

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Practical Attacks against MDM Solutions (and What Can You Do About It)

SESSION ID: MBS-R02

Michael Shaulov

CEO and Co-Founder

Lacoon Mobile Security
@LacoonSecurity



Agenda

- ◆ 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
- ◆ Hacking iOS devices?



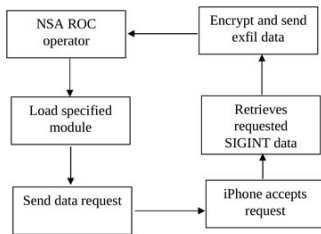
TOP SECRET//COMINT//REL TO USA, FVEY

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

TOP SECRET//COMINT//REL TO USA, FVEY



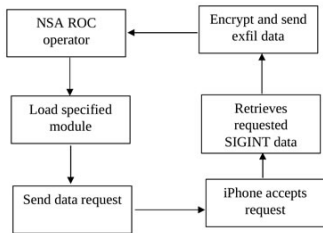
TOP SECRET//COMINT//REL TO USA, FVEY

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], \$32222, [REDACTED]@nsa.gov

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

TOP SECRET//COMINT//REL TO USA, FVEY





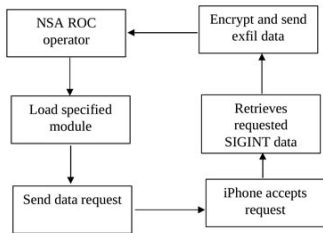
TOP SECRET//COMINT//REL TO USA, FVEY

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

TOP SECRET//COMINT//REL TO USA, FVEY



 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 sent a text to its 145,000 Blackberry users

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

<http://www.youtube.com/watch?v=R63CRBNLE2o>



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Part 0. Why Hack Enterprise Mobile Devices?



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

IDC Research

Mobile Devices: an Attractive Attack Target



- ◆ Snooping on corporate emails and application data
- ◆ Infiltrating internal LANs
- ◆ Eavesdropping
- ◆ Extracting contact lists, call and text logs
- ◆ Tracking location

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Enterprise Mobile Data Protection. Solutions?

Enterprise Security and Data Protection Solutions

- ◆ Mobile Device Management (MDM)
- ◆ Secure Containers
- ◆ Wrappers
- ◆ VDI

MDMs, Secure Containers & Wrappers

- ◆ 3 features
 - ◆ Encrypt business data
 - ◆ Encrypt communications to the business
 - ◆ Detection Jailbreak/ Rooting of devices



Self-Defense Apps

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Part 1. Your Data





12 Hours | 1000USD

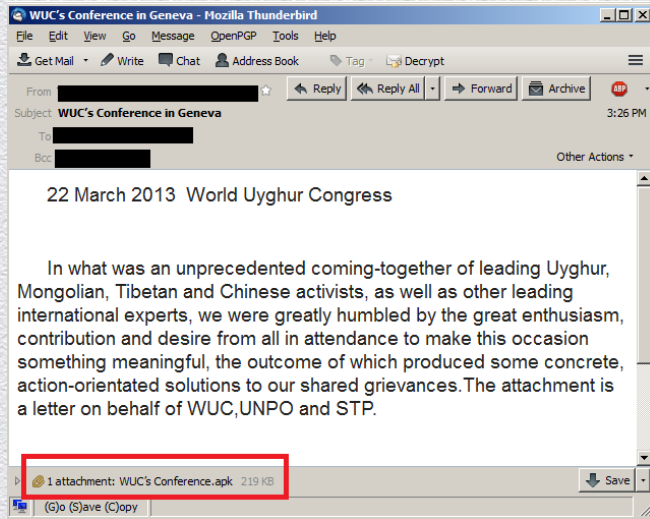


RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Attack Demo Android

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



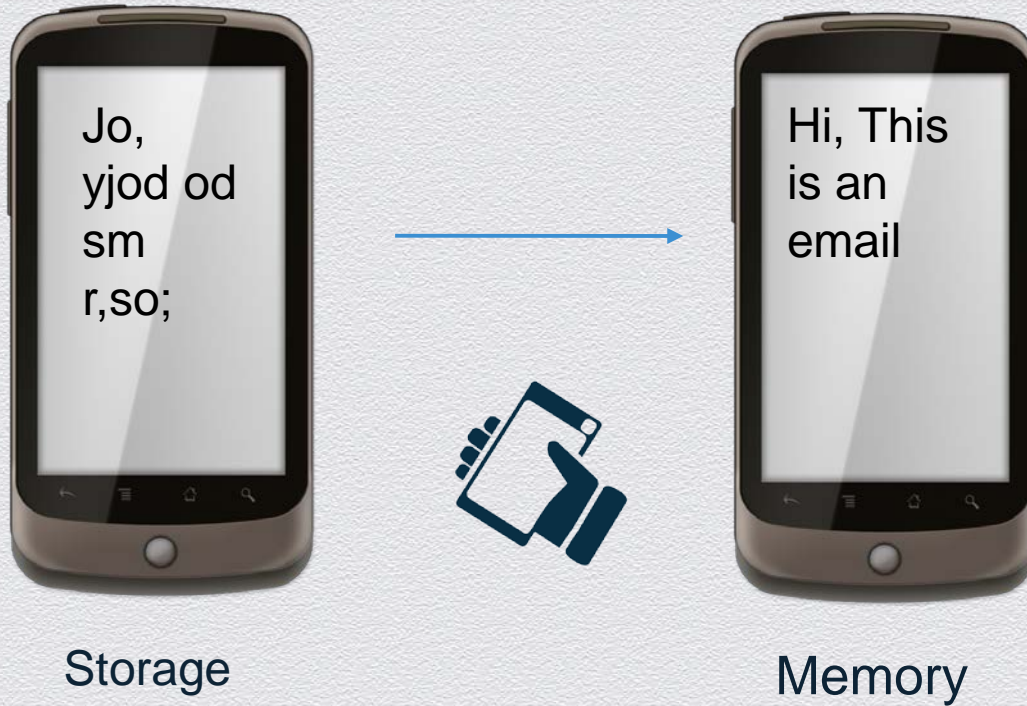
Storage

Step 3: Bypass Containerization



Storage

Step 3: Bypass Containerization



Step 3: Bypass Containerization



Storage



Memory



Exfiltrate
information

How Many Privilege Escalation Exploits in the Wild?

Date	Name	CVE / Bug #	Affected Devices
12/2012	Exynos	CVE-2012-6422	Most Samsung Devices (Galaxy S2/3, Note...)
6/2013	MasterKey 1	CVE-2013-4787	All devices
8/2013	MasterKey 2	#9695860	All devices
11/2013	MasterKey 3	#9950697	All devices
11/2013	V-Root	CVE-2013-6282	All devices, bypass SEAndroid...

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Part 2. Your Information





Point n' Click | Free (0 USD)



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

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

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



AndroRAT Demo

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Part 3. Your Life



RSA[®]CONFERENCE2014

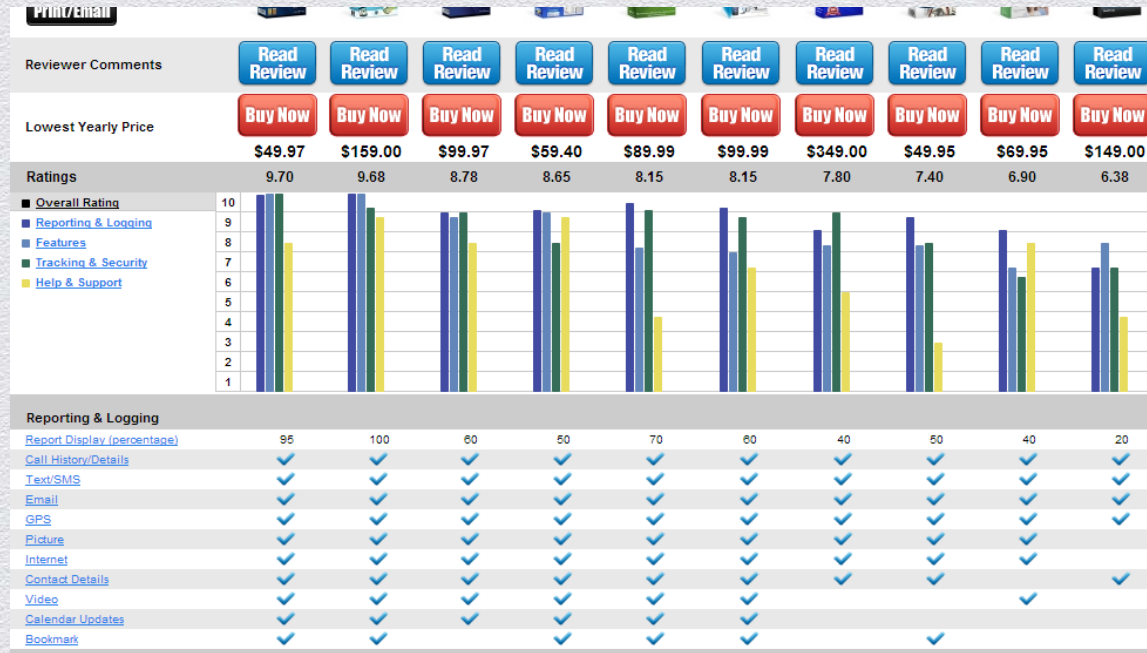
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Mobile Device Trojans as a Service (M-TaaS)





Read the Manual | 60 USD Per Year



Commercial Mobile Surveillance Tools

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

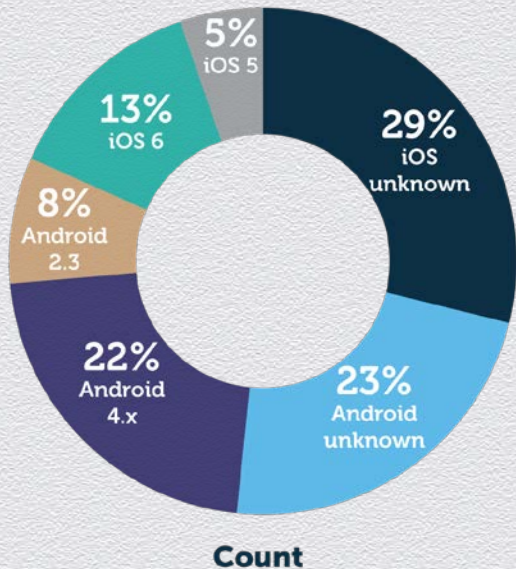


mSPY Demo

Survey: Cellular Network 2M Subscribers

Sampling: 650K

mRAT Distribution by OS



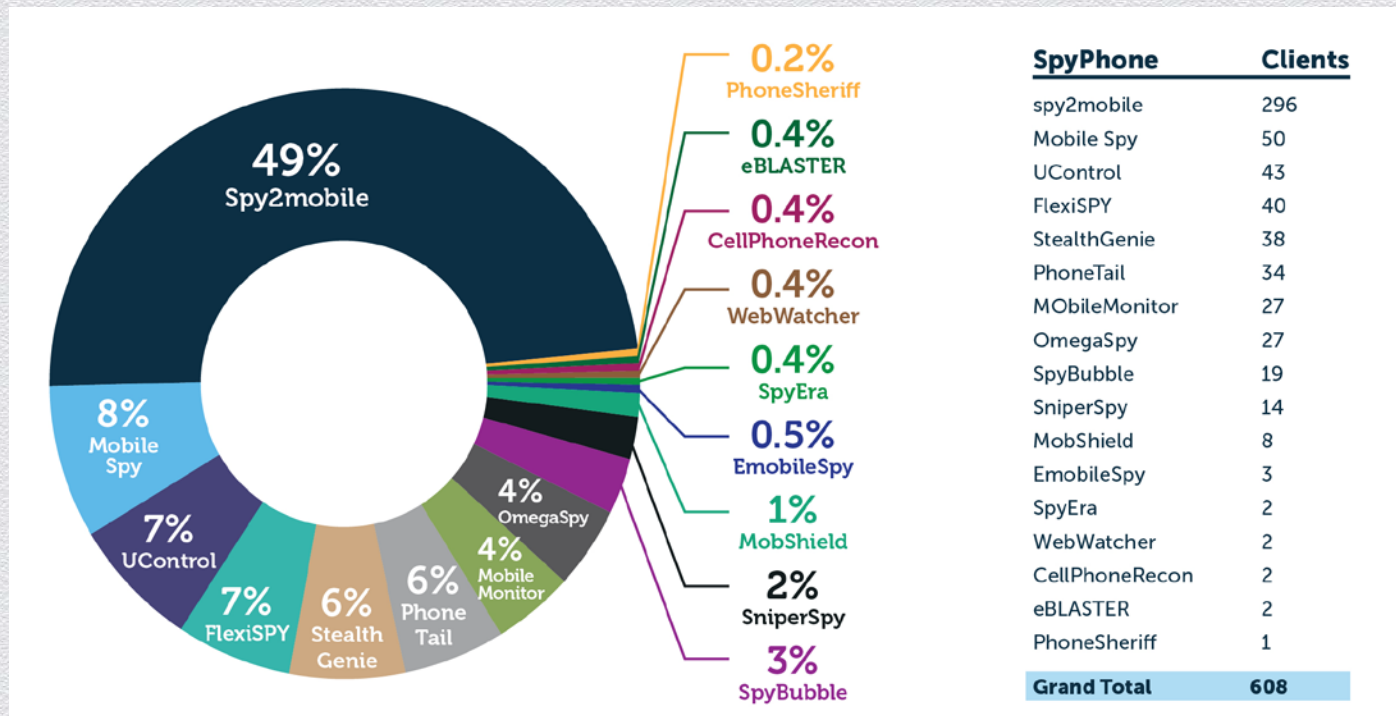
Infection rates:

June 2013:

1 / 1000 devices

Survey: Cellular Network 2M Subscribers

Sampling: 650K





Attack: iPhone

Step 1: Attack the Device

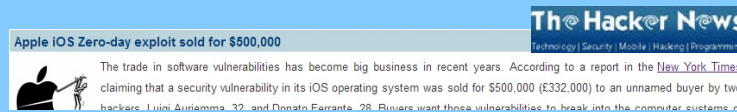


Step 2: Install a Backdoor

- ◆ Use the Jailbreak
- ◆ Perform the hooking to the secure container
- ◆ Remove any trace of the Jailbreak

Step 2: Install a Backdoor

Community



Jailbroken



xCon

Bypassing Jailbreak Detection

Recently, a sizable handful of applications in Apple's own App Store have been implementing procedures to check for risks of jailbreaking your device (e.g. banking companies don't want the blame for some rogue keylogger disguised as their apps. Video streaming apps are notorious for this; the companies don't want users bypassing restrictions to watch malicious intent or lack thereof.

Step 3: Bypass Containerization



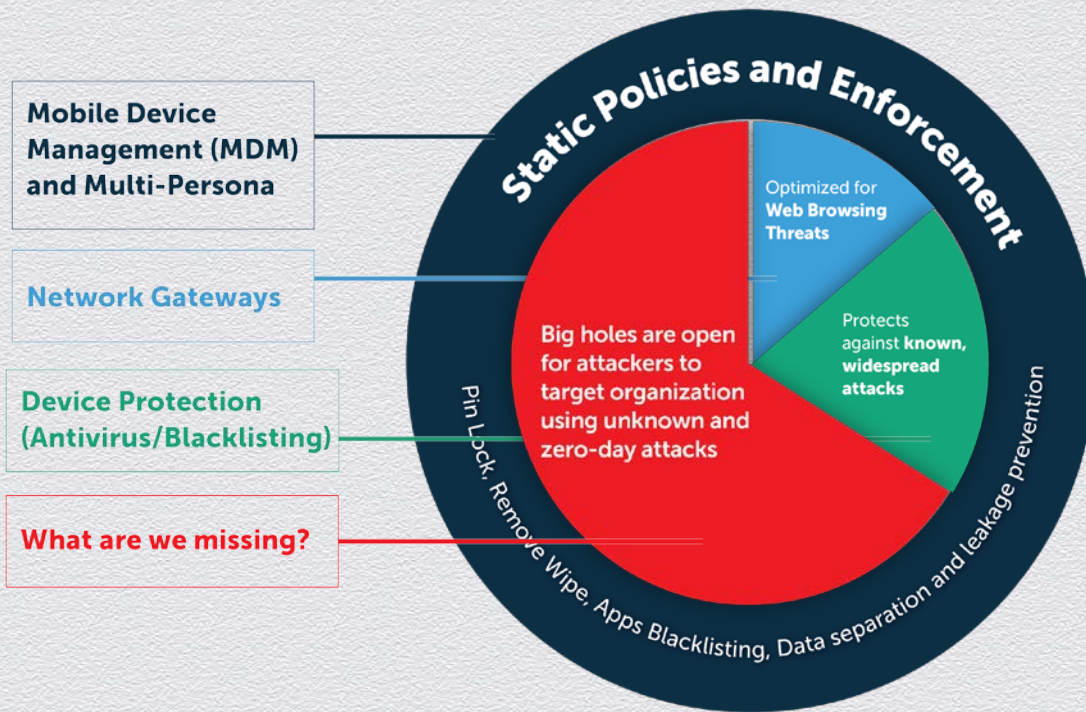
RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Mitigation

Current Solutions in Use to Protect Mobility



Mitigation: Current Controls

Mobile Device Management
(MDM)

Multi-Persona

Wrapper

Active Sync

NAC

Mitigation: Current Controls

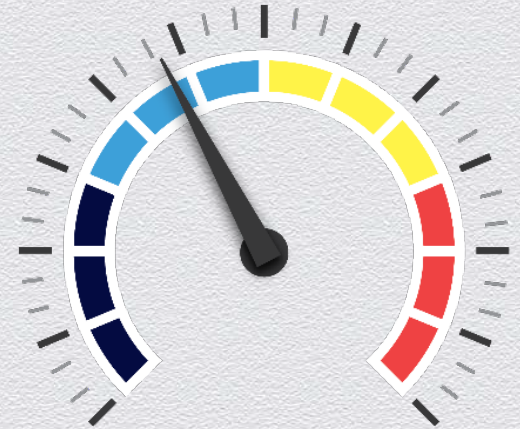
Mobile Device Management
(MDM)

Multi-Persona

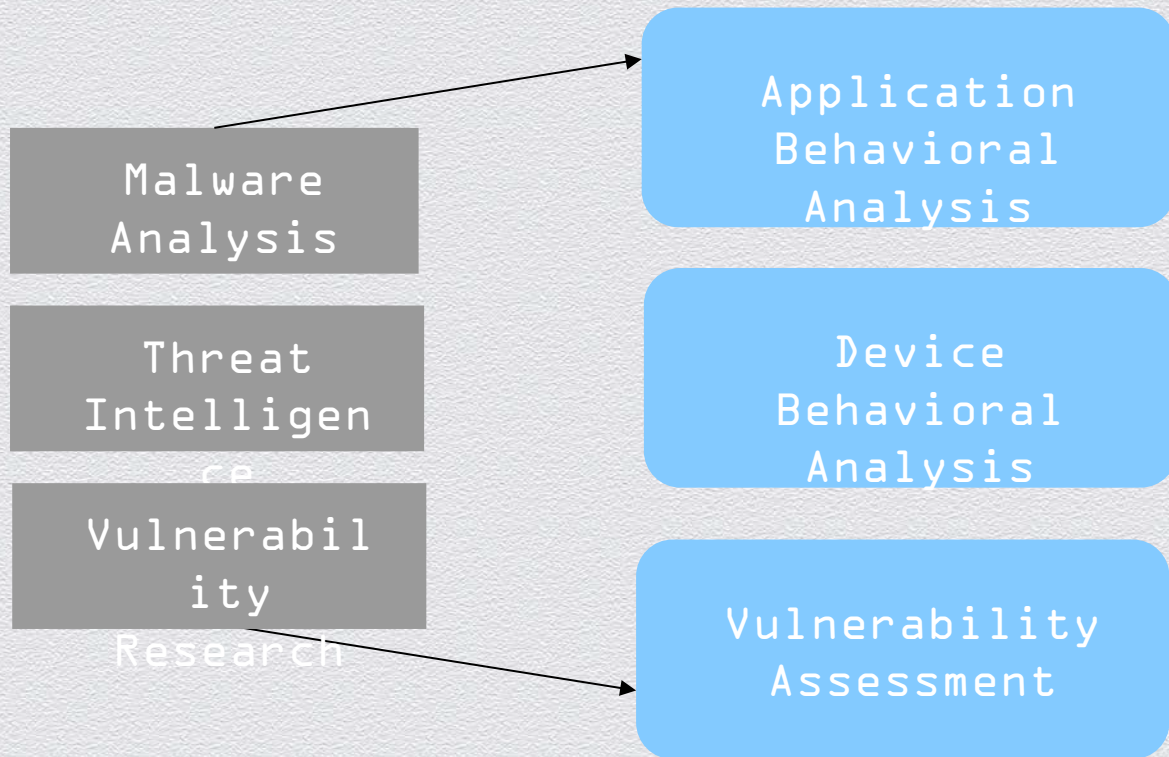
Wrapper

Active Sync

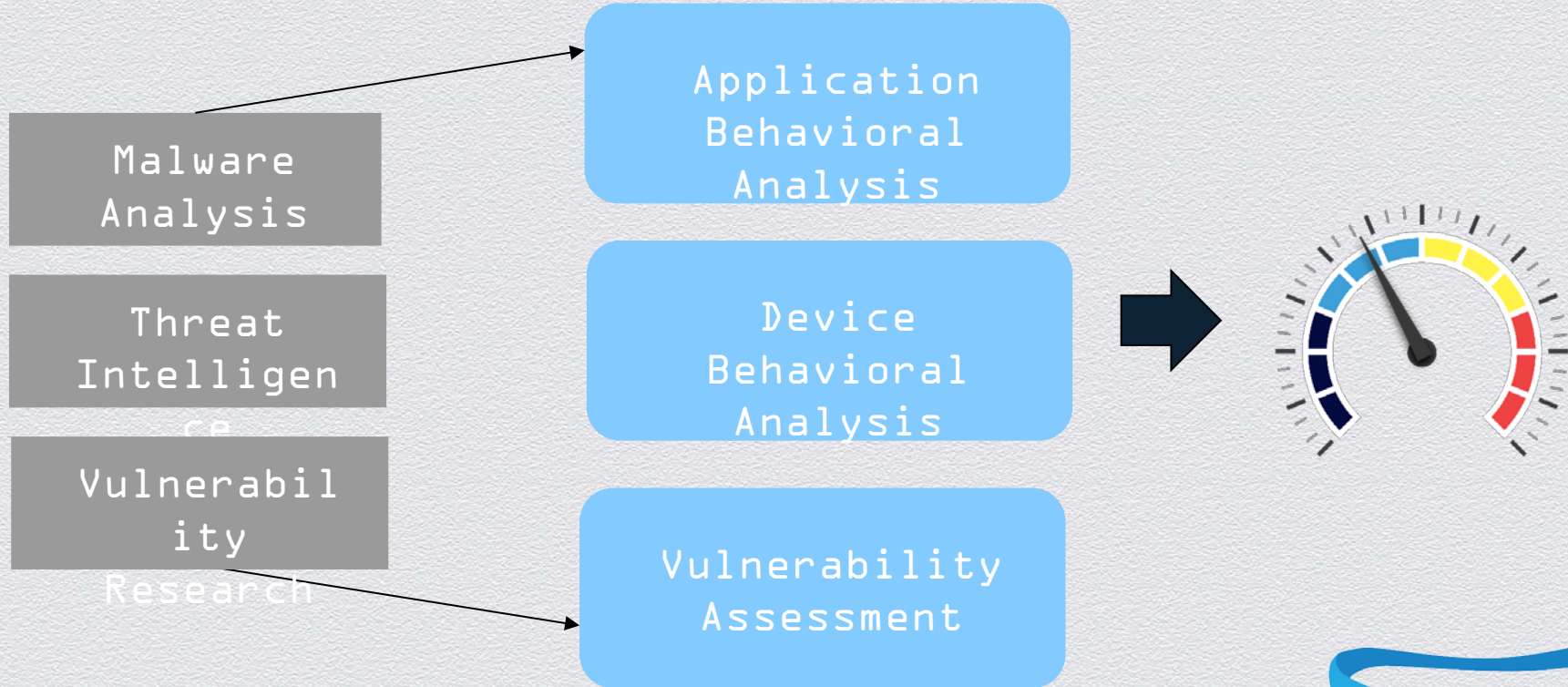
NAC



Detection: Adding Behavior-based Risk



Detection: Adding Behavior-based Risk



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Thank you!

michael@lagoon.com
@LagoonSecurity