Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

MOBILE PHONES EMERGE AS SECURITY THREAT TARGETS

Due to their portability and advanced computing features, mobile phones are becoming popular devices for Web surfing. Just like PCs, however, these gadgets are also susceptible to various security threats. Users must thus remain cautious when using their mobile phones to surf the Internet to keep their phones malware free.

Enterprises Join the Mobile Bandwagon

Today's technology-driven market has given way to the proliferation of mobile phones with advanced features to cater to consumers' need to stay connected.

Today's technology-driven market has given way to the proliferation of mobile phones with advanced features to cater to consumers' need to stay connected. It is thus not surprising that the worldwide mobile phone sales has increased. Based on Gartner research, the mobile phone sales increased by 13.8 percent in the second quarter of 2010 while the smartphone sales marked a 50.5 percent growth. *Symbian* was the most popular smartphone OS, accounting for a 41.2 percent share, though *Android* was the most popular OS in the United States.

Web surfing via mobile phones also became more popular, as comScore found that 31.9 percent of the subscribers in the United States used their phones to go online. The other popular online activities include downloading applications and accessing social networking sites or blogs with shares of 30 and 20.8 percent, respectively.

Businesses are also eying mobile phone use to address the expanding yet specific demands of modern consumers. In a paper, ISACA listed down some of the benefits that using mobile phones pose to business operations, namely:

- **Increased productivity.** Mobile phones that can access corporate email inboxes and other information on the Internet can benefit employees who need to work off-site.
- **Better customer service.** Mobile phones with advanced features allow sales and account officers to access their corporate customer relationship management (CRM) systems and other pertinent data via the Internet, regardless of location. This allows them to provide immediate solutions to their customers' concerns.
- **Real-time customer response.** ISACA noted a 35 percent improvement in customer satisfaction with businesses that have integrated mobile device management with their operations.

TREND MICRO

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

Security Concerns Hover over Mobile Phone Use

Contemporary mobile phones may have become a hit but their heavy use also made them likely targets of security threats. In the past few months, TrendLabs saw cases of mobile malware infection and exploitation plague users.

Phones Shipped with Malware

News of smartphones that came preinstalled with malicious files circulated on the Internet when telecommunications giant Vodafone distributed 3,000 worm-infected HTC Android smartphones. The worm, detected as WORM_SILLY.QT, was found capable of performing denial-of-service (DoS) attacks via SYN flooding.

Samsung also inadvertently distributed malware along with its new S8500 Wave smartphone. It has been reported to have shipped worm-infected units to Germany. The worm, detected as WORM_AUTORUN.WAV, attempts to infect a user's PC when the phone is connected to it. The worm then connects to various websites to possibly download other malicious files and exposes the user's system to backdoor programs and spyware.

Malware Pose as Applications

Apps are one of the major factors that make a mobile phone appealing. As such, manufacturers ensure that they make interesting mobile phone apps readily available via their respective portals.

Apps are one of the major factors that make a mobile phone appealing. As such, manufacturers ensure that they make interesting mobile phone apps readily available via their respective portals.

Apps are one of the major factors that make a mobile phone appealing. As such, manufacturers ensure that they make interesting mobile phone apps readily available via their respective portals. However, not all the apps one finds on these portals are safe to use. In fact, last December, Google removed 50 suspicious-looking apps from the *Android Market* after proving that these used various banks' names without their permission.

TrendLabs senior threat researcher Paul Ferguson also found a suspicious-looking application aka *ZvirOK* on *Symbian*-based mobile phones. Detected as SYMBOS_FLOCK.I, *ZvirOK* sends the message *mumymxxx joker90* to the number *7650* by executing a simple Python script detected as TROJ_FLOCK.I.

TREND MICRO

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

The first-ever *Android* Trojan was also uncovered, which came disguised as *Windows Media Player.* Detected as ANDROIDOS_DROIDSMS.A, the Trojan uses the default SMS Center and Permission function *android_permission. SEND_sms* to send text messages to numbers such as *3353* or *3354* with the message string *798657,* which may cause users to be charged premium message fees. Fortunately, the malware code did not work properly due to programming errors.

If that is not enough, another malicious *Android* app was found capable of spying on a user's geographic location. The app aka *Tap Snake,* detected as ANDROIDOS_DROISNAKE.A, is capable of sending out a user's GPS location via HTTP POST to the site *gpsdatapoints.appspot.com/addpoint.* The information can then be retrieved by a remote user using another app aka *GPS SPY.*

Jailbreaking and Its Impact

As apps become seemingly integral to mobile phones, users are jailbreaking their devices just to download alternative apps. A developer named Comex even released a jailbreaking tool dubbed *JailbreakMe,* detected as TROJ_PIDIEF.HLA, for Apple's iPhone 4 and other products that run on *iOS.*

In reality, however, this tool exploits two separate vulnerabilities, which may lead to arbitrary code execution and unauthorized control of the affected device. Apple has already released patches to address these, as the security implications these pose are serious. Using the same technique the tool used may allow cybercriminals to push malware onto *iOS*-based devices.

> Trend Micro threat analyst Edgardo Diaz, Jr. says, "The more security conscious may wonder if increased consumer choice is all that the jailbreakers are interested in or if they are also interested in spreading malware."

Trend Micro threat analyst Edgardo Diaz, Jr. believes that jailbreaking for smartphones and iPhones may benefit consumers, as this gives them the option to download any app they want. However, it also brings to light security concerns such as the real intentions of developers and how vendors conduct security reviews to detect possible threats. As Diaz puts it, "The more security conscious may wonder if increased consumer choice is all that the jailbreakers are interested in or if they are also interested in spreading malware."

TREND MICRO

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

Mobile Web Threats

The popularity of Web browsing via mobile phones among consumers created an opportunity for cybercriminals to expand their target base. Unfortunately, however, most mobile users unconcerned.

In fact, a Trend Micro survey found that 44 percent of the more than 1,000 respondents were lax with regard to surfing via mobile phones. They were more concerned with losing data caused by actual phone loss than information theft caused by Web threats and phishing or spam attacks. Even worse, only 23 percent of the respondents utilized mobile phone security software. This lack of vigilance among users makes them vulnerable to the Web threats that loom in the mobile space.

New Venues, Same Precautions

Given the many mobile phone risks, users must exercise caution to avoid downloading malicious files onto their devices. Even better, they should utilize their phones' security features and install a solution powered by an efficient security infrastructure to prevent malware infection.

Given the many mobile phone risks, users must exercise caution to avoid downloading malicious files onto their devices. Even better, they should utilize their phones' security features and install a solution powered by an efficient security infrastructure to prevent malware infection.

Enterprises should take note of the following best practices if they let their employees use mobile devices for business-related operations:

- Identify where sensitive data should be stored, who controls and accesses it, and how this is protected. If possible, encrypt sensitive data for security purposes.
- Monitor how employees use their mobile devices to connect to the corporate network and determine what specific measures can ensure the best level of security.
- Establish centralized management processes for business and personal information residing in and accessed by mobile devices. This will not only be cheaper but will also make managing multiple devices easier. Only designated IT personnel should be able to set the data access levels and modify the security settings of mobile devices.

Such initiatives can only prove effective, however, if enterprises ensure that their employees are given proper training about using their mobile devices to access corporate data and the security risks this poses.

TREND MICRO

References:

- Apple Inc. (August 11, 2010). *Apple.* "About the Security Content of the *iOS 4.0.2* Update for iPhone and iPod Touch." http://support.apple.com/kb/HT4291 (Retrieved September 2010).
- Bernadette Irinco. (August 17, 2010). *TrendLabs Malware Blog.* "Malicious *Android* App Spies on User's Location." http://blog.trendmicro.com/malicious-android-app-spies-on-users-location/ (Retrieved September 2010).
- Bernadette Irinco. (August 10, 2010). *TrendLabs Malware Blog.* "First *Android* Trojan in the Wild." http://blog.trendmicro.com/first-android-trojan-in-the-wild/ (Retrieved September 2010).
- Bernadette Irinco. (August 28, 2009). *TrendLabs Malware Blog.* "Mobile Users Unfazed by Web Threats." http://blog.trendmicro.com/mobile-users-unfazed-by-web-threats/ (Retrieved September 2010).
- Brian Prince. (January 11, 2010). *eWeek.com.* "Google Removes Suspicious Mobile Apps from *Android Market."* http://www.eweek.com/c/a/Security/Google-Removes-Suspicious-Mobile-Apps-from-Android-Market-758811/ (Retrieved September 2010).
- comScore. (July 8, 2010). *comScore.* "comScore Reports May 2010 U.S. Mobile Subscriber Market Share: Google's *Android* Platform Continues to Snatch Smartphone Market Share." http://www.comscore.com/Press_Events/Press_Releases/2010/7/comScore_Reports_May_2010_U.S._Mobile_Subscriber_Market_Share (Retrieved September 2010).
- Danielle Veluz. (March 12, 2010). *TrendLabs Malware Blog.* "Malware Gets Smart with Vodafone Smartphones." http://blog.trendmicro.com/malware-gets-smart-with-vodafone-smartphone/ (Retrieved September 2010).
- Danielle Veluz. (June 5, 2010). *TrendLabs Malware Blog.* "Infected S8500 Wave Phones Make It to Germany." http://blog.trendmicro.com/infected-s8500-wave-phones-make-it-to-germany/ (Retrieved September 2010).
- Edgardo Diaz, Jr. (August 17, 2010). *TrendLabs Malware Blog.* "The Security Implications of *iOS* Jailbreaking." http://blog.trendmicro.com/the-security-implications-of-ios-jailbreaking/ (Retrieved September 2010).
- Gartner Inc. (August 12, 2010). *Gartner.* "Gartner Says Worldwide Mobile Device Sales Grew 13.8 Percent in Second Quarter of 2010, but Competition Drove Prices Down: *Android* Became the World's Third Most Popular Smartphone OS and Claimed the Top Spot in the U.S." http://www.gartner.com/it/page.jsp?id=1421013 (Retrieved September 2010).
- ISACA. (2010). *ISACA.* "Securing Mobile Devices." http://www.isaca.org/Knowledge-Center/Research/Documents/SecureMobileDevices-Wht-Paper-20July2010-Research.pdf (Retrieved September 2010).

- Jonathan Leopando. (August 4, 2010). *TrendLabs Malware Blog.* "Online iPhone Jailbreak Uses *iOS* Vulnerabilities." http://blog.trendmicro.com/online-iphone-jailbreak-uses-ios-vulnerabilities/ (Retrieved September 2010).
- Jonathan Leopando. (June 30, 2010). *TrendLabs Malware Blog.* "New *Symbian* Malware on the Scene." http://blog.trendmicro.com/new-symbian-malware-on-the-scene/ (Retrieved September 2010).
- Trend Micro Incorporated. (2010). *Threat Encyclopedia.* "ANDROIDOS_DROISNAKE.A." http://threatinfo.trendmicro.com/vinfo/grayware/ve_graywareDetails.asp?GNAME=ANDROIDOS_DROISNAKE.A (Retrieved September 2010).
- Trend Micro Incorporated. (August 10, 2010). *Threat Encyclopedia.* "ANDROIDOS_DROIDSMS.A." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=ANDROIDOS_DROIDSMS.A (Retrieved September 2010).
- Trend Micro Incorporated. (August 4, 2010). *Threat Encyclopedia.* "TROJ_PIDIEF.HLA." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_PIDIEF.HLA (Retrieved September 2010).
- Trend Micro Incorporated. (June 29, 2010). *Threat Encyclopedia.* "TROJ_FLOCK.I." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_FLOCK.I (Retrieved September 2010).
- Trend Micro Incorporated. (June 25, 2010). *Threat Encyclopedia.* "SYMBOS_FLOCK.I."http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=SYMBOS_FLOCK.I (Retrieved September 2010).
- Trend Micro Incorporated. (June 4, 2010). *Threat Encyclopedia.* "WORM_AUTORUN.WAV." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_AUTORUN.WAV (Retrieved September 2010).
- Trend Micro Incorporated. (June 16, 2009). *Threat Encyclopedia.* "WORM_SILLY.QT." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SILLY.QT (Retrieved September 2010).