Practical Attacks against Mobile Device Management (MDM)

Daniel Brodie
Senior Security Researcher
Lacoon Mobile Security

March 14, 2013

About: Daniel

- Security researcher for almost a decade
- Focus
  - Vulnerabilities
  - OS
    - Mobile (Android/iOS) and PC (Windows,Linux,OS X)
- Researcher at Lacoon Mobile Security
  - Developing a dynamic analysis framework for analyzing spyphones and mobile malware

About: Michael

- Decade of experience researching and working in the mobile security space
  - From feature-phones to smartphones
  - Mobile Security Research Team leader at NICE Systems
- CEO and co-founder of Lacoon Mobile Security

Agenda

- Introduction to MDM and Secure Containers
- Rise of the Spyphones
- Bypassing secure container encryption capabilities
- Recommendations and summary

MDM AND SECURE CONTAINERS 101

Mobile Device Management

- Policy and configuration management tool
- Helps enterprises manage BYOD and mobile computing environment
- Offerings include separating between business data and personal data

MDM: Penetration in the Market

"Over the next five years, 65 percent of enterprises will adopt a mobile device management (MDM) solution for their corporate liable users"

– Gartner, Inc. October 2012

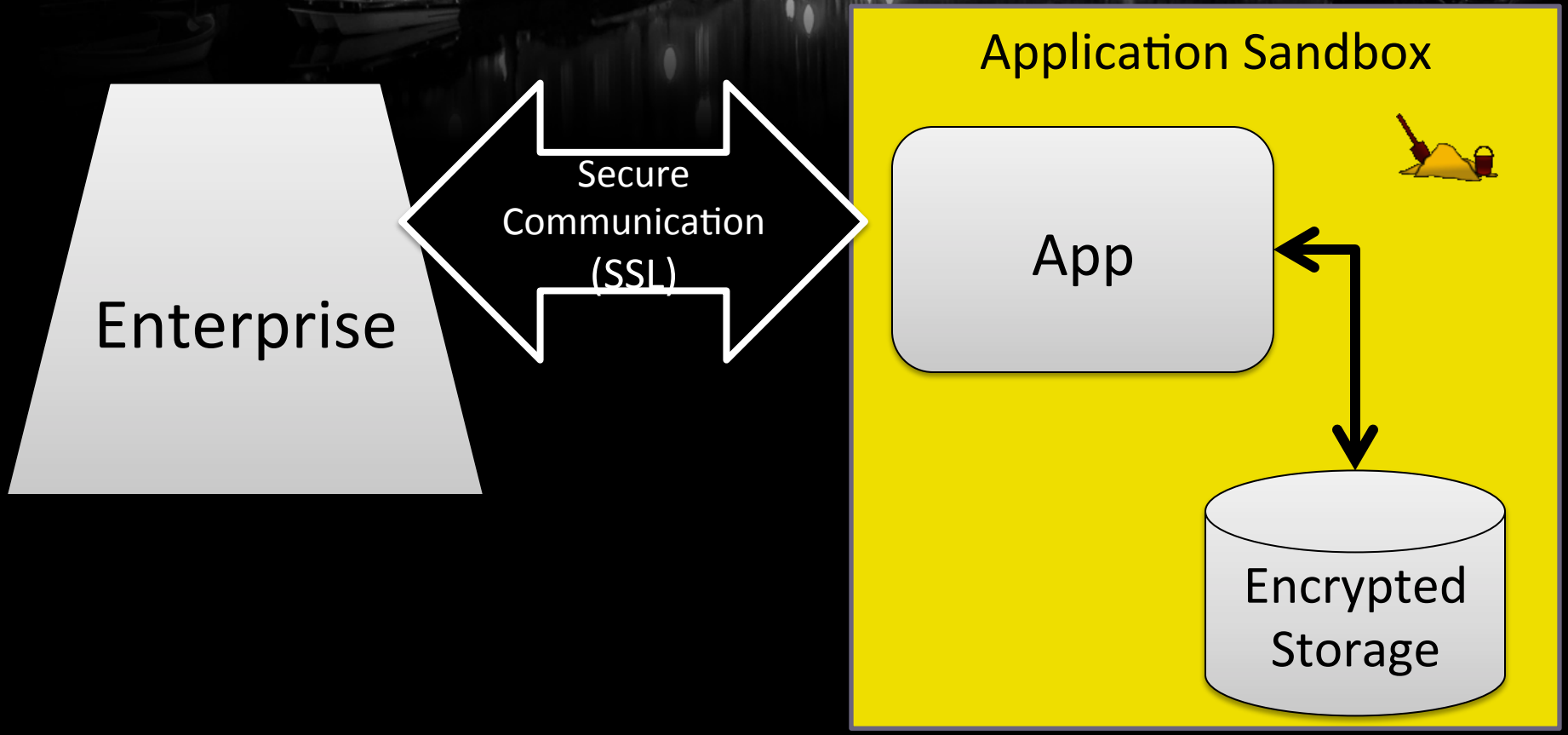
MDM Key Capabilities

- Software management
- Network service management
- Hardware management
- Security management
  - Remote wipe
  - Secure configuration enforcement
  - Encryption

Secure Containers

- All leading MDM solutions provide secure containers
  - MobileIron
  - AirWatch
  - Fiberlink
  - Zenprise
  - Good Technologies

Behind the Scenes: Secure Containers



Behind the Scenes: Secure Containers

- Runs in the mobile's OS supplied sandbox
- Encrypts all the data locally
- Communicates with the enterprise using standard encryption (SSL)

RISE OF THE SPYPHONES

The Mobile Threatscape

Business Impact

Targeted:
- Personal
- Organization
- Cyber espionage

Consumer-oriented. Mass.
Financially motivated, e.g.:
- Premium SMS
- Fraudulent charges
- Botnets

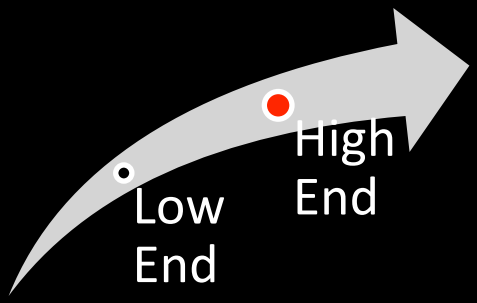
Complexity

Spyphone Capabilities

Eavesdropping and Surround Recording	Extracting Call and Text Logs
Tracking Location	Infiltrating Internal LAN
Snooping on Emails and Application Data	Collecting Passwords

Examples

More Than 50 Different Families in the Wild



The High-End

- FinSpy
  - Gamma Group
- DaVinci RCS
  - Hacking Team
- LuckyCat
  - Chinese
- LeoImpact

ITEM #	DESCRIPTION	MODEL	QTY	UNIT PRICE (Euros)
A	**Remote Intrusion Solution**			
1	**FinSpy**			
1.1	**FinSpy Software**			
1.1.1	FinSpy Proxy License FinSpy Master License FinSpy Generation License	FSPL FSML FSGL	1	188,549.00
1.1.2	FinSpy Agent License (per client)	FSAGL	2	12,887.00
1.1.3	FinSpy Activation License: - Windows - OSX (Q4/2010)	FSPCAL	10	2,646.00
	Including FinLifeline Support: FinSpy Update & Upgrade (Year 1)			
1.2	**FinSpy Hardware**			
1.2.1	FinSpy Master Server	FSM	1	6,112.00
1.2.2	FinSpy Agent Workstation	FSAG	2	1,112.00
1.2.3	FinSpy Common & Spare Parts	FSC	1	12,223.00
1.4	**FinSpy - Installation & Training**			
	FinSpy Installation and Product Training Number of Students: 2-4	FSTI	1	19,445.00

The Low-End

- Starting at $4.99 a month! What a steal!
  - For iOS, Android, Blackberry, Windows Mobile/ Phone, Symbian, …
- Professional worldwide support
- Very simple and mainstream
  - So simple that even your mother could use it
    - On your father
- Available at a reseller near you!

Spyphones: Varying Costs, Similar Results

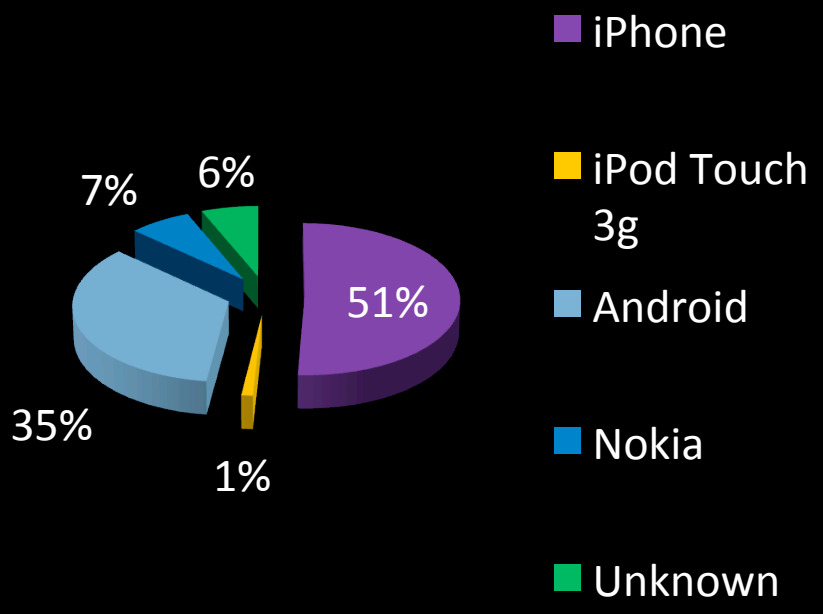
- From high-end to low-end
  - Difference is in infection vector -> price
- End-result is the same
  - For $5, you get nearly all the capabilities of a $350K tool

SPYPHONE DEMO

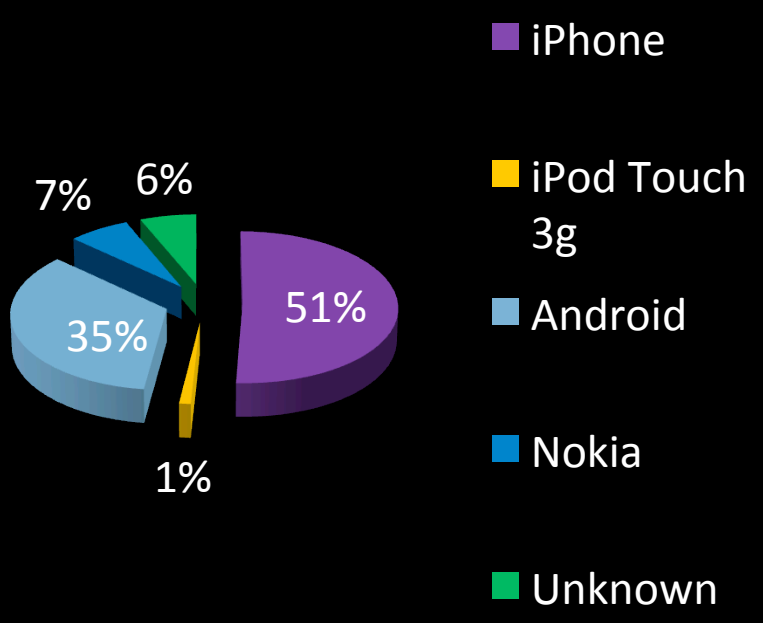
Spyphones in the Wild

- Partnered with worldwide cellular network operators:
  - Sampled 250K subscribers
  - Two separate sampling occasions
- Infection rates:
  - March 2012: 1 in 3000 devices
  - October 2012: **1 in 1000 devices**

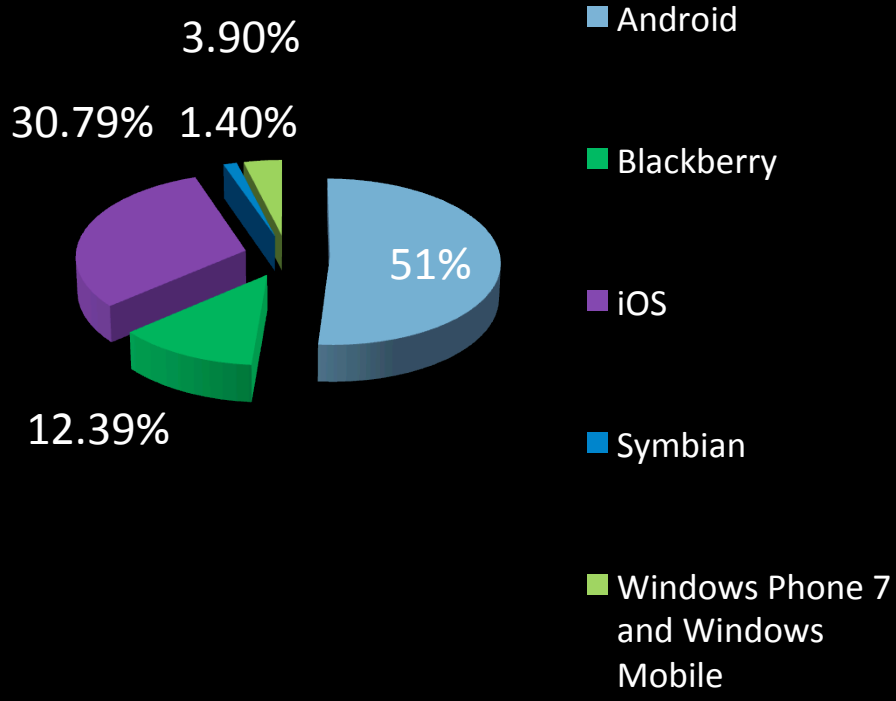
Spyphone Distribution by OS



Spyphone Distribution by OS



Mobile OS Market Share



Comscore, March 2012

IT'S ALRIGHT,
IT'S OK,
"SECURE CONTAINER"
IS THE WAY?

Secure Container Re-Cap

- Secure Containers:
  - Detect JailBreak/Root
  - Prevent malicious application installation
  - Encrypt data
  - Part of the OS sandbox

Opening the Secure Container (1)

- JailBreaking (iOS)/ Rooting (Android) detection mechanism
  - "Let Me Google That For You"
  - Usually just check features of JB/ Root devices (e.g. is Cydia/ SU installed)
- Cannot detect exploitation

Opening the Secure Container (2)

- Prevention of malicious app installation (Android)
  - Targeted towards mass malware
- Third-Party App restrictions
  - Should protect against malware
- Has been bypassed
  - Wait a few slides…

ANDROID DEMO

Android Demo: Technical Details (1)

- Publish an app through the market
  - Use “Two-Stage”: Download the rest of the dex later- and only for the targets we want
- Get the target to install the app
  - Through spearphishing or physical access to the device

Android Demo: Technical Details (2)

- Privilege Escalation
  - We used the Exynos exploit. (Released Dec., 2012)
- Create a hidden 'suid' binary and use it for specific actions
  - Place in a folder with --x--x--x permissions
- Undetected by generic root-detectors

Android Demo: Technical Details (3)

- We listen to events in the logs
  - For <=2.3 we can just use the logging permissions
  - For >4.0 we use access the logs as root
- When an email is read….

L...	Time	PID	TID	Application	Tag	Text
I	01-24 12:47:3...	2099	2134		ClipboardS...	mCBPickerDialog enter case. MSG_DISMISS_DIALOG
D	01-24 12:47:3...	2099	2153		KeyguardVi...	setHidden false
D	01-24 12:47:3...	2099	2153		KeyguardVi...	setHidden false
D	01-24 12:47:3...	2099	2153		KeyguardVi...	setHidden false
D	01-24 12:47:3...	2099	2153		KeyguardVi...	setHidden false
I	01-24 12:47:3...	3569	5579		GATE	<GATE-M>DEV_ACTION_COMPLETED</GATE-M>
I	01-24 12:47:3...	2099	2134		ClipboardS...	mCBPickerDialog enter case. MSG_DISMISS_DIALOG
D	01-24 12:47:3...	2099	2153		KeyguardVi...	setHidden false
D	01-24 12:47:3...	2099	2153		KeyguardVi...	setHidden false
D	01-24 12:47:3...	2099	2153		KeyguardVi...	setHidden false
D	01-24 12:47:3...	2099	2153		KeyguardVi...	setHidden false
I	01-24 12:47:3...	1904	2052		SurfaceFli...	id=17 Removed HomeScreenActivity idx=2 Map Size=4

Android Demo: Technical Details (3)

- We dump the heap using /proc/<pid>/maps and /mem
  - Then search for the email structure, extract it, and send it home

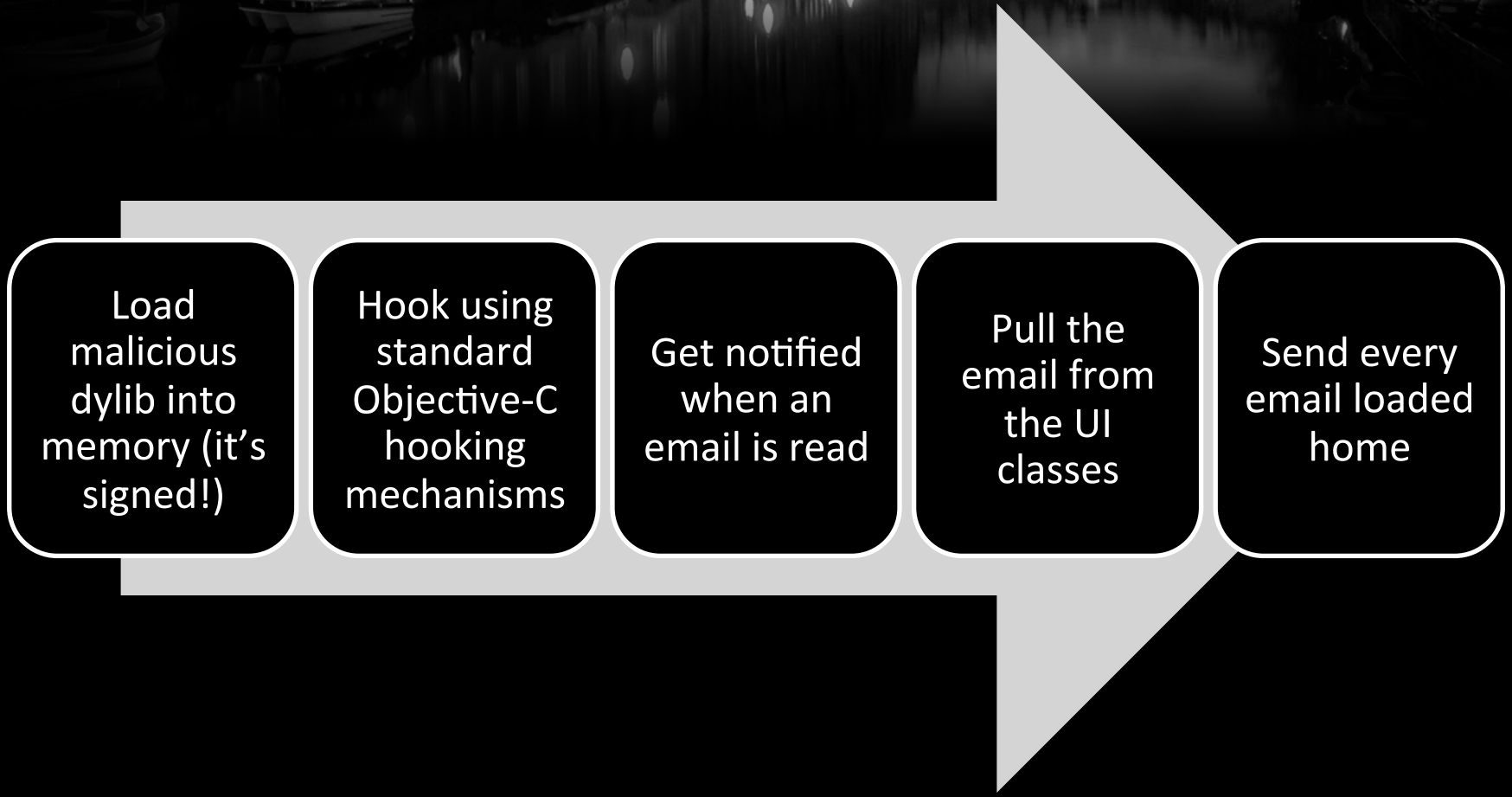
```
00153C90  02 00 00 00 C3 0A 00 00 3C 21 44 4F 43 54 59 50  ....Q...<!DOCTYP
00153CA0  45 20 48 54 4D 4C 20 50 55 42 4C 49 43 20 22 2D  E HTML PUBLIC "-
00153CB0  2F 2F 57 33 43 2F 2F 44 54 44 20 48 54 4D 4C 20  //W3C//DTD HTML
00153CC0  33 2E 32 2F 2F 45 4E 22 3E 0D 0A 3C 48 54 4D 4C  3.2//EN">..<HTML
00153CD0  3E 0D 0A 3C 48 45 41 44 3E 0D 0A 3C 4D 45 54 41  >..<HEAD>..<META
00153CE0  20 48 54 54 50 2D 45 51 55 49 56 3D 22 43 6F 6E   HTTP-EQUIV="Con
00153CF0  74 65 6E 74 2D 54 79 70 65 22 20 43 4F 4E 54 45  tent-Type" CONTE
00153D00  4E 54 3D 22 74 65 78 74 2F 68 74 6D 6C 3B 20 63  NT="text/html; c
00153D10  68 61 72 73 65 74 3D 57 69 6E 64 6F 77 73 2D 31  harset=Windows-1
00153D20  32 35 32 22 3E 0D 0A 3C 4D 45 54 41 20 4E 41 4D  252">..<META NAM
00153D30  45 3D 22 47 65 6E 65 72 61 74 6F 72 22 20 43 4F  E="Generator" CO
00153D40  4E 54 45 4E 54 3D 22 4D 53 20 45 78 63 68 61 6E  NTENT="MS Exchan
```

IOS DEMO

iOS Demo: Technical Details (1)

- Install signed application
  - Using Enterprise/Developer certificate
- Use the JailBreak
  - To complete the hooking
- Remove any trace of the JailBreak

iOS Demo: Technical Details (2)



CONCLUSIONS

Secure Containers…Secure?

- “Secure” Containers depend on the integrity of the host system
  1. If the host system is uncompromised: what is the added value?
  2. If the host system is compromised: what is the added value?
- We’ve been through this movie before!

Infection is Inevitable

- MDM provides Management, not absolute Security
- Beneficial to separate between business and personal data
- Main use-case
  - Remote wipe of enterprise content only
  - Copy & Paste DLP

Mitigating Spyphone Threats

- Use MDM as a baseline defense for a multi-layer approach
- Needs rethinking outside the box (mobile)
- Solutions on the network layer:
  - C&C communications
  - Heuristic behavioral analysis
  - Sequences of events
  - Data intrusion detection

THANK YOU!

QUESTIONS?