Colorado Information Analysis Center

INTELLIGENCE BULLETIN

## (U) Security Risks Associated with Smartphones

(U//FOUO) The following is intended to provide a brief overview of the security risks associated with smartphones[a]. By increasing awareness and changing user habits many potential threats can be mitigated. Some of these security risks are unique to specific smartphones. It is likely that security risks to smartphones will increase as the software used on smartphones becomes less diverse.

### (U) Overview of Threats

(U//FOUO) Smartphones feature an diverse array of computer capabilities which expose them to many of the vulnerabilities previously confined to computers.[1] These threats have evolved from targeting personal computers (PCs) to hitting smartphones much quicker than some security experts anticipated. It took almost fifteen years for these types of attacks to evolve for PCs, but these attacks have been adapted for smartphones much more quickly. The malicious software (malware) currently targeting smartphones attempts to gather personal information stored on the phone and sell it. Since users often store more of this type of information on smartphones than PCs, in some cases it has become more profitable for hackers to create malware for smartphones than PCs.[2]

- (U) One of the biggest risks tied to smartphone use is that many employees use them to check their work email, download work-related documents, and correspond with colleagues. Theft of data off of these types of devices therefore presents not only a threat to loss of personal data, but also to confidential business data.[3]

(U) The number of malware and spyware programs found on smartphones has more than doubled in the past six months.[4] Smartphones are vulnerable to these malicious programs because:

- (U) Network access codes, usernames, and passwords are often unsecured or set for automatic login on these phones;[5]
- (U) Smartphones can magnify malware distributions that employ email spam and phishing messages because users are more likely to interact with files masquerading as personal communications while they are on their smartphones rather than their PCs; and[6]
- (U) Users cannot as easily detect cues that a website is fraudulent on smartphones because smartphone screens are small and the website cannot be seen in its entirety.[7]

[a] (U) **Smartphone:** “Smartphones are a handheld device that integrates mobile phone capabilities with the more common features of a handheld computer or PDA. Smartphones allow users to store information, e-mail, install programs, along with using a mobile phone in one device. For example a Smartphone could be a mobile phone with some PDA functions integrated into the device, or vice versa.” http://www.webopedia.com/TERM/S/smartphone.html

(U) Geolocation data on some smartphones can compromise undercover law enforcement and military personnel if those phones are hacked. Many of the applications that users download to their smartphones can transmit data that can help cyber criminals determine where that person is located. Additionally, undercover law enforcement and military personnel who send photos they have taken on their smartphones via SMS text messages may not realize that embedded global positioning system (GPS) data may also be transmitted, allowing recipients and possibly hackers to determine the longitude and latitude of where the picture was taken.[8]

(U) It is possible for hackers to access and compromise Bluetooth[USBUS] headsets while they are in use or if the Bluetooth feature is enabled on a smartphone.[b] Two different types of Bluetooth attacks include:

- (U) Bluesnarfing: Hackers can user a Bluetooth-enabled smartphone to compromise and gather data from the phone book, calendar, and pictures from the smartphone. It is possible for hackers to also gather the smartphone's PIN and other codes.[9]
- (U) Bluebugging: Hackers compromise a Bluetooth-enabled smartphone and secretly initiate phone calls without the users' knowledge. Often the phone calls are to premium rate lines, usual international, thus making money for the attacker.[10]

### (U) Threats to Specific Smartphones and Their Software

(U//FOUO) The most common forms of smartphones are iPhones, Blackberries, and Droids.

- (U) Apple's[USBUS] iPhone is used by more than 70% of Fortune 100 companies and is the third most commonly employed smartphone by businesses in the world.[11]
    - (U) Last November a student in Australia breached iPhone security with a worm that spread between phones along wireless networks and could have been used to read text messages, emails, and other information stored on the device.[12]
- (U) The Blackberry platform is much more secure than other smartphones, however, hackers often target this smartphone because of the challenge its platform presents and its abundance in business communities.[13]
    - (U) A significant issue for Blackberries is that the desktop software that syncs the phone with non-enterprise-server email accounts[c] encrypts the data, while the actual Blackberry does not encrypt data housed on the phone. This shortcoming means that the data is passed from the phone unencrypted to the computer, potentially exposing it to unauthorized persons.[14]
        - (U) When using an enterprise server, the data that is transferred between the device and the server is encrypted. Users can ensure that the data on the device is encrypted by enabling content protection.[d] Content

[b] (U) Hackers can download programs like Backtrack for free to gain the ability to easily hack into smartphones and Bluetooth headsets.

[c] (U) These email accounts are more likely to be personal accounts as most businesses user enterprise servers for their email systems that are connected to smartphones.

[d] (U) To enable content protection, go to options > security options > general settings, and set content protection to enabled.

protection can be enabled for the phone's address book; however, doing so will disable the caller ID function.[15]

- (U) Hackers will likely use spyware to target Blackberries because of heavy corporate use of the smartphone. Spyware allows hackers to lift corporate data from the phones.[16]

- (U) All Droid smartphones use Google's[USBUS] Android software. The Droid is the newest smartphone, and similar to the iPhone, relies heavily on the use of applications.
  - (U) The Android operating system 2.0 onwards includes a design flaw that allows the users' login credentials and cookies to be harvested. This flaw is associated with the phone's settings which are configured to save passwords. It is dangerous to users who connect to unsecure Internet networks because these networks could allow hackers to gather the users' passwords.[17]
  - (U) Android users are also at risk when they install applications onto their phones and grant them certain access rights because some rogue applications can allow other applications to download without the users' knowledge. These applications can gather the users' information and send it to a hacker, or they can include the right to send premium SMS messages from the phone which will incur charges on the users' bill.[18]

## (U) Outlook

(U//FOUO) It is likely that attacks targeting smart phones will grow sophisticated enough that they will pose a threat to cellular networks via denial of service (DoS) or distributed denial of service (DDoS)[e] attacks:

- (U//FOUO) If hackers are able to compromise smartphones so that they are in control of the devices, it is possible that hackers could use the phones to send wireless data packages to the carrier's network and overload it with the packages and eventually disable it, a DoS attack;[19]
- (U//FOUO) Hackers could perpetrate a DDoS attack by using malicious software with high bandwidth applications on a large number of smartphones simultaneously; and
- (U//FOUO) Hackers could create a denial of service condition on a cellular provider's network by spreading malware through SMS text messages via a worm.[20]

**(U) Terms**

(U) **DoS:** "Short for ***d****enial*-***o****f*-***s****ervice attack,* a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic." http://www.webopedia.com/TERM/D/DoS_attack.html

(U) **DDoS:** "Short for ***D****istributed* ***D****enial* ***of*** ***S****ervice*, it is an attack where multiple compromised systems (which are usually infected with a Trojan) are used to target a single system causing a Denial of Service (DoS) attack." http://www.webopedia.com/TERM/D/DDoS_attack.html

(U) **Worm:** "A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down" http://www.webopedia.com/TERM/W/worm.html

[e] (U) Traditional DDoS attacks occur when hackers take control of large groups of computers and then order them to all access one website or service at the same time, overloading the servers and eventually crashing or disabling the site. http://www.cio.com/article/508076/BlackBerry_Security_Exec_Warns_of_Smartphone_DDoS_Attacks

(U//FOUO) However, the threat to cellular networks from malicious software spread through smartphones is likely to remain limited over the short term because, unlike desktop computers, of which 90% use the same operating systems software, smartphones use a diverse array of operating systems software and hardware. Consequently, a vulnerability affecting one type of device is unlikely to affect a majority of smartphones on a particular network. Additionally, since smartphones presently constitute only a small share of the devices using a given cellular network, any single piece of malicious software can target only a fraction of the users on the network.[21] The vulnerability of cellular networks may grow as smartphone use increases or if smartphone technology becomes more standardized across devices and among carriers. The emergence of a common system architecture and software systems will greatly increase the opportunities for hackers to target smartphones in the future.[22]

(U) Smartphone hackers will likely continue to use spear phishing attacks to target smartphone users because, due to the abundance of spear phishing attacks, there is little chance that anti-virus (AV) software will be written for many of the spear phishing attacks executed on smartphones since AV companies may never be aware of the existence of specific attacks.[23]

**(U) Terms**

(U) **Spear phishing: "**A type of phishing attack that focuses on a single user or department within an organization, addressed from someone within the company in a position of trust and requesting information such as login IDs and passwords. Spear phishing scams will often appear to be from a company's own human resources or technical support divisions and may ask employees to update their username and passwords. Once hackers get this data they can gain entry into secured networks. Another type of spear phishing attack will ask users to click on a link, which deploys spyware that can thieve data." http://www.webopedia.com/TERM/S/spear_phishing.html

### (U) Protective Measures

(U) Many of the vulnerabilities that exist in smartphones can be mitigated by following simple protective measures:

- (U) Keep device and desktop software up to date;[24]
- (U) Use strong passwords for smartphones and their applications that include at least one capital and lower-case letter, one number, and one symbol. Do not choose options that allow the smartphone to remember passwords;[25]
- (U) Disable remote connectivity for features such as Bluetooth when they are not in use;[26]
- (U) Encrypt files on the smartphone if it holds personal or corporate information. Use an encryption password that is strong;[27]
- (U) Be suspicious of URLs sent in unsolicited email or text messages. While the links may appear to be legitimate, they may actually direct recipients to a malicious web site;[28]
- (U) Avoid downloading files from suspicious sites. Look for a web site certificate before downloading files from an unknown website;[29]
- (U) Change the default password on your smartphone;[30]
- (U) Do not leave smartphones unattended in public or easily accessible areas;[31]
- (U) Enable security software already installed on smartphones;[32]

- (U) Install anti-virus software on your smartphone; and[33]
- (U) Clear smartphone memory before disposing of it.[34]

**(U//FOUO) This report addresses the following CIAC Standing Information Needs: CIAC-SIN-05.**
**(U//FOUO) This report addresses the following DHS Standing Information Needs: HSEC-20-00000-ST-2010.**

# INTELLIGENCE GAPS

- (U) Which anti-virus software has shown to be the most effective for smartphones?

## CIAC Customer Satisfaction Survey

Please take a moment to complete this survey and help evaluate the quality, value, and relevance of our intelligence product. Your response will help us serve you more effectively and efficiently in the future. Thank you for your cooperation and assistance. Click here to take survey.

[1] (U//FOUO) "Hackers Targeting Advanced  Cellular Phones." *Department of Homeland Security*: 10 June 2010.

[2] (U) "Smartphone Malware Multiplies." *Dark Reading*: 7 June 2010: http://www.darkreading.com/insiderthreat/security/attacks/showArticle.jhtml?articleID=225402185

[3] (U) "Smartphone Security Risks and Best Practices Research." *Net Security*: 16 September 2010: http://www.net-security.org/article.php?id=1492

[4] (U) "Smartphone Malware Multiplies." *Dark Reading*: 7 June 2010: http://www.darkreading.com/insiderthreat/security/attacks/showArticle.jhtml?articleID=225402185

[5] (U) "10 Best IT Practices for Smartphone Security." *TechNewsWorld*: 15 September 2010: http://www.technewsworld.com/rsstory/70826.html?wlc=1287761057

[6] (U) "10 Best IT Practices for Smartphone Security." *TechNewsWorld*: 15 September 2010: http://www.technewsworld.com/rsstory/70826.html?wlc=1287761057

[7] (U) "10 Best IT Practices for Smartphone Security." *TechNewsWorld*: 15 September 2010: http://www.technewsworld.com/rsstory/70826.html?wlc=1287761057

[8] (U) "Hacked Smartphones Pose Military Threat." *Computerworld*: 16 August 2010: http://www.computerworld.com/s/article/9180768/Hacked_smartphones_pose_military_threat

[9] (U) "Blue Tooth Security." *IT Security* 18 May 2010: http://blog.itsecurityexpert.co.uk/2007/05/bluetooth-security.html

[10] (U) "Blue Tooth Security." *IT Security* 18 May 2010: http://blog.itsecurityexpert.co.uk/2007/05/bluetooth-security.html

[11] (U) "Australia Warns of iPhone Security Risk." 20 October 2010: http://www.google.com/hostednews/afp/article/ALeqM5gw3h9CaSr41wcnCsPda4CD5mqnyw?docId=CNG.a748b69f22077ddd5d23e00c220bc69a.381

[12] (U) "Australia Warns of iPhone Security Risk." 20 October 2010: http://www.google.com/hostednews/afp/article/ALeqM5gw3h9CaSr41wcnCsPda4CD5mqnyw?docId=CNG.a748b69f22077ddd5d23e00c220bc69a.381

[13] (U) "Not So Fast Blackberry, You're not as Secure as We Thought." *Wireless Ground*: 4 October 2010: http://blog.wirelessground.com/blackberry-not-secure/

[14] (U) "Not So Fast Blackberry, You're not as Secure as We Thought." *Wireless Ground*: 4 October 2010: http://blog.wirelessground.com/blackberry-not-secure/

[15] (U) "Protecting Your Blackberry." *Biz Security*: http://bizsecurity.about.com/od/informationsecurity/a/blkberry.htm?mr=952

[16](U) "Smartphone Malware Multiplies." *Dark Reading*: 7 June 2010: http://www.darkreading.com/insiderthreat/security/attacks/showArticle.jhtml?articleID=225402185

[17] (U) "Vulnerabilities in the Palm Pre and Android Smartphones Detailed that can see Credentials Stolen and Conversations Interrupted." *SC Magazine*: 11 August 2010: http://www.scmagazineuk.com/vulnerabilities-in-the-palm-pre-and-android-smartphones-detailed-that-can-see-credentials-stolen-and-conversations-intercepted/article/176735/

[18] (U) "Android holes Allow Secret Installation of Apps." *The H Security*: 11 November 2010: http://www.h-online.com/security/news/item/Android-holes-allow-secret-installation-of-apps-1134940.html

[19] (U) "Blackberry Security Exec Warns of Smartphone DDoS Attacks." *CIO*: 18 November 2010: http://www.cio.com/article/508076/BlackBerry_Security_Exec_Warns_of_Smartphone_DDoS_Attacks

[20] (U//FOUO) "Hackers Targeting Advanced Cellular Phones." *Department of Homeland Security*: 10 June 2010.

[21] (U//FOUO) "Hackers Targeting Advanced Cellular Phones." *Department of Homeland Security*: 10 June 2010.

[22] (U//FOUO) "Hackers Targeting Advanced Cellular Phones." *Department of Homeland Security*: 10 June 2010.

[23] (U) "Threats Against Smartphones are Rising." *Biz Security*: http://bizsecurity.about.com/od/informationsecurity/a/smartphone_security.htm

[24] (U) "Cybersecurity for Electronic Devices: Cyber Security Tip ST05-017." *U.S. Computer Emergency Readiness Team:* http://www.us-cert.gov/cas/tips/ST05-017.html

[25] (U) "Cybersecurity for Electronic Devices: Cyber Security Tip ST05-017." *U.S. Computer Emergency Readiness Team:* http://www.us-cert.gov/cas/tips/ST05-017.html

[26] (U) "Cybersecurity for Electronic Devices: Cyber Security Tip ST05-017." *U.S. Computer Emergency Readiness Team:* http://www.us-cert.gov/cas/tips/ST05-017.html

[27] (U) "Cybersecurity for Electronic Devices: Cyber Security Tip ST05-017." *U.S. Computer Emergency Readiness Team:* http://www.us-cert.gov/cas/tips/ST05-017.html

[28] (U) "Defending Cell Phones and PDAs Against Attack: Cyber Security Tip ST06-007." *U.S. Computer Emergency Readiness Team:* http://www.us-cert.gov/cas/tips/ST06-007.html

[29] (U) "Defending Cell Phones and PDAs Against Attack: Cyber Security Tip ST06-007." *U.S. Computer Emergency Readiness Team:* http://www.us-cert.gov/cas/tips/ST06-007.html

[30] (U//FOUO) "Hackers Targeting Advanced Cellular Phones." *Department of Homeland Security*: 10 June 2010.

[31] (U//FOUO) "Hackers Targeting Advanced Cellular Phones." *Department of Homeland Security*: 10 June 2010.

[32] (U) "Department of Homeland Security Open Source Enterprise Daily Digest": 27 October 2009.

[33](U) "Threats Against Smartphones are Rising." *Biz Security*: http://bizsecurity.about.com/od/informationsecurity/a/smartphone_security.htm

[34] (U) "Threats Against Smartphones are Rising." *Biz Security*: http://bizsecurity.about.com/od/informationsecurity/a/smartphone_security.htm