

Practical Attacks against Mobile Device Management (MDM) Solutions

SESSION ID: MBS-T08

Dan Koretsky

Sr. Security Strategist
Lacoon Mobile Security
@LacoonSecurity



Agenda

- ◆ Intro to Mobile Cyber-Espionage
 - ◆ The proliferation of mobile surveillance toolkits
- ◆ Your Data
 - ◆ Exploits to target enterprise data on mobile devices
- ◆ Your information
 - ◆ Point & Click mRATs to target business activity
- ◆ Your Life
 - ◆ Mobile device Trojans as a Service (M-TaaS) to target it all

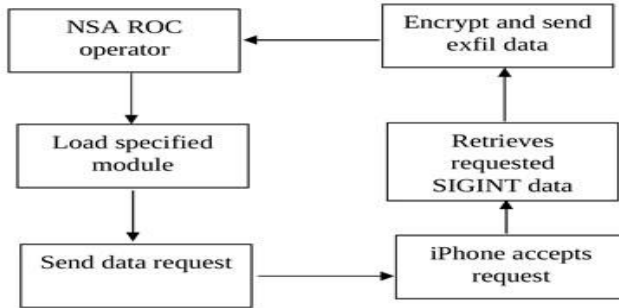


DROPOUTJEEP

ANT Product Data

(TS//SI//REL) DROPOUTJEEP is a STRAITBIZARRE based software implant for the Apple iPhone operating system and uses the CHIMNEYPOOL framework. DROPOUTJEEP is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.

10/01/08



(U//FOUO) DROPOUTJEEP – Operational Schematic

(TS//SI//REL) DROPOUTJEEP is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted.

(TS//SI//REL) The initial release of DROPOUTJEEP will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release.

Unit Cost: \$ 0

Status: (U) In development

POC: U//FOUO [REDACTED], S32222, [REDACTED]@nsa.gov



Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

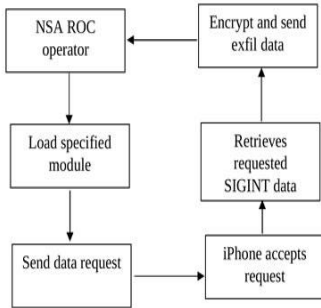


DROPOUTJEEP

ANT Product Data

(TS//SI//REL) DROPOUTJEEP is a STRAITBIZARRE based software implant for the Apple iPhone operating system and uses the CHIMNEYPOOL framework. DROPOUTJEEP is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.

10/01/08



(U//FOUO) DROPOUTJEEP - Operational Schematic

(TS//SI//REL) DROPOUTJEEP is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted.

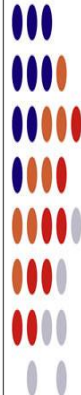
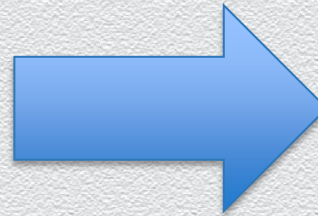
(TS//SI//REL) The initial release of DROPOUTJEEP will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release.

Unit Cost: \$ 0

Status: (U) In development

POC: U//FOUO [redacted], S32222, [redacted]@nsa.gov

Derived From: NSACSSM 1-52
Dated: 20070108
Declassify On: 20320108



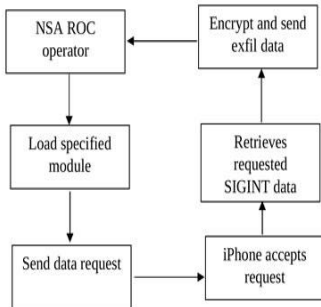


DROPOUTJEEP

ANT Product Data

10/01/08

(TS//SI//REL) DROPOUTJEEP is a STRAITBIZARRE based software implant for the Apple iPhone operating system and uses the CHIMNEYPOOL framework. DROPOUTJEEP is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.



(U//FOUO) DROPOUTJEEP - Operational Schematic

(TS//SI//REL) DROPOUTJEEP is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted.

(TS//SI//REL) The initial release of DROPOUTJEEP will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release.

Unit Cost: \$ 0

Status: (U) In development

POC: U//FOUO [redacted], S32222, [redacted]@nsa.gov

Derived From: NSACSSM 1-52
Dated: 20070108
Declassify On: 20320108



VUPEN[®]
security


FINFISHER[™]
IT INTRUSION

]HackingTeam[



SS8[®]

 E-mail this to a friend

 Printable version

UAE Blackberry update was spyware

By Ben Thompson

BBC Middle East Business Report, Dubai

An update for Blackberry users in the United Arab Emirates could allow unauthorised access to private information and e-mails.

The update was prompted by a text from UAE telecoms firm Etisalat, suggesting it would improve performance.

Instead, the update resulted in crashes or drastically reduced battery life.

Blackberry maker Research in Motion (RIM) said in a statement the update was not authorised, developed, or tested by RIM.

Etisalat is a major telecommunications firm based in the UAE, with 145,000 Blackberry users on its books.



Etisalat sent a text to its 145,000 Blackberry users



Why Hack Mobile Devices?



By 2016, 65% of smartphones and tablets will be used in BYOD environments

IDC Research

Impacts of a Mobile Attack



- ◆ Snooping on corporate emails and application data
- ◆ Record calls and SMSs
- ◆ Infiltrating internal LANs
- ◆ Activate the Microphone
- ◆ Extracting contact lists, call and text logs
- ◆ Track locations
- ◆ Steal App Data



**Enterprise Mobile
Data Protection.
Solutions?**

MDMs, Secure Containers & Wrappers

3 main features:

- **Encrypt business data**
- **Encrypt communications to the business**
- **Detect Jailbreak / Rooting of devices**

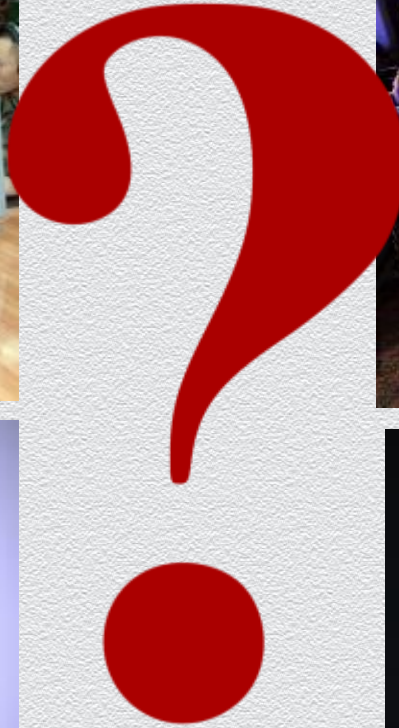


Self-Defense Apps



Part 1.
Your Data

Who Are These Attackers?



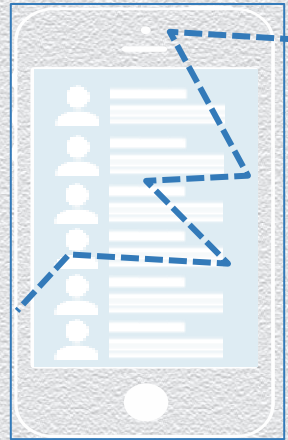
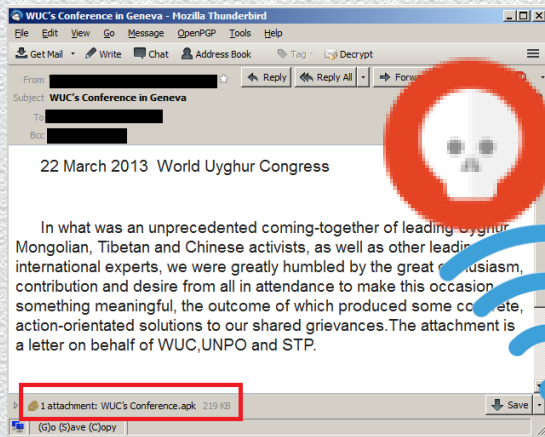


12 Hours | 1000USD



Attack Demo on Containers & Wrappers

Anatomy of an Attack



Infect the Device

1

Install a Backdoor
(a.k.a. Rooting)

2

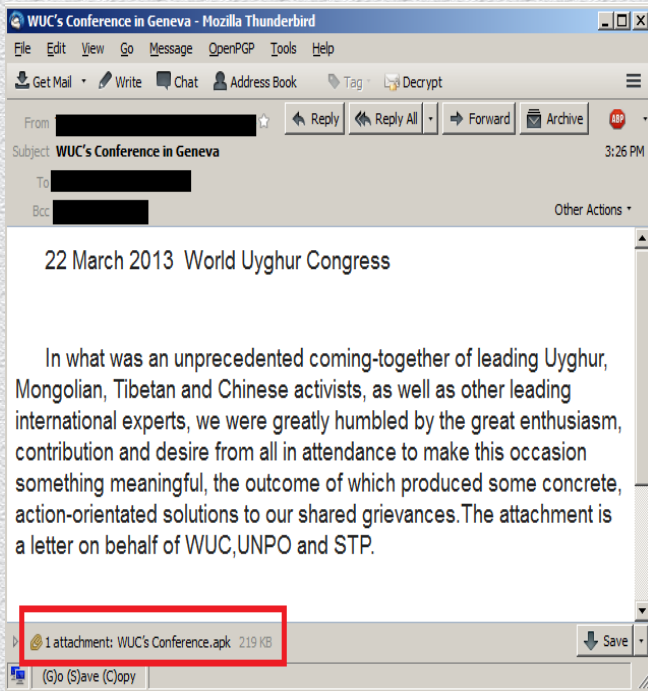
- Administrative
- Vulnerability
- Exploit

Bypass the
Containerization

3

- Exfiltrate Information in Plain Text

Step 1: Attack the Device



Step 2: Install a Backdoor / aka Rooting

- ◆ Administrative
 - ◆ Every process can run as an administrative (root) user if it is able to trigger a vulnerability in the OS
- ◆ Vulnerability
 - ◆ Each Android device had/ has a public vulnerability
- ◆ Exploit
 - ◆ Detection mechanisms don't look at apps that exploit the vulnerability

Step 3: Bypass Containerization



Storage

Step 3: Bypass Containerization



Storage



Step 3: Bypass Containerization



Storage



Memory

Step 3: Bypass Containerization



Storage



Memory



Exfiltrate information

How Many Privilege Escalation Exploits are Out There?

Date	Name	CVE / Bug #	Affected Devices
12/2012	Exynos	CVE-2012-6422	Most Samsung Devices (Galaxy S2/3, Note...)
2013	MasterKey 1-3	CVE-2013-4787, #9695860 #9950697	3 vulnerabilities which affect all devices
2013	V-Root	CVE-2013-6282	All devices, bypass SEAndroid...
06/2014	TowelRoot	CVE-2014-3153	Most new android devices

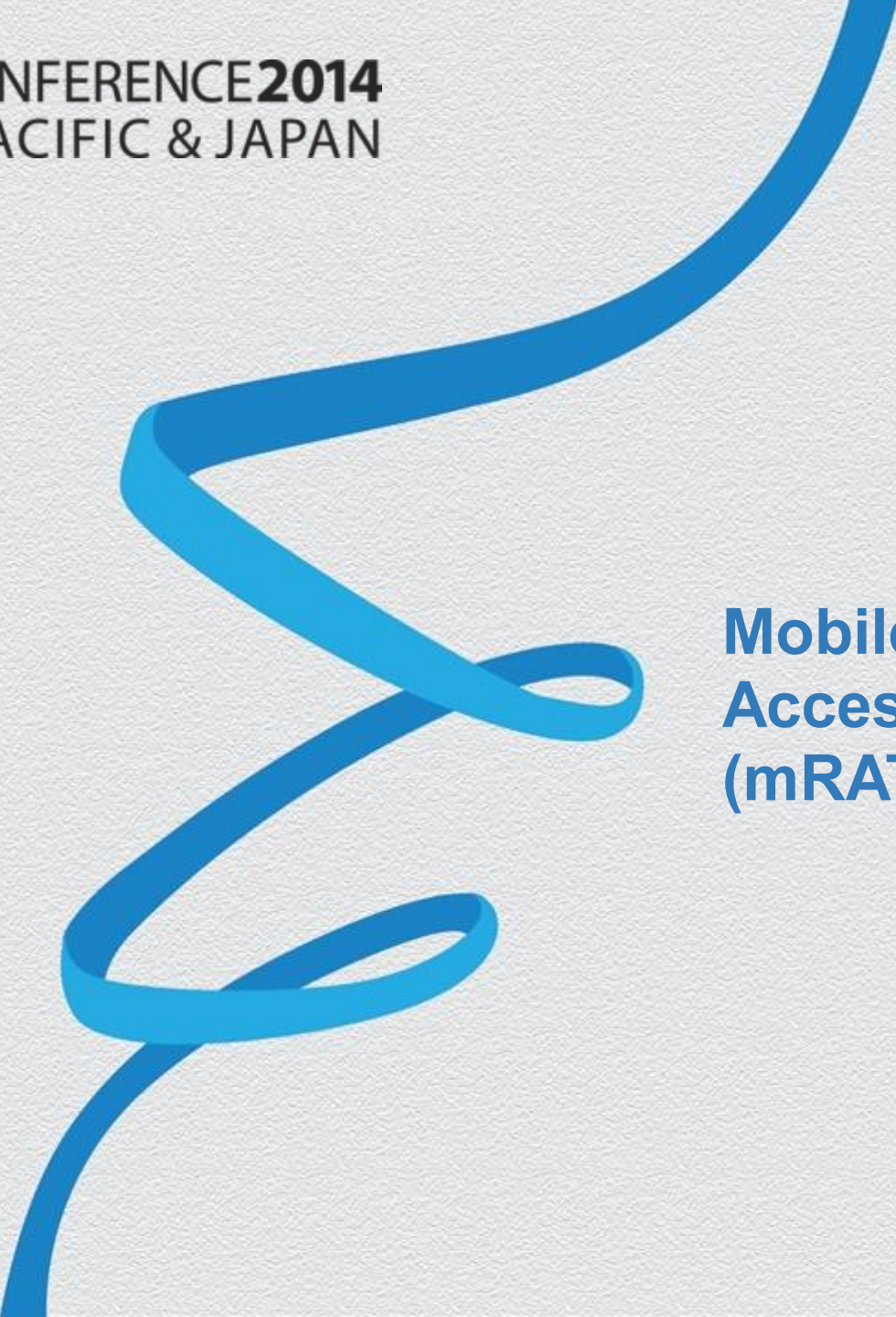


Part 2.
Your Information





Point n' Click | Free (0 USD)



Mobile Remote Access Trojans (mRATs)

AndroRAT – Point n' Click mRAT Generator

- ◆ Injects polymorphic mobile remote access Trojan to any Android application
- ◆ Released as Open Source on Nov 2012
- ◆ <https://github.com/DesignativeDave/androrat>
- ◆ Forked many times
- ◆ Available on many dark forums



AndroRAT Demo



Part 3.
Your Life



**Mobile Trojans as a
Service (M-TaaS)**

**(Commercial
Surveillance Tools)**





Read the Manual | 60 USD per Year

Spy on Android to get the truth today!

Searching for sparkling wells of truth? Tired of being led to ? Not sure you really know what's your employees or family members are up to ? Stop worry-wracking your brain and heart over it ! Now you get a chance to make lies disappear from your life by monitoring their Android!

[BUY NOW](#)



FEATURES



RECORD CALLS

Truth is a treasure worth digging for. Dig for it by using mSpy as a call recording tool. Log suspicious contacts in the phone book. Record calls received from them and listen to the recordings from the comfort of your home.



TRACK GPS LOCATION

Fear that it's time for hidden secrets to be revealed? Worried about someone's safety? Find out where they are, where they will be, and where they have been. Track their location and their route history with mSpy.



SPY ON TEXT MESSAGES

Some text messages can leave you in pain or lift a huge weight off your shoulders. Especially if they weren't meant for you. Ready to face the truth? View the content of all text messages sent and received by the target Android phone.



SPY ON GMAIL

It's no secret that Gmail ranks among the top apps for Android. Suspect that your target Android user is hiding something from you? Monitor their Gmail conversations and get the answers you are looking for.



VIEW MULTIMEDIA FILES

Smartphones have become the go-to device for many users who want to take photos and videos on the fly. Need to find out as much info as possible about someone? Install mSpy onto their Android device and look through all the multimedia files.



INTERCEPT INSTANT MESSAGES

Does your tracking needs include spying on instant messengers? Use mSpy to read messages exchanged via Skype, WhatsApp, and Viber. Need to monitor Facebook chats?

[Click here to DM!](#)

Set up new phone

Add Phone

Dashboard

Contacts

Call Logs

Text Messages

Call Recordings

Locations

Photos

Video Files

Recordings

Browser History

Emails

Events

Block Websites

Skype

WhatsApp

Facebook Tracking

Viber

Installed Apps

Keylogger

Phone Management

Device Info

Android, Build: 4.3.1 IMEI: 357378050044204

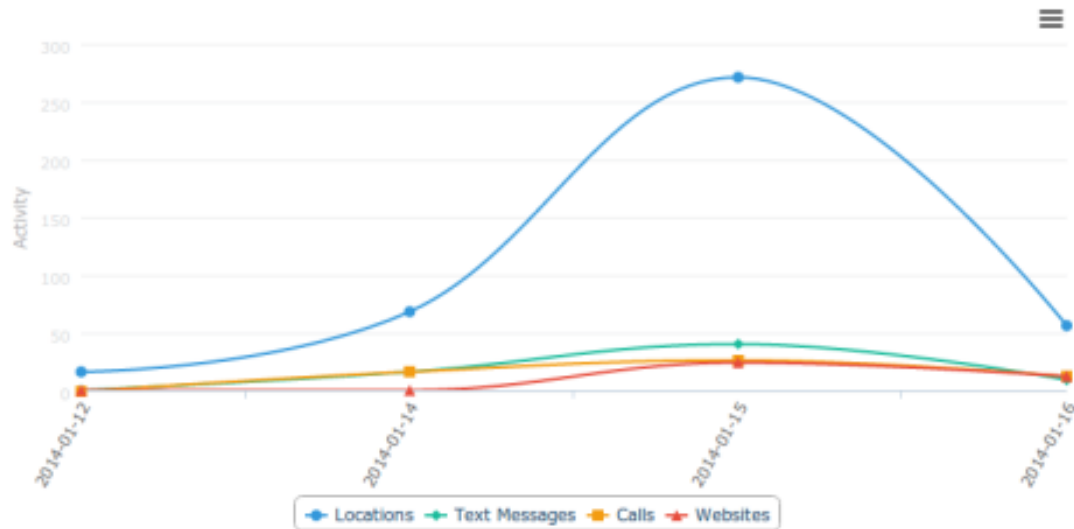
14% Wi-Fi: Off Location tracker: On

Account Info

Plan: Premium
Phone ID: Q1690033
Subscription: 07/09/2014 11:49 AM

Extend Subscription

Cell Phone Activity



Synchronization method: Don't Sync Wi-Fi Only All Connections

10 Most Calling Contacts

See More

Locations


SFO Terminal 3, San Francisco

See More

Rank	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
10-9 Excellent	PhoneSheriff	mSpy	Mobile Spy	My Mobile Watchdog	MobiStealth	StealthGenie	SpyPhone Basic Internet	SpyBubble	eBlaster Mobile	Flexispy
8-6 Good										
5-4 Average										
3-2 Poor										
1-0 Bad										
Print/Email										
Reviewer Comments	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review	Read Review
Lowest Yearly Price	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now	Buy Now
	\$49.97	\$159.00	\$99.97	\$59.40	\$89.99	\$99.99	\$349.00	\$49.95	\$69.95	\$149.00
Ratings	9.70	9.68	8.78	8.65	8.15	8.15	7.80	7.40	6.90	6.38
Overall Rating										
Reporting & Logging										
Report Display (percentage)	95	100	80	50	70	80	40	50	40	20
Call History/Details	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Text/SMS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Email	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
GPS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Picture	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Internet	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Contact Details	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Video	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Calendar Updates	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Bookmark	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Features										
Compatibility Score (percentage)	100	100	100	40	100	80	100	100	60	100
Number of Phones	1	1	3	5	1	1	1	1	1	1
Stealth	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ability to Filter or Search	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Keyword Alerts	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web Blocking	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Lacoon Research – Targeted Infection Realities

mRAT Distribution by Operating System

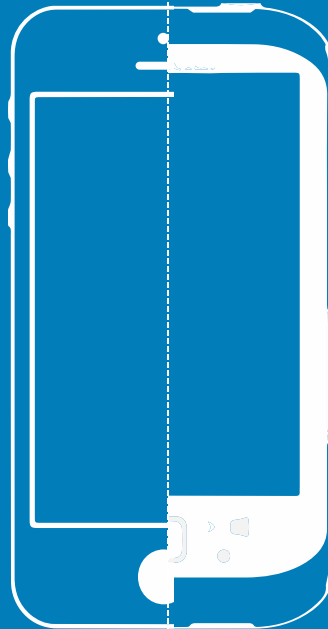


1/1000
Devices
is Infected

iOS unknown
29%

iOS 6
13%


iOS 5
5%



Android unknown
23%

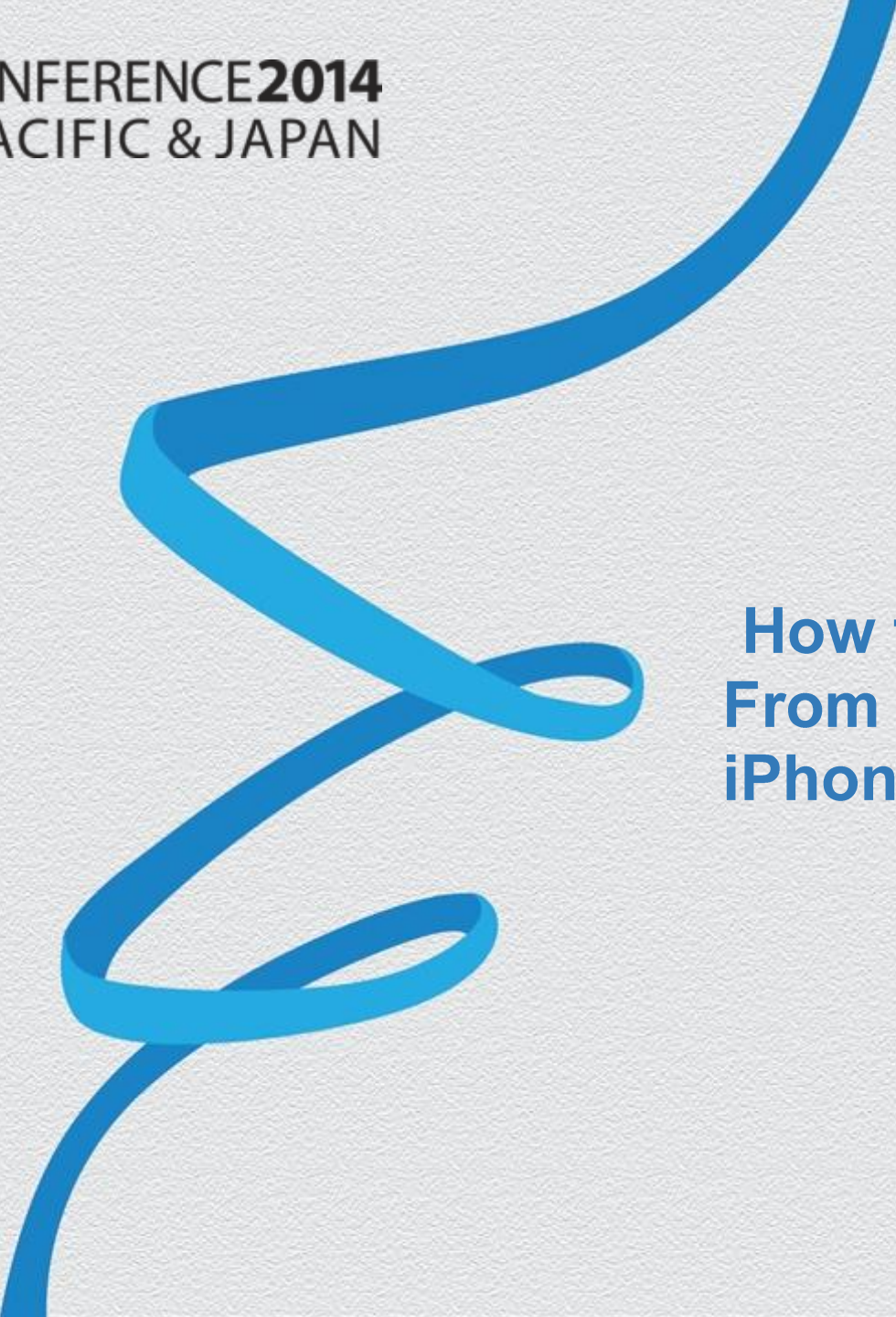
Android 4.x
22%

Android 2.3
8%



47%
of the
infected devices
were iOS

Sampling of 650,000 devices in July, 2013



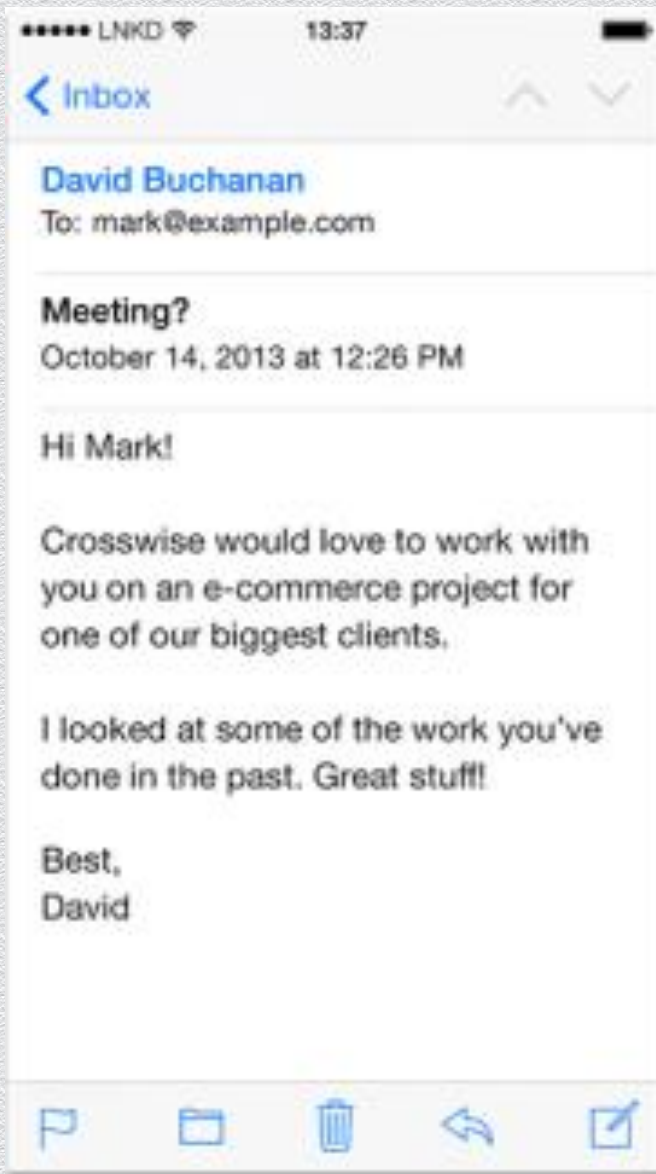
How to Extract Data From a non-JB iOS7 iPhone?

Malicious Configuration Profiles



Malicious Configuration Profiles





Without Intro



With Intro



MitM Attack Demo

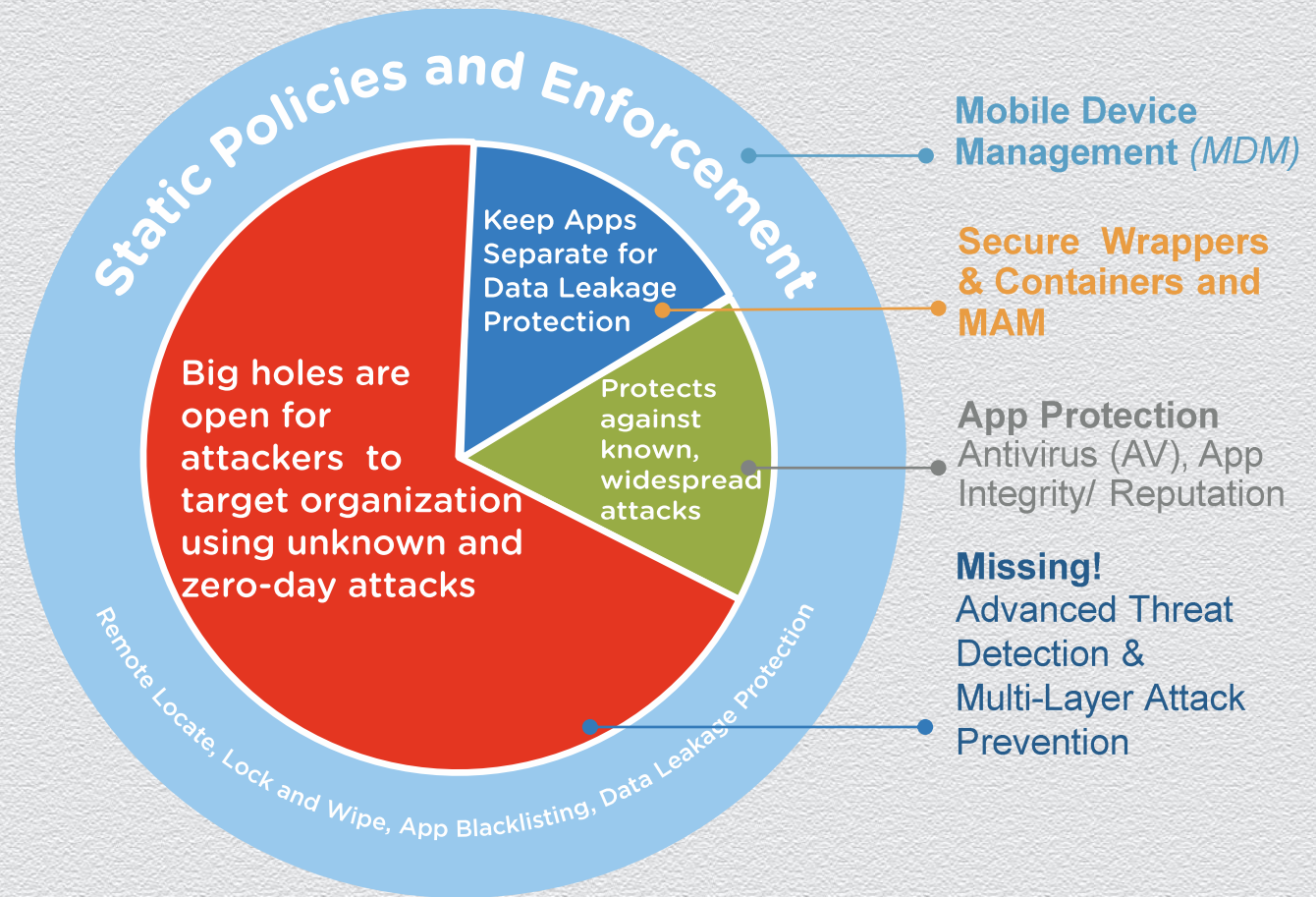


Mitigation

Current Solutions in Use to Protect Mobility

72% of IT admins believe there is a gap between current mobile security solutions and the threats that businesses face today.

-Forrester Research



Current Mitigation: Static Controls

Mobile Device Management
(MDM)

Containers

Wrapper

Active Sync

NAC

Required Mitigation: Real-time, Adjustable Controls

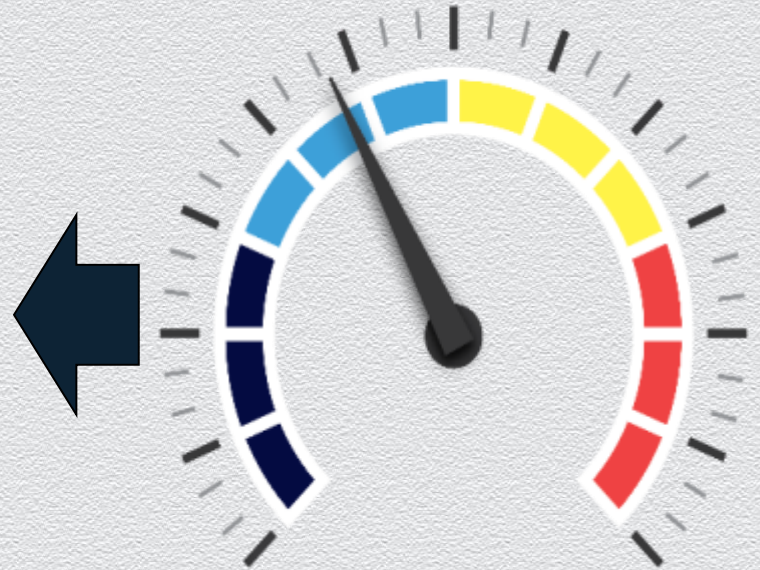
Mobile Device Management (MDM)

Containers

Wrapper

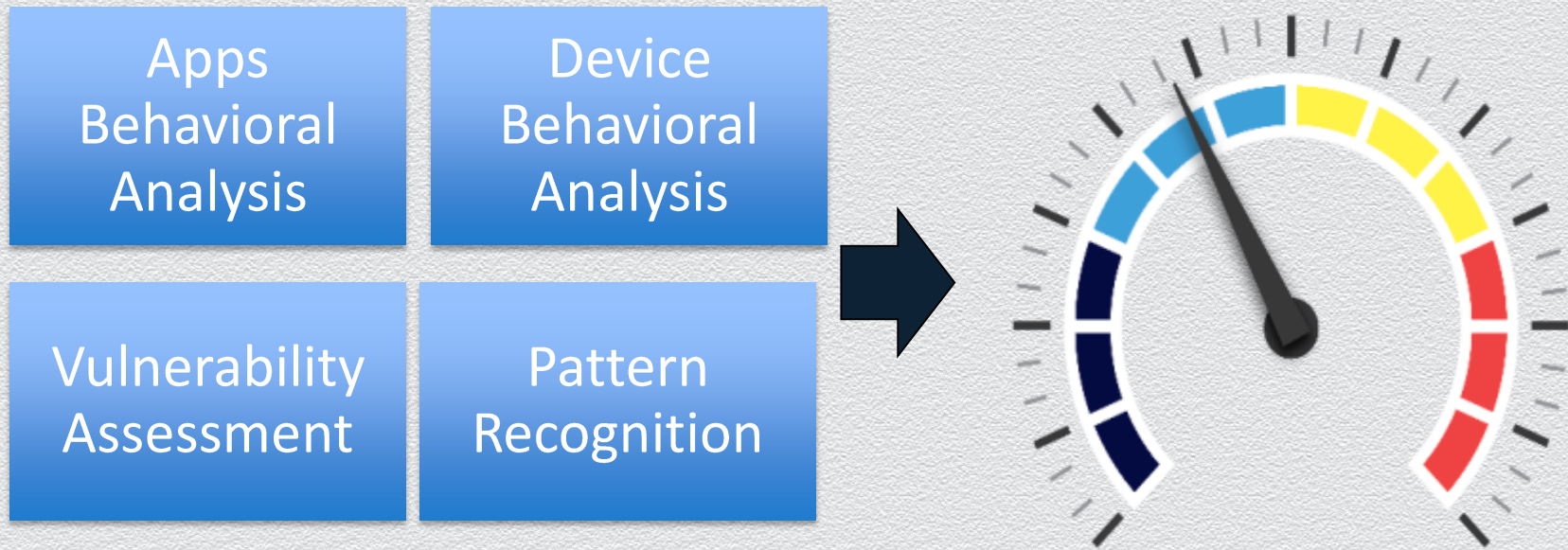
Active Sync

NAC



Preserve User Privacy
and Experience

Use Multi-Layer Detection to Calculate Device Risk



Thank You.

Contact details:

www.lacoon.com

DANK@lacoon.com

Twitter: @LacoonSecurity