Practical Attacks against Virtual Desktop Infrastructure (VDI) Solutions

Dan Koretsky, Sr. Security Strategist

Lacoon Mobile Security

About Dan

- 7 years of security research
  - From PC to Mobile
- Researcher and developer at Lacoon Mobile Security
  - Analysing malware and researching trends to translate to business impact
  - Research around IOS and Android vulnerabilities and security events around the world

Quick Disclaimer

This talk is NOT about:

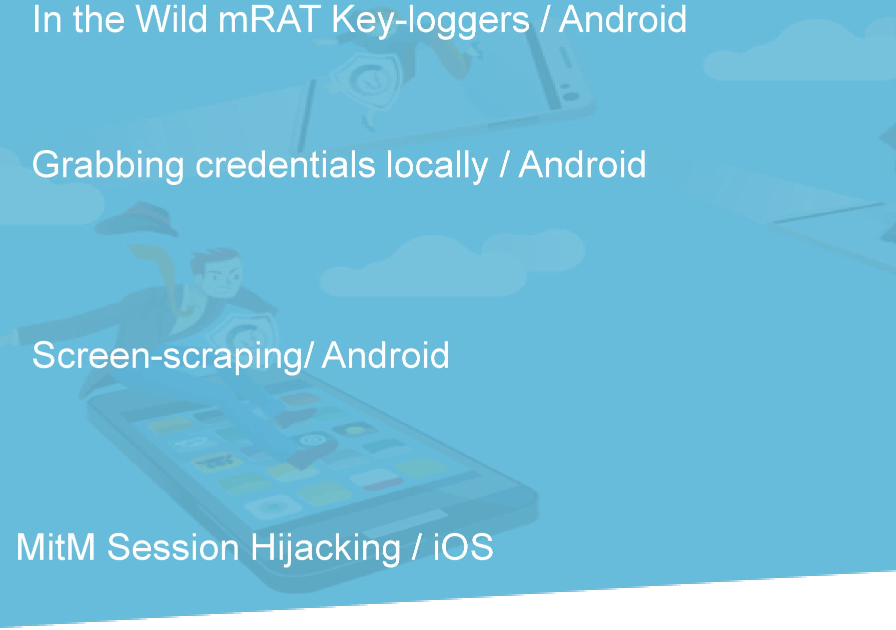
- Dismiss VDI value as an enterprise mobile solution
- Specific vendor implementation

This talk is about:

- Quantifying risks that can compromise VDI sessions
- Providing a framework to assess and mitigate the risks

Agenda

- Mobile VDI 101
- Practical Mobile Threats against VDI
- Augmenting VDI with Defense-in-Depth Mobile Security
- Conclusions



Threat 1 In the Wild mRAT Key-loggers / Android

Threat 2 Grabbing credentials locally / Android

Threat 3 Screen-scraping/ Android

Threat 4 MitM Session Hijacking / iOS

Mobile VDI 101

Enablement

Simplify IT support of BYO devices

It can meet the increasing demand for BYO initiatives by delivering apps and desktops as an on-demand service.

DLP / Lost Device

On-demand session

No content is saved on the device

Intrusion

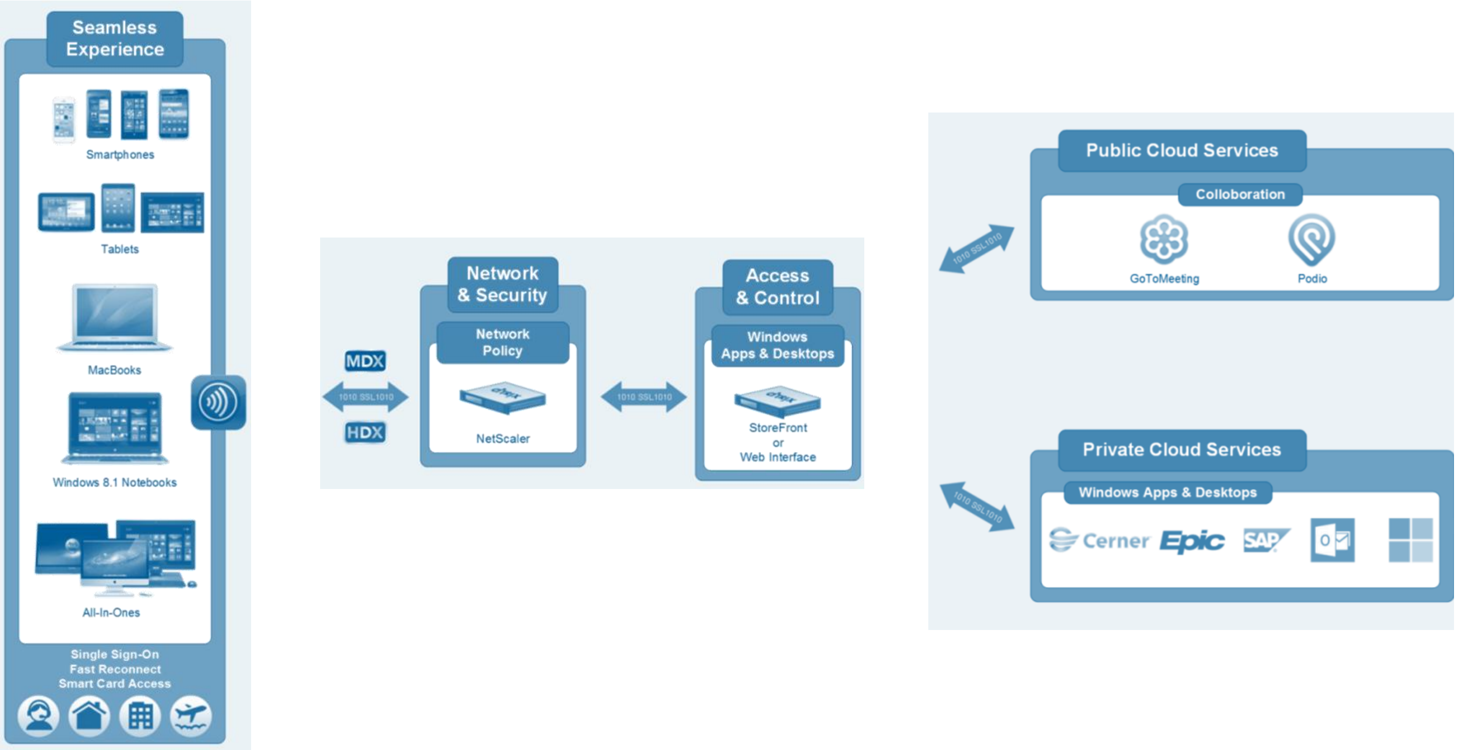
“Virtual desktop security to protect sensitive information

Centrally secured virtual desktops and apps in the datacenter reduce the risk of data loss or intrusion when delivered to any device. Corporate access remains secure while intellectual property and sensitive private information stays safe.”

Good Marketing

?

VDI Architecture - Example



Seamless Experience

Smartphones

Tablets

MacBooks

Windows 8.1 Notebooks

All-In-Ones

Single Sign-On
Fast Reconnect
Smart Card Access

MDX

1010 SSL1010

HDX

Network & Security

Network Policy

NetScaler

1010 SSL1010

Access & Control

Windows Apps & Desktops

StoreFront
or
Web Interface

1010 SSL1010

Public Cloud Services

Collaboration

GoToMeeting

Podio

1010 SSL1010

Private Cloud Services

Windows Apps & Desktops

Cerner Epic SAP

VDI Players

2 major mobile VDI enterprise players:

- Citrix
- VMware

Threats to Mobile VDI Solutions

Using an mRAT for its Keylogging Capabilities

Threat 1

What is a Mobile Remote Access Trojan (mRAT)

Emails

App Data

Key Logger

Screen Scraper

Memory Scraping

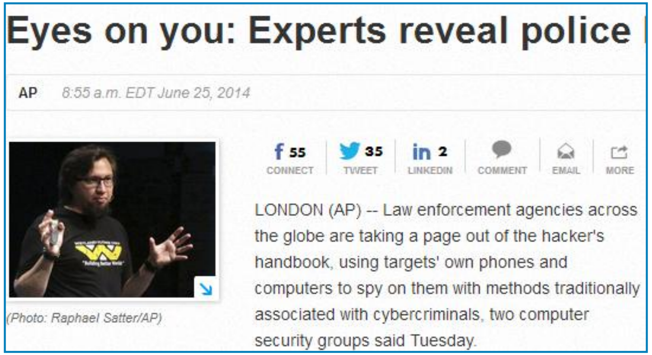
Contact Lists, Call & Text Logs

Files and Photos

Microphone and Camera

Track Location

Recent High-Profiled Examples

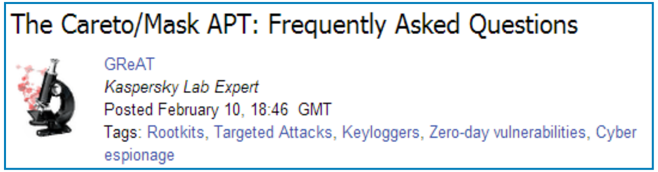


Eyes on you: Experts reveal police

AP 8:55 a.m. EDT June 25, 2014

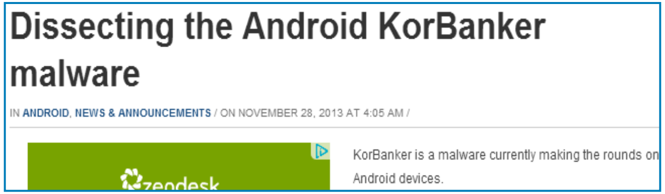
(Photo: Raphael Satter/AP)

LONDON (AP) -- Law enforcement agencies across the globe are taking a page out of the hacker's handbook, using targets' own phones and computers to spy on them with methods traditionally associated with cybercriminals, two computer security groups said Tuesday.



The Careto/Mask APT: Frequently Asked Questions

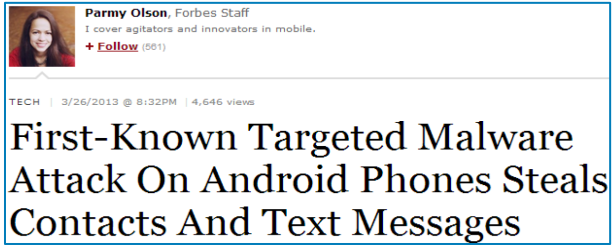
GReAT
Kaspersky Lab Expert
Posted February 10, 18:46 GMT
Tags: Rootkits, Targeted Attacks, Keyloggers, Zero-day vulnerabilities, Cyber espionage



Dissecting the Android KorBanker malware

IN ANDROID, NEWS & ANNOUNCEMENTS / ON NOVEMBER 28, 2013 AT 4:05 AM /

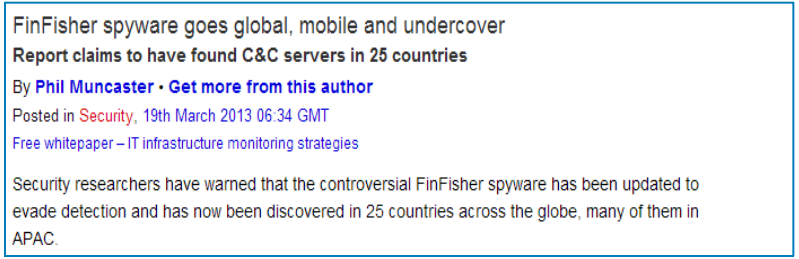
KorBanker is a malware currently making the rounds on Android devices.



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



FinFisher spyware goes global, mobile and undercover

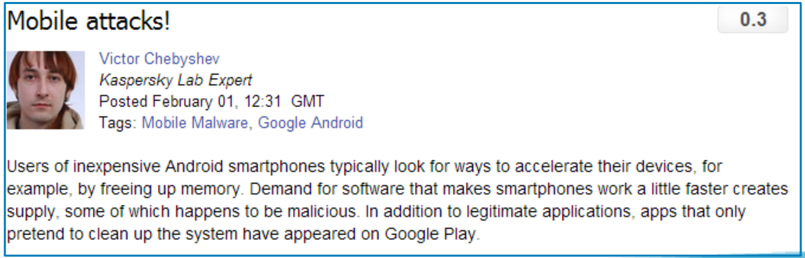
Report claims to have found C&C servers in 25 countries

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.



Mobile attacks!

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.

XSSER

- Attacked the Hong Kong protesters
- Targetted both android and iOS
- More details in our blog:
  - www.lacoon.com/blog

mRAT Spectrum

FinSpy Mobile

]HackingTeam[

DROPOUTJEEP
ANT Product Data

Gov / Mil mRATs

$300K-$12M

Government -> Terrorists / Activists

DENDROID

ANDRORAT APK BINDER
FIRST EVER ANDROID RAT APP BINDER + BUILDER
CLICK HERE!

DROIDJACK

Darknet mRATs

Free - $300

Cybercriminal -> ?

mSPY

FLEXISPY

Surveillance / Monitoring Tools

Free - $100

Everyone -> Everyone

mRAT Spectrum

]HackingTeam[

"Hacking Team is really a very basic software with a public payload based on CVE bugs PUBLIC. Not different than any commercial spyware on internet. Even with lower features."

-- Mobile Malware Google Group

FLEXISPY

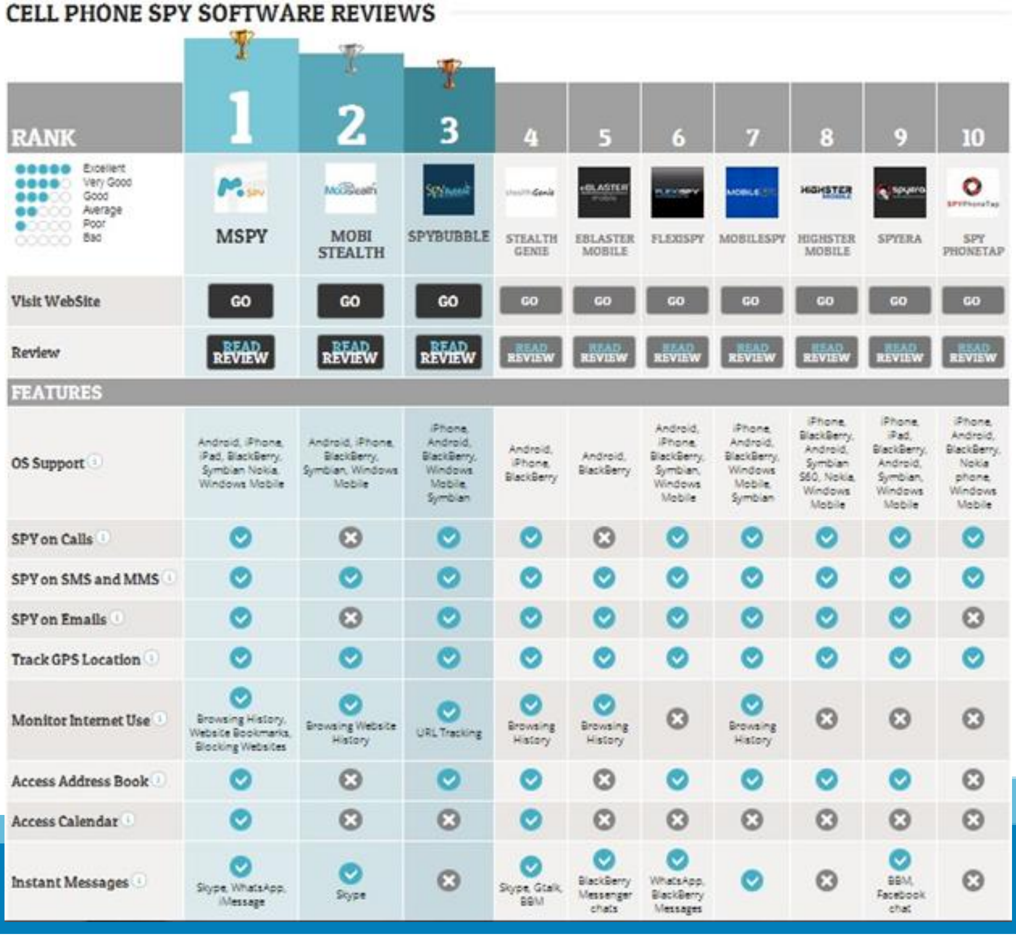
Gov / Mil mRATs

Surveillance / Monitoring Tools

$300K-$12M
Government -> Terrorists / Activists

Free - $100
Everyone -> Everyone

Commercial Surveillance Software



CELL PHONE SPY SOFTWARE REVIEWS

RANK	1	2	3	4	5	6	7	8	9	10
●●●●● Excellent ●●●●○ Very Good ●●●○○ Good ●●○○○ Average ●○○○○ Poor ○○○○○ Bad	MSPY	MOBI STEALTH	SPYBUBBLE	STEALTH GENIE	EBLASTER MOBILE	FLEXISPY	MOBILESPY	HIGHSTER MOBILE	SPYERA	SPY PHONETAP
Visit WebSite	GO	GO	GO	GO	GO	GO	GO	GO	GO	GO
Review	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW
FEATURES										
OS Support	Android, iPhone, iPad, BlackBerry, Symbian Nokia, Windows Mobile	Android, iPhone, BlackBerry, Symbian, Windows Mobile	iPhone, Android, BlackBerry, Windows Mobile, Symbian	Android, iPhone, BlackBerry	Android, BlackBerry	Android, iPhone, BlackBerry, Symbian, Windows Mobile	iPhone, Android, BlackBerry, Windows Mobile, Symbian	iPhone, BlackBerry, Android, Symbian S60, Nokia, Windows Mobile	iPhone, iPad, BlackBerry, Android, Symbian, Windows Mobile	iPhone, Android, BlackBerry, Nokia phone, Windows Mobile
SPY on Calls	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓
SPY on SMS and MMS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SPY on Emails	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗
Track GPS Location	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Monitor Internet Use	✓ Browsing History, Website Bookmarks, Blocking Websites	✓ Browsing Website History	✓ URL Tracking	✓ Browsing History	✓ Browsing History	✗	✓ Browsing History	✗	✗	✗
Access Address Book	✓	✗	✓	✓	✗	✓	✓	✓	✓	✗
Access Calendar	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗
Instant Messages	✓ Skype, WhatsApp, iMessage	✓ Skype	✗	✓ Skype, Gtalk, BBM	✓ BlackBerry Messenger chats	✓ WhatsApp, BlackBerry Messages	✓	✗	✓ BBM, Facebook chat	✗

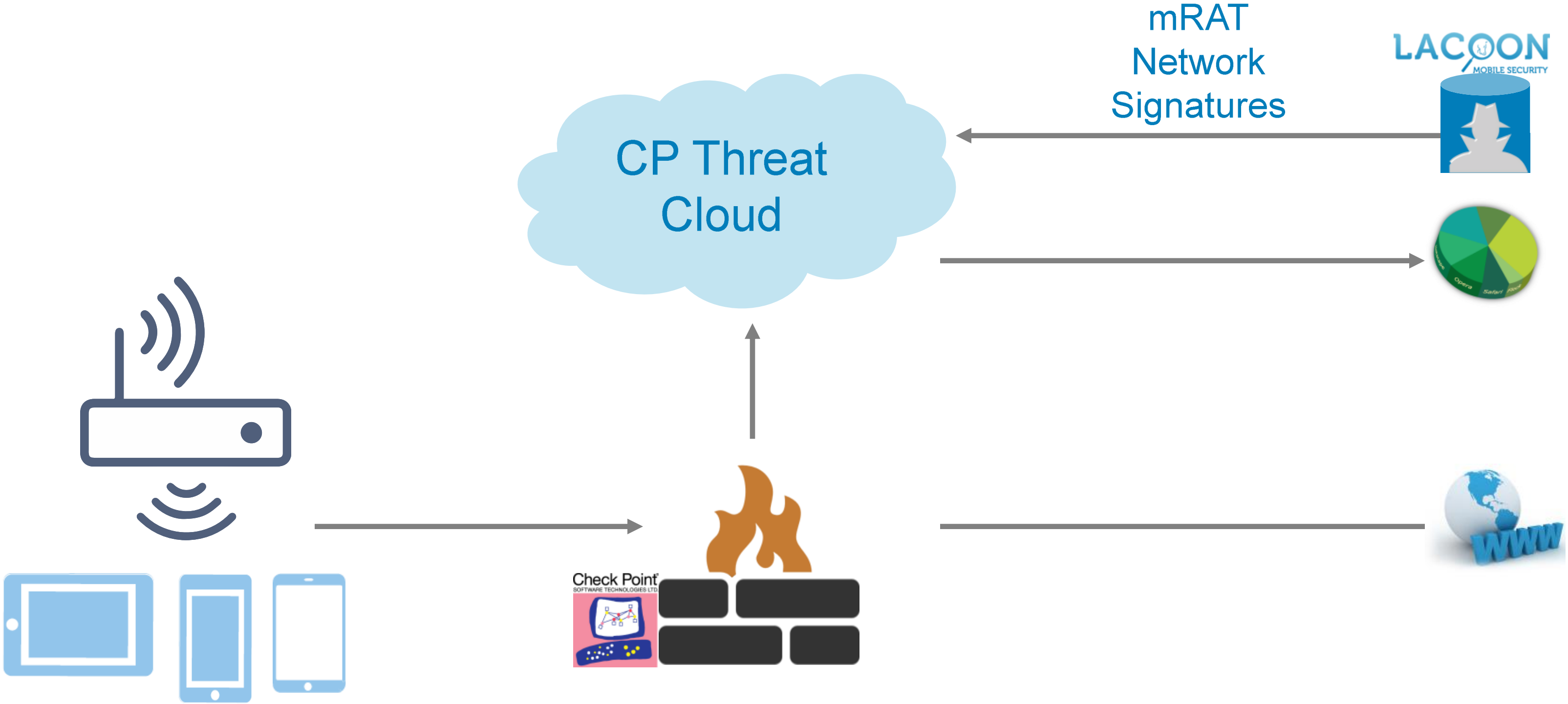
Survey: mRATs in the Enterprise
A Checkpoint-Lacoon Research

Data sample

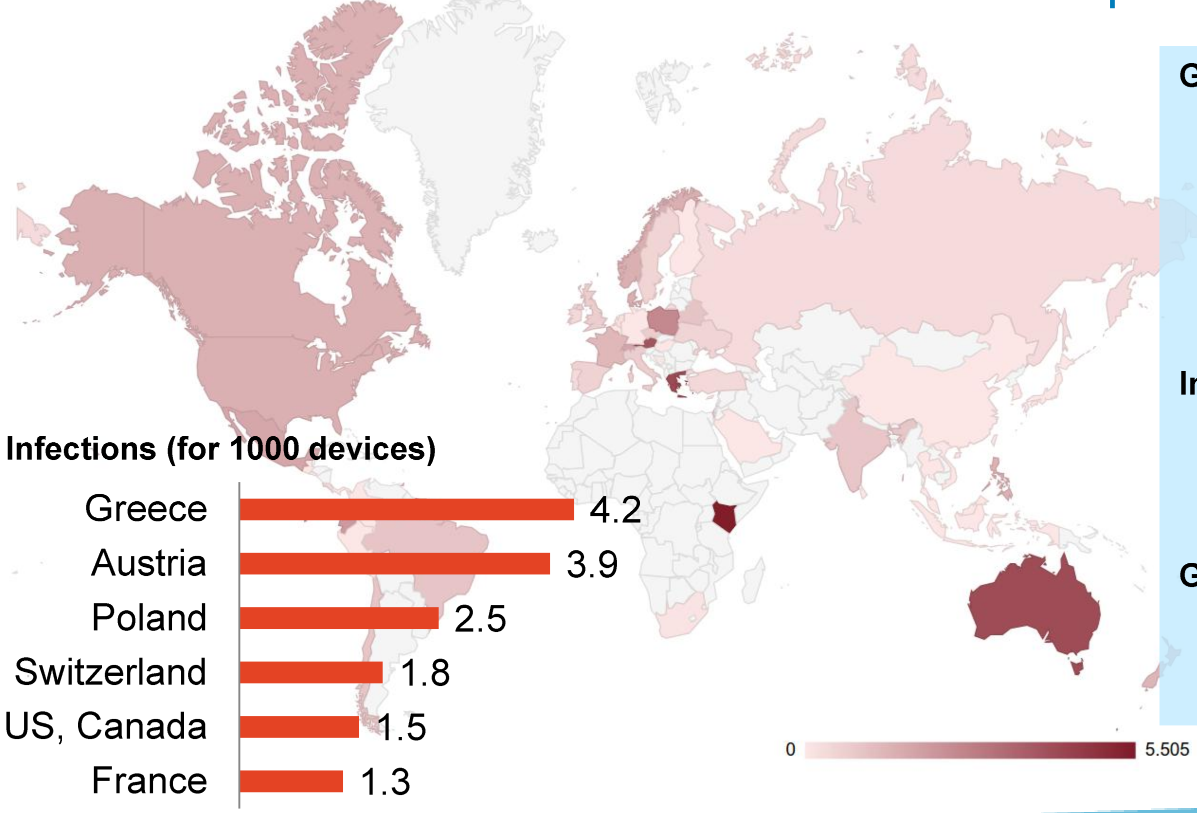
Mobile devices communicating through corporate WiFi access points, connected to the Checkpoint firewall

Traffic from 3208 corporate gateways

Survey: mRATs in the Enterprise
A Checkpoint-Lacoon Research



How common are mobile threats in the Enterprise?


Infections (for 1000 devices)

General Research:

- **3208 corporate gateways**
- **123 countries (48 with infections)**
- **506 gateways with infections**
- **570k android devices**
- **4500 infected android devices**
- **3200 infected iOS devices**

Infection Rate Estimate

- **220 gateways with device estimation**
- **Infected devices: 644**
- **1.2 devices per 1000: (0.12%)**

Gateways with at least 2000 devices

- **50% have infections**
- **Higher infection rate (2.2 in the US)**
- **1 in every 3 devices infected is an iOS**

Some Proportions

- What’s 0.1% infection rate to me?
  - 5000 device enterprise – average 5 infected devices
- Is my enterprise at risk?
  - For a 2000 device enterprise – 50% chance of infection

Recap

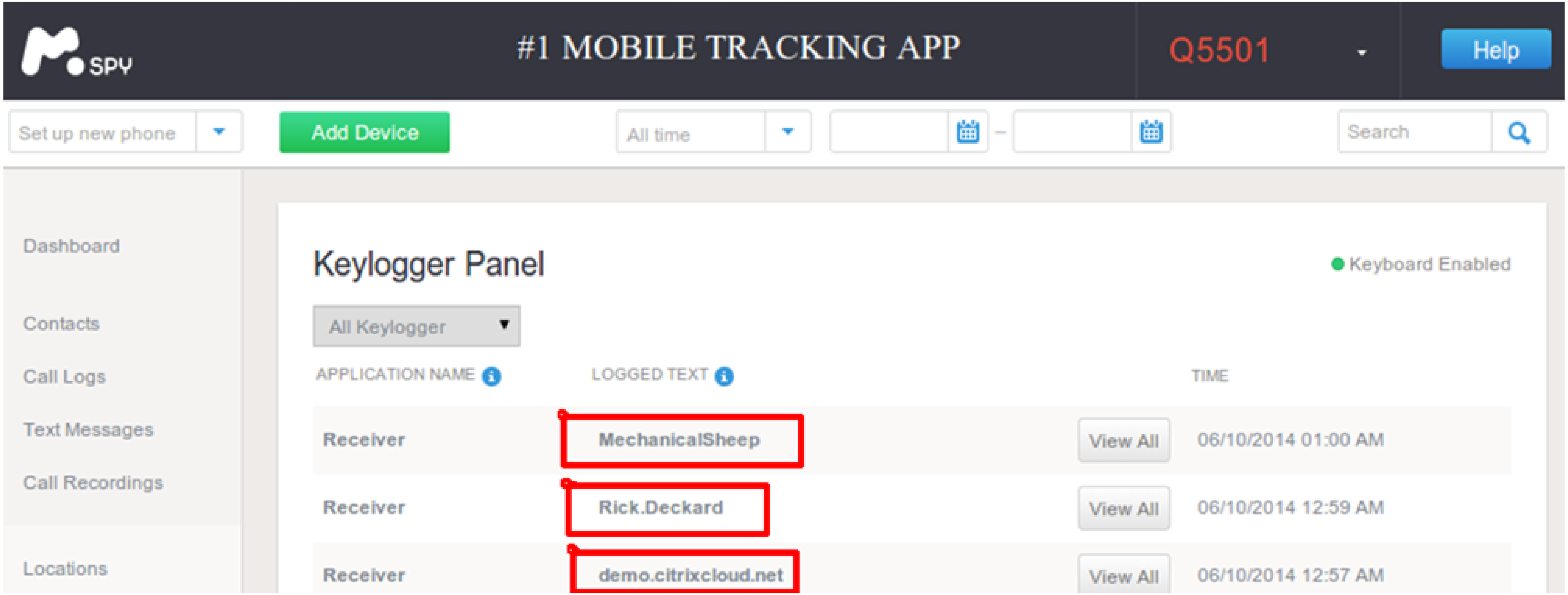
- Looked at both solutions
  - Test servers (citrixcloud, pivot3's testdrive)
- Vmware is more of a slim VDI while Citrix has additional capabilities
- Very configurable
- Both provide a myriad of clients and login capabilities

Threat 1
Using a Widely Popular mRAT on an Android-based Device

- Keylogging for data or authentication info
- mSpy
  - Checkpoint-Lacoon “mRATs in the Enterprise” survey
    - Mostly used in the enterprise
    - Detected in 48 countries, such as USA, Britain, and France

Cost: >$50

mSpy



Keylogger Panel

● Keyboard Enabled

APPLICATION NAME	LOGGED TEXT		TIME
Receiver	MechanicalSheep	View All	06/10/2014 01:00 AM
Receiver	Rick.Deckard	View All	06/10/2014 12:59 AM
Receiver	demo.citrixcloud.net	View All	06/10/2014 12:57 AM

Different Keylogging options

- Repackage keyboard – done on SwiftKey in 2013
  - Used by mRAT’s as a custom keyboard
  - Targetting a country is as easy as repackaging its language pack
- MitM on the active input method – grants the BIND_INPUT_METHOD permission
  - Pretty complicated and requires elevated privileges
- Input Manager Service is a native process, hooking it at the InputDispatcher->dispatchOnce gives access to all input events
  - Practically all Android ROMs use default symbol visibility

Grabbing Credentials Locally on Android

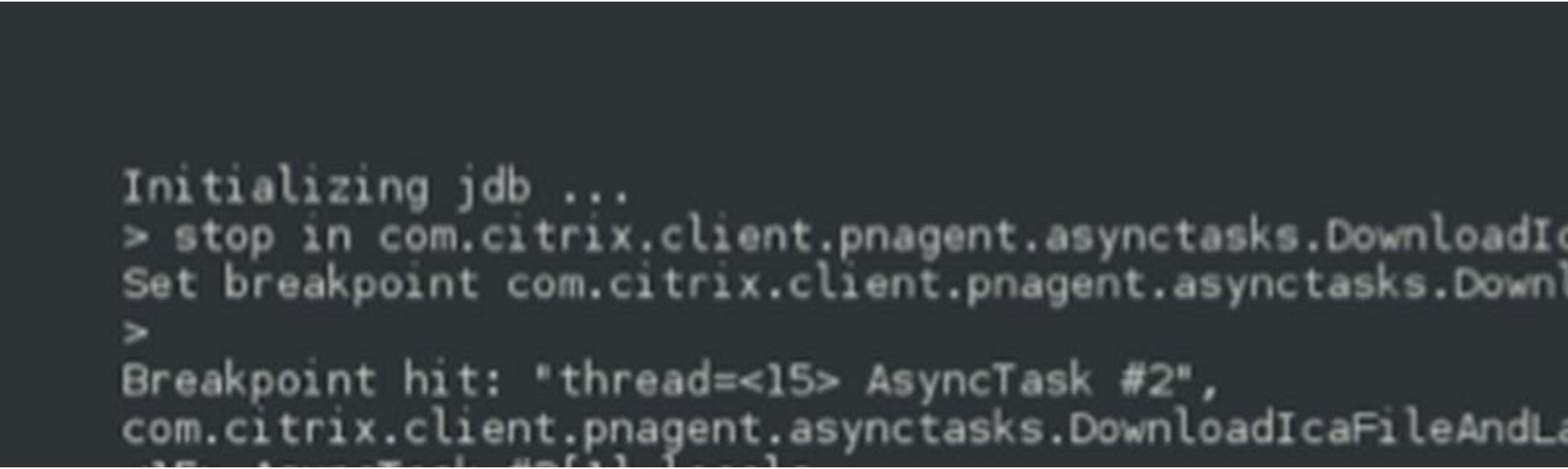
Threat 2

Threat 2
Grabbing Credentials Locally on Android

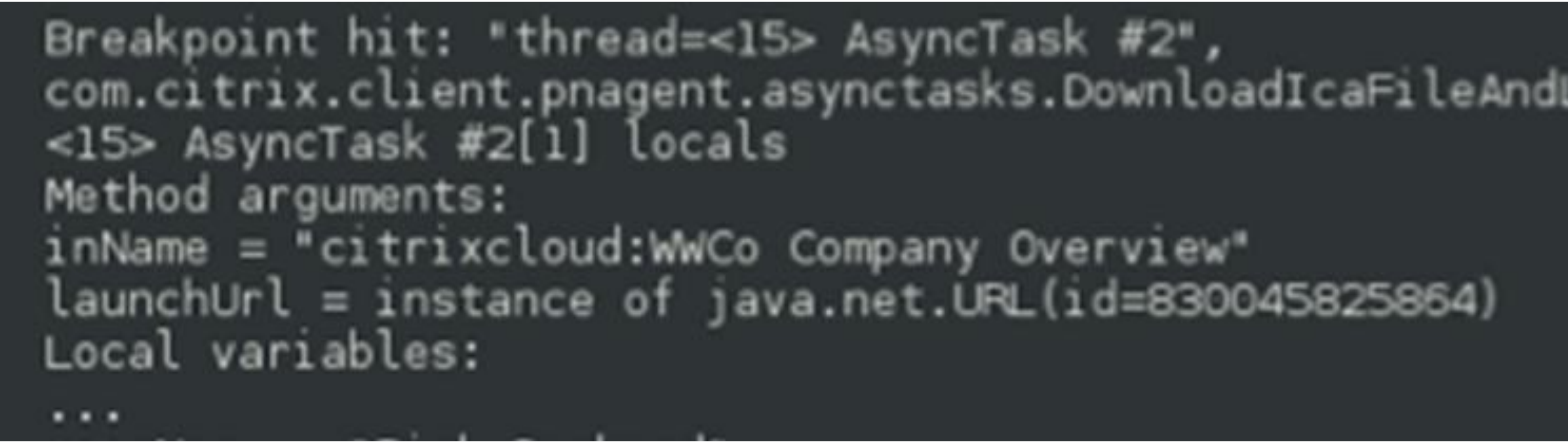
- Keylogging has its own problems
- Target the client itself to grab credentials

Threat 2
Grabbing Credentials Locally on Android

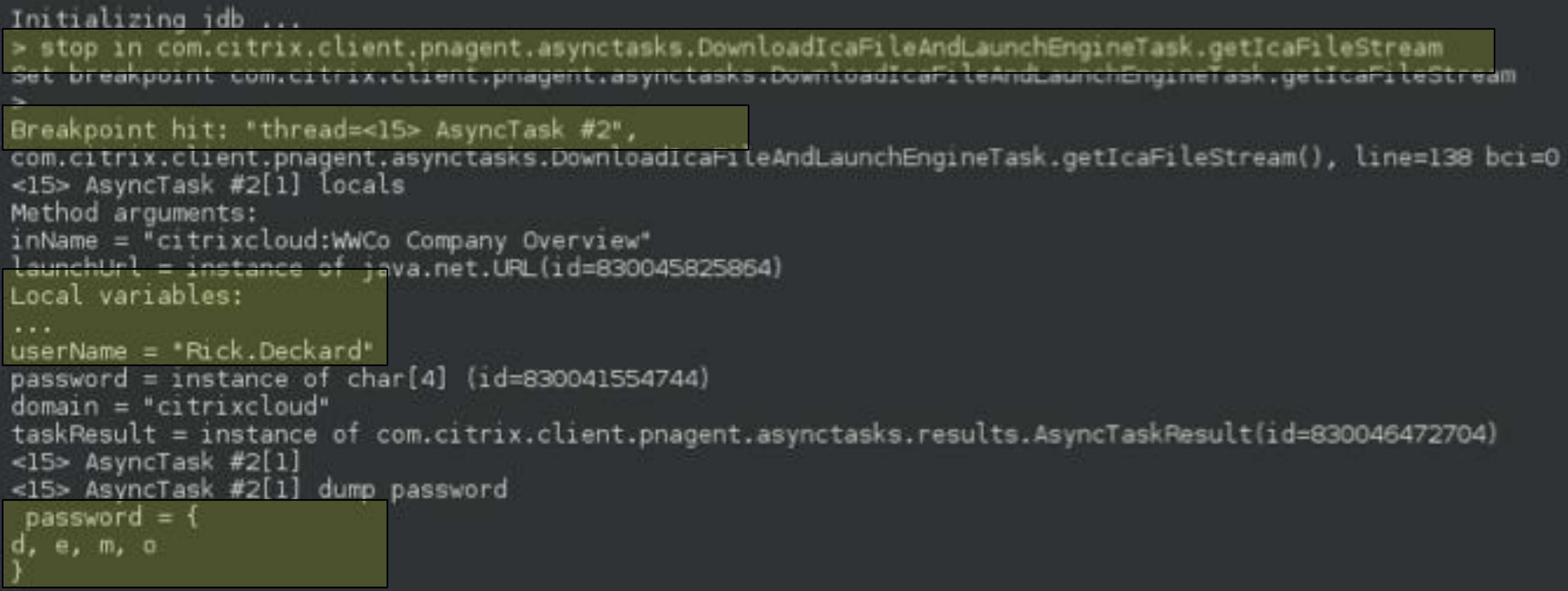
1. Run a Privilege Elevation vulnerability
    1. TowelRoot (CVE-2014-315), VROOT (CVE-2013-6282),…
    2. Exploit does not leave identifiable root marks unless programmed to
2. Enable jdwp debugging on all the apps installed on the device
3. Connect as a debugger to the VDI client
4. Set a breakpoint on a function that handles the credentials



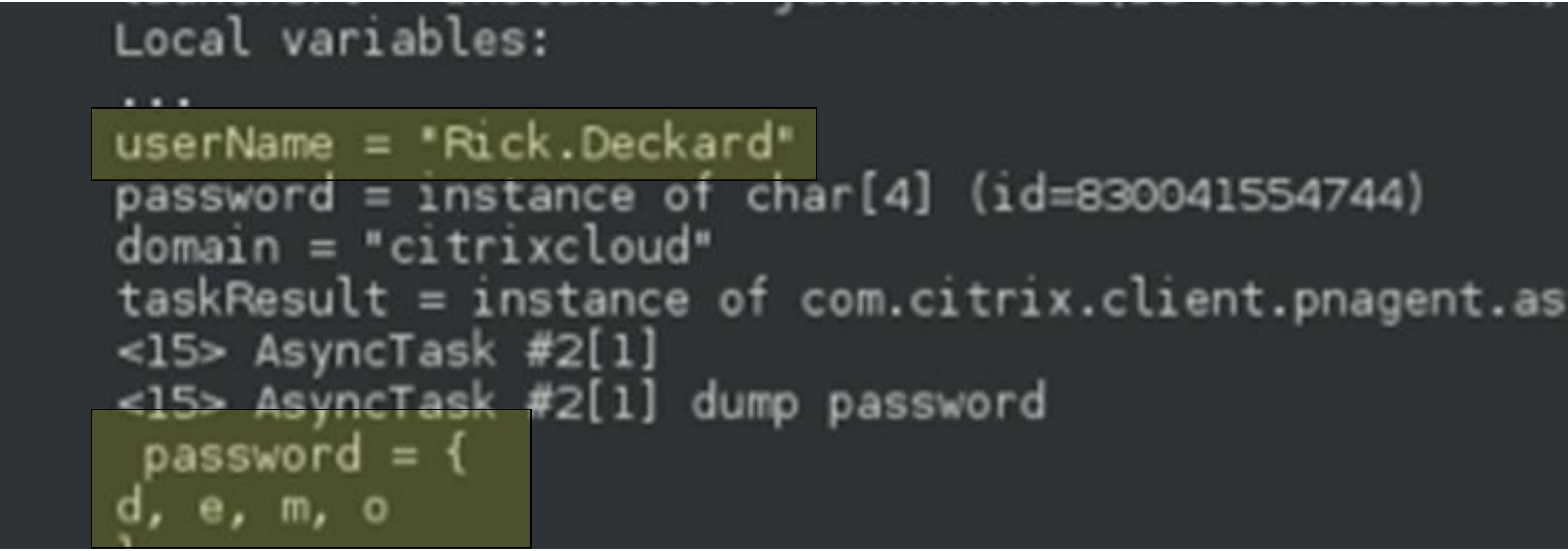
```
Initializing jdb ...
> stop in com.citrix.client.pnagent.asynctasks.DownloadIc
Set breakpoint com.citrix.client.pnagent.asynctasks.Downl
>
Breakpoint hit: "thread=<15> AsyncTask #2",
com.citrix.client.pnagent.asynctasks.DownloadIcaFileAndLa
<15> AsyncTask #2[1] locals
```



```
Breakpoint hit: "thread=<15> AsyncTask #2",
com.citrix.client.pnagent.asynctasks.DownloadIcaFileAnd
<15> AsyncTask #2[1] locals
Method arguments:
inName = "citrixcloud:WWCo Company Overview"
launchUrl = instance of java.net.URL(id=830045825864)
Local variables:
...
```



```
Initializing jdb ...
> stop in com.citrix.client.pnagent.asynctasks.DownloadIcaFileAndLaunchEngineTask.getIcaFileStream
Set breakpoint com.citrix.client.pnagent.asynctasks.DownloadIcaFileAndLaunchEngineTask.getIcaFileStream
>
Breakpoint hit: "thread=<15> AsyncTask #2",
com.citrix.client.pnagent.asynctasks.DownloadIcaFileAndLaunchEngineTask.getIcaFileStream(), line=138 bci=0
<15> AsyncTask #2[1] locals
Method arguments:
inName = "citrixcloud:WWCo Company Overview"
launchUrl = instance of java.net.URL(id=830045825864)
Local variables:
...
userName = "Rick.Deckard"
password = instance of char[4] (id=830041554744)
domain = "citrixcloud"
taskResult = instance of com.citrix.client.pnagent.asynctasks.results.AsyncTaskResult(id=830046472704)
<15> AsyncTask #2[1]
<15> AsyncTask #2[1] dump password
 password = {
d, e, m, o
}
```



```
Local variables:
...
userName = "Rick.Deckard"
password = instance of char[4] (id=830041554744)
domain = "citrixcloud"
taskResult = instance of com.citrix.client.pnagent.as
<15> AsyncTask #2[1]
<15> AsyncTask #2[1] dump password
 password = {
d, e, m, o
```

Enabling jdwp debugging on apps

- By ptrace-ing the init process to dynamically change the ro.debugabble property
  - Similar to what setpropx does
- By starting the jdwp thread in the relevant process
  - Easily done by calling the dvmJdwpStartup with ptrace

Possibilities to hook apps

JDWP

easy way to simply sit on a specific java function after enabling debugging

XPosed / Cydia Substrate

Also great way to dynamically hook a function without needing to resort to debugging

- Uses a small jar injected into every process by zygote to initiate hooking, dalvik changes not neccesary
- Can be hidden with root privileges

Screen Scraping against Android

Threat 3

Threat 3
Screen Scraping against Android

Two possible methods

- Leverage the clipboard access support
- Record the screen automatically when the mRAT detects that the VDI client is connected

Screen Scraping using Clipboard Access Support

Run a Privilege Escalation vulnerability

- TowelRoot (CVE-2014-315), VROOT (CVE-2013-6282),…
- Exploit does not leave identifiable root marks

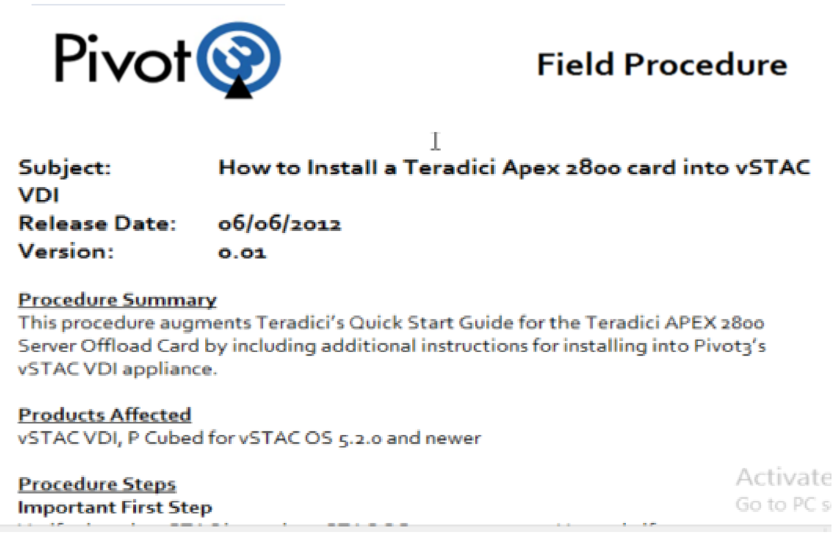
Monitor the current foreground activity using standard Android APIs getRunningTasks/getForgroundApp

Inject keyboard events to cause content to be copied from the file to the clipboard

- Using InputManager’s injectInputEvent (as root/system) we can inject input events
- Specifically Ctrl+A, Ctrl+C will work for most interesting applications

Screen Scraping using Clipboard Access Support

Inside the VDI client



Pivot

Field Procedure

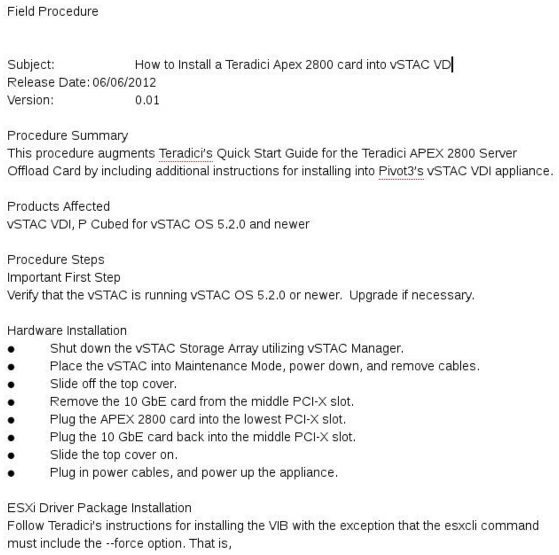
Subject: **How to Install a Teradici Apex 2800 card into vSTAC VDI**
Release Date: **06/06/2012**
Version: **0.01**

Procedure Summary
This procedure augments Teradici's Quick Start Guide for the Teradici APEX 2800 Server Offload Card by including additional instructions for installing into Pivot3's vSTAC VDI appliance.

Products Affected
vSTAC VDI, P Cubed for vSTAC OS 5.2.0 and newer

Procedure Steps
Important First Step

Data extracted from VDI client



Field Procedure

Subject: How to Install a Teradici Apex 2800 card into vSTAC VDI
Release Date: 06/06/2012
Version: 0.01

Procedure Summary
This procedure augments Teradici's Quick Start Guide for the Teradici APEX 2800 Server Offload Card by including additional instructions for installing into Pivot3's vSTAC VDI appliance.

Products Affected
vSTAC VDI, P Cubed for vSTAC OS 5.2.0 and newer

Procedure Steps
Important First Step
Verify that the vSTAC is running vSTAC OS 5.2.0 or newer. Upgrade if necessary.

Hardware Installation
- Shut down the vSTAC Storage Array utilizing vSTAC Manager.
- Place the vSTAC into Maintenance Mode, power down, and remove cables.
- Slide off the top cover.
- Remove the 10 GbE card from the middle PCI-X slot.
- Plug the APEX 2800 card into the lowest PCI-X slot.
- Plug the 10 GbE card back into the middle PCI-X slot.
- Slide the top cover on.
- Plug in power cables, and power up the appliance.

ESXi Driver Package Installation
Follow Teradici's instructions for installing the VIB with the exception that the esxcli command must include the --force option. That is,

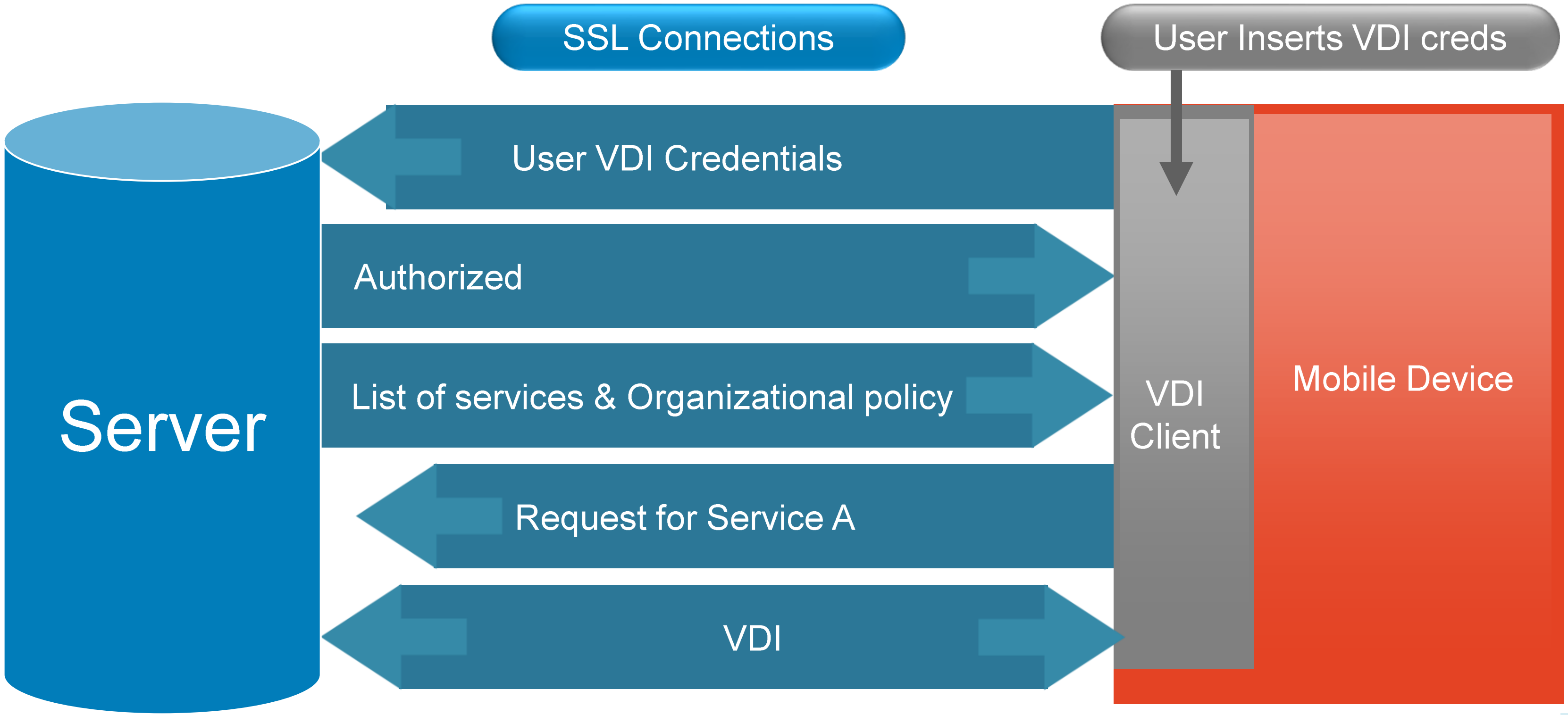
Screen Scraping using Screen Recording

1. Run a Privilege Escalation vulnerability
   - TowelRoot (CVE-2014-315), VROOT (CVE-2013-6282),…
   - Exploit does not leave identifiable root marks
2. Monitor the current foreground activity using standard Android APIs
   - getRunningTasks/getForgroundApp
3. Start recording the screen using one of the recording apis (go into depth)
   - 4.4 has a nice new screenrecorder – but possible even earlier by accessing framebuffer
   - SurfaceView.setSecure would need to be patched on 4.2 and up

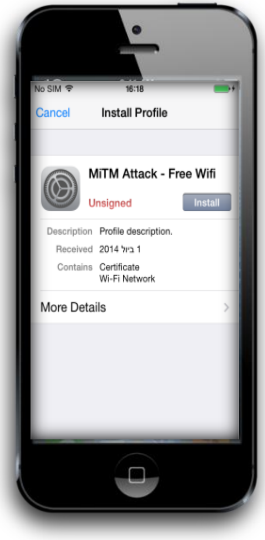
Man-in-the-middle (MITM)

Threat 4

VDI Protocol Flow



Malicious Configuration Profiles



Install Profile

MiTM Attack - Free Wifi

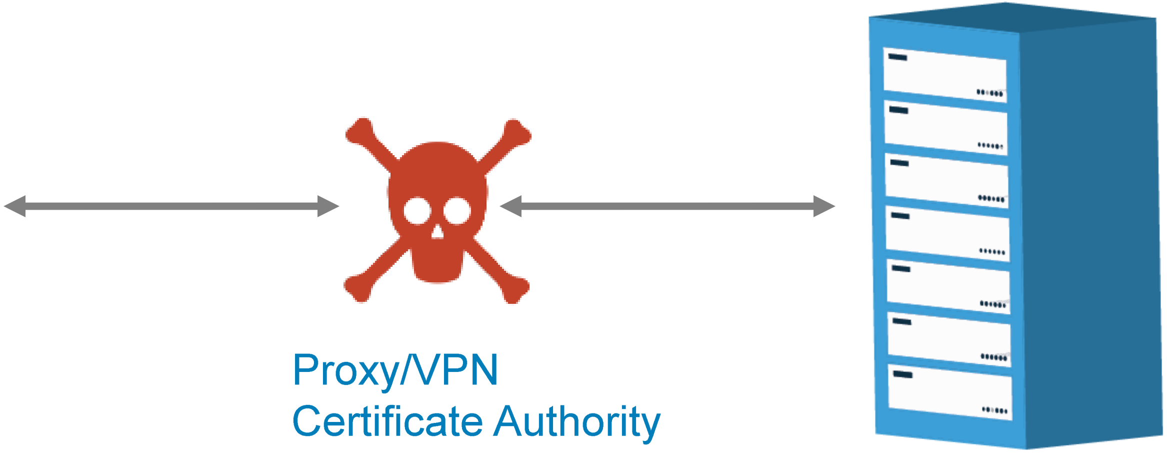
Unsigned

Description Profile description.

Received 1 ביול' 2014

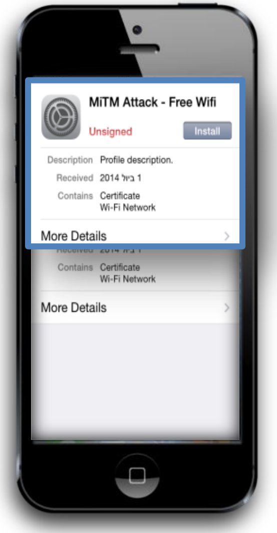
Contains Certificate
Wi-Fi Network

More Details



Proxy/VPN
Certificate Authority

Threat #4: MitM against iOS



MiTM Attack - Free Wifi

Unsigned

Description Profile description.

Received 1 ביול' 2014

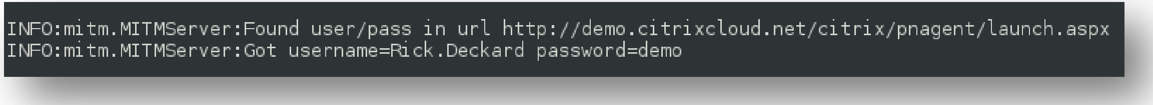
Contains Certificate
Wi-Fi Network

More Details

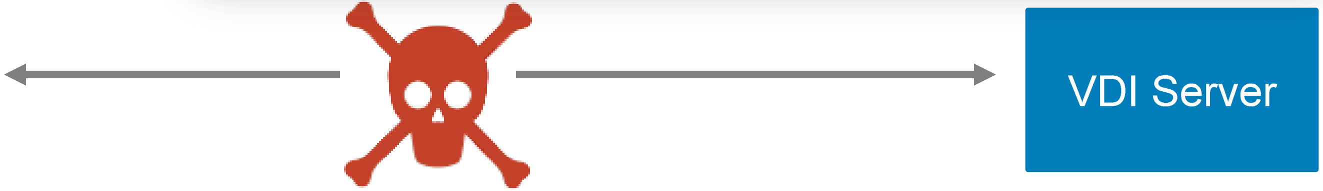
Contains Certificate
Wi-Fi Network

More Details

This is an email with a phishing link to a configuration profile. It will be replaced with a screenshot.



```
INFO:mitm.MITMServer:Found user/pass in url http://demo.citrixcloud.net/citrix/pnagent/launch.aspx
INFO:mitm.MITMServer:Got username=Rick.Deckard password=demo
```



More possibilities with MitM attacks

- Duplicating the actual screen/input stream to a separate machine
  - VmWare Horizon Viewer uses either a proprietary protocol or RDP
  - Citrix Receiver uses a proprietary protocol called ICA – not widely analyzed yet
- Simulate commands to the client and/or server
  - Can be used to do implementation specific actions, including gaining VPN credentials, etc…

Conclusions

VDI depends on the integrity of the host system

- Protects the data as long as the device is uncompromised
- If the underlying device is compromised, so is the VDI solution

Mobile VDI Motivation

Key Requirements for BYOD / CYOD

- Enablement ✓
- DLP / Lost Device ✓
- Intrusion ✗

Mobile VDI Motivation

Key Requirements for BYOD / CYOD

- Enablement ✓
- DLP / Lost Device ✓
- Intrusion ✓

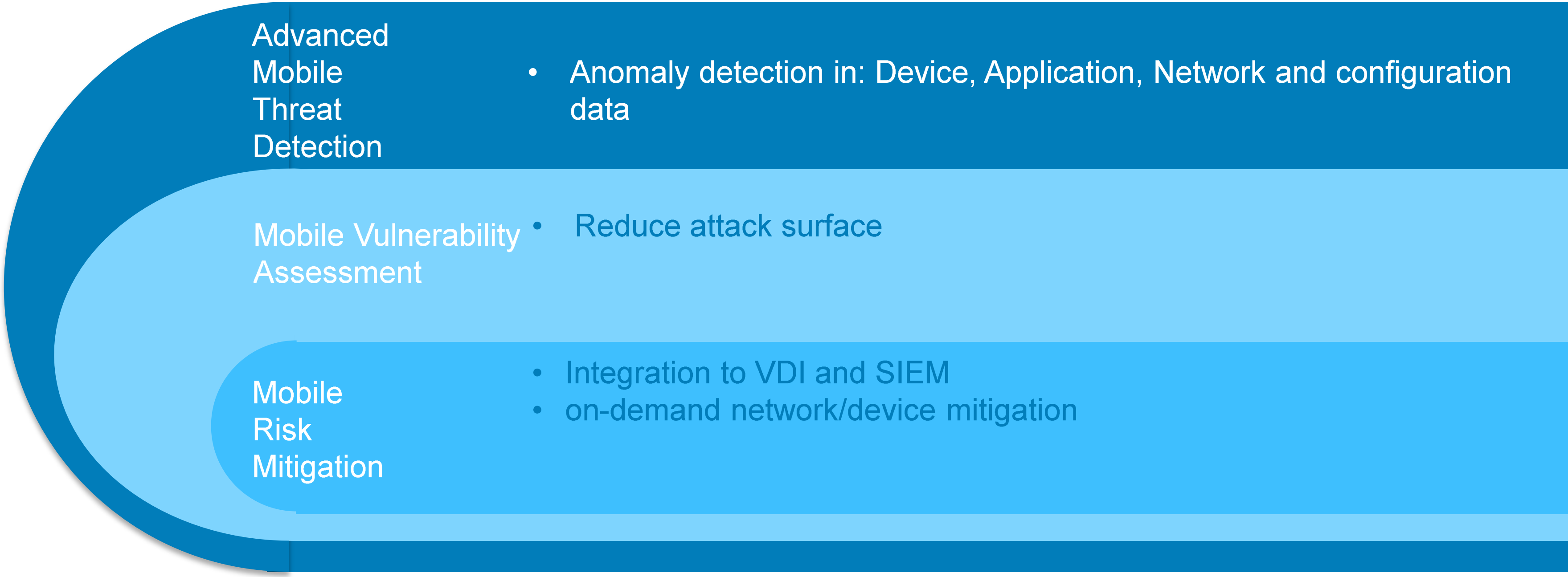
Building the necessary mobile security strategy

A Layered Mobile Security Approach

A multi-layer approach to mobile security.

Detect. Assess. Respond to Mobile Threats.

A Layered Mobile Security Approach



Advanced Mobile Threat Detection

- Anomaly detection in: Device, Application, Network and configuration data

Mobile Vulnerability Assessment

- Reduce attack surface

Mobile Risk Mitigation

- Integration to VDI and SIEM
- on-demand network/device mitigation

Thanks to those that helped on the Checkpoint-Lacoon mRATs in the Enterprise Survey!

Lacoon

- Pavel Berengoltz
- Shai Yanovski
- Shalom Bublil
- Daniel Brodie
- Shayna Tischler
- Amir Kessler
- Noam Modai
- Alon Boxiner

Checkpoint

- Inna Myslyuk
- Gali Carmel
- Ron Davidson
- Inbar Raz
- Alon Kantor
- Irena Damsky
- Hadass Rozental
- Maya Horowitz

LACOON
MOBILE SECURITY

Thank You!

Email: contact@lacoon.com

Twitter: @LacoonSecurity

www.lacoon.com/blog