Mobile Application Security

March 18, 2015

SECURITY
REIMAGINED

Agenda

How Threat Actors Exploit Apps

Malware

Adware

Vulnerable Apps

Undesired Behavior

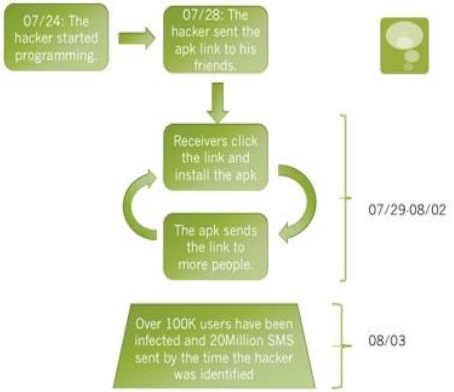
FireEye

FireEye Mobile Threat Assessment Report

- **A Comprehensive Mobile Threat Assessment of 7 Million iOS and Android Apps:**
  - Both Android and Apple mobile device users are under attack
  - More than 5 billion downloaded Android apps are vulnerable to remote atta
  - Aggressive ad libraries can leak personal data over the network
  - Popular apps were exposed to a common vulnerability
  - There has been a dramatic rise in attempts to steal financial data (500% increase)
  - Attackers are using a new delivery channel for iOS malware that bypasses the Apple App Store review process
    - Over 1,400 iOS apps publicly available on the Internet with variants of security issues
  - FireEye's analysis indicates that mobile devices pose threats on many fronts

- https://www2.fireeye.com/WEB2015RPTMobileThreatAssessment.html

Case Study: XXShenqi SMS Attack



- Aug 3rd, 2014 – Largest SMS phishing attack in China
- 100,000+ users infected, 20+ million SMS sent
- On average, each user was charged RMB30/USD5
- User receives SMS with a malicious URL; clicking the link causes the malicious app to be side-loaded
- Send malicious URL to victim's contact list
- App calls WelcomeActivity class to evade signature-based anti-virus solutions
- Details harvested: username, password, citizen ID number, real name

Source: https://www.fireeye.com/blog/threat-research/2014/08/the-history-of-xxshenqi-and-the-future-of-sms-phishing.html

Case Study: Mobile Banking Trojan

Android.KorBanker

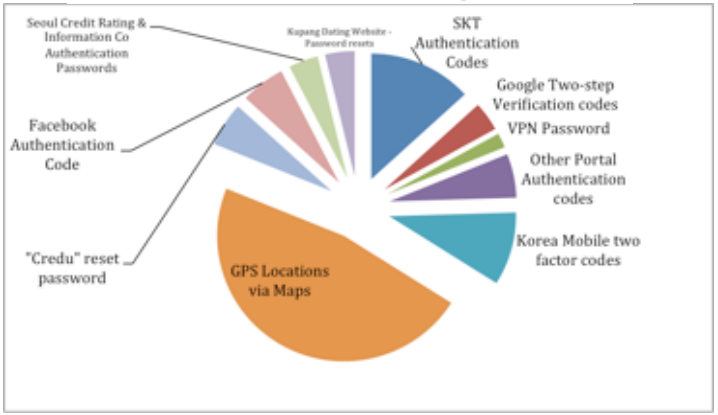
Easy as 1-2-3

- Uninstall original banking app from mobile device
- Install fake banking app
- Harvest banking credentials

Target Banks

- Hana Bank
- IBK One
- KB Kookmin Bank
- NH Bank
- Woori Bank
- Shinhan Bank

'KorBanker' steals SMS messages, takes authentication codes in the process

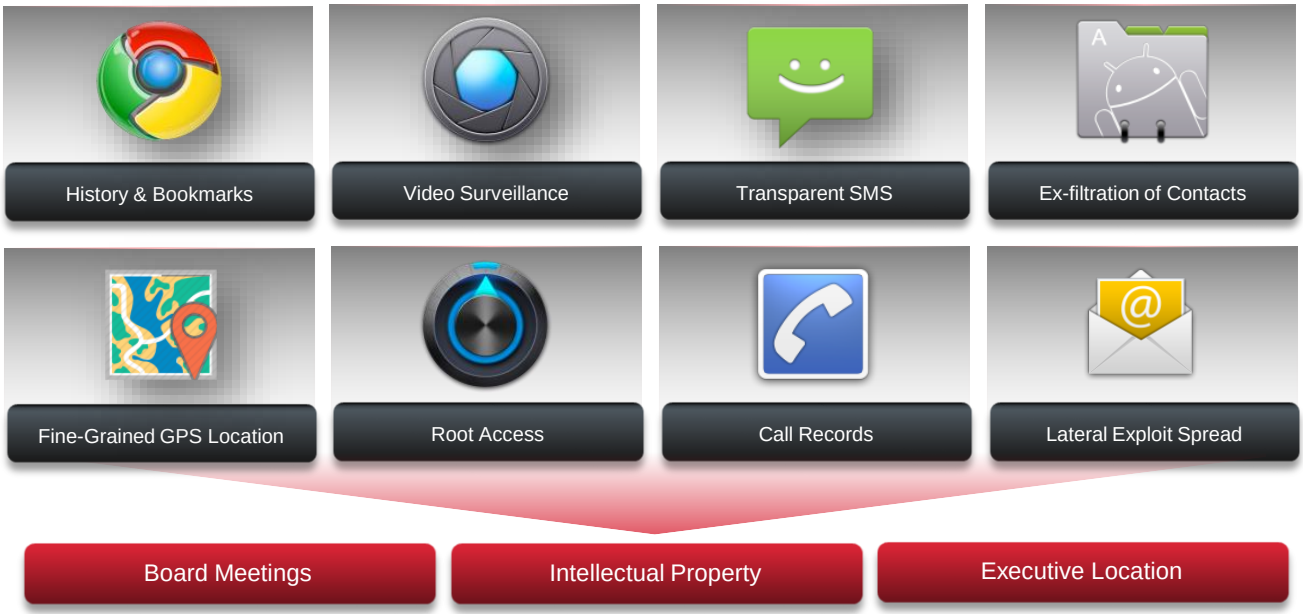


Text messages containing VPN passwords and authentication codes for Google and Facebook are found on a command-and-control server for Android malware

iOS Attacks

- iOS malware is still rare due to the strict review process of Apple's app store
- Threats against non-jailbroken devices are more targeted and sophisticated, but they are not impossible to create
- iOS malware can perform many of the same types of attacks as Android malware including data exfiltration and surveillance
- The 2014 Masque attack which allowed for malicious apps to replace existing legitimate ones had huge security impacts
- Mobile-device management (MDM) technology cannot distinguish the malware-laden app from the original app

Tip of the Iceberg



Uncovering the Mobile Threat

1. Does the app violate security policies?

2. What kind of behaviour does the app exhibit?

3. Is the app malicious?

FireEye

Mobile Application Security

Managed Services – Enterprise
Managed mobile threat prevention for Enterprise customers, with MDM integration and customized policy enforcement.

Managed Services – BYOD/SME
Managed mobile threat prevention for BYOD/SME customers, with automated policy enforcement.

Mobile Threat Intelligence
Leverage technology to capture mobile threat intelligence from service provider infrastructure, generate leads and publish regional security reports.

Mobile App Analysis
Mobile application security auditing and analysis.

Secure App Store
Identify and separate high-risk apps from Enterprise distribution.

Thank You

SECURITY
REIMAGINED