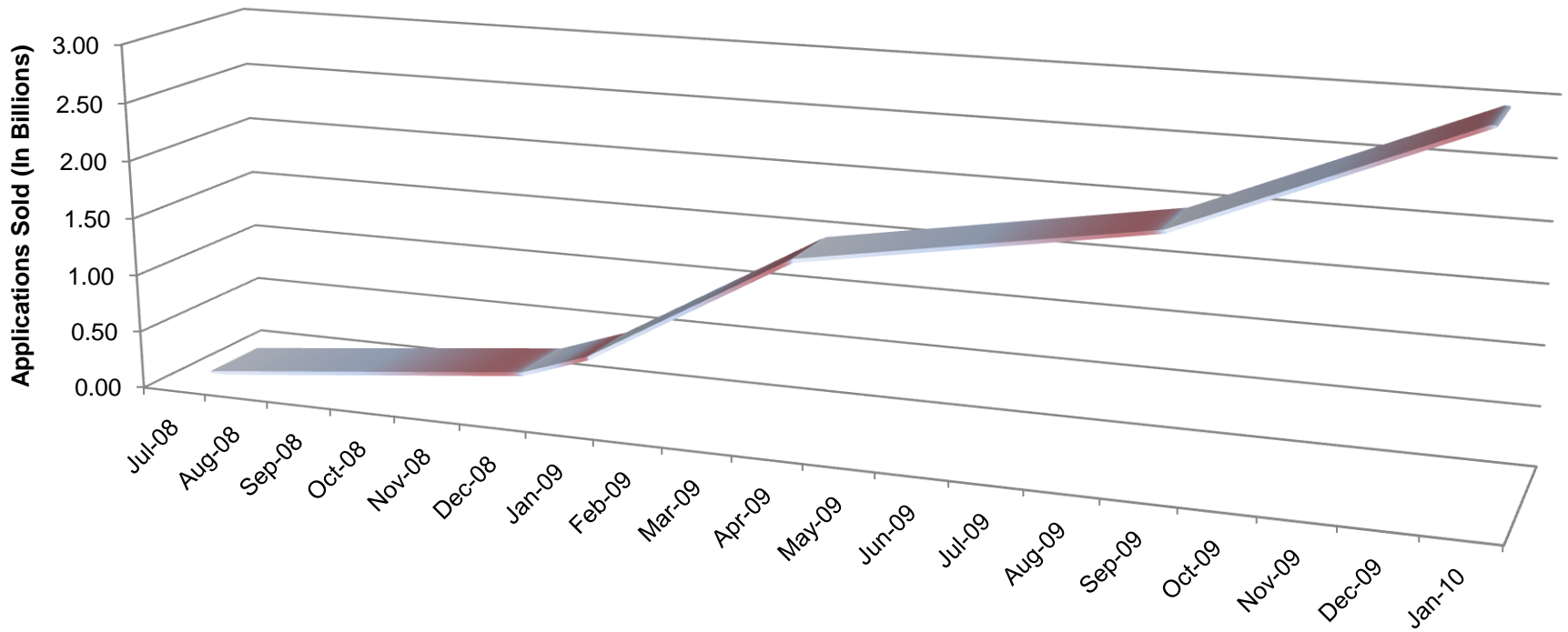


Data Source: DISTMO Appstore Analytics
www.appstore.info

Application Counts



iPhone Applications Sold



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

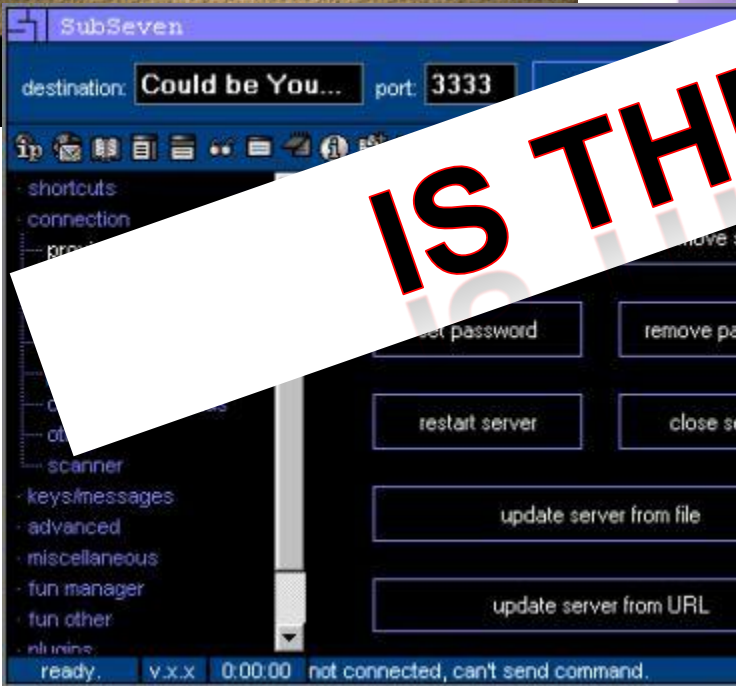
Back To The Future



Back To The Future



IS THIS 1999?!





Malicious Mobile Applications In The Wild

FlexiSpy

- <http://www.flexispy.com>
- \$149 - \$350 PER YEAR depending on features
- Features
 - Remote Listening
 - C&C Over SMS
 - SMS and Email Logging
 - Call History Logging
 - Location Tracking
 - Call Interception
 - GPS Tracking
 - Symbian, Blackberry, Windows Mobile Supported

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
- Features
 - SMS Logging
 - Call Logging
 - GPS Logging
 - Web URL Logging
 - BlackBerry, iPhone (Jailbroken Only), Android, Windows Mobile or Symbian

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”

Etisalat (SS8)

- Cell carrier in United Arab Emirates (UAE)
- Pushed via SMS as “software patch” for Blackberry smartphones
- Upgrade urged to “enhance performance” of Blackberry service
- Blackberry PIN messaging as C&C
- Sets FLAG_HIDDEN bit to true
- Interception of outbound email / SMS only
- Discovered due to flooded listener server cause retries that drained batteries of affected devices
- Accidentally released the .jar as well as the .cod (oopsie?!)

Storm8 Phone Number Farming

- iMobsters and Vampires Live (and others)
- “Storm8 has written the software for all its games in such a way that it automatically accesses, collects, and transmits the wireless telephone number of each iPhone user who downloads any Storm8 game,” the suit alleges. “ ... Storm8, though, has no reason whatsoever to access the wireless phone numbers of the iPhones on which its games are installed.”
- “Storm8 says that this code was used in development tests, only inadvertently remained in production builds, and removed as soon as it was alerted to the issue.”
- **These were available via the iTunes App Store!**
- <http://www.boingboing.net/2009/11/05/iphone-game-dev-accu.html>

Symbian Sexy Space

- Poses as legitimate server ACSServer.exe
- Calls itself 'Sexy Space'
- Steals phone and network information
- Exfiltrates data via hacker owned web site connection
- Can SPAM contact list members
- Basically a “botnet” for mobile phones
- **Signing process**
 - Anti-virus scan using F-Secure
 - Approx 43% proactive detection rate (PCWorld)
 - Random selection of inbound manually assessed
- **Symbian signed this binary as safe!**
- <http://news.zdnet.co.uk/security/0,1000000189,39684313,00.htm>

Symbian MergoSMS

- The worm spreads as self-signed (untrusted) SIS installers
- Installer contains sub-SIS installers some of them signed by Symbian.
- Spreads by sending text messages
 - Contain variable messages in Chinese and a link to a website
 - Going to link results in worm download
- On phone reboot malware runs, downloads worm payload, completing infection
- The worm was spread on Chinese file sharing web sites
- **Originally spread as games, themes, etc. for Symbian Series60 3rd & 5th edition phones.**
- http://www.f-secure.com/v-descs/trojan_symbos_merogosms.shtml

09Droid – Banking Applications Attack

- Droid app that masquerades as any number of different target banking applications
- Target banks included
 - Royal Bank of Canada
 - Chase
 - BB&T
 - SunTrust
 - Over 50 total financial institutions were affected
- May steal and exfiltrate banking credentials
- **Approved and downloaded from Google's Android Marketplace!**
- <http://www.theinquirer.net/inquirer/news/1585716/fraud-hits-android-apps-market>
- <http://www.pcadvisor.co.uk/news/index.cfm?RSS&NewsID=3209953>
- <http://www.f-secure.com/weblog/archives/00001852.html>

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

- Games available on legitimate application download sites
- Originally written by Chinese company Huike
- Repackaged in Russia by unknown authors to include malware
- Calls premium rate 800 numbers
- Three days idle before first dial
- Idles one month between subsequent outbound dialing
- **Distributed via common Windows Mobile shareware sites**
- <http://www.eweek.com/c/a/Security/Malware-Hidden-in-Windows-Mobile-Applications-424076/>



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
 - Applied at the corporate IT level
 - Can't be modified by a lower level security mechanism

- Application level security policies
 - May be pushed down from corporate policy
 - Otherwise applied at handset itself
 - Restricts access to specific resources
 - Sandboxing
 - Code Signing

Common Mobile Security Mechanisms

- Mobile Anti-Virus
 - Implemented at the handset itself
 - Fails due to the same reasons PC antivirus is failing today

- Application market place security screening
 - Applied by the marketplace owner
 - Currently opaque and ill defined
 - Misplaced trust already acquired

Code Signing

- Subset of Blackberry API considered “controlled”
- Use of controlled package, class, or method requires appropriate code signature
- Blackberry Signature Tool comes with the Blackberry JDE
- Acquire signing keys by filling out a web form and paying \$20
 - This not is a high barrier to entry
 - 48 hours later you receive signing keys
- Install keys into signature tool

Code Signing Process

- Hash of code sent to RIM for API tracking purposes only
- RIM does not get source code
- COD file is signed based on required keys
- Application ready to be deployed

- **Easy to acquire anonymous keys**

Blackberry IT Policies

- Requires connection to Blackberry Enterprise Server (BES)
- Supersedes lower levels of security restrictions
- Can prevent devices from downloading third-party applications over wireless
- Prevent installation of specific third-party applications
- Control permissions of third party applications
 - Allow Internal Connections
 - Allow Third-Party Apps to Use Serial Port
 - Allow External Connections
- **MOSTLY “Default Allow All” policy for BES and non-BES devices**

Blackberry Application Policies

- Can be controlled at the BES
- If no BES present, controls are set on the handheld itself
- Can only be MORE restrictive than the IT policy, never less
- Control individual resource access per application
- Control individual connection access per application
- **MOSTLY “Default Allow All” policy for BES and non-BES devices**

V4.7.0.148 Default 3rd Party Application Permissions

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

V5.0.0.328 Default 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 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













Potential Effects and Behaviors











Installation Methods

- Accessing a web site using the mobile browser and choosing to download the application over the network (OTA Installation)
- Running the application loader tool on the desktop system and choosing to download the application onto the device using a physical connection to the computer
- Using enterprise management solutions to push the application to the entire user community
- **Get it into the global application marketplace and let the user choose to install it for you!**

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

Technical Methods

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



Command and Control Channels

- `initCandC(int a)`
 - Initializes inbound SMS listener if passed `a == 1`
 - Kills spyware otherwise
 - Listens for commands and acts accordingly

TXSDIE	TXSPHLON	TXSPHLOFF	TXSPIMON	TXSPIMOFF
TXSSLINON	TXSSLINOFF	TXSSLOUTON	TXSSLOUTOFF	TXSGLON
TXSGLOFF	TXSEXFILSMS	TXSEXFILSMSDG	TXSEXFILEMAIL	TXSEXFILGET
TXSEXFILPOST	TXSEXFILTCP	TXSEXFILUDP	TXSEXFILDNS	TXSDUMPGPS
TXSDUMPPL	TXSDUMPEMAIL	TXSDUMPMIC	TXSDUMPCON	TXSPROTO
TXSPORT[PORT]	TXSPHONE:[PN]	TXSURL[URL]	TXSGTIME:[N]	TXSPING
TXS:[HOST]	TXSIP:[IP]	TXSEM:[EMAIL]		



Detecting Malicious Mobile Code

Detecting Malicious Mobile Code

- Signature Based Detection
 - This is how the current anti-virus world is failing
 - Requires “known” signatures for detection
 - Too reactive

- Resource Usage White Listing
 - Require individual configuration and white listing of resources
 - Make it fine grained enough to be effective
 - Balancing act resulting in user complaints about ease of use

Detecting Malicious Mobile Code

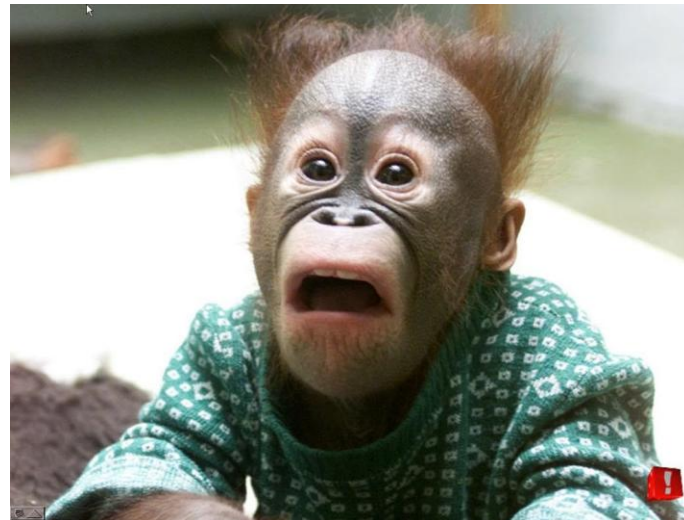
- Sandbox Based Execution Heuristics
 - Run the application and detect malicious activity
 - Requires execution in a sandbox and is reactive
 - Can't ensure complete execution

- Static Decompilation and Analysis
 - Enumeration of sources of sensitive taint and exfiltration sinks
 - Control/Data flow mapping for tracing sensitive taint from source to sink
 - Compare findings against expected values

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

Questions?

VERACODE