LACOON MOBILE SECURITY

Secure your organization from all mobile threats

Practical Attacks against Mobile Device Management Solutions

Michael Shaulov, CEO
michael@lacoon.com

Daniel Brodie, Sr Security Researcher
daniel@lacoon.com

About: Daniel

- Security researcher for nearly a decade
  - From PC to Mobile

- Researcher and Developer at Lacoon
  - Developing an App Analysis framework for spyphones and mobile malware

LACOON MOBILE SECURITY

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

LACOON MOBILE SECURITY

Targeted Attacks: From PC to Malware

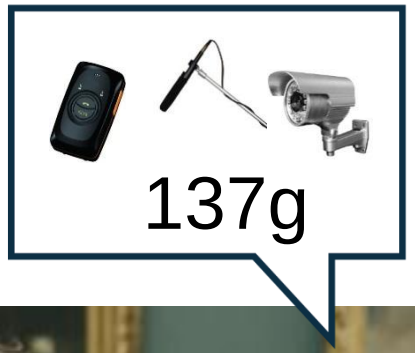
Convergence of Personal and Business

Ubiquitous

Perfect Surveillance Hardware

LACOON MOBILE SECURITY

Targeted Attacks: From PC to Malware



Convergence of Personal and Business

Ubiquitous

Perfect Surveillance Hardware

LACOON MOBILE SECURITY

Targeted Attacks: From PC to Malware

Convergence of Personal and Business

Ubiquitous

Perfect Surveillance Hardware

LACOON MOBILE SECURITY

Agenda

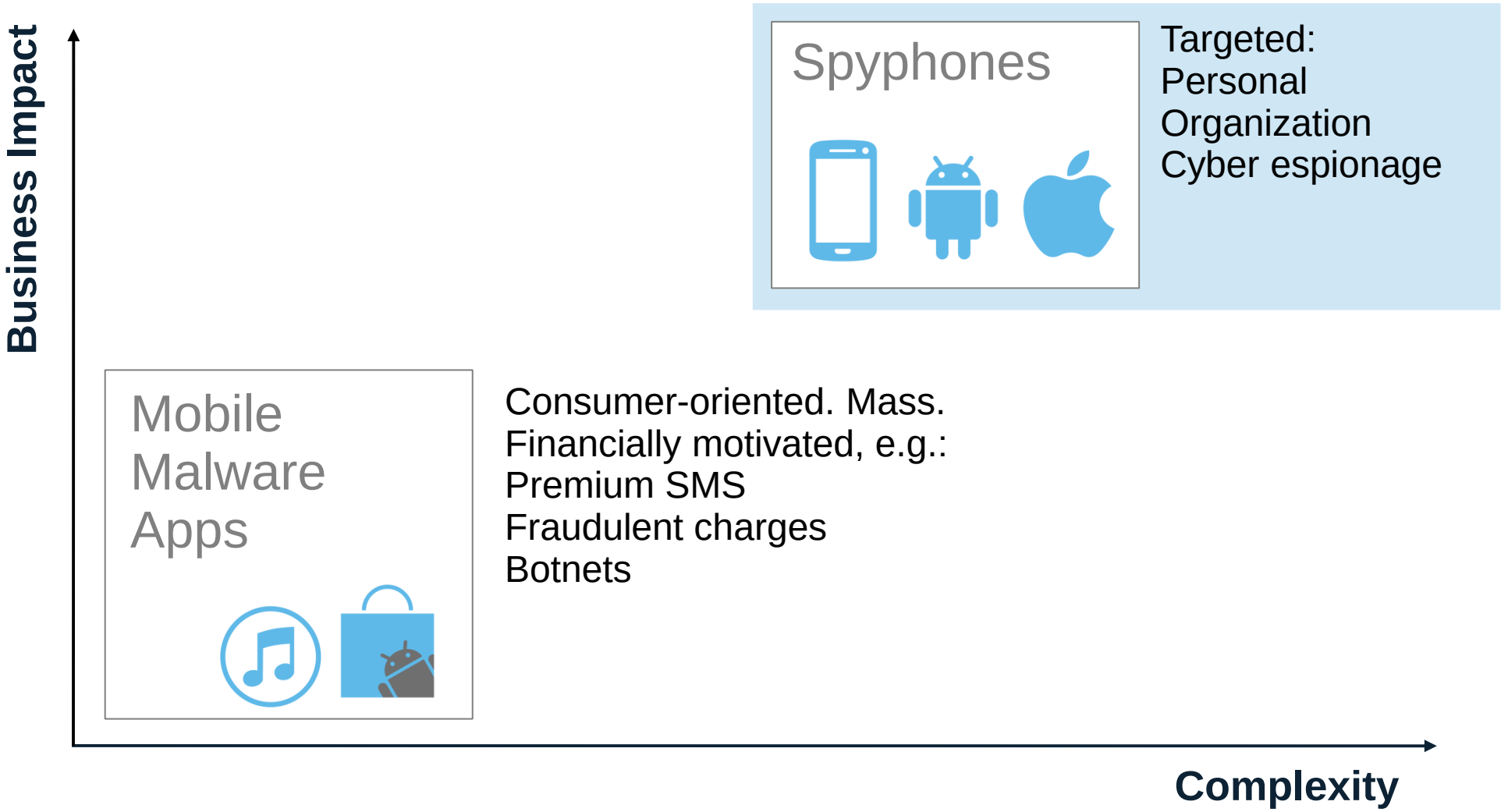
- Rise of the spyphones
- Introduction to MDM and Secure Containers
- Bypassing secure container encryption capabilities
- Recommendations and summary

LACOON MOBILE SECURITY

TARGETED MOBILE THREATS

LACOON MOBILE SECURITY

The Mobile Threatscape



LACOON MOBILE SECURITY

Mobile Remote Access Trojans (aka Spyphones)

LACOON MOBILE SECURITY

Recent High-Profiled Examples

FinFisher spyware goes global, mobile and undercover

Report claims to have found C&C servers in 25 countries

By **Phil Muncaster** · **Get more from this author**

Posted in Security, 19th March 2013 06:34 GMT

Free whitepaper – IT infrastructure monitoring strategies

Security researchers have warned that the controversial FinFisher spyware has been updated to evade detection and has now been discovered in 25 countries across the globe, many of them in APAC.

January 14, 2013, 8:00AM

Rocra Espionage Malware Campaign Uncovered After Five Years of Activity

by Michael Mimoso

Follow @Mike_Mimoso

Parmy Olson, Forbes Staff

I cover agitators and innovators in mobile.

+ Follow (561)

TECH | 3/26/2013 @ 8:32PM | 4,646 views

First-Known Targeted Malware Attack On Android Phones Steals Contacts And Text Messages

'Crisis' OS X Trojan made by lawful intercept vendor, HackingTeam

Russian AV vendor Dr Web says the company behind it has a version for smartphones too.

Liam Tung (CSO Online (Australia)) — *27 July, 2012 07:48*

Mobile attacks! 0.3

Victor Chebyshev

Kaspersky Lab Expert

Posted February 01, 12:31 GMT

Tags: Mobile Malware, Google Android

Users of inexpensive Android smartphones typically look for ways to accelerate their devices, for example, by freeing up memory. Demand for software that makes smartphones work a little faster creates supply, some of which happens to be malicious. In addition to legitimate applications, apps that only pretend to clean up the system have appeared on Google Play.

'Luckycat' APT Campaign Building Android Malware

Trend Micro researchers discover evidence of cyberespionage actors targeting Android users as well

Jul 30, 2012 | 09:09 PM | 0 Comments

By **Kelly Jackson Higgins**

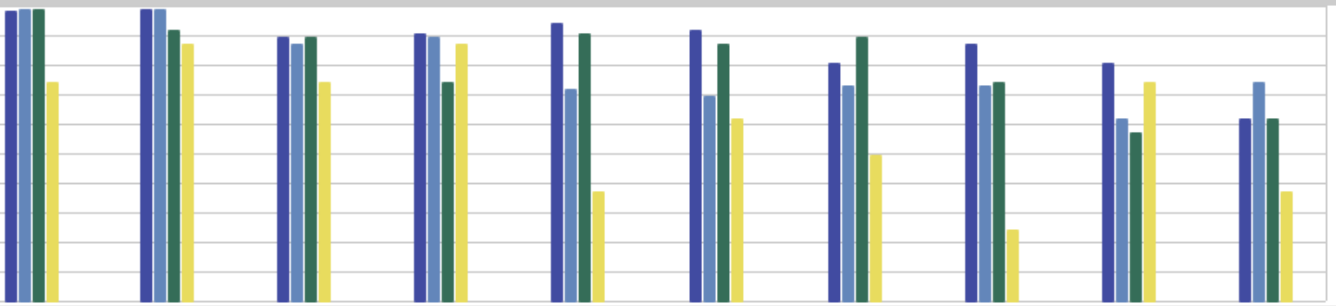
Dark Reading

DEF CON 20 -- Las Vegas, NV -- Windows long has been the favorite target of cyberespionage actors, but newly discovered evidence shows they are also setting their sites on mobile platforms, namely the Android.

LACOON MOBILE SECURITY

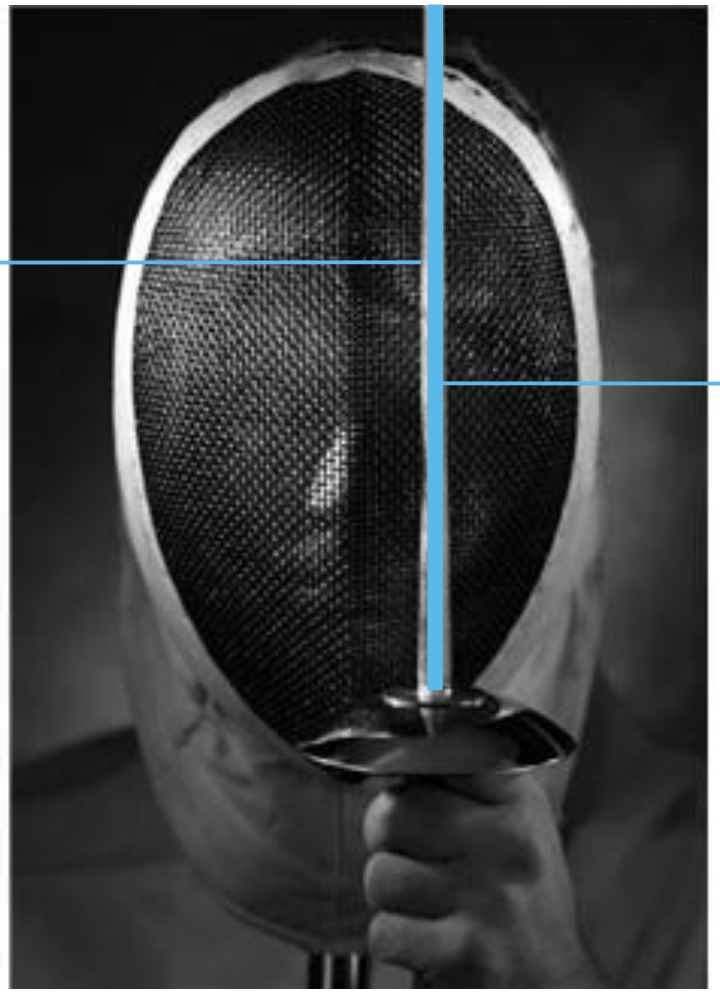
Commercial mRATS

Rank	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
10-9 Excellent 8-6 Good 5-4 Average 3-2 Poor 1-0 Bad Print/Email	PhoneSheriff	mSpy	Mobile Spy	My Mobile Watchdog	MobiStealth	StealthGenie	SpyPhone Basic Internet	SpyBubble	eBlaster Mobile	Flexispy
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										
Features										
Tracking & Security										
Help & Support										
Reporting & Logging										
Report Display (percentage)	95	100	60	50	70	60	40	50	40	20
Call History/Details	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Text/SMS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Email	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓



LACOON MOBILE SECURITY

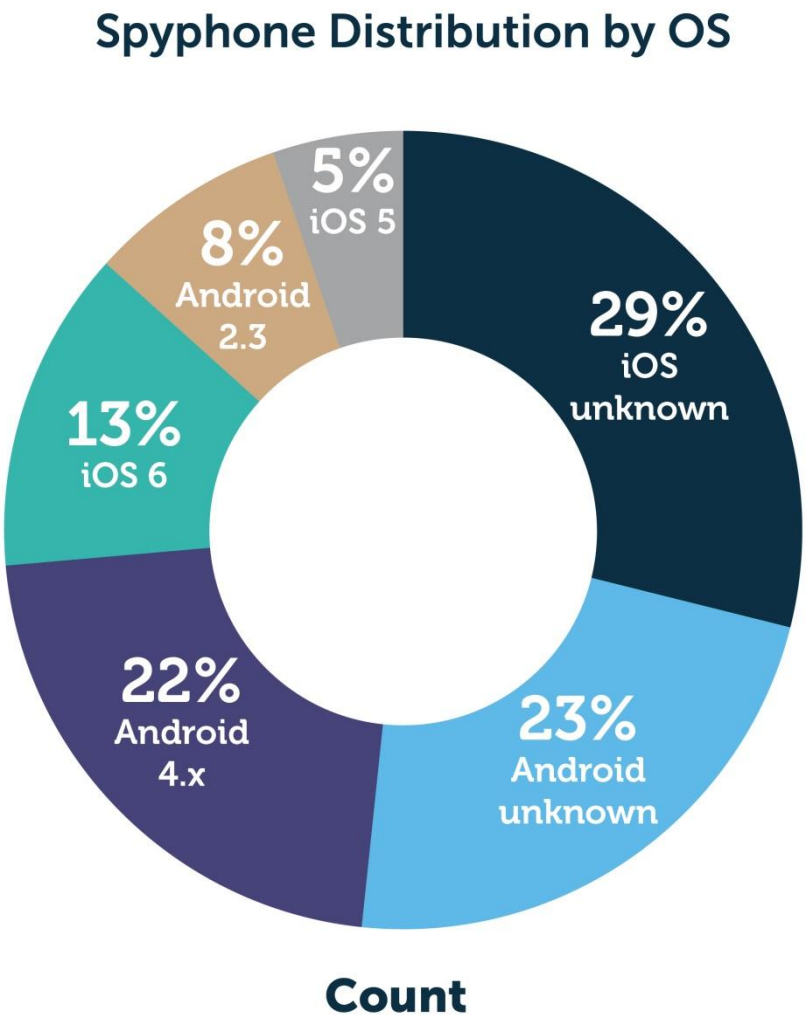
A Double-Edged Sword



LACOON MOBILE SECURITY

Survey: Cellular Network 2M Subscribers

Sampling: 500K



Infection rates:

June 2013:

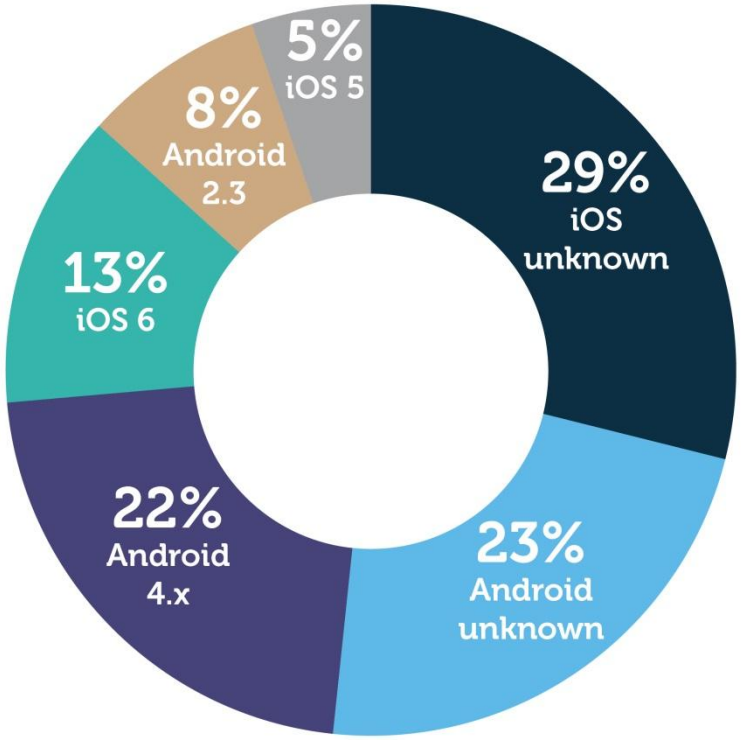
1 / 800 devices

LACOON MOBILE SECURITY

Survey: Cellular Network 2M Subscribers

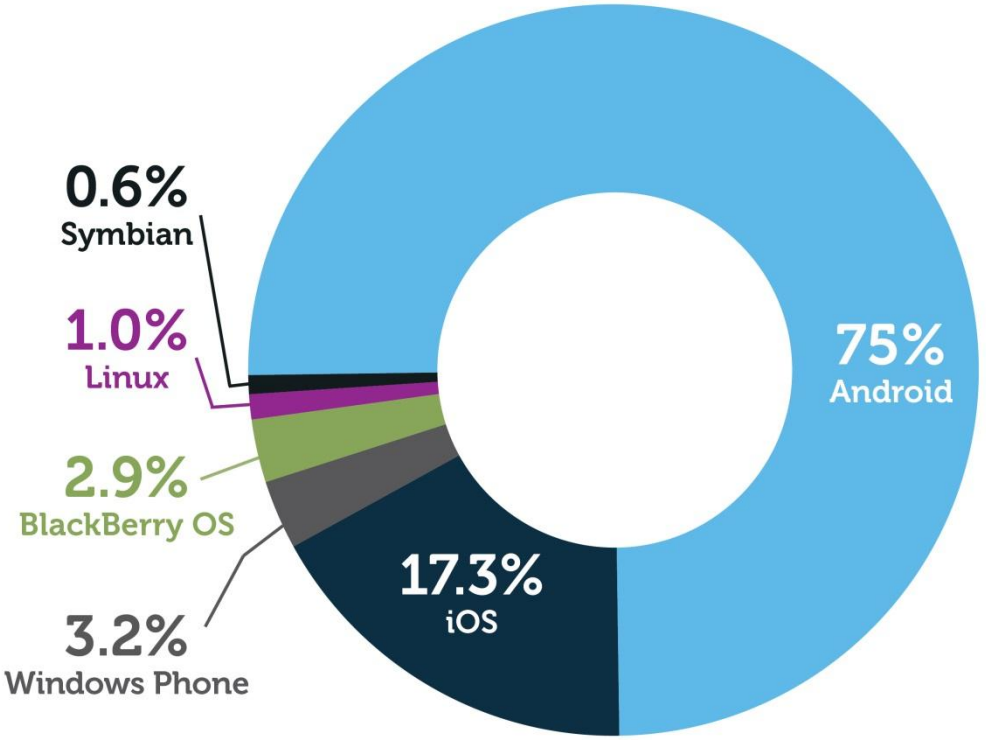
Sampling: 500K

Spyphone Distribution by OS



Count

Mobile OS Market Share



Market Share

Source: IDC Worldwide Quarterly Mobile Phone Tracker, May 2013

LACOON MOBILE SECURITY

MDM and SECURE CONTAINERS 101

LACOON MOBILE SECURITY

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 5 years,

65% of enterprises

will adopt a mobile device management (MDM) solution for their corporate liable users"

Gartner, Inc. October 2012

LACOON MOBILE SECURITY

MDM Key Capabilities

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

LACOON MOBILE SECURITY

Secure Containers

All leading MDM solutions provide secure containers

MobileIron

AirWatch

Fiberlink

Zenprise

Good Technology

LACOON MOBILE SECURITY

Behind the Scenes: Secure Containers

Enterprise

Application
Sandbox

Encrypted Storage

LACOON MOBILE SECURITY

MDMs and Secure Containers

3 assumptions:

- **Encrypt business data**
- **Encrypt communications to the business (SSL/ VPN)**
- **Detect Jailbreak/ Rooting of devices**

LACOON MOBILE SECURITY

MDMs and Secure Containers

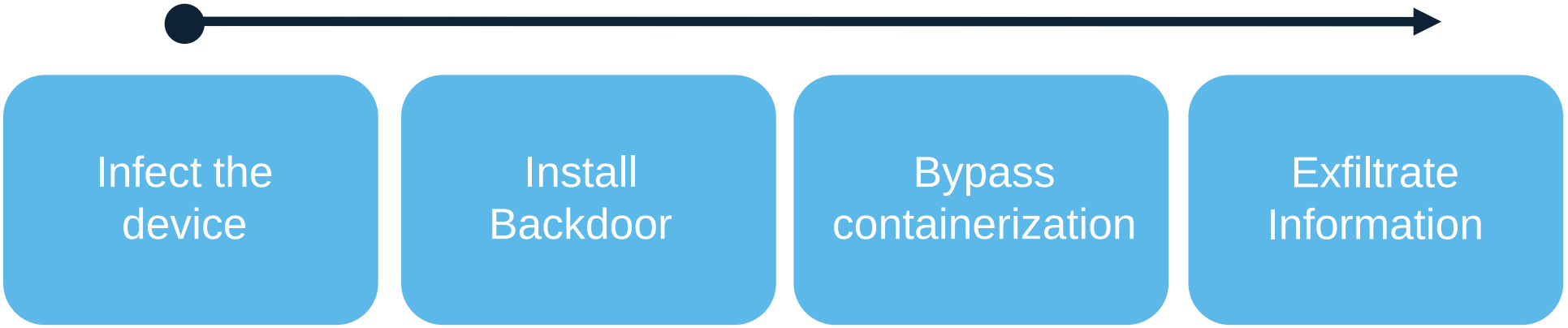
Let’s test these assumptions…

LACOON MOBILE SECURITY

BYPASSING MOBILE DEVICE MANAGEMENT (MDM) SOLUTIONS

LACOON MOBILE SECURITY

Overview

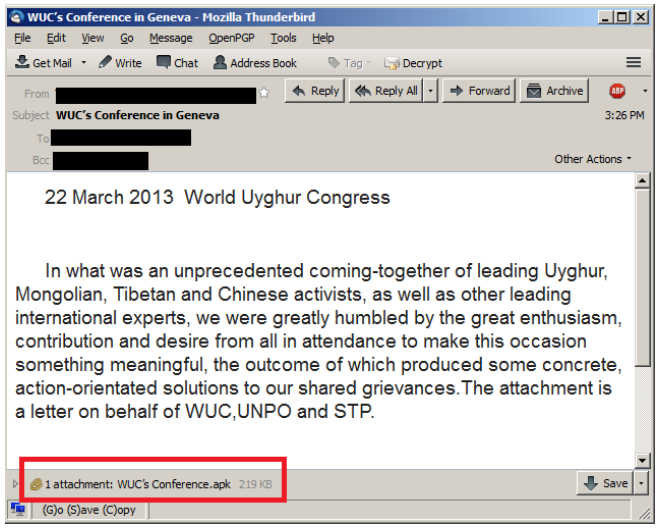


LACOON MOBILE SECURITY

DEMO

ANDROID

Step 1: Infect the Device



LACOON MOBILE SECURITY

Step 1: Technical Details

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

LACOON MOBILE SECURITY

Step 2: Install a Backdoor (i.e. Rooting)

Root

Any process can run as root user if it is able to trigger a vulnerability in the OS

Vulnerability

Android device vulnerabilities are abundant

Exploit

On-Device detection mechanisms can’t look at apps exploiting the vulnerability

LACOON MOBILE SECURITY

Step 2: Technical Details

Privilege escalation

We used the Exynos exploit (Released Dec., 2012)

Create the hidden ‘suid’ binary and use it for specific actions

Place in a folder with --x--x--x permissions

Undetected by generic root detectors

LACOON MOBILE SECURITY

Step 3: Bypass Containerization

Storage

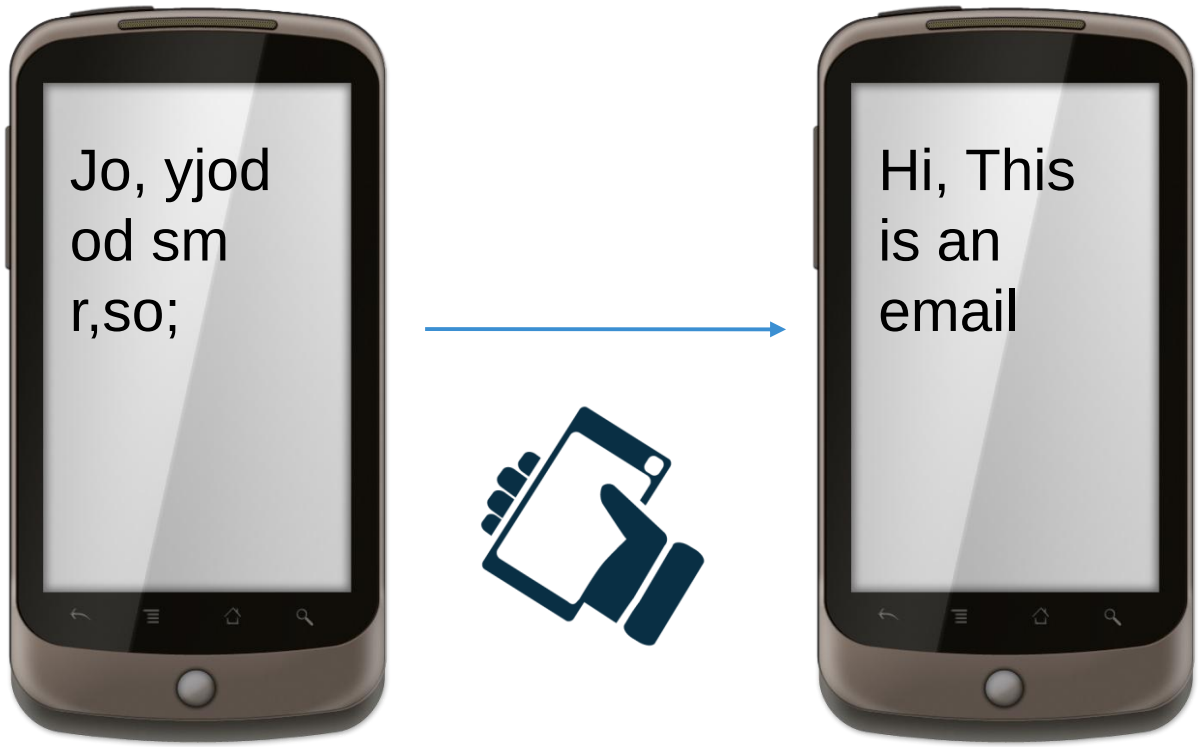
LACOON MOBILE SECURITY

Step 3: Bypass Containerization

Storage

LACOON MOBILE SECURITY

Step 3: Bypass Containerization



LACOON MOBILE SECURITY

Step 3: Technical Details

We listen to events in the log

For <= 2.3 we can just use the logging permissions

For >4.0 we 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

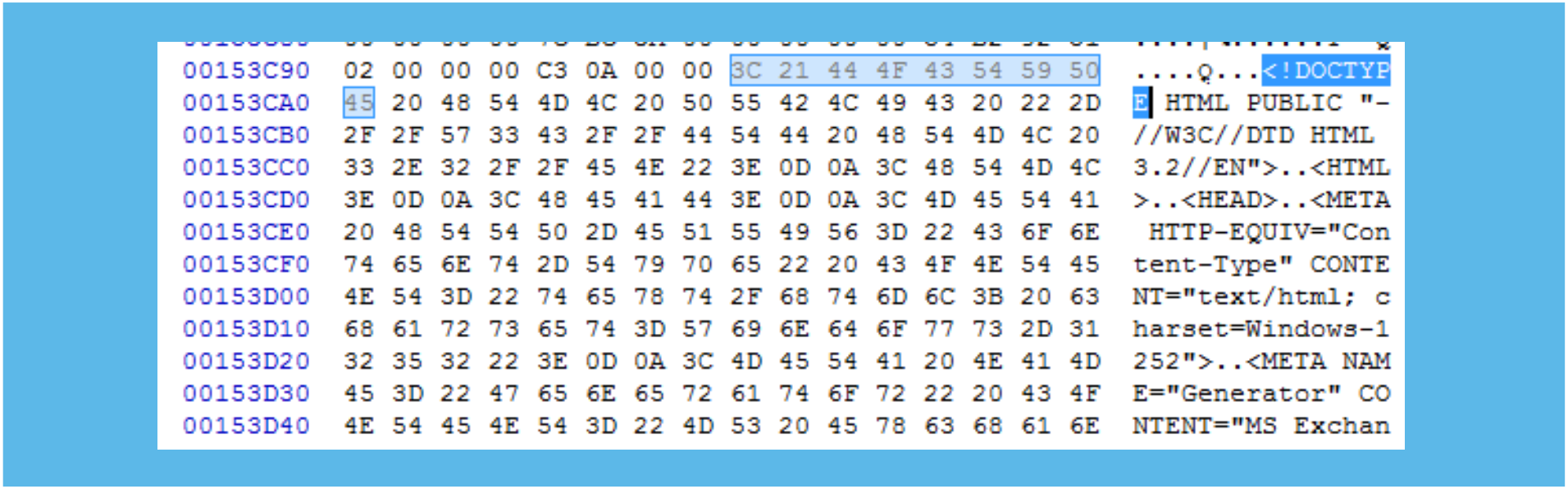
Step 4: Exfiltrate Information

LACOON MOBILE SECURITY

Step 4: Technical Details

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
```

LACOON MOBILE SECURITY

DEMO

IOS

LACOON MOBILE SECURITY

Step 1: Infect the device

LACOON MOBILE SECURITY

Step 2: Install a Backdoor (i.e. Jailbreaking)

Community

Andy Greenberg, Forbes Staff
Covering the worlds of data security, privacy and hacker culture.
+ Follow (757)

Forbes

SECURITY | 2/08/2013 @ 8:00AM | 53,976 views

Evasion Is The Most Popular Jailbreak Ever: Nearly Seven Million iOS Devices Hacked In Four Days

Jailbroken

10 Reasons Why You Should Jailbreak Your iPhone

Dylan Love | Feb. 4, 2013, 2:31 PM | 192,667 | 5

BUSINESS INSIDER

Home | Tech | Finance | Markets

xCon

Bypassing Jailbreak Detection

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

LACOON MOBILE SECURITY

Step 2: Technical Details

Install signed application

Using Enterprise/ Developer certificate

Use the Jailbreak

To complete the hooking

Remove any trace of the Jailbreak

LACOON MOBILE SECURITY

Step 3: Bypass Containerization

Load malicious dylib into memory (it's signed!)

Hook using standard Objective-C hooking mechanisms

Get notified when an email is read

Pull the email from the UI classes

LACOON MOBILE SECURITY

MITIGATION TECHNIQUES

LACOON MOBILE SECURITY

MDM

MDMs are good for:

- **Management**
- **Compliance Enforcement**
- **DLP**
- **Physical Loss**

However…

LACOON MOBILE SECURITY

LACOON MOBILE SECURITY

LACOON MOBILE SECURITY

Do We Have Visibility?

LACOON MOBILE SECURITY

Can We Assess Risk in Real-Time?

LACOON MOBILE SECURITY

Can We Mitigate Targeted Threats?

LACOON MOBILE SECURITY

LACOON MOBILE SECURITY

Attacks are going to happen

It’s a question of assessing risk

And mitigating the effects

LACOON MOBILE SECURITY

“Life is inherently risky. There is only one big risk you should avoid at all costs, and that is the risk of doing nothing.”

Denis Waitley

LACOON MOBILE SECURITY

Risk Metrics / Visibility

Vulnerabilities and Usage

Is the device up-to-date?

Any known vulnerabilities pertaining to the OS?

Is the device connecting to a public hotspot?

App Behavioral Analysis

What is the common app behavior? (static analysis)

What is the app doing? (dynamic analysis)

Funky Correlation of Events

Is the device sending an SMS when the phone is locked?

LACOON MOBILE SECURITY

Network Behavioral Analysis

- Anomaly detection of communications of apps
- Outgoing content inspection (unencrypted)
- Blocking of exploit and drive-by attacks

Thank You.

Michael Shaulov, CEO
michael@lacoon.com

Daniel Brodie, Sr Security Researcher
daniel@lacoon.com

LACOON MOBILE SECURITY