BYOD DESTRUCTION

Steve Anson

Director, Forward Defense

www.forwarddefense.com

BYOD Pros and Cons

PROS

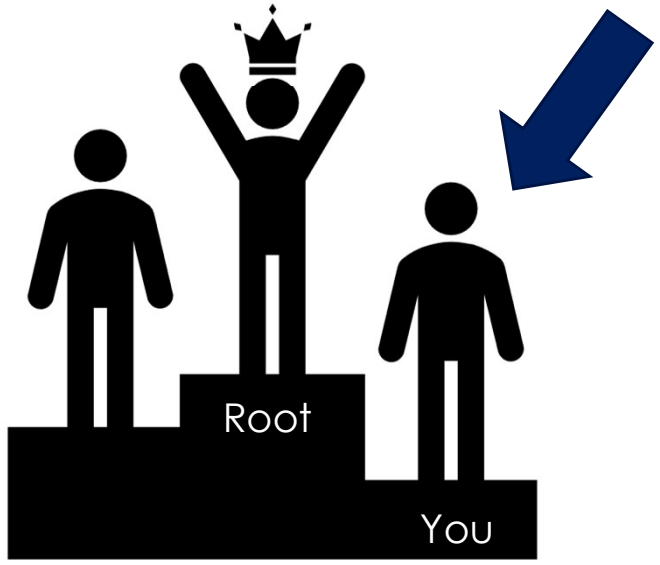
- Financial
- Convenience
- Employee Satisfaction
- Productivity

CONS

- Lost devices
- Controlling Remote Access
- Security Vulnerabilities
- Risk

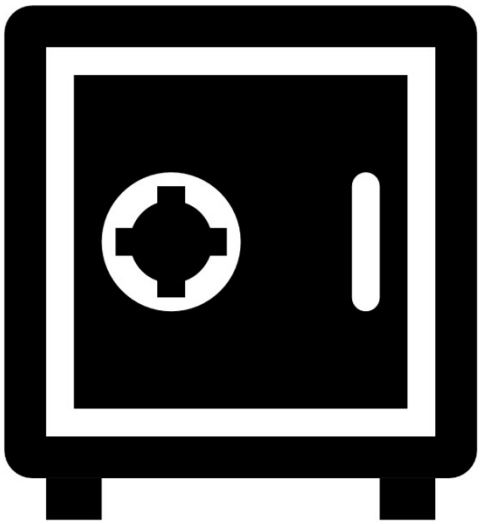
Mobile Devices are Not Like Computers

- You are not root



Mobile Devices are Not Like Computers

- Secure Boot Loader
- System Area
- Data Area

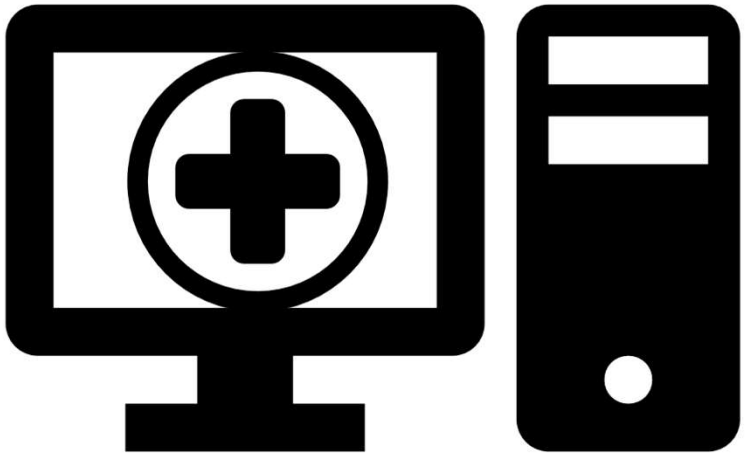


Mobile Devices are Not Like Computers

- App sandboxing
- App permissions
- File permissions

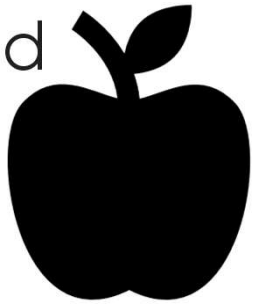
Patch Management for Computers

- OS vendor pushes out patches
- Software vendors push out patches
- We test and deploy the patch



Apple iOS Patches

- Unified ecosystem
- Patches pushed out by Apple
- User controls installation unless centrally managed
- Still subject to problems



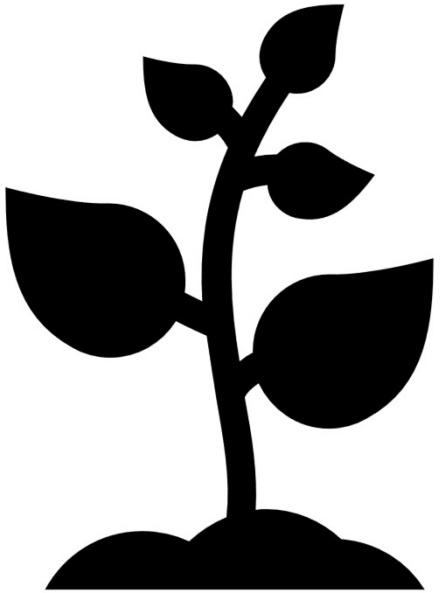
https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

Android Vulnerabilities

- Dirty COW (Copy on Write)
  - Impacted devices allow modification in memory of readable files
- Stagefright
  - Allowed malicious MMS to execute code without user interaction

Android Patches

- Fractured ecosystem



Android Patches

- Patches go from Google -> Manufacturer -> Carrier and are glacially slow
- Vulnerabilities therefore persist for ages

App Security

- Mobile App security sucks
- 2016 NowSecure Mobile Security Report
  - 25% of apps tested had serious vulnerabilities
  - More popular apps are more likely to have flaws
  - Newer versions are frequently more vulnerable than old versions due to introduction of new features

Malicious Apps

- And some apps are just evil on purpose…
- "McAfee Labs detected over 16 million mobile malware infestations in the third quarter of 2017 alone, nearly doubling the number we saw a year earlier."
  - -McAfee Mobile Threat Report Q1, 2018

Forensics/IR Challenges Different than with Computers

- Difficult to go direct to the media
  - Computers we can pull hard drive and image, bypassing logon
  - With mobile devices, secure boot loaders, signing certificates, NAND storage, and encryption make that tougher
- Lack of ability to access app data
- Lack of ability to access system partition

Forensics/IR Challenges Different than with Computers

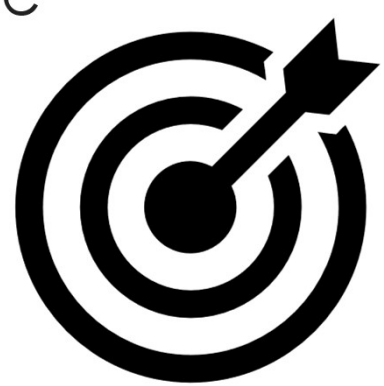
- Difficult to parse data from the vast number of proprietary mobile apps
- Cellebrite, XRY, Axiom
- Santoku
- iTunes backup

BYOD Challenges

- Lack of consistency in devices
  - Android, iOS, those other guys
  - Android ecosystem challenges
- Lack of control
  - Legal issues if hacked
  - Legal issues if wiped
  - Inability to control other uses

Mobile Device Management / Enterprise Mobility Management

- Centralize access points and enforce compliance to policy
- May containerize business data on device
- Allow remote control of device
- Provide VPN on a per app basis
- Remote wipe



Mobile Device Management / Enterprise Mobility Management

- Even the best aren't perfect
  - Vincent Tan released an examination of a leading Enterprise Mobile Security solution in which he was able to defeat most of its security controls at Black Hat 2016
  - Similar evisceration of Samsung Knox in 2016 as well

- https://www.blackhat.com/us-16/briefings.html#bad-for-enterprise-attacking-byod-enterprise-mobile-security-solutions

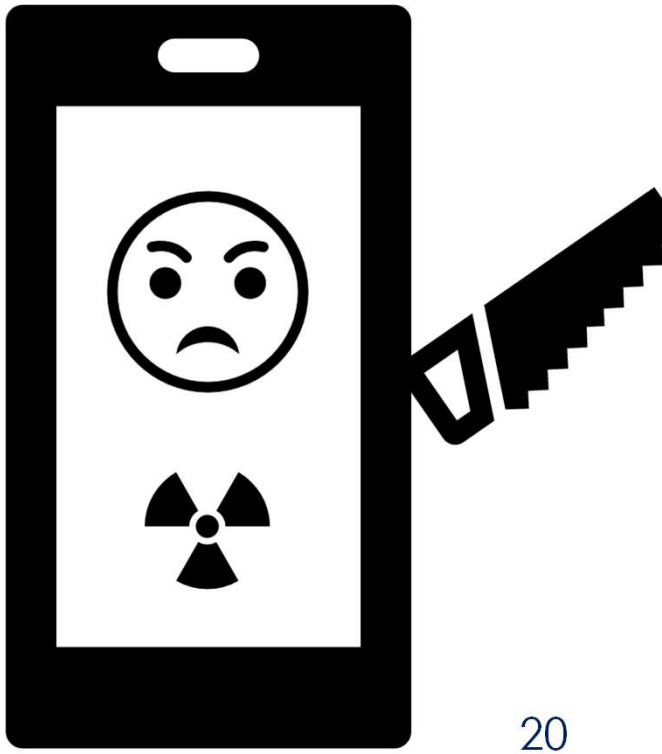
BYOD is Not Secure

- From a security standpoint, BYOD is a really stupid idea
- But not everything is about security
- Increased productivity, employee morale, support mobile workers

So…how do we cope?

Recommendations

- Consider all BYOD devices evil
- Don't trust, and still verify
- Implement defense and detection in depth

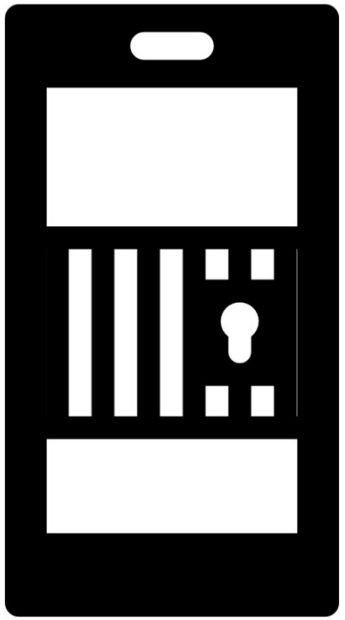


Recommendations

- You are knowingly allowing evil to hang out
- No one security solution is sufficient

Recommendations

- 1.Use MDM/EMM
- 2. Restrict BYOD devices to an isolated network segment
- 3. Treat the segment as hostile

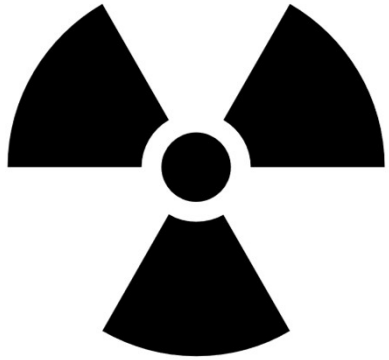


Use MDM/EMM

- Evaluate multiple vendors
- Choose best for your needs
- “Secure” containers are an extra layer of defense
- Enforce as much security on devices as you can
- Centralize authentication and entry points
- Feed logs into your SIEM

Use an Isolated Segment

- Separate (or guest) WLAN
- Wired networks
  - 802.1x for Network Access Control
  - Assign to separate VLAN
- VPN should also drop to a separate VLAN
- Ideally, routes only to the Internet

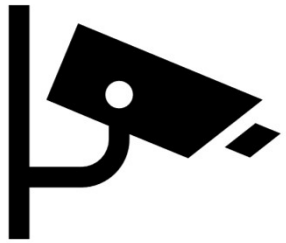


Treat as Hostile

- Establish security monitoring on that segment
- Threat hunt on that segment
- OSSIM and Security Onion are great, free options
- Combine various open source tools into integrated network security monitoring and SIEM solutions

Treat as Hostile

- Use threat intelligence feeds like OTX
- IDS signatures (Snort/Suricata)
- Run anomalies to ground (Bro, pcap)
- Increase monitoring on network intersections
- Application-aware firewalls with IPS and anti-malware to detect and block offenders



@ForwardDefense

@ForwardDefense