DEFENDING IN THE DARK

OCT 2017

NowSecure™

Andrew Hoog

CEO | NowSecure

Twitter - @ahoog42

E-mail - ahoog@nowsecure.com

- Computer scientist
- Mobile security & forensics researcher
- Author, expert witness & inventor

Contents

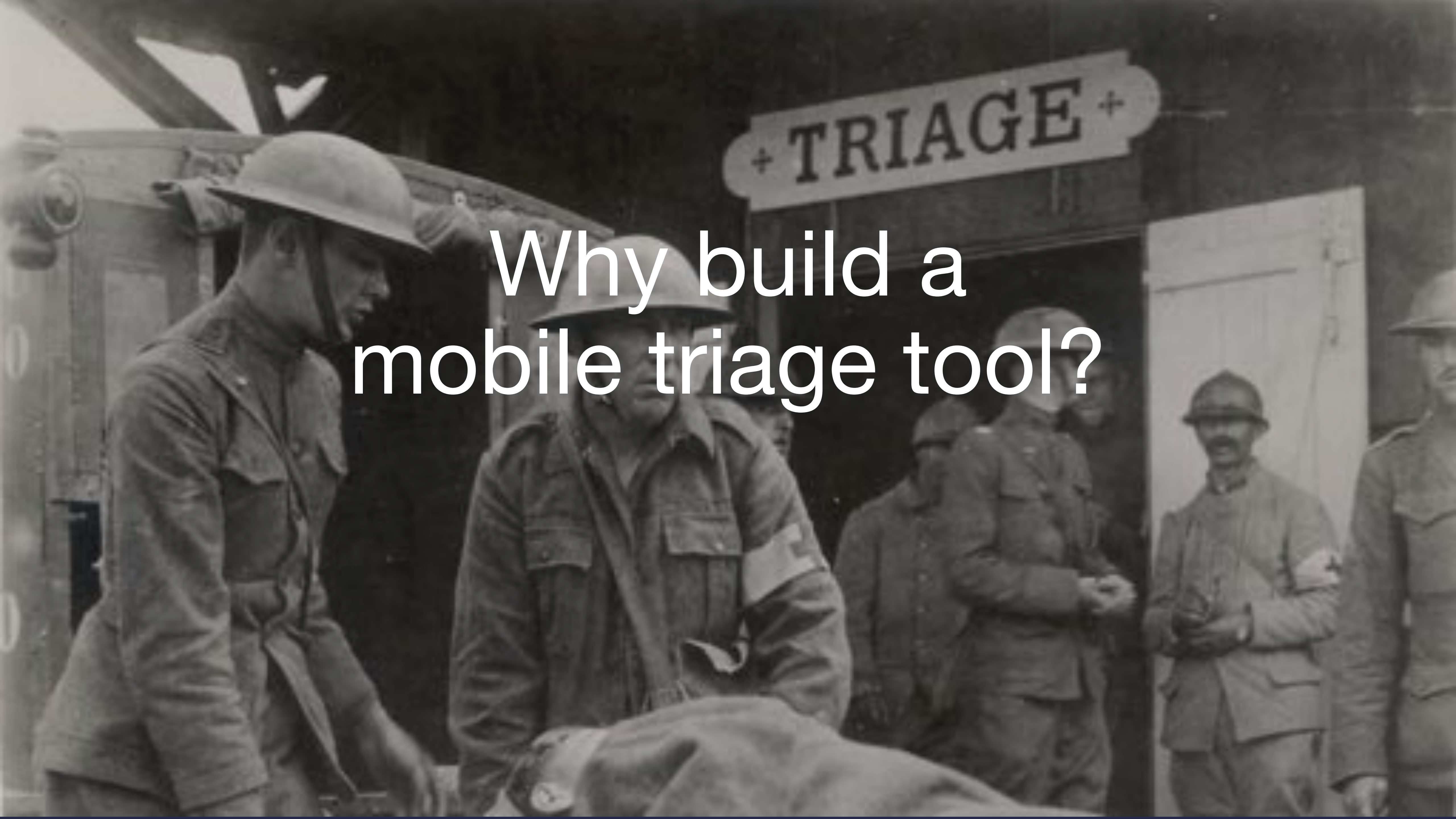
Why build a mobile triage tool?

Platform security enhancements

Limitations of current forensic tools

Introducing ios-triage

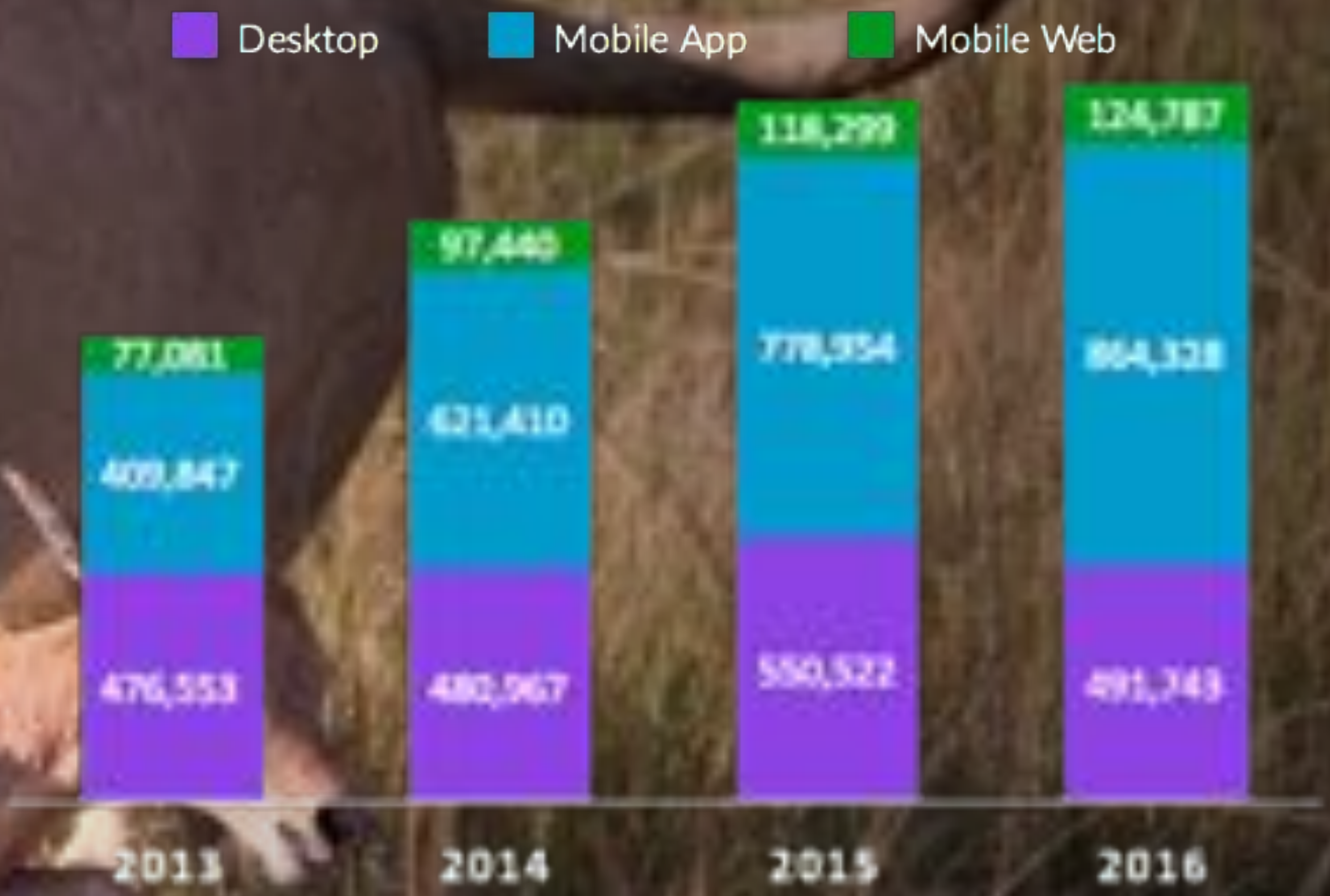
Summary, next steps, and questions



Why build a mobile triage tool?

PREDATOR FOLLOWS PREY: 2 OF 3 MINUTES ARE MOBILE

TOTAL MINUTES SPENT ON DIGITAL MEDIA



http://www.comscore.com/layout/set/popup/content/download/36073/1978401/version/1/file/2016_US_Mobile_App_Report.pdf

MOBILE DEVICES COLLECT INCREDIBLE AMOUNTS OF DATA

Personal data

- SMS
- Contacts
- Browser history
- GPS

Corporate data

- E-mail
- Contacts
- Documents
- Intellectual property

Rich sensor data

NowSecure™

ANDROID AND IOS HAVE VULNERABILITIES

642

Google Android CVEs
so far in 2017

1,333 CVEs over lifetime (2009-2017)

293

Apple iOS CVEs
so far in 2017

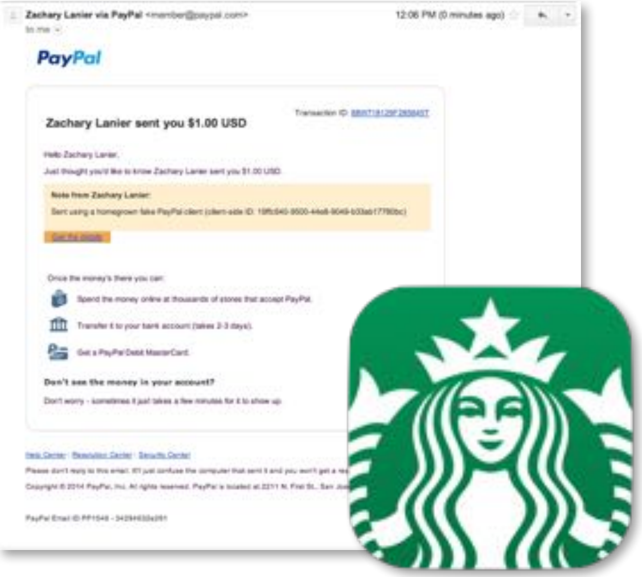
1,277 CVEs over lifetime (2007-2017)

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

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

DEVICES ARE TARGETED

CYBERCRIME FOR FINANCIAL GAIN



Zachary Lanier via PayPal <member@paypal.com> 12:06 PM (0 minutes ago)
to me

PayPal

Zachary Lanier sent you $1.00 USD

Transaction ID: [illegible]

Hello Zachary Lanier,

Just thought you'd like to know Zachary Lanier sent you $1.00 USD.

Note from Zachary Lanier:
Sent using a homegrown fake PayPal client (client-side ID: 19fb040-9500-44e8-9049-b03ab17780bc)

Get the details

Once the money's there you can:

- Spend the money online at thousands of stores that accept PayPal.
- Transfer it to your bank account (takes 2-3 days).
- Get a PayPal Debit MasterCard.

Don't see the money in your account?

Don't worry - sometimes it just takes a few minutes for it to show up.

Help Center | Resolution Center | Security Center

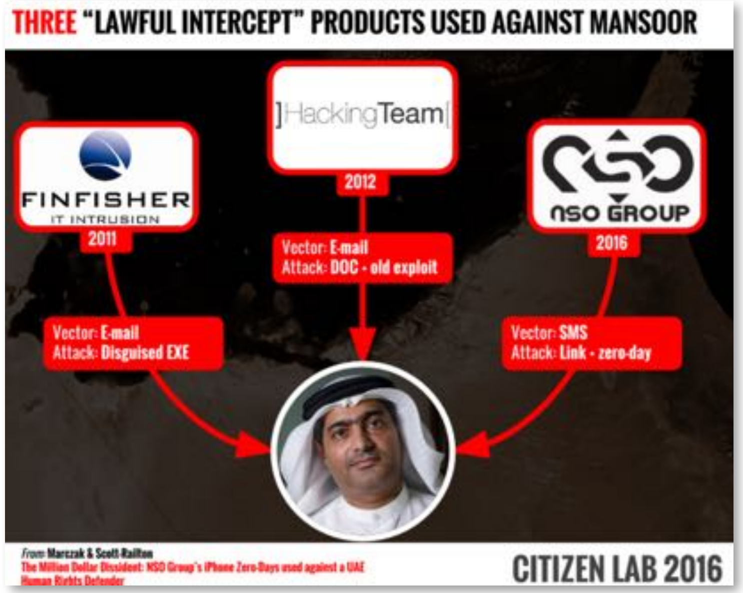
Please don't reply to this email. It'll just confuse the computer that sent it and you won't get a re

Copyright © 2014 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jo

PayPal Email ID PP1046 - [illegible]

Hack of Quest Diagnostics App Exposes Data of 34,000 Patients

TARGETED ATTACKS

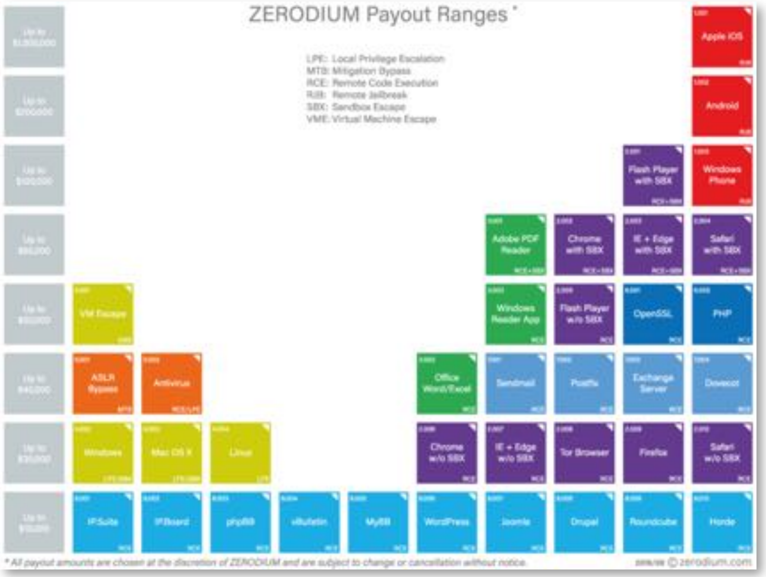


THREE "LAWFUL INTERCEPT" PRODUCTS USED AGAINST MANSOOR

From Marczak & Scott-Railton
The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender

CITIZEN LAB 2016

THRIVING MARKET FOR MOBILE EXPLOITS



* All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.

www © zerodium.com

NowSecure™

HISTORIC RECURRENCE: WEB AND PC ATTACKS AS PROXY

- Malware
- Ransomware
- Targeted attacks

"History may not repeat itself but it sure does rhyme."
—*Mark Twain (reputedly)*

NowSecure™

Platform security enhancements complicate defense/response

THE APERTURE IS SPIRALING SHUT

Legacy tools and methods don’t work for mobile

Platform security enhancements disarm responders/defenders

Platform architecture and API restrictions limit visibility

Attackers know more than the rest of us (asymmetric advantage)

Security telemetry is ephemeral, only one point in time

1. PROHIBITING ADMIN/ROOT ACCESS

PROS

- Sandboxing & lack of root access limits impact of security flaws – known and unknown
- Improves privacy by restricting app's access to sensitive device and other app data

CONS

- Attackers continue to find ways to elevate privileges, giving them them the advantage
- Security software cannot run on the system with sufficient access to detect/prevent attacks

2. HAMSTRINGING SECURITY TOOLS ON MOBILE DEVICES

PROS

- Forces OS vendors to build security into their system
- Prevents the installation of security apps that might harbor vulnerabilities (e.g., some PC-based security software has serious flaws)
- Security apps generate data that can easily be abused

CONS

- Attackers continue to find ways to elevate privileges, giving them them the advantage
- Security software cannot run on the system with sufficient access to detect/prevent attacks

3. RESTRICTING BACKUPS

PROS

- Reduces overall attack surface
- Data from a device is far less accessible to attackers

CONS

- Information critical to investigating a security breach is no longer accessible to defenders
- Attackers barely have to cover their tracks with few footprints left behind
- Important device-specific artifacts (e.g. the actual app binary) not available for analysis

4. ELIMINATING ACCESS TO APIs & DEVICE DATA

PROS

- End users' privacy & data cannot be violated (un)intentionally by developers
- Reducing complexity and quantity of APIs reduces overall attack surface

CONS

- Defenders lack even the most basic visibility into what's happening on the device
- (Near) continuous monitoring is impossible via an app
- Forces defenders to physically connect a device to extract relevant telemetry

5. IMPLEMENTING SECURE BOOT MECHANISMS

PROS

- An attacker with physical access to your device can't boot an alternative ROM & extract data
- Ability to implement "Trusted Computing" capabilities like trusted platform modules (TPMs) and vendor-specific extensions (e.g., KNOX, Qualcomm Haven, etc.)

CONS

- Defenders cannot access system images or critical device data for an investigation
- Security-conscious experts cannot install alternative operating systems
- Security research, instrumentation & honeypots become incredibly difficult

Overcoming the limitations of current forensic tools

LIMITS OF AVAILABLE FORENSIC TOOLS AS RELATES TO MOBILE

- Same fundamentals, but different angle – we need more than court-admissible evidence
- Can’t access some data due to platform security enhancements
- Less emphasis on app data and integrity of operating system and apps, key areas defenders examine for compromise

WHAT A FORENSIC ANALYST IS LOOKING FOR

SMS

STORED AND DELETED DATA

(e.g., iMessages, SMS, e-mail, etc.)

USER LOCATION HISTORY

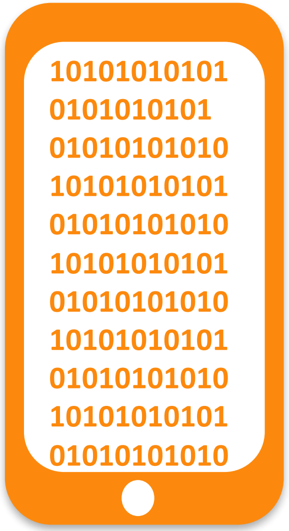
101010101010
101010101010
101010101010
101010101010
101010101010
101010101010

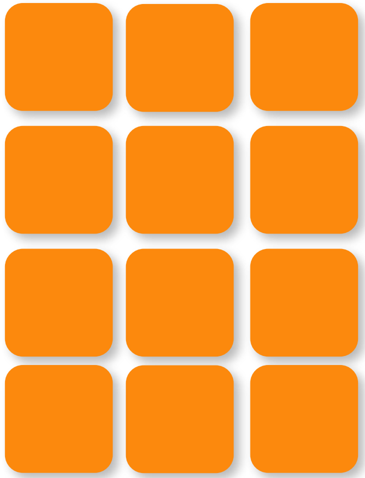
TIMELINE OF EVENTS

(based on the recoverable data)

NowSecure™

WHAT A DEFENDER/RESPONDER IS LOOKING FOR





DEVICE INTEGRITY INFORMATION

(e.g., OS, boot loader, how healthy is the device itself?)

APP DATA

(e.g., installed/uninstalled apps, security flaws, data collected)

TRAFFIC DESTINATIONS

(e.g., was data exfiltrated and if so, where to and is it persistent?)

Introducing ios-triage

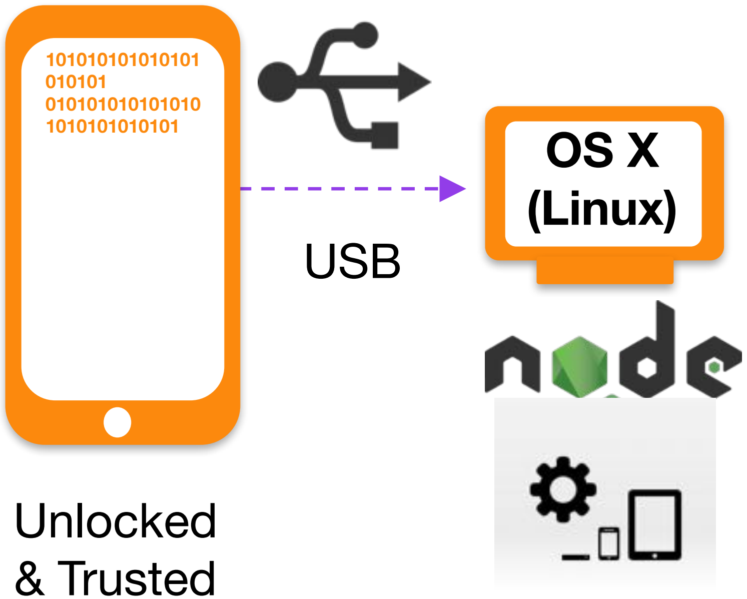
ios-triage

WHAT IT IS:	a mobile incident response tool
WHO IT’S FOR:	incident responders, defenders, hackers
WHAT IT DOES:	extracts mobile artifacts that matter, presents them for analysis, combines and correlates them with other relevant data
HOW IT’S DIFFERENT:	provides more visibility into data relevant to defending against or responding to mobile security incidents
WHERE TO GET IT:	https://github.com/ahoog42/ios-triage

NowSecure™

TOOLSET ARCHITECTURE/WORKFLOW

1 EXTRACT



Unlocked
& Trusted

libimobiledevice.

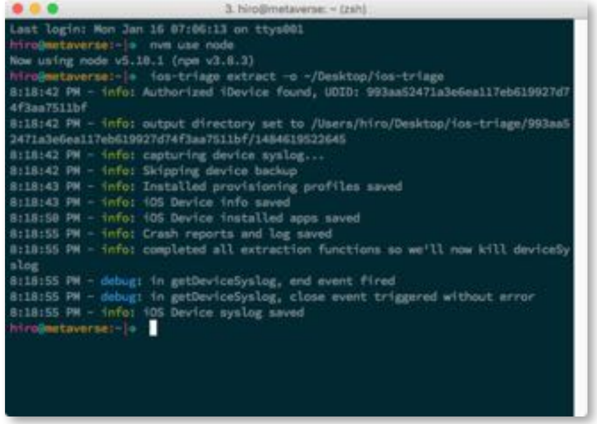
2 PROCESS

```
<dir>/UDID/epoch/artifacts

/processed

/report
```

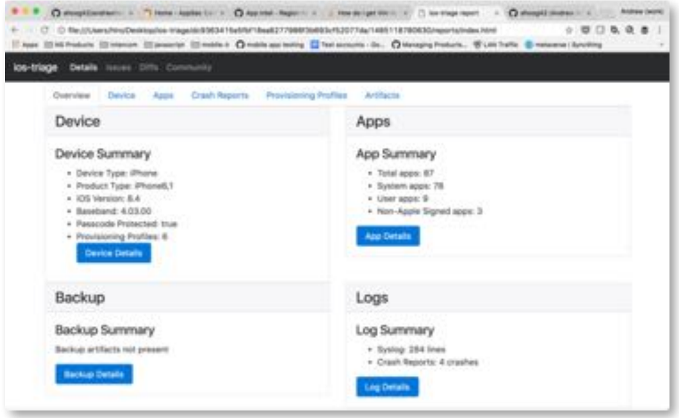
Multiple epochs
(i.e., timestamps)



```
3. hiro@metaverse: ~ (zsh)
Last login: Mon Jan 16 07:06:13 on ttys001
hiro@metaverse:~|⇒  nvm use node
Now using node v5.10.1 (npm v3.8.3)
hiro@metaverse:~|⇒  ios-triage extract -o ~/Desktop/ios-triage
8:18:42 PM - info: Authorized iDevice found, UDID: 993aa52471a3e6ea117eb619927d7
4f3aa7511bf
8:18:42 PM - info: output directory set to /Users/hiro/Desktop/ios-triage/993aa5
2471a3e6ea117eb619927d74f3aa7511bf/1484619522645
8:18:42 PM - info: capturing device syslog...
8:18:42 PM - info: Skipping device backup
8:18:43 PM - info: Installed provisioning profiles saved
8:18:43 PM - info: iOS Device info saved
8:18:50 PM - info: iOS Device installed apps saved
8:18:55 PM - info: Crash reports and log saved
8:18:55 PM - info: completed all extraction functions so we'll now kill deviceSy
slog
8:18:55 PM - debug: in getDeviceSyslog, end event fired
8:18:55 PM - debug: in getDeviceSyslog, close event triggered without error
8:18:55 PM - info: iOS Device syslog saved
hiro@metaverse:~|⇒ 
```

ios-triage process

3 REPORT



Device

Device Summary

- Device Type: iPhone
- Product Type: iPhone6,1
- iOS Version: 8.4
- Baseband: 4.03.00
- Passcode Protected: true
- Provisioning Profiles: 6

Apps

App Summary

- Total apps: 87
- System apps: 78
- User apps: 9
- Non-Apple Signed apps: 3

Backup

Backup Summary

Backup artifacts not present

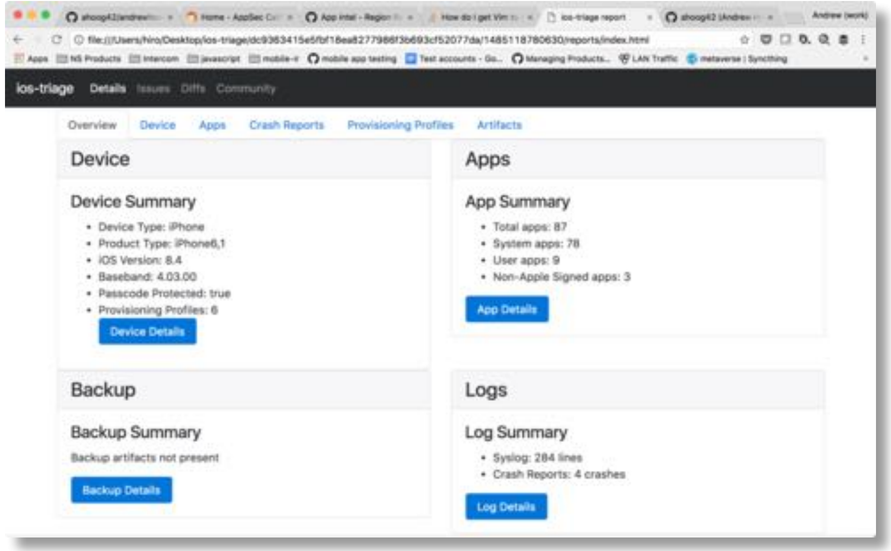
Logs

Log Summary

- Syslog: 284 lines
- Crash Reports: 4 crashes

NowSecure™

LIVE DEMO - DETAILS



Device

Device Summary

- Device Type: iPhone
- Product Type: iPhone6,1
- iOS Version: 8.4
- Baseband: 4.03.00
- Passcode Protected: true
- Provisioning Profiles: 6

Apps

App Summary

- Total apps: 87
- System apps: 78
- User apps: 9
- Non-Apple Signed apps: 3

Backup

Backup Summary

Backup artifacts not present

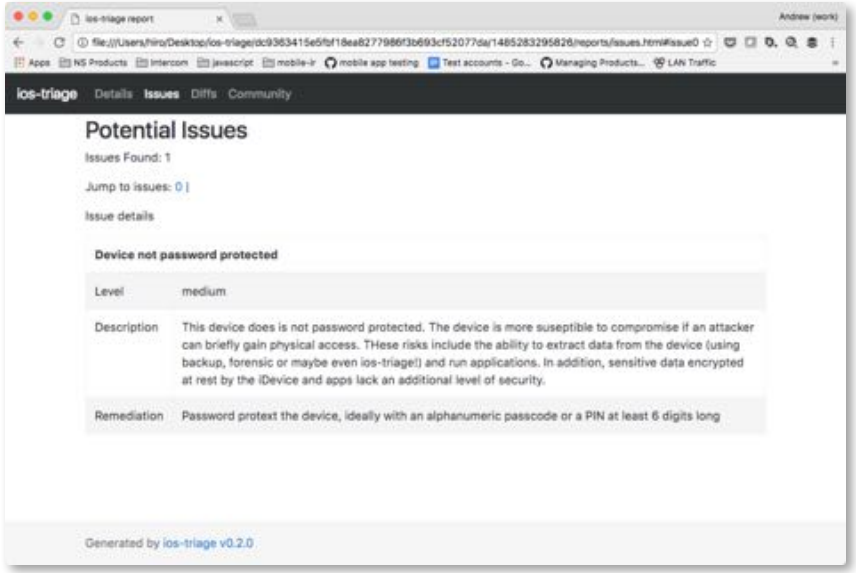
Logs

Log Summary

- Syslog: 284 lines
- Crash Reports: 4 crashes

- Overview of device & app analysis
- Detailed view of artifact data for all domains
- App specific telemetry including entitlements, background modes, privacy sensitive requests & transport security exceptions

LIVE DEMO - ISSUES



Potential Issues

Issues Found: 1

Jump to issues: 0 |

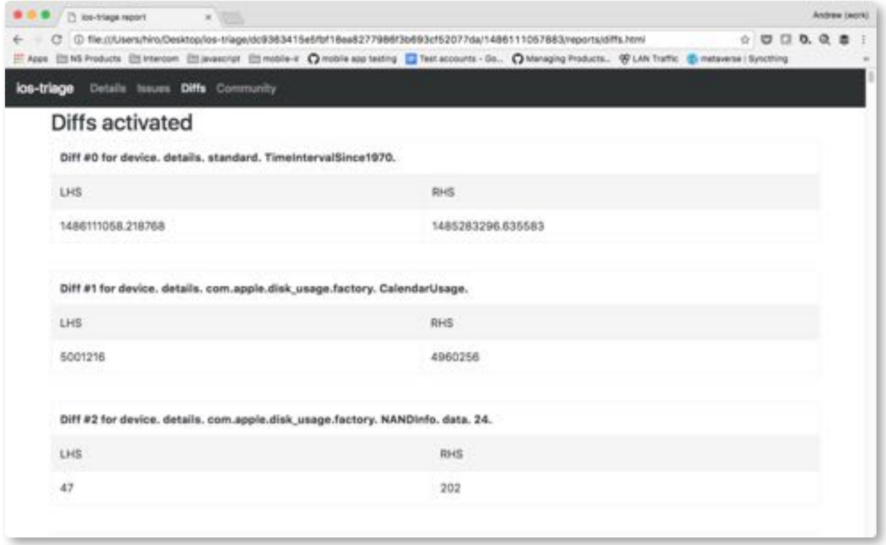
Issue details

Device not password protected	
Level	medium
Description	This device does is not password protected. The device is more suseptible to compromise if an attacker can briefly gain physical access. THese risks include the ability to extract data from the device (using backup, forensic or maybe even ios-triage!) and run applications. In addition, sensitive data encrypted at rest by the iDevice and apps lack an additional level of security.
Remediation	Password protext the device, ideally with an alphanumeric passcode or a PIN at least 6 digits long

Generated by ios-triage v0.2.0

- Flag issues in one central location
- Includes the issue, level of impact, description & remediation tips
- Flexible & extensible transformation of processed artifacts into issues

LIVE DEMO - DIFFS



Diffs activated

Diff #0 for device. details. standard. TimeIntervalSince1970.

LHS	RHS
1486111058.218768	1485283296.635583

Diff #1 for device. details. com.apple.disk_usage.factory. CalendarUsage.

LHS	RHS
5001216	4960256

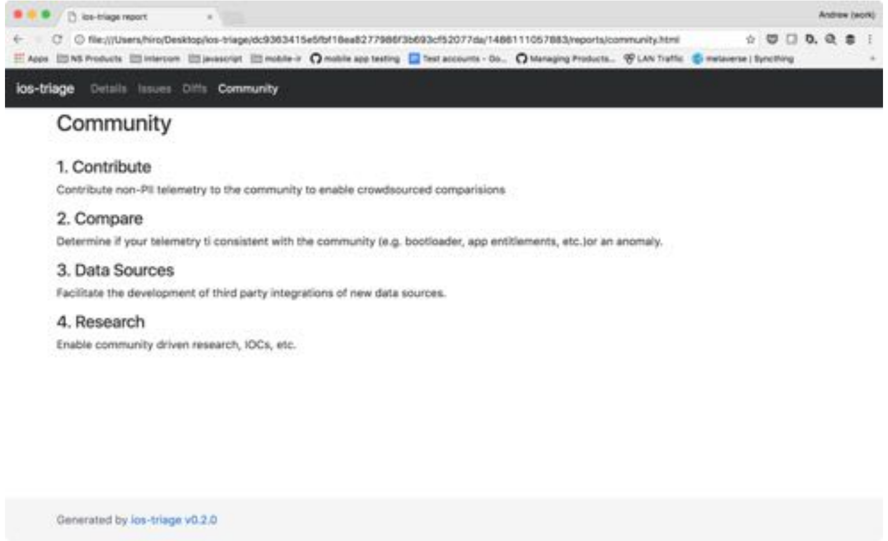
Diff #2 for device. details. com.apple.disk_usage.factory. NANDInfo. data. 24.

LHS	RHS
47	202

- Display `diff` in the output from two separate reports
- Ability to track changes to a device over time

NowSecure™

LIVE DEMO - COMMUNITY



Community

1. Contribute

Contribute non-PII telemetry to the community to enable crowdsourced comparisions

2. Compare

Determine if your telemetry ti consistent with the community (e.g. bootloader, app entitlements, etc.)or an anomaly.

3. Data Sources

Facilitate the development of third party integrations of new data sources.

4. Research

Enable community driven research, IOCs, etc.

Generated by ios-triage v0.2.0

- Contribute non-PII telemetry
- Detect anomalies
- Add new third-party data sources
- Enable community-driven research (e.g. IOCs, TTP, etc.)

DIFFS BETWEEN iOS 8.x & 10.x+

- iOS 8 showed deleted apps, useful to detect if a forensics app was:
  - Installed
  - Then removed after exfiltration
- Inability to download the actual apps installed on the device
  - Allowing attackers to hide
  - Hinder the ability to determine IOCs, TTPs, etc

FUTURE WORK

- Allow sharing of non-identifying data to create crowd-sourced database
- Move to a database backend
- Download iOS apps via iTunes & perform static analysis
- Integrate several third-party data sources
- Release android-triage

HOW YOU CAN CONTRIBUTE

- Run the tool
- Contact me with feedback, bugs, suggestions
  - Twitter: @ahoog42
  - GitHub: https://github.com/ahoog42
  - Email: ahoog@nowsecure.com
- Participate in crowd-sourced efforts
- Pitch in on future development work

Summary & Next Steps

KEY TAKEAWAYS

1. The platforms build security out rather than in (i.e., attackers can penetrate the “walled garden,” but defenders/responders can’t see what’s going on because we play by the rules)

2. As a result, following the trajectory of traditional computer security is impossible unless the industry changes or we summon the power to make it change

3. We need to diminish attackers’ asymmetric advantage, but without more sharing of more data, we have ephemeral data we can’t compare to anything

NowSecure™

Contact Info

- Project homepage: https://github.com/ahoog42/ios-triage

Contact info

- Twitter: @ahoog42
- Email: ahoog42@gmail.com
- NowSecure email: ahoog@nowsecure.com