Top Threats to Mobile Computing

cloud security alliance℠

Document Sponsor: Ping Identity®

Contributors

Lead

Dan Hubbard, Open DNS

Co-chairs

Cesare Garlati, Trend Micro

Freddy Kasprzykowski, Microsoft

David Lingenfelter, Fiberlink

Other Contributors

Jon-Michael Brook, Symantec

Alice Decker, Trend Micro

Eric Fisher, FishNet Security

Allen Lum, Control Solutions

Steven Michalove, Microsoft

Guido Sanchidrian, Symantec

Sam Wilke

CSA Global Staff

Aaron Alva, Research Intern

Luciano JR Santos, Research Director

Kendall Scoboria, Graphic Designer

Evan Scoboria, Webmaster

John Yeoh, Research Analyst

Overview // About CSA

The Cloud Security Alliance (CSA) is a non-profit organization comprised of security industry practitioners, corporations and associations with a mission to promote security best practices within cloud computing.

CSA's Top Threats working group is dedicated to tracking and reporting on top threats in cloud computing. The group's research has identified a high number of cases regarding the use and integration of mobile devices in the cloud. As a result, CSA determined it was important to create a "Top Threats to Mobility" report designed to complement the original "Top Threats to the Cloud" document.

The creation of this report was assigned to the newly formed CSA Mobile working group, which is responsible for providing fundamental research to help secure mobile endpoint computing from a cloud-centric vantage point.

Overview // Survey Methodology

- The Top Threats to Mobile Computing survey was released in July 2012. Survey results are from 210 CSA members from 26 countries globally.
- Respondents are approximately 80% "experts in the field of information security," which includes security admins, consultants and cloud architects. Twenty percent of respondents hold these roles at cloud service providers.
- The survey asked users to rank top threats in order of both their concern and likelihood of a threat occurring this year, next year, or not likely to happen.
- This Top Threats to Mobile Computing presentation was peer reviewed in June-July 2012.

Overview // Survey Focus

- For this first version, CSA restricted the framework to devices (smartphones and tablets), that connect to the Internet primarily through cellular access networks such as 3G and 4G. CSA made a conscious decision to **not** include laptops with cellular access, Chromebooks, and other similar devices. This may change in future versions of the report.
- This presentation is intended to guide information security professionals in educating others about security concerns in mobile computing.

Evil 8 // Top Threats to Mobile

1. Data loss from lost, stolen or decommissioned devices.
2. Information-stealing mobile malware.
3. Data loss and data leakage through poorly written third-party apps.
4. Vulnerabilities within devices, OS, design and third-party applications.
5. Unsecured WiFi, network access and rogue access points.
6. Unsecured or rogue marketplaces.
7. Insufficient management tools, capabilities and access to APIs (includes personas).
8. NFC and proximity-based hacking.

Survey // Raw Results

	1	2	3	4	5	6	7	8	Rating Average	Response Count
Data loss from lost, stolen, or decommissioned devices	**33.9% (59)**	12.6% (22)	12.1% (21)	9.2% (16)	10.9% (19)	5.2% (9)	7.5% (13)	8.6% (15)	3.39	174
Unsecure or rogue marketplaces	8.6% (15)	12.1% (21)	13.2% (23)	9.2% (16)	15.5% (27)	14.9% (26)	**17.8% (31)**	8.6% (15)	4.70	174
Information-stealing mobile malware	**17.9% (31)**	15.0% (26)	13.3% (23)	12.1% (21)	16.2% (28)	12.7% (22)	7.5% (13)	5.2% (9)	3.88	173
Unsecured WiFi, network access, and rogues access points	8.0% (14)	15.5% (27)	**16.7% (29)**	14.4% (25)	10.9% (19)	13.8% (24)	14.9% (26)	5.7% (10)	4.34	174
Insufficient management tools, capabilities, and access to API's (includes personas)	4.0% (7)	9.8% (17)	10.3% (18)	11.5% (20)	17.2% (30)	13.2% (23)	**21.8% (38)**	12.1% (21)	5.16	174
Data loss / data leakage through poorly written 3^{rd}-party apps	9.2% (16)	**19.0% (33)**	17.8% (31)	16.7% (29)	10.3% (18)	13.2% (23)	8.0% (14)	5.7% (10)	4.01	174
NFC and proximity-based hacking	3.4% (6)	4.6% (8)	2.9% (5)	8.0% (14)	5.2% (9)	15.5% (27)	15.5% (27)	**44.8% (78)**	6.40	174
Vulnerabilities within devices, OS, design, 3^{rd}-party apps	14.9% (26)	11.5% (20)	13.8% (24)	**19.0% (33)**	13.8% (24)	11.5% (20)	6.9% (12)	8.6% (15)	4.10	174
									Answered Question	174
									Skipped Question	40

THREAT 1 // Data loss from lost, stolen, or decommissioned devices

Overview of Threat

By their nature, mobile devices are with us everywhere we go. The information accessed through the device means that theft or loss of a mobile device has immediate consequences. Additionally, weak password access, no passwords, and little or no encryption can lead to data leakage on the devices. Users may also sell or discard devices without understanding the risk to their data.

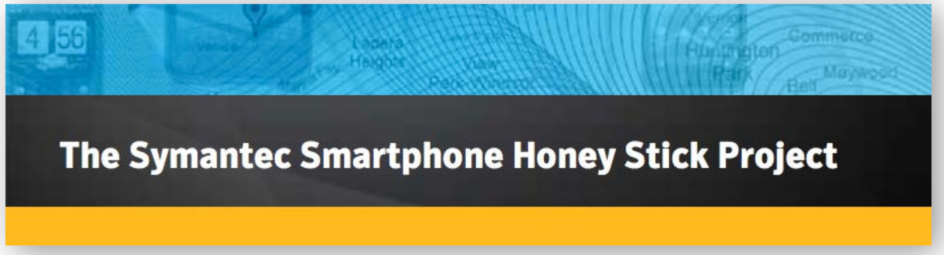
Threat Level: High

The current threat happens frequently, as it is a top concern across executives and IT admins.

THREAT 1 // Example

Threat Example

Data loss from lost, stolen, or decommissioned devices is a high frequency concern with both company and employee-owned mobile devices. Additionally, vendors like Apple have fallen victim to lost or stolen prototypes of yet-to-be-released devices.



http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=symantec-smartphone-honey-stick-project

Symantec Smartphone Honey Stick Project

Symantec released 50 “lost” smartphones, each harboring a collection of simulated personal and corporate information. The results were astonishing:

- 83% had attempts to access business apps
- 89% had attempts to access personal apps
- 96% had attempts to access at least some type of data

http://www.streetwise-security-zone.com/members/streetwise/adminpages/honeystickproject

- 50% of finders contacted the owner and offered to help return the phone
- The most popular apps accessed were:
    - Contacts
    - Private Pictures
    - Social Networking
    - Webmail
    - Passwords

THREAT 2 // Information-Stealing Malware

Overview of Threat

Android devices, in particular, offer many options for application downloads and installations. Unlike iOS devices, which need to be jailbroken, Android users can easily opt to download and install apps from third-party marketplaces other than Google's official "Play Store" marketplace. To date, the majority of malicious code distributed for Android has been disseminated through third-party app stores, predominantly in Asia. Most of the malware distributed through third-party stores has been designed to steal data from the host device.

Threat Level: High

Android malware in particular is becoming a more popular attack surface for criminals who traditionally have used PCs as their platforms. Kaspersky Labs found that malware targeting Android users nearly tripled in the 2nd quarter of 2012 from the 1st quarter (14,923 malicious programs in Q2, up from 5,441 in Q1).[1]

[1] http://www.securelist.com/en/analysis/204792239/IT_Threat_Evolution_Q2_2012#3

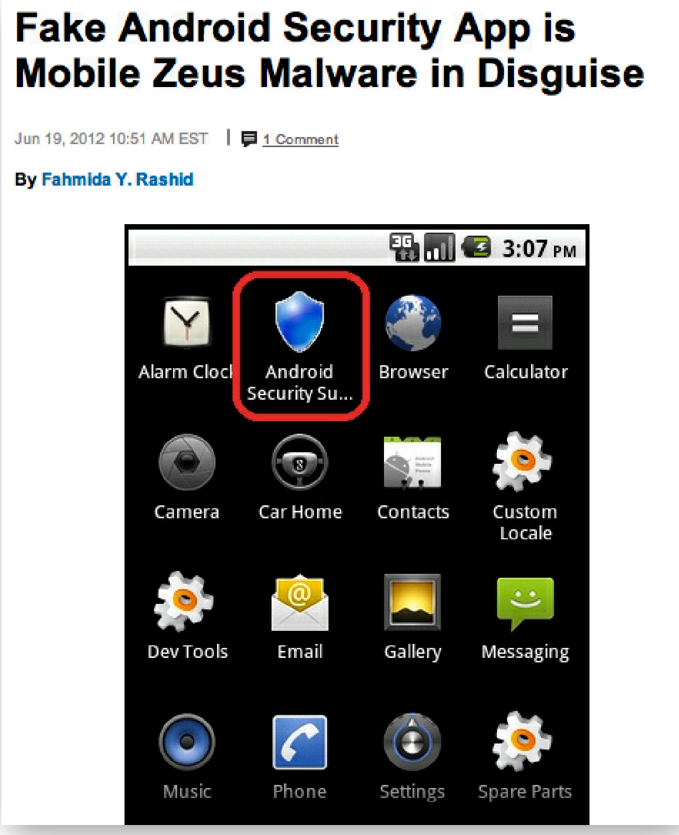
THREAT 2 // Example

Threat Example

One of the most prevalent pieces of malicious code for Android is called “Zitmo.” This is a mobile version of the Zeus malware, which is designed to steal information from the device by defeating the SMS-based banking two-factor authorization.

Another example is the Nickspy Trojan, which began infecting mobile devices in 2011. This application disguises itself as a Google Plus app but contains the ability to record phone conversations to an audio file, which it uploads to a remote server managed by the app’s originators.

http://blog.fortinet.com/zitmo-hits-android/



Fake Android Security App is Mobile Zeus Malware in Disguise

Jun 19, 2012 10:51 AM EST | 1 Comment

By Fahmida Y. Rashid

http://securitywatch.pcmag.com/none/299291-fake-android-security-app-is-mobile-zeus-malware-in-disguise

THREAT 3 // Data Loss and Data Leaking through Poorly-Written Applications

Overview of Threat

Applications for smartphones and tablets have grown exponentially on iOS and Android. Although the main marketplaces have security checks, certain data collection processes are of questionable necessity; all too often, applications either ask for too much access to data or simply gather more data than they need or otherwise advertise.

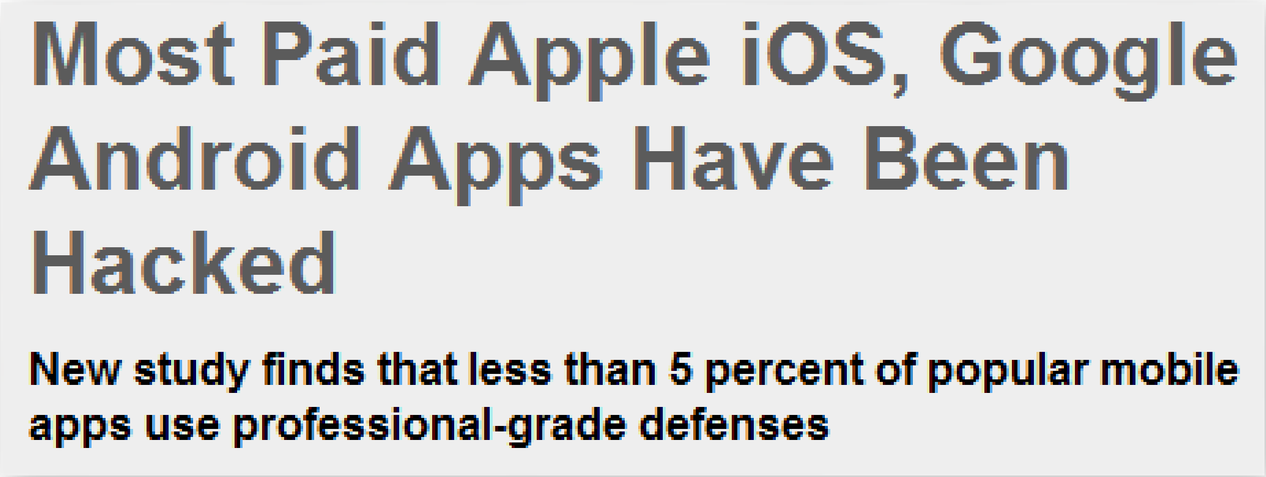
Threat Level: Medium

Although data loss and leaking through poorly-written applications happens across mobile operating systems, it is not exploited nearly as often as other threats in the Evil 8.

THREAT 3 // Example

Threat Example

3rd -Party Mobile Applications
A report published by Arxan, a private software security company, states that more then 90% of top paid mobile apps have been hacked.



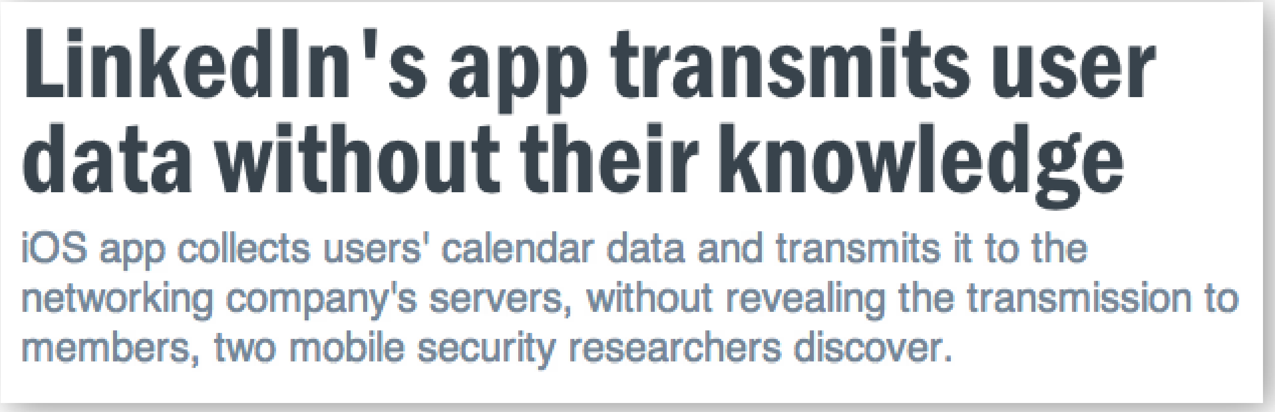
Most Paid Apple iOS, Google Android Apps Have Been Hacked

New study finds that less than 5 percent of popular mobile apps use professional-grade defenses

http://www.darkreading.com/mobile-security/167901113/security/application-security/240005962/most-paid-apple-ios-google-android-apps-have-been-hacked.html

LinkedIn
Recently LinkedIn got in some hot water over privileged access to calendar data within their iPad and iPhone apps.

Without user knowledge, LinkedIn’s application on iOS devices transmitted passwords, meeting notes, and other information from calendar entries.



LinkedIn's app transmits user data without their knowledge

iOS app collects users' calendar data and transmits it to the networking company's servers, without revealing the transmission to members, two mobile security researchers discover.

http://news.cnet.com/8301-1009_3-57447966-83/linkedins-app-transmits-user-data-without-their-knowledge/

THREAT 4 // Vulnerabilities in Hardware, OS, Applications and Third-Party Apps

Overview of Threat

Mobile hardware, OS, applications and third-party apps contain defects (vulnerabilities) and are susceptible to exfiltration and/or injection of data and/or malicious code (exploits). The unique ecosystem inherent in mobile devices provides a specialized array of security concerns to hardware, OS, and application developers, as mobile devices increasingly contain all of the functionalities attributed to desktop computing, with the addition of cellular communication abilities.

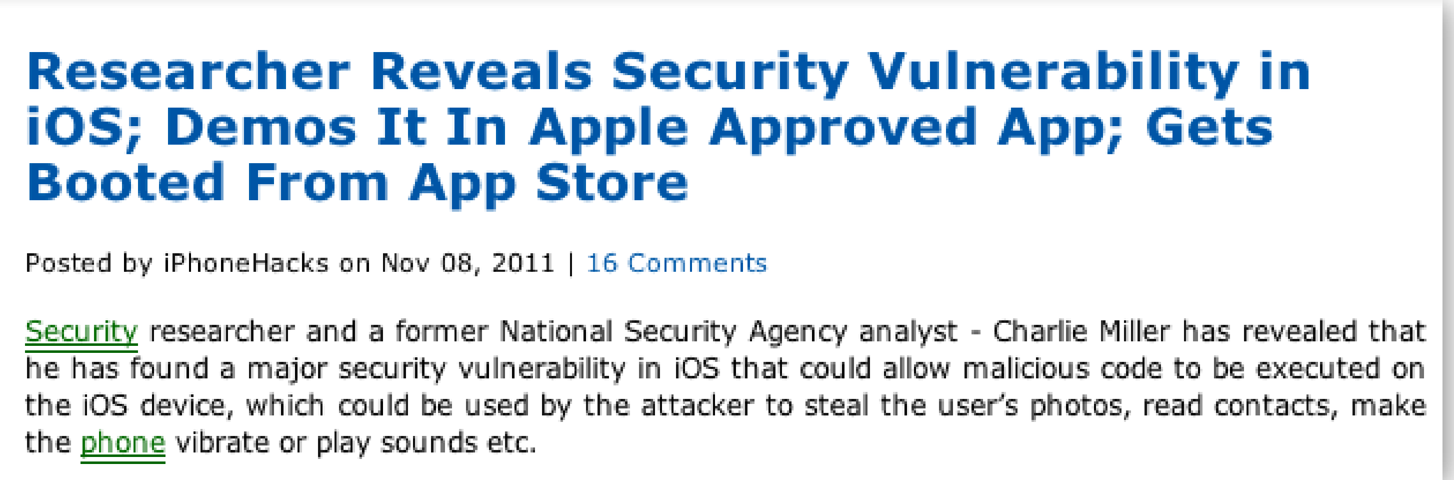
Threat Level: Medium

Although the threat is high, the number of exploits in the wild is not.

THREAT 4 // Example

Threat Example

Examples include: exponential growth in mobile malware, hardware that sends data back to manufacturer, and weak coding techniques that are easy to exploit by criminals (unsafe sensitive data storage/transmission, hardcoded password/keys, data leakage) in third-party apps and most likely in applications.

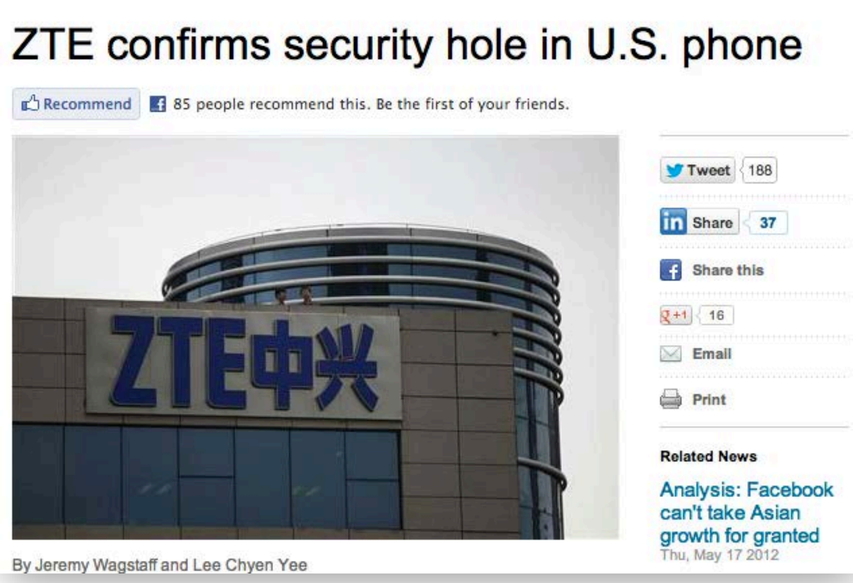


Researcher Reveals Security Vulnerability in iOS; Demos It In Apple Approved App; Gets Booted From App Store

Posted by iPhoneHacks on Nov 08, 2011 | 16 Comments

Security researcher and a former National Security Agency analyst - Charlie Miller has revealed that he has found a major security vulnerability in iOS that could allow malicious code to be executed on the iOS device, which could be used by the attacker to steal the user's photos, read contacts, make the phone vibrate or play sounds etc.

http://www.iphonehacks.com/2011/11/researcher-reveals-security-vulnerability-in-ios-demos-it-in-apple-approved-app-gets-booted-from-app-store.html



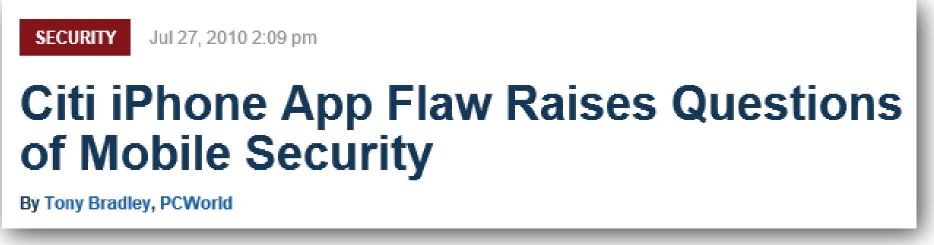
ZTE confirms security hole in U.S. phone

Related News

Analysis: Facebook can't take Asian growth for granted
Thu, May 17 2012

By Jeremy Wagstaff and Lee Chyen Yee

http://www.reuters.com/article/2012/05/18/us-zte-phone-idUSBRE84H08J20120518



SECURITY Jul 27, 2010 2:09 pm

Citi iPhone App Flaw Raises Questions of Mobile Security

By Tony Bradley, PCWorld

http://www.pcworld.com/businesscenter/article/201994/citi_iphone_app_flaw_raises_questions_of_mobile_security.html

Threat 5 // Unsecured WiFi / Network Access / Rogue Access Points

Overview of Threat

Unsecured WiFi has been around for years. However, as more users are mobile and data plans become more limited, users will increasingly use WiFi in public locations. The number of locations that provide WiFi, in particular free WiFi, has exploded over the last few years. This has increased the attack surface for users who connect to these networks. In the last year, there has been a proliferation of attacks on hotel networks, a skyrocketing number of open rogue access points installed, and the reporting of eavesdropping cases.

Threat Level: High

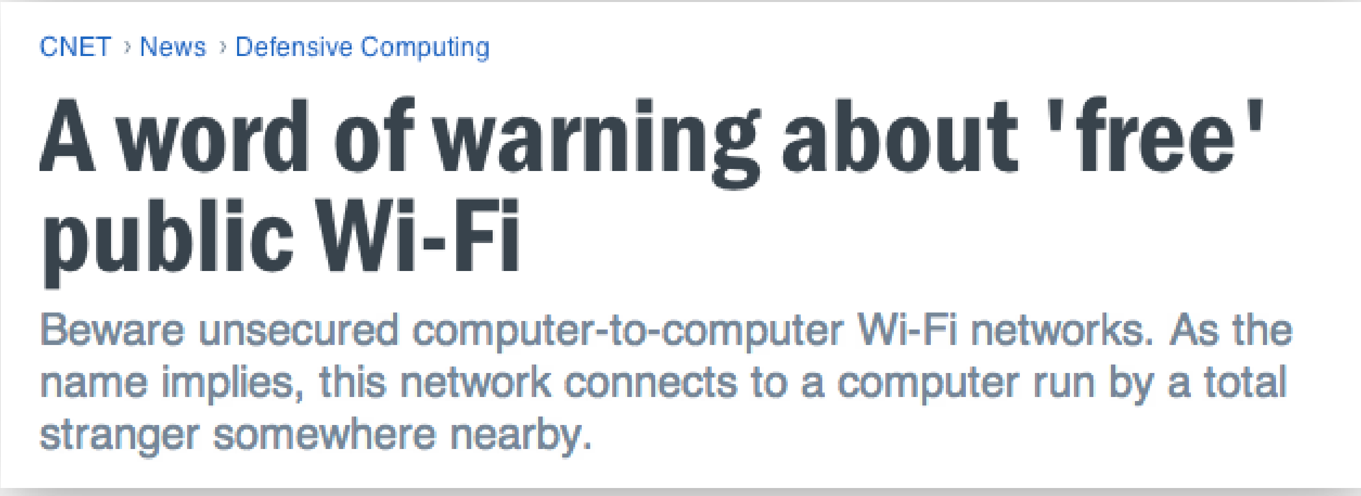
Increased access to public WiFi, along with increased use of mobile devices, creates a heightened opportunity for abuse of this connection. Firesheep is a perfect example of how one can gain access to data through public unsecured WiFi.

Threat 5 // Example

Threat Example

Firesheep

Faceniff is the Android version of the Firesheep Firefox extension that uses packet sniffing technology to intercept unencrypted cookies, thereby compromising a user's login credentials.



CNET › News › Defensive Computing

A word of warning about 'free' public Wi-Fi

Beware unsecured computer-to-computer Wi-Fi networks. As the name implies, this network connects to a computer run by a total stranger somewhere nearby.

http://news.cnet.com/8301-13554_3-9941355-33.html

Hotel & Airport Hacking

Unsecured wireless networks at hotels have proven to be ideal places for hackers to commit a wide variety of crimes. Fake WiFi access points are designed to look like real hotel WiFi networks. These malicious networks may contain the hotel's name or other deceptive descriptions.

Threat 6 // Unsecured or Rogue Marketplaces

Overview of Threat

Android devices, in particular, offer many options for application downloads and installations. Unlike iOS devices, which need to be jailbroken, Android users can easily opt to download and install apps from third-party marketplaces other than Google's official "Play Store" marketplace. To date, the majority of malicious code distributed for Android has been distributed through third-party app stores, predominantly in Asia. Most of the malware distributed through third-party stores has been designed to steal data from the host device.

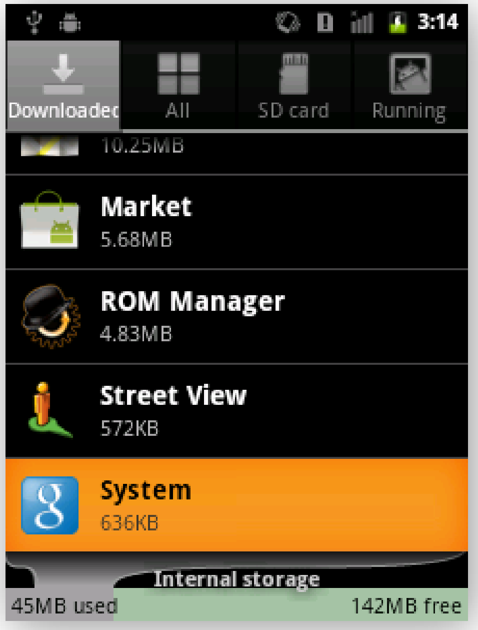
Threat Level: High

Android malware in particular is being distributed through these marketplaces more and more frequently.

Threat 6 // Example

Threat Example

TigerBot is a bot designed to gather confidential data from a mobile device and uses SMS to control the installed bot. This has been discovered on several marketplaces in Asia.



10.25MB

Market
5.68MB

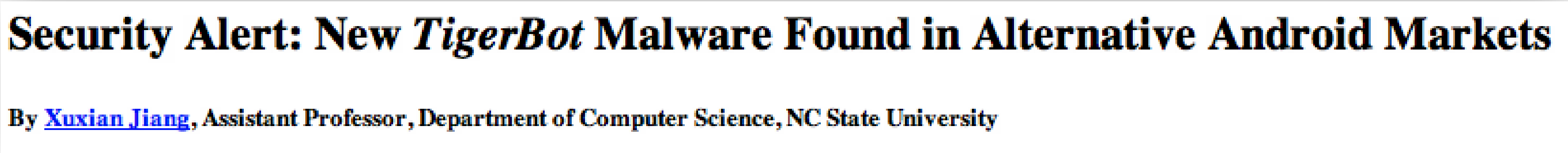
ROM Manager
4.83MB

Street View
572KB

System
636KB

Internal storage
45MB used
142MB free

http://www.csc.ncsu.edu/faculty/jiang/TigerBot/



Security Alert: New *TigerBot* Malware Found in Alternative Android Markets

By Xuxian Jiang, Assistant Professor, Department of Computer Science, NC State University

http://www.csc.ncsu.edu/faculty/jiang/TigerBot/

In the image to the left, the TigerBot malware hides from the user by masking itself as a popular icon, such as Google's search app, and a generic application name (ie. "System").

Threat 7 // Insufficient Access to APIs, Management Tools, and Multi-Personas

Overview of Threat

Granting users and developers access to a device's low-level functions is a double edged sword, as attackers, in theory, could also gain access to those functions. However, a lack of access to system-level functions to trusted developers could lead to insufficient security. Additionally, with most smartphone and tablet operating systems today, there is little, if any, guest access or user status. Thus, all usage is in the context of the admin, thereby providing excessive access in many instances.

Threat Level: Medium

The instances of this threat in the wild are not as frequent as several other threats in the Evil 8.0.

Threat 7 // Example

Threat Example

Lack of Access to APIs/OS Architecture

An anti-virus vendor may not have the ability to read programs in memory for real-time protection, leading to malicious code being run. Additionally, operating systems may limit access to core OS architecture, entirely leaving anti-virus vendors out of the equation, as is the case with Apples iOS.

Apple Explains Why iOS Don't Need No Steenkin' Anti-Virus

http://www.forbes.com/sites/timworstall/2012/06/04/apple-explains-why-ios-dont-need-no-steenkin-anti-virus/

User Error

Additionally, a user may simply leave the phone unlocked, which allows someone with access to read and modify all information on the phone, including configuration settings.

Threat 8 // NFC and Proximity-Based Hacking

Overview of Threat

Near field communication (NFC) allows mobile devices to communicate with other devices through short-range wireless technology. NFC technology has been used in payment transactions, social media, coupon delivery, and contact information sharing. Due to the information value being transmitted, this is likely to be a target of attackers in the future.

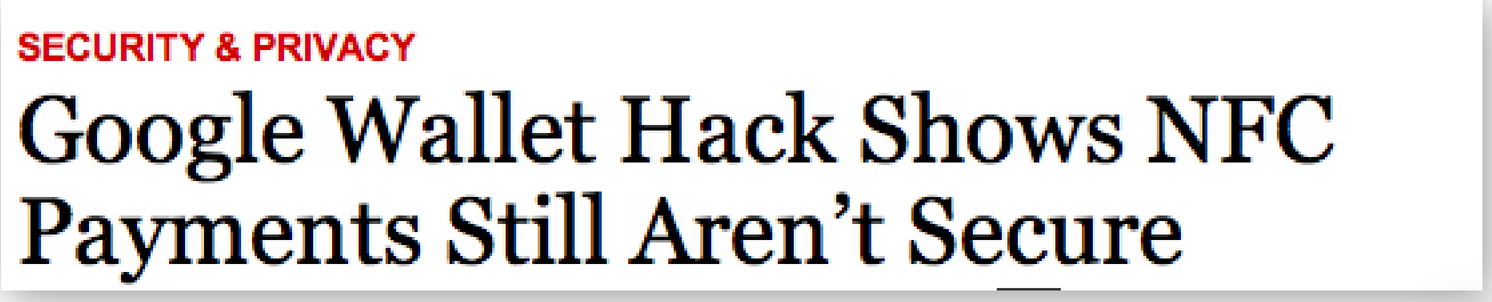
Threat Level: Low

This threat is still in proof-of-concept phase.

Threat 8 // Example

Threat Example

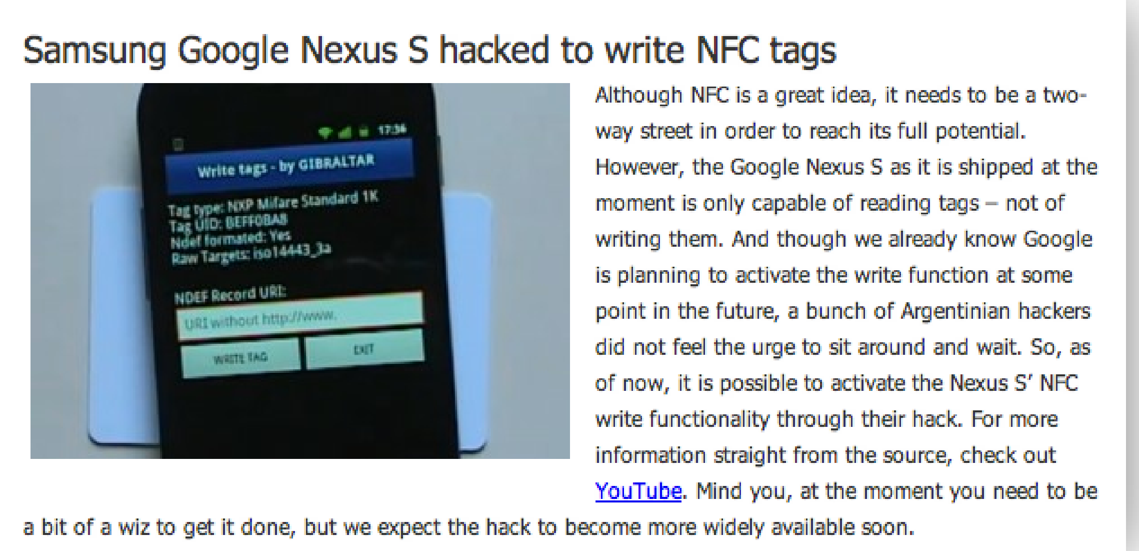
A drive-by payment occurs when, based on the user's physical location or proximity, an attacker can receive currency from the user's smart phone (AKA digital wallet).



SECURITY & PRIVACY

Google Wallet Hack Shows NFC Payments Still Aren't Secure

http://techland.time.com/2012/02/10/google-wallet-hack-shows-nfc-payments-still-arent-secure/



Samsung Google Nexus S hacked to write NFC tags

Although NFC is a great idea, it needs to be a two-way street in order to reach its full potential. However, the Google Nexus S as it is shipped at the moment is only capable of reading tags – not of writing them. And though we already know Google is planning to activate the write function at some point in the future, a bunch of Argentinian hackers did not feel the urge to sit around and wait. So, as of now, it is possible to activate the Nexus S' NFC write functionality through their hack. For more information straight from the source, check out YouTube. Mind you, at the moment you need to be a bit of a wiz to get it done, but we expect the hack to become more widely available soon.

http://www.samsungnexuss.com/samsung-google-nexus-s-hacked-to-write-nfc-tags/

Other Survey Results of Interest

64% of respondents believe that NFC and proximity-based hacking will happen in 2013.

81% of respondents believe that unsecured WiFi and rogue access points are already happening today. This is of particular concern, as the proliferation of mobile devices consequently increases our use of and reliance on WiFi networks.

THANK YOU!

For more information,
please visit
www.cloudsecurityalliance.org

Email
mobile_tt@cloudsecurityalliance.org