RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: AIR-W03R

The Incident Response Playbook for Android and iOS

Andrew Hoog

CEO and Co-founder
NowSecure
@ahoog42
@NowSecureMobile

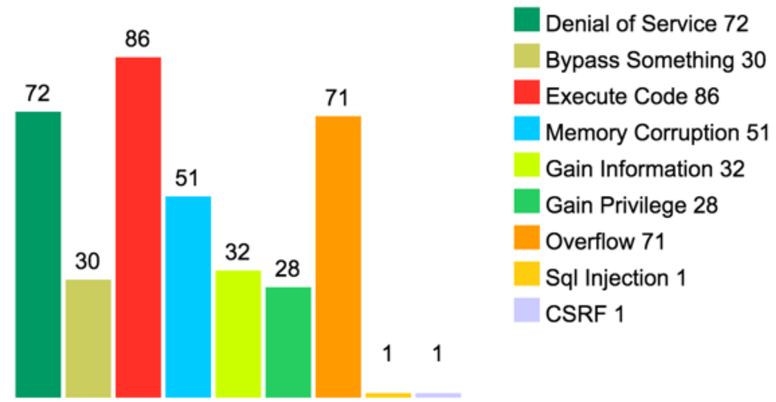
Andrew Hoog

- Author of three books
  - Incident Response for Android and iOS
    - Free and open-source
  - Android Forensics: Investigation, Analysis and Mobile Security for Google Android
  - iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices
- Expert witness
- Computer scientist
- Mobile security researcher

The State of Mobile Security

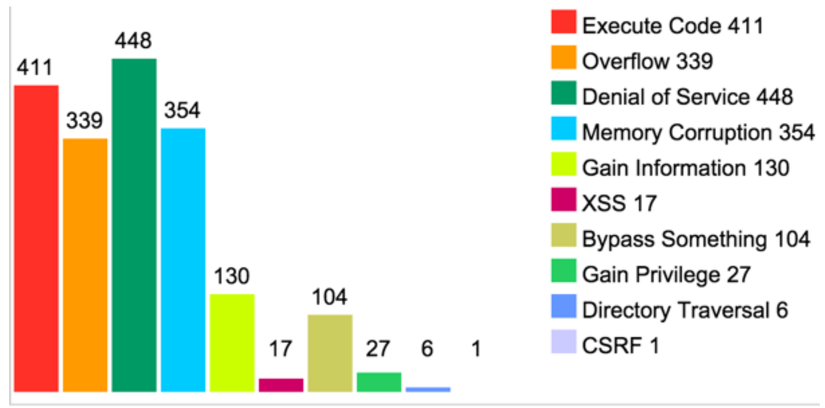
Mobile Devices Are Vulnerable

Lifetime Android CVEs by type (130 in 2015)



http://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

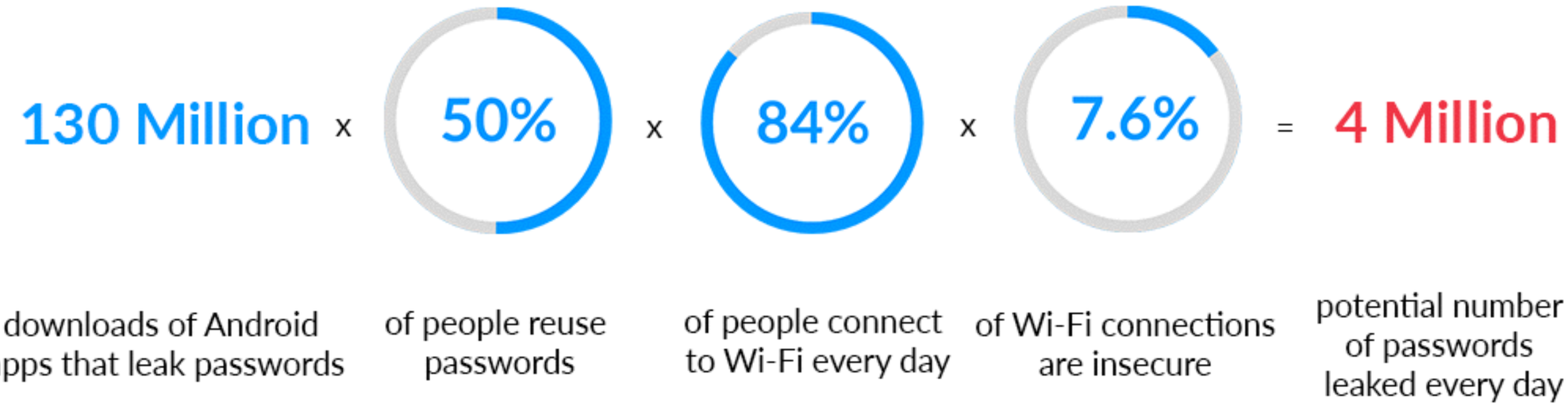
Lifetime iOS CVEs by type (375 in 2015)



http://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49

Mobile Apps Are Leaking Data

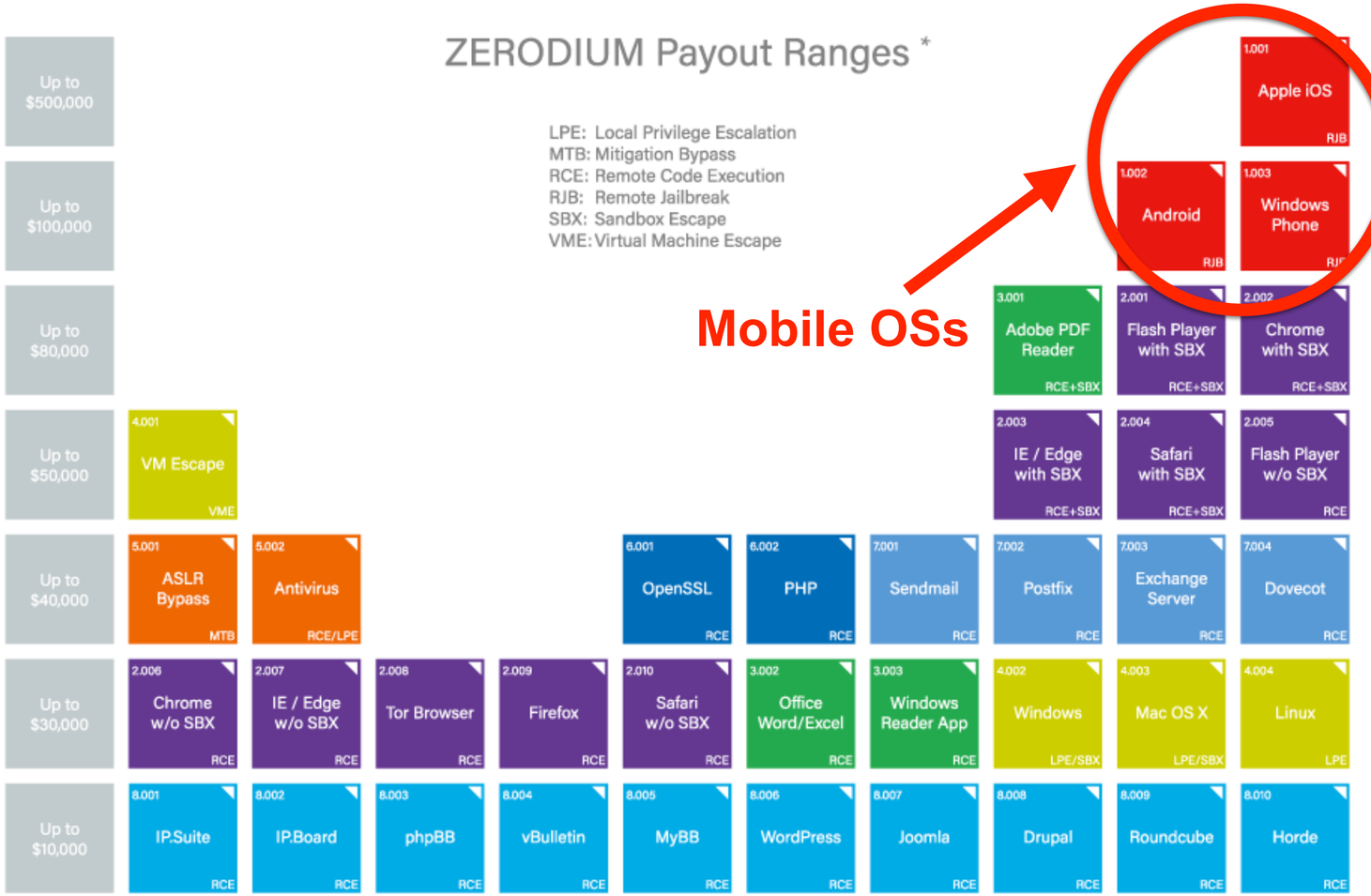
Example: Log-in credentials leaking each day



Source - Assessing impact of leaky apps: Usernames and passwords

Mobile Data Is Valuable

- Governments, malicious actors will pay to compromise mobile
- Hacking Team weaponizes mobile security flaws for surveillance
- Zerodium sells zero-day exploits and offers $1 million rewards for remote, untethered iOS jailbreaks

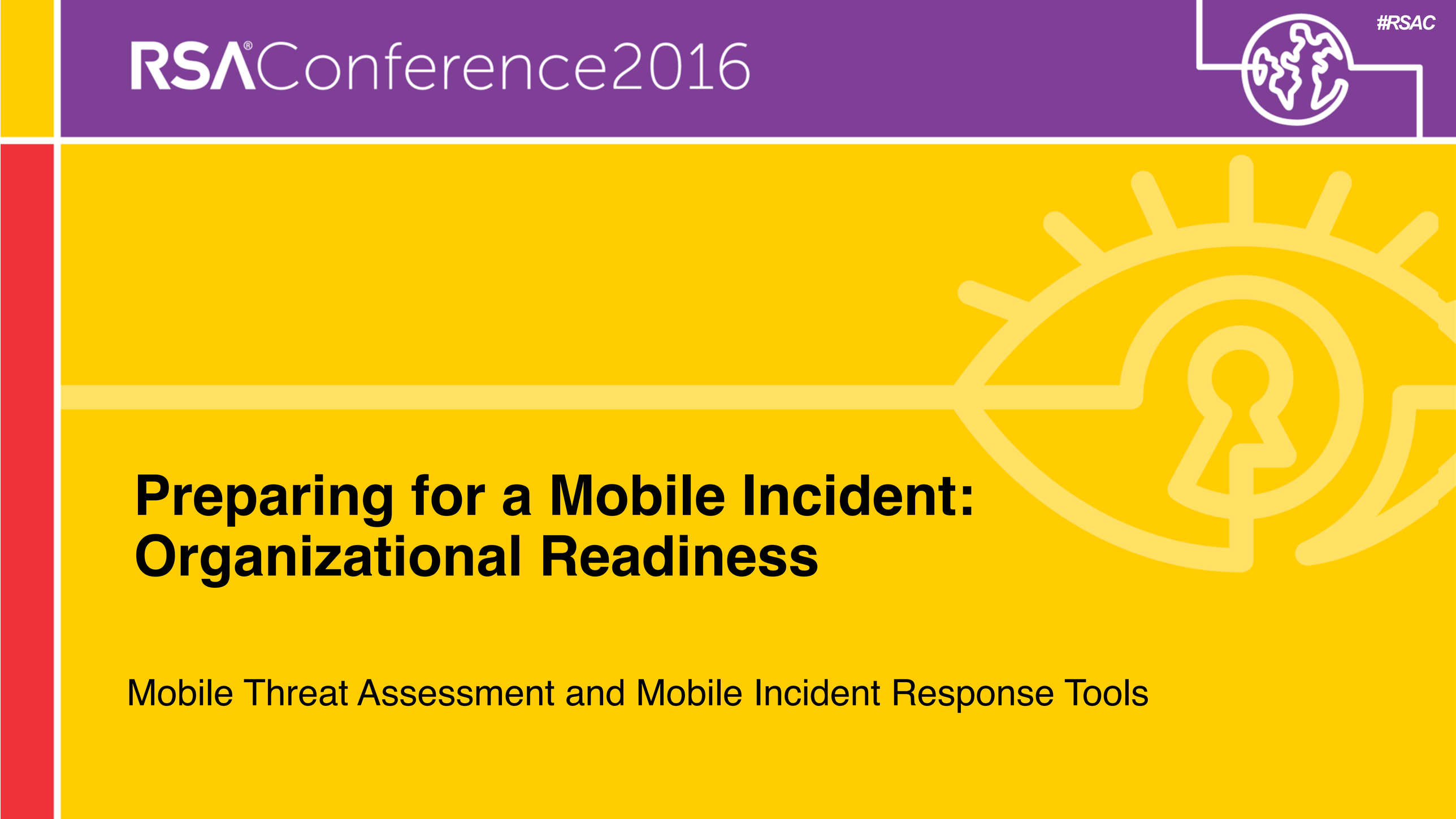


https://www.zerodium.com/program.html

Mobile Incident Response Challenges

Mobile technology is different than traditional computers

- Devices are always on and always connected
- BYOD and dual use impacts incident response
- App sandboxing requires different approach to endpoint defense
- Mobile IR tools are completely different and limited in number



Preparing for a Mobile Incident: Organizational Readiness

Mobile Threat Assessment and Mobile Incident Response Tools

Mobile Threat Assessment

Step 1: Perform a mobile inventory

- Identify assets: devices, operating systems, installed apps
  - Mobile device management (MDM) software
  - Exchange ActiveSync (EAS)
  - Network traffic analysis at corporate ingress/egress
- Historical device data is crucial to response

Few organizations have yet performed such an audit

Mobile Threat Assessment

Step 2: Correlate your inventory with mobile security intelligence

- Operating system vulnerabilities (OS CVEs)
- Leaky and insecure apps
- Known malware in the wild
- Other known risks (e.g., malicious Wi-Fi networks, SSL re-signing, etc.)

Organizations need to collaborate and share threat information so that enterprises can effectively detect and respond to threats.

Mobile Threat Assessment

Step 3: Work the problem

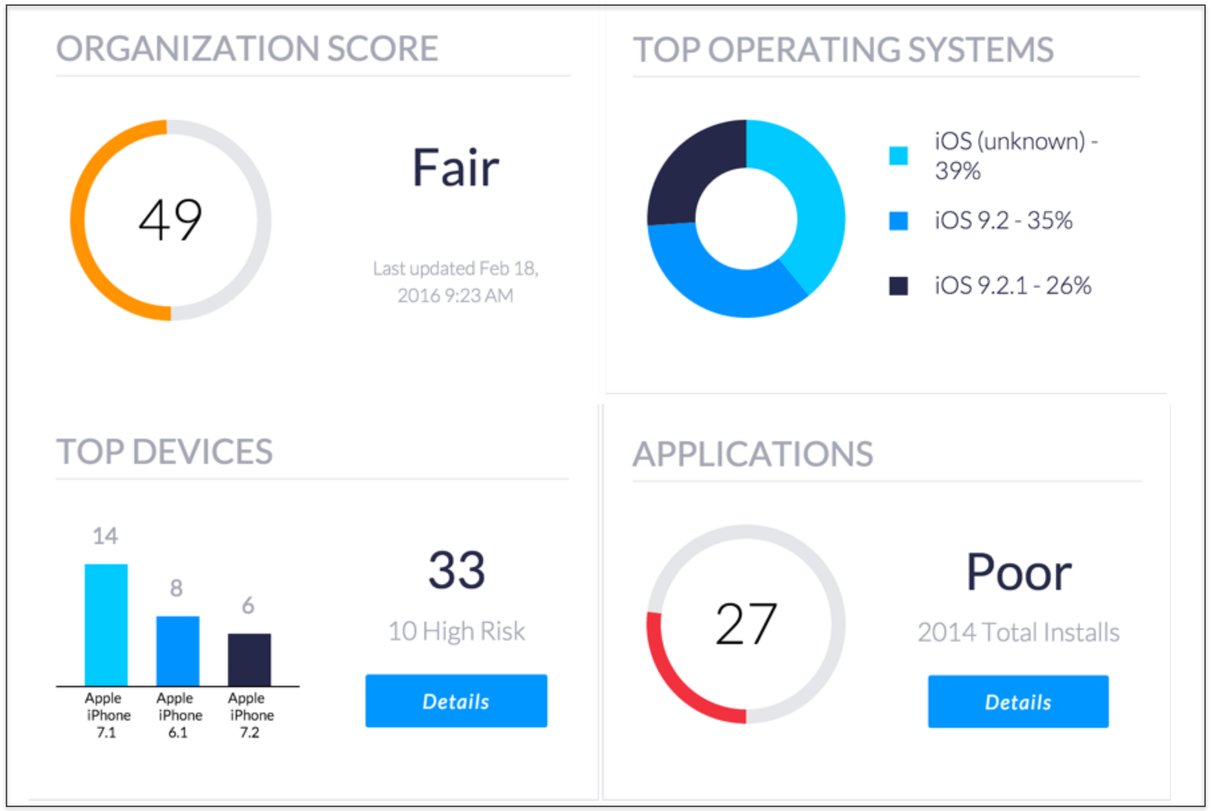
- Identify security risks
- Perform cost/benefit analysis
- Eliminate “low hanging fruit” and unacceptable risk
- Document remaining risks
- Prepare mobile IR playbooks

Most enterprises lack visibility into the amount of mobile risk they own

Identification and Response at Scale

Applying detection and response to 1000s of devices

Infected device



Example of an aggregated view of continual analysis data

Build Your Mobile IR Tool Box

- When an incident occurs
  - Need tools built for mobile
  - Need to be able to use the tools
  - Need baseline/historical data
- Santoku Linux - an open-source Linux distro for mobile forensics, security and malware analysis

1. Continual Analysis Tools (SCAN)

THE SCAN PRINCIPLE OF MOBILE SECURITY

VULNERABILITIES

S **SYSTEM**
Operating systems have security flaws. Sometimes patches don't exist or devices can't be updated, leaving users vulnerable.

C **CONFIGURATION**
Users impact the security of their devices through settings like passcodes, encryption, device profiles and more.

A **APP**
Even the most well-known app vendors release apps that contain major security vulnerabilities. Apps leak sensitive personal and business data.

N **NETWORK**
Mobile devices go everywhere and connect to many networks. Open/public networks are the perfect opportunity to intercept personal data.

1. Continual Analysis Tools

- Baseline device properties and behavior
- Provide historical view of a device
- Helpful for comparative analysis and anomaly detection

Free/Open Source Tools

- Vulnerability Test Suite (VTS) for Android
- iVerify-oss

2. Acquisition Tools

- Device acquisition
  - Backup
  - Logical
  - Physical
- Proxying network traffic

Free/Open Source Tools

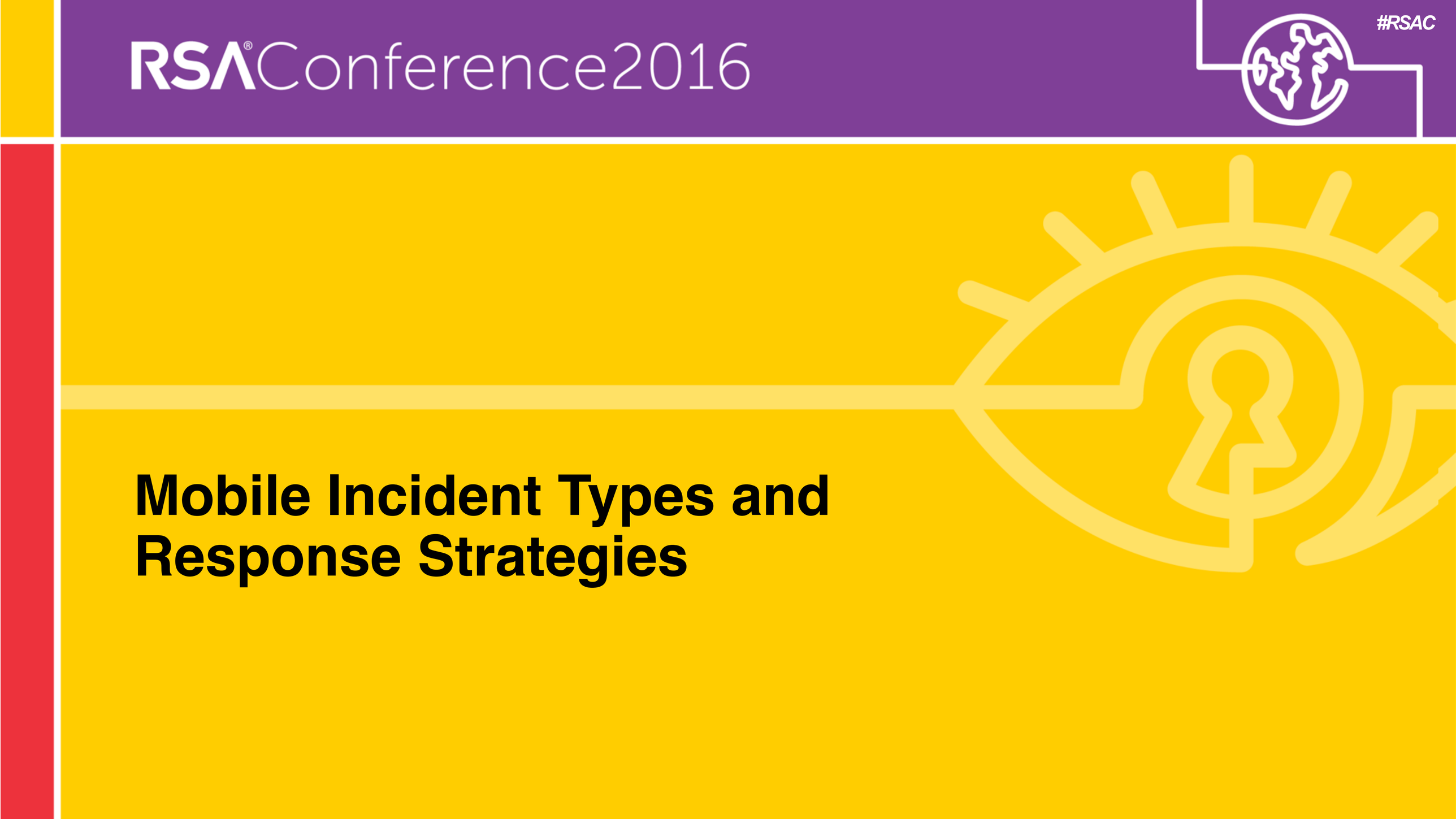
- iTunes (backup)
- libimobiledevice
- AF Logical OSE
- FROST
- LiME
- Burp Suite
- ZAP

3. Analysis Tools

- Forensic analysis
  - Timeline analysis
  - Searching
  - File carving
- Behavioral and comparative analysis
- Malware analysis
- Network analysis

Free/Open Source Tools

- Android Brute Force Encryption
- ExifTool
- Scalpel
- Sleuthkit
- Wireshark
- Nmap



Mobile Incident Types and Response Strategies

Mobile Incidents You May Encounter

Eight Common Mobile Incident Types

INCIDENT TYPE	PREVALENCE	MAX IMPACT	RISK
Internal Investigation	High	Medium	High
Insider Attack	Medium	High	High
Lost or Stolen Device	High	Low	Medium
Vulnerable or Leaky App	Medium	Medium	Medium
Malicious Imposter App	Low	High	Medium
Data Breach	Low	High	Medium
Device Acting Suspiciously	Medium	Low	Low
Malware on Device	Low	Medium	Low

Identification

- Device Indicators of Compromise (IOCs)
  - Increased battery drain
  - Unusual network traffic
  - Certificate errors
  - Unusual log messages
  - Crash reports
- App Reputation Monitoring
  - Unauthorized use of brand
  - Apps connecting to your transactional servers
- User Reported

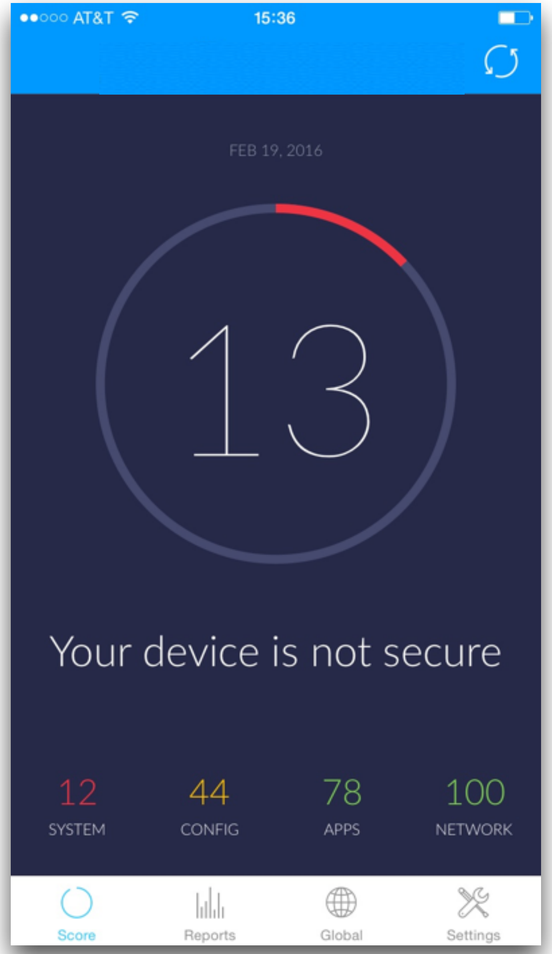
Containment

Once you have identified and logged an incident

- Gain access to device, if possible
- Capture device, OS and app baseline
- Determine if network analysis is appropriate
- Isolate the device (airplane mode, Faraday bag, etc.)
- Perform full forensic acquisition

Note on Handling Incidents Off-Network

- Capturing device baseline is possible
- Can leverage VPN for network analysis
- Individuals care deeply about the security of their device and will work with the IR team to resolve an incident



Caveat: if device inspection feels intrusive, people will either not report or not cooperate

Eradication

- Once incident is identified
  - Analyze attack artifacts
  - Determine if threat can be removed
  - Identify all impacted (if malware on app store)
  - Remove threat or wipe corporate data

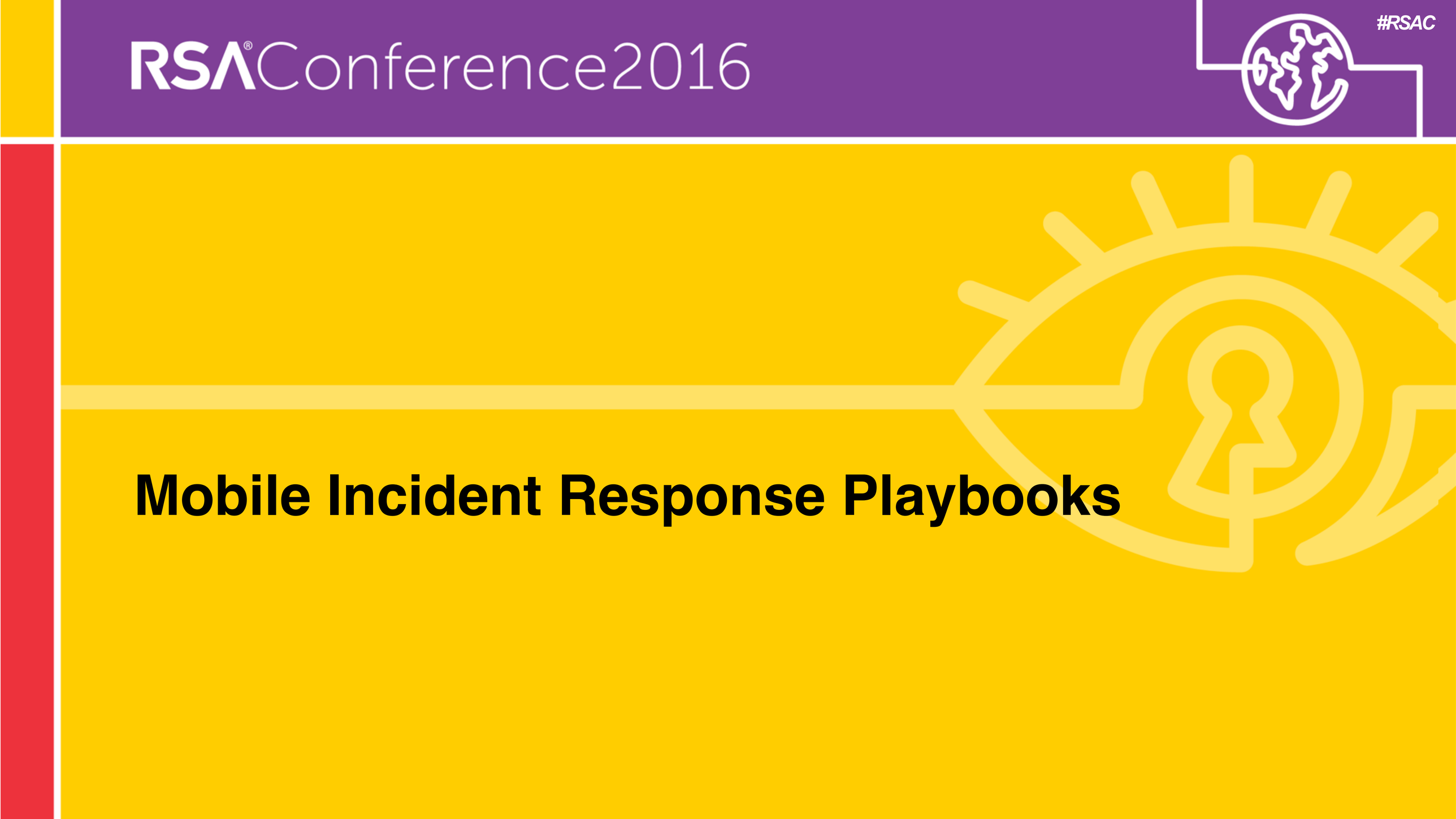
Recovery

- Mobile recovery typically involves
  - Re-provision mobile devices
  - Ensure attacker didn’t move laterally within your organization
  - Monitor accounts and systems connected to mobile device and impacted user(s)

Note: Effectiveness of social engineering attacks is greatly increased

Lessons Learned

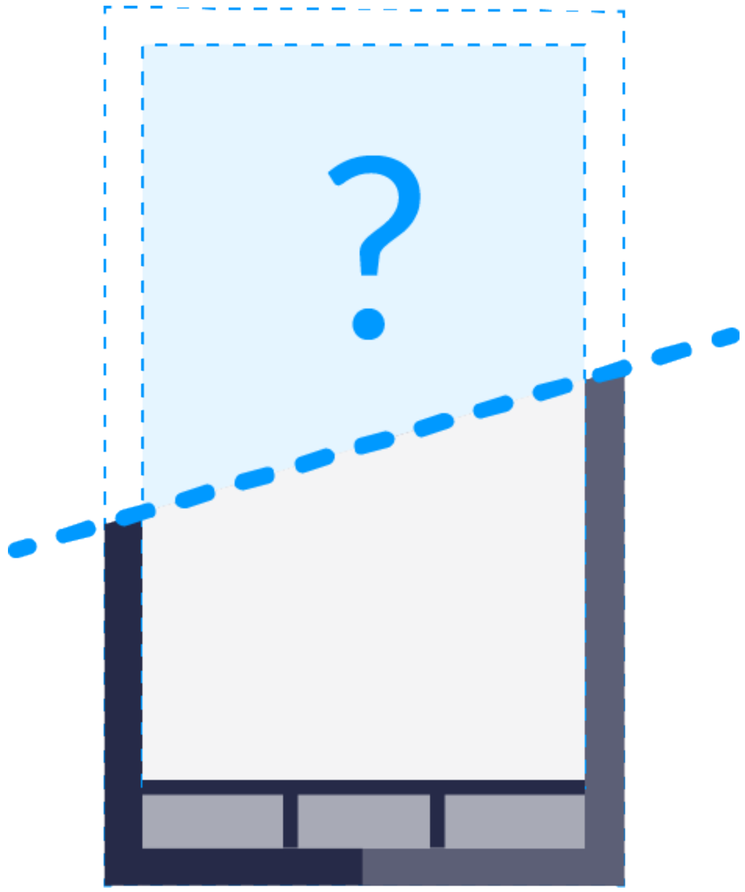
- Team debrief:
  - What went wrong, what worked, what can be improved
  - Recommended policies and procedures changes, user education, etc.
- Determine IOCs
  - Attribution
  - Share threat intel data
- Inoculate against future attacks
  - Static signatures generally ineffective
  - Focus on anomaly detection
  - Shared insights and cross-referenceable data



Mobile Incident Response Playbooks

Lost Phone

1. Attempt to locate and remotely lock device
2. Inspect continual analysis data for anomalies
3. Wipe corporate data if step 2 fails
4. Determine potential impact of incident with baseline data:
   - Identity and role of user
   - Data on their device
   - Apps they used

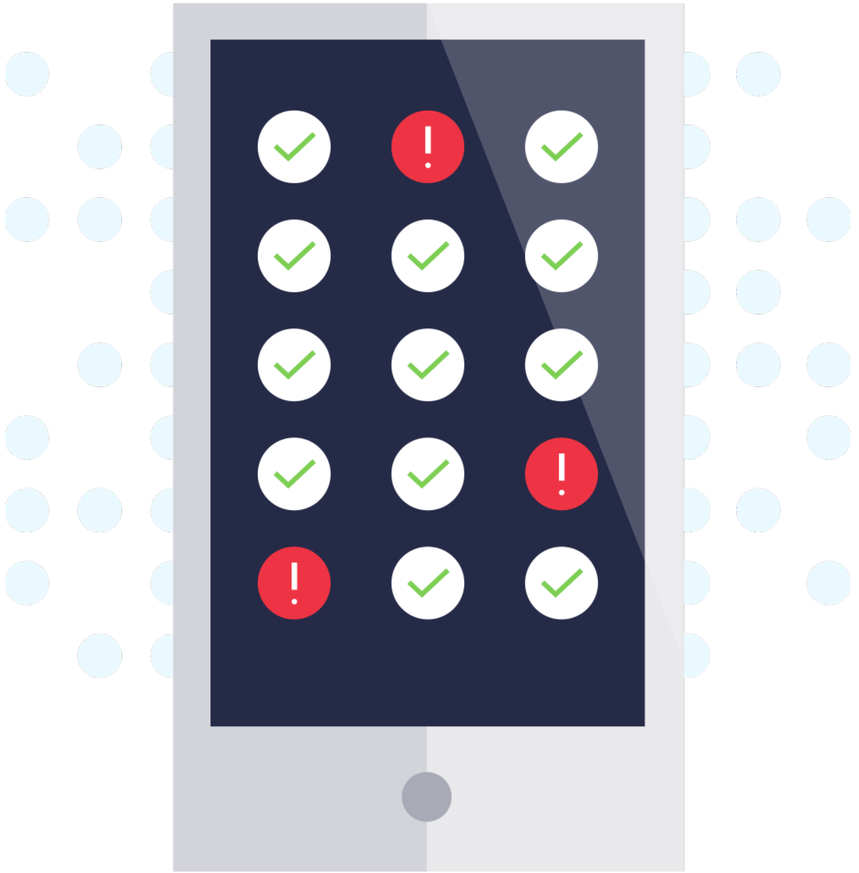


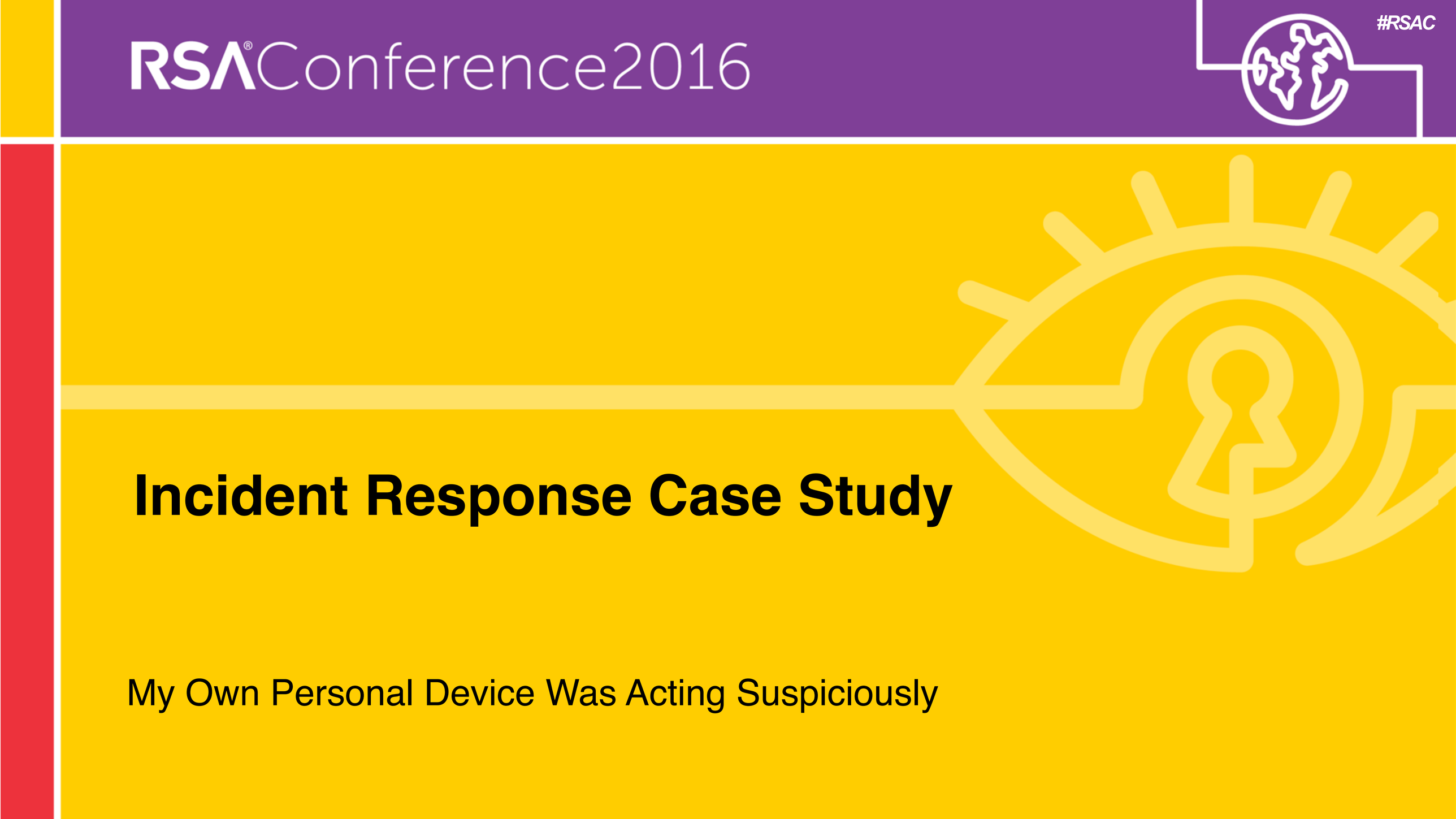
Device Acting Suspiciously

1. Capture device, OS and app baseline
2. Perform network analysis if appropriate
3. Isolate the device (airplane mode, Faraday bag, etc.)
4. Perform full forensic acquisition (if you have physical access)
5. Analyze device and app artifacts
6. If incident confirmed, determine eradication and recovery steps

Malware on App Store

1. Secure a copy of the malware
2. Analyze the app
   - Compare to intelligence about known malware
   - Perform static and dynamic analysis
3. Identify impacted users
   - Server logs with user agent
   - App/Play store security processes
4. Determine remediation steps - attempt to block at server level
5. Develop recovery and eradication steps



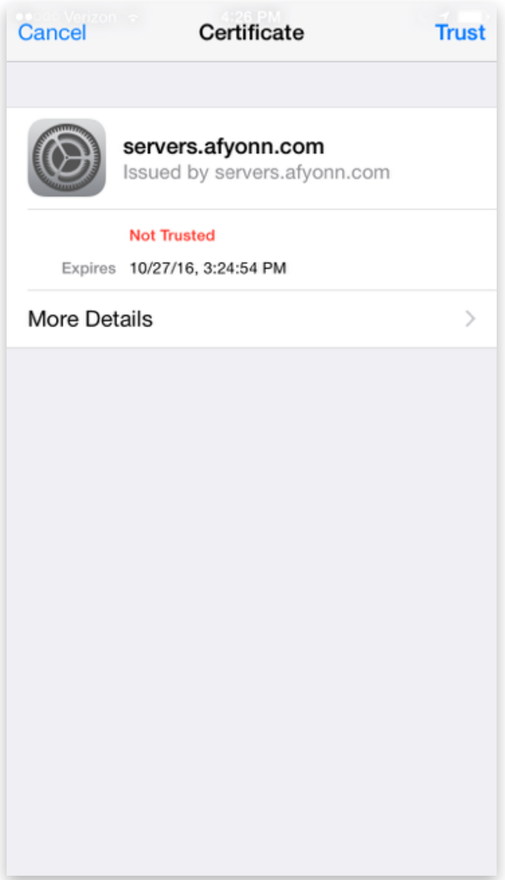


Incident Response Case Study

My Own Personal Device Was Acting Suspiciously

It All Began On Saturday Feb. 13

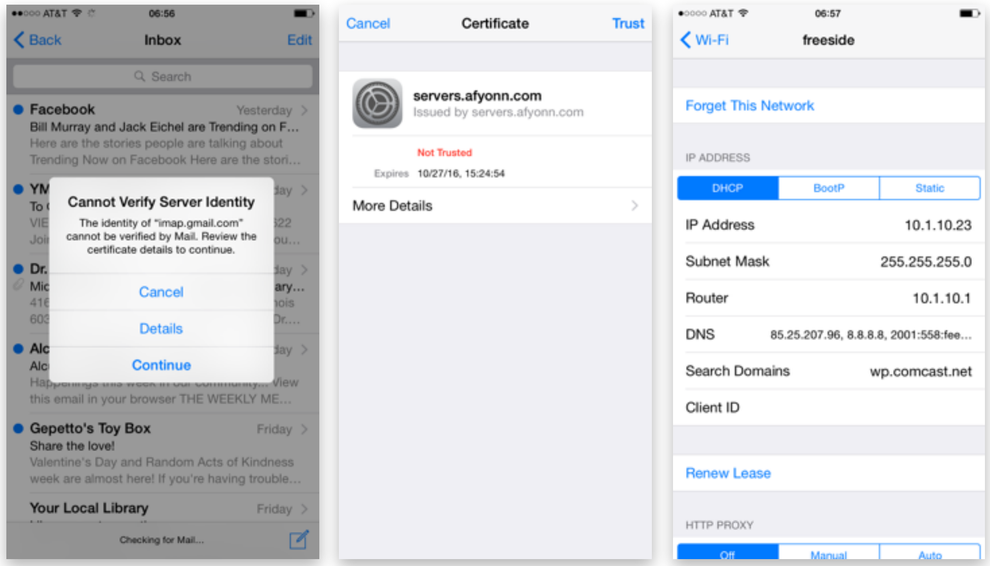
- Certificate error
- Examined the details
- Determined there was an issue
  - Documented the issue
  - Contacted corporate security team
- Attempted to re-create on iPad, other iOS devices, laptop, desktop



iPhone Screen-shots

Info Gathering and Identification

- Symptoms
  - Gmail app wouldn't sync
  - Wi-Fi certificate errors
- Analyzed certificate
  - Hosted in shared environment
  - Istanbul
  - Both used self-signed HTTPS certificate
  - Issued by: ssl@servers.carsimedya.com



iPhone screen-shots

Continuing Investigation

- Suspicious DNS entries
  - Queried IP address - resolved to a server in Germany
  - Same DNS as carsimedya.com
  - Social media and SEO related
  - Investigated router configuration
- Theories
  - Targeted attack
  - Mass router compromise (using known or zero-day vulnerability)

Conclusion

Summary and Applying What You've Learned

Summary

- Mobile IR is different than traditional IR
  - Limited administrative access
  - You need different tools
- The keys to mobile incident response success are:
  - Historical device data
  - Timely collection of device data post-incident
- Trial by fire is not the answer in mobile IR
  - Rehearse your plan
  - Rehearse it again

Your Next Steps

- **Next week:** identify who at your organization is responsible for mobile incident response and whether you have the capability internally
- **Within three months:** conduct a proactive mobile risk assessment, build your mobile IR toolkit, familiarize yourself with the tools
- **Within six months you should:** establish your response playbooks and rehearse them

Thank you

@ahoog42
ahoog@nowsecure.com