RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Touchlogging on iOS and Android

SESSION ID: MBS-W01

Neal Hindocha
Senior Security Consultant
Trustwave Spiderlabs

Nathan McCauley
Security Engineering Manager
Square

How it all began...

- Analyzed financial malware on Windows.
- What made it so powerful?
- Can the same be done on mobile?

Demo

Capturing TouchEvents on iOS

Overview

- Goal: To get X and Y coordinates from touch events on mobile devices (iOS and Android)
  - Bonus: Capture screenshots

- Current situation
  - Attack vectors
  - Defenses

The Value of Pictures

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Capturing TouchEvents on iOS

Capturing Touch Events on iOS

- Jailbreak
- Method swizzling
- Capture screenshots
- Send to remote server

iOS Mitigations

- Jailbreak detection
  - Not always appropriate or helpful
- Check for method swizzling
- Check for screen mirroring

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

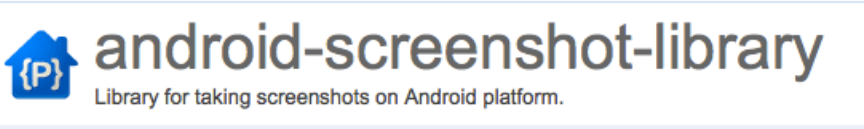
Capturing TouchEvents on Android

Rooted Android Devices

Getevent

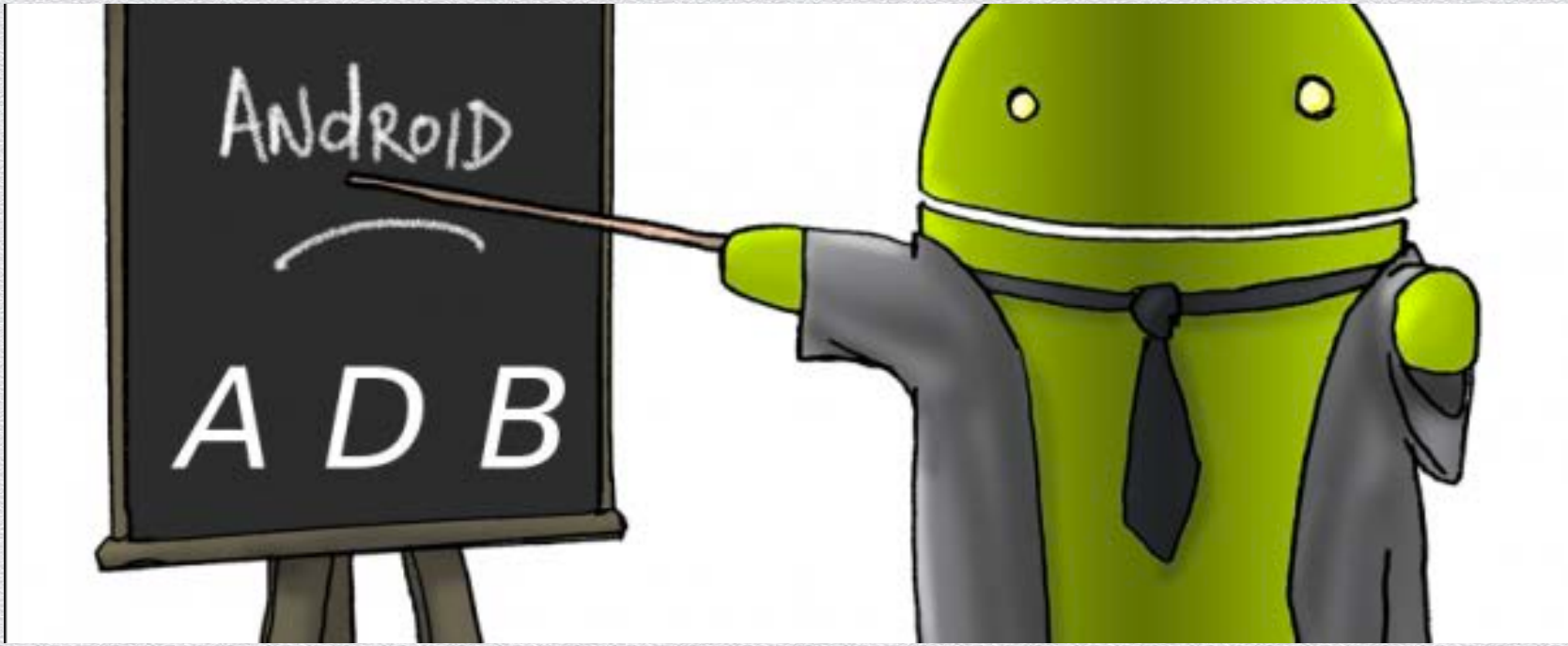
```
getevent
add device 1: /dev/input/event9
  name:     "compass"
add device 2: /dev/input/event8
  name:     "curcial-oj"
add device 3: /dev/input/event7
  name:     "lightsensor-level"
add device 4: /dev/input/event6
  name:     "buzz-nav"
add device 5: /dev/input/event5
  name:     "buzz-keypad"
add device 6: /dev/input/event4
  name:     "proximity"
add device 7: /dev/input/event3
  name:     "synaptics-rmi-touchscreen"
add device 8: /dev/input/event2
  name:     "projector-Keypad"
add device 9: /dev/input/event1
  name:     "projector_input"
add device 10: /dev/input/event0
  name:     "h2w headset"
```

+



Square | Trustwave SpiderLabs

Non-Rooted Android Devices



Demo

Capturing TouchEvents on Android

Non-Rooted Android Devices

- Live wallpaper
  - No permissions required
  - Only works on home-screen and in widgets

Demo

Capturing TouchEvents on Android with a Live Wallpaper

Non-Rooted Android Devices

- Overlay
  - Entire screen
    - Captures touch events everywhere
      - Cannot forward events
  - Part of screen
    - Need to know the running app
      - May interfere with the running app (30px)

Android Mitigations

- Ensure USB debugging disabled
- Check for installed apps' permissions
  - Whitelist or blacklist apps
  - Look for permission SYSTEM_ALERT_WINDOW
- Utilize your install base, where appropriate

Current Risks

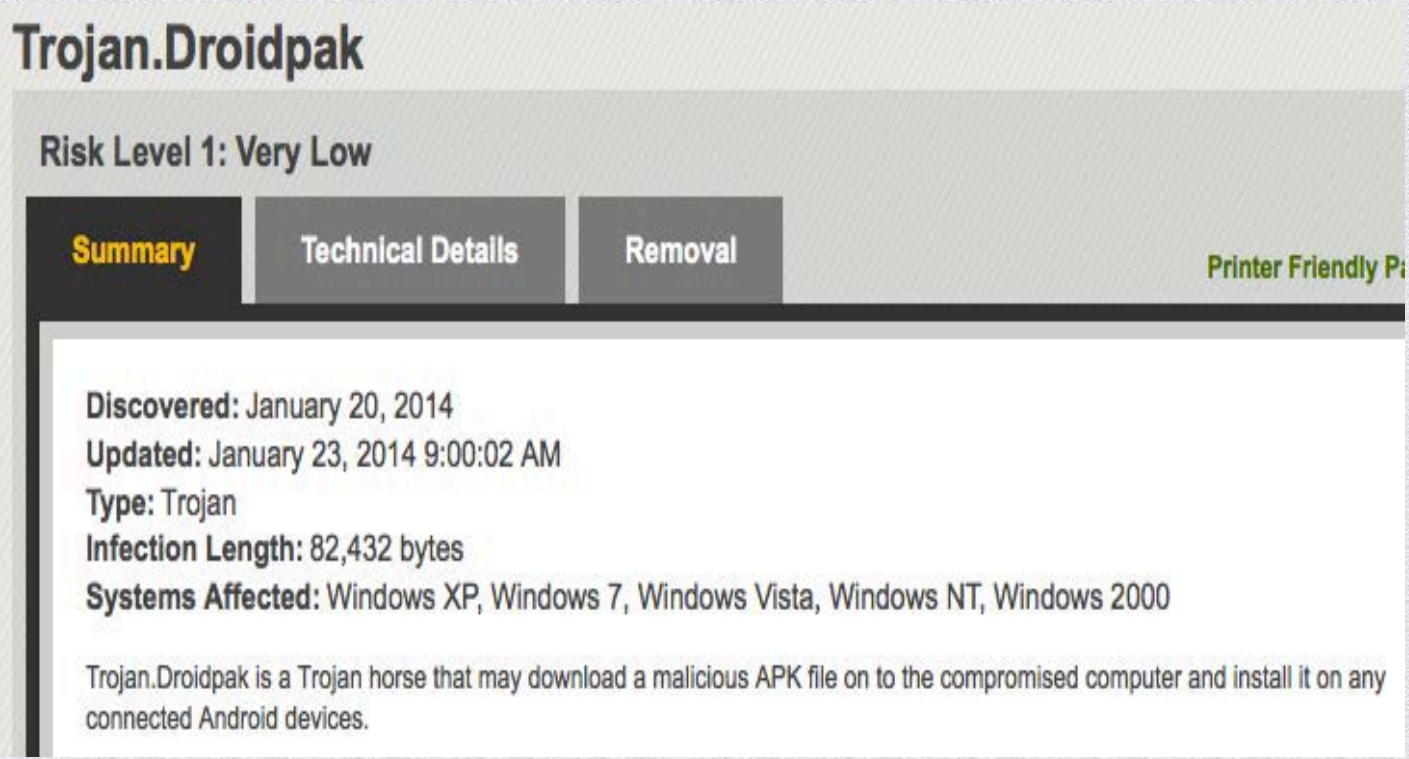
Risk

- Targeted attack
- Devices “on-display”
- Devices accessible to the public
- Malware

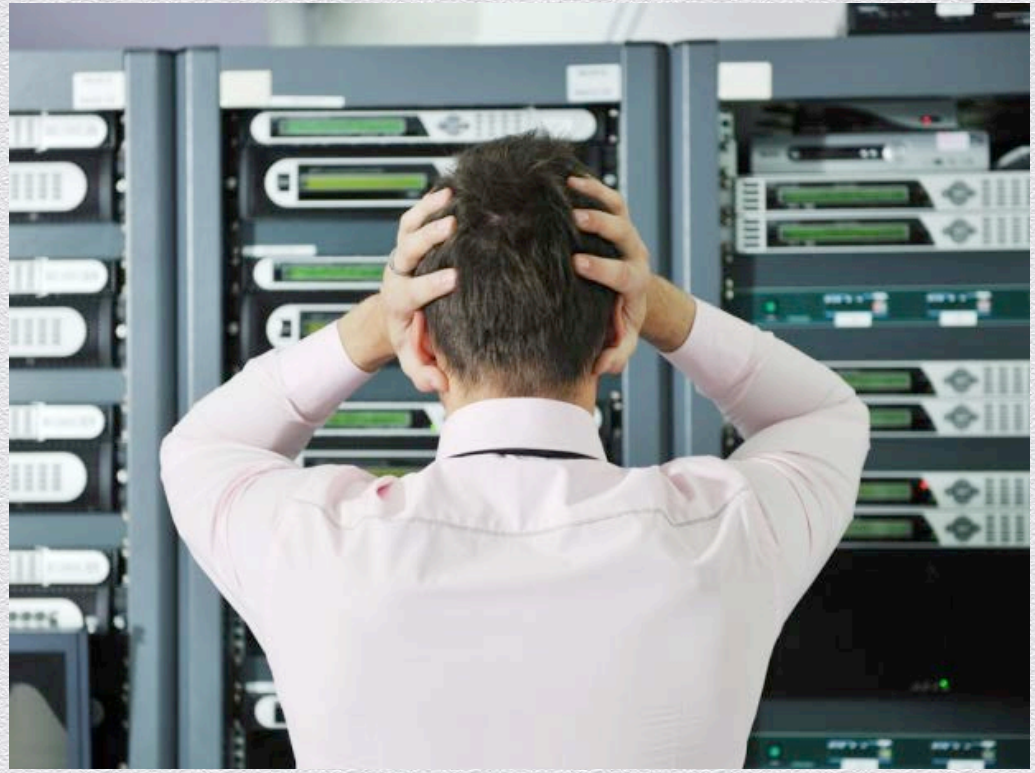
Malware

- Cloud and mobile
  - Information, not OS, is important
- Attackers
  - Financial gain
  - They adapt to new security measures

Malware


Trojan.Droidpak
Risk Level 1: Very Low
Summary
Technical Details
Removal
Printer Friendly Pa
Discovered: January 20, 2014
Updated: January 23, 2014 9:00:02 AM
Type: Trojan
Infection Length: 82,432 bytes
Systems Affected: Windows XP, Windows 7, Windows Vista, Windows NT, Windows 2000
Trojan.Droidpak is a Trojan horse that may download a malicious APK file on to the compromised computer and install it on any connected Android devices.

Vulnerabilities



Mitigations

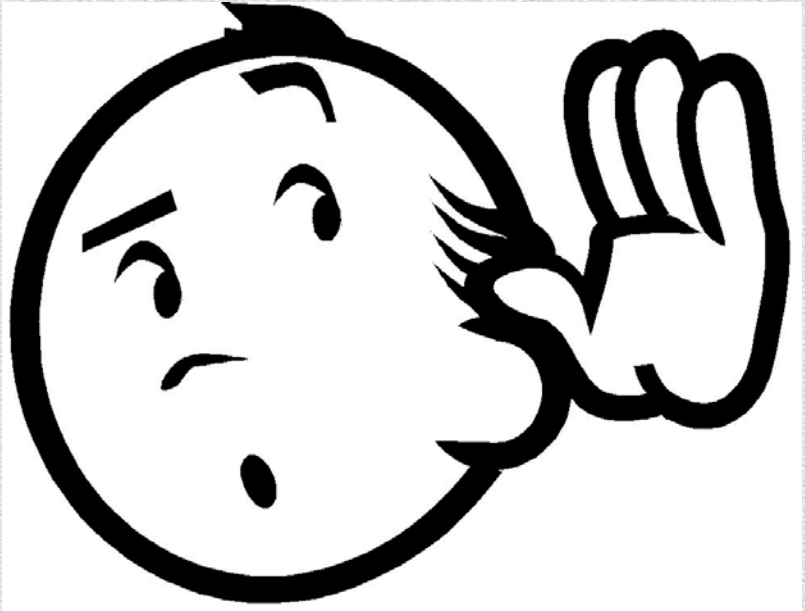
Mitigation Guidelines

- Follow development best practices
- Do not run on jailbroken / rooted devices
  - Not always possible
- On Android disable USB debugging
- Utilize your install base

Other

Other ways of capturing events

- Hacked Keyboard
- Sensors
- Microphone



Conclusion

- Touch Events can be captured on jailbroken iOS, rooted and non-rooted Android.
- Logging coordinates requires very little diskspace / bandwidth, and has virtually no performance impact
- Coordinates reveal a lot even without screenshots, and with screenshots, they reveal everything
- Difficult, but not impossible, to protect against

Thank You!

Neal Hindocha
Senior Security Consultant
nhindocha@trustwave.com

Nathan McCauley
Security Engineering Manager
mccauley@squareup.com