

MOBILE LANDSCAPE: SECURITY RISKS AND OPPORTUNITIES

Mobile malware are growing in number and prevalence due to the rise in the demand for mobile devices. The evolution and emergence of several mobile OSs like Google's Android OS and Apple's iOS provided cybercriminals additional routes with which to instigate malicious activities.

Mobile Malware Then and Now

Mobile devices have become an integral part of day-to-day business and personal communication and computing activities. The functionality now available to users has evolved far beyond calling and text messaging to include Web-based activities. This enabled users to stay connected wherever they are and caused them to more heavily rely on their mobile devices.

► The functionality now available to users has evolved far beyond calling and text messaging to include Web-based activities.

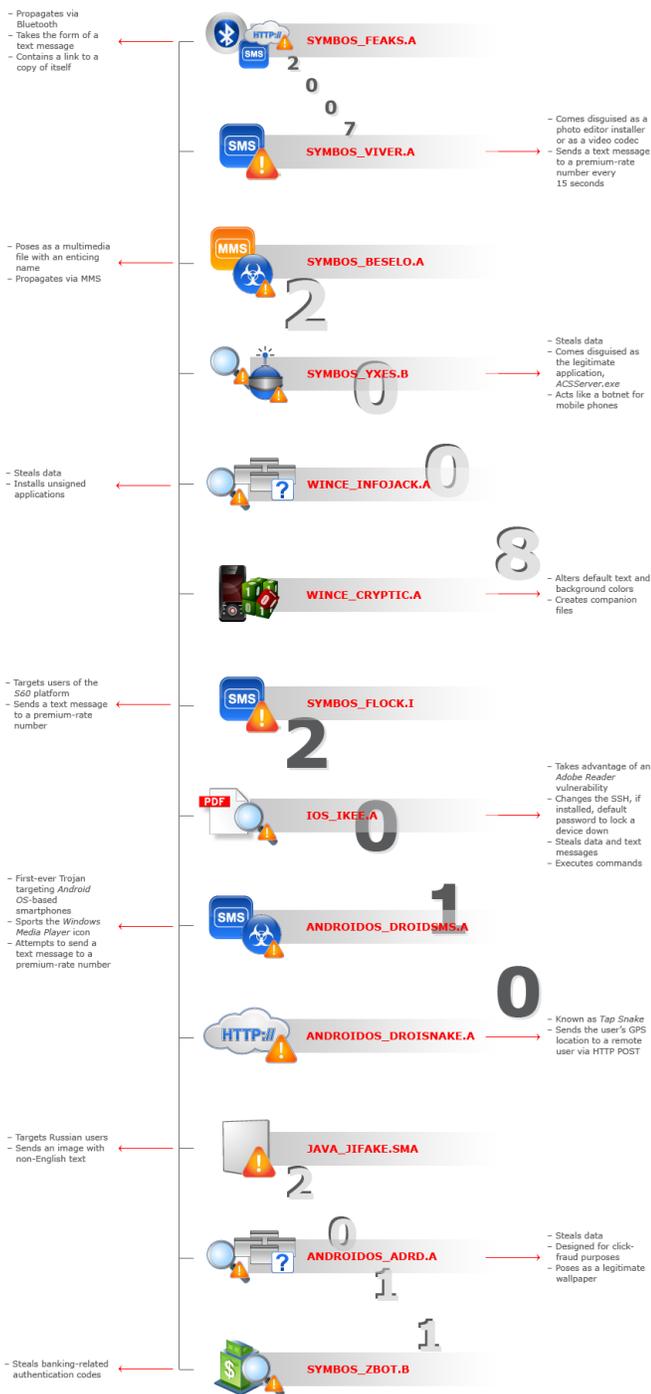
In 2010, Gartner reported that the mobile device sales increased by 31.8 percent from 2009. The smartphone sales also increased by 72.1 percent from 2009. As such, it is not surprising that cybercriminals are targeting the growing mobile device market.

As early as 2006, Trend Micro has seen various mobile malware, most of which targeted Symbian- and Windows-based mobile phones. Some of the notable "traditional mobile malware" are discussed in more detail below.

- In November 2008, TrendLabsSM engineers came across a WinCE malware detected as WINCE_CRYPTIC.A that alters an infected mobile phone's default text and background colors. It creates companion files that contain the infection code using the same file name as the phone's storage card. In effect, running the contents of the storage card executes the malicious files.
- WINCE_INFOJACK.A runs on the WinCE environment as well. It steals information like OS version, model, and platform from an infected mobile phone. It also installs unsigned applications and leaves the infected phone vulnerable to other malware infections.
- A notorious Symbian OS malware detected as SYMBOS_YXES.B steals data like subscriber, phone, and network information, which it then sends to a remote site. It comes disguised as ACSSEver.exe, a legitimate application, but calls itself Sexy Space. It acts like a botnet for mobile phones. It sends text messages to an affected user's contacts but is considered a signed program.
- SYMBOS_BESELO.A, meanwhile, poses as a multimedia file that uses a name like beauty, love, or sex to lure users into executing it. It drops files and propagates by sending an MMS that uses an enticing file name.
- In May 2007, a Symbian OS malware disguised as a photo editor installer or as a video codec was seen. Detected as SYMBOS_VIVER.A, it sends text messages to a specific premium-rate number every 15 seconds without the affected user's consent.

- Two months earlier, **SYMBOS_FEAKS.A** was found propagating via Bluetooth in the form of text messages to affected mobile phone users' contacts. The said messages contain a link that when clicked leads to a copy of the malware.

MOBILE MALWARE EVOLUTION



Even though the above-mentioned mobile malware are no longer in the limelight, they remain active today. In June 2010, senior threat researcher Paul Ferguson came across a malicious application called *ZvirOK* aka *SYMBOS_FLOCK.I*. This *Symbian OS* malware targets users of the *S60* platform. When executed, it sends a text message to a specific premium-rate number, which eventually costs the affected user a lot of money.

Out with the Old, in with the New

The first-ever Trojan targeting Google's *Android OS* smartphones was discovered in August 2010. Detected as *ANDROIDOS_DROIDSMS.A*, it sports the *Windows Media Player* icon to lure users into downloading it. When executed, it attempts to send a text message to a premium-rate number.

In the same month, an *Android OS* app dubbed *Tap Snake* was also spotted. Detected as *ANDROIDOS_DROISNAKE.A*, it sends an affected user's GPS location via HTTP POST to a remote user upon acceptance of the app's end-user license agreement (EULA).



The most recent *Android OS* malware aka *ANDROIDOS_ADRD.A* came disguised as a legitimate wallpaper. It was specially crafted for the purpose of instigating click fraud. Like its predecessors, it steals device information that is then sent to a remote site.

Mobile phones that run the *Android OS* are more prone to attacks due to its open nature. This is compounded by the fact that submitting apps to the *Android Market* does not involve a strict approval process.

With Great Ease Comes Great Risks

In August 2010, a developer known as Comex released a jailbreaking tool for Apple's iPhone to the public. Users who want to download apps from stores other than Apple's *App Store* can visit a specially crafted site to easily jailbreak their iPhones or other Apple products running on iOS. The tool aka *IOS_IKEE.A* takes advantage of an *Adobe Reader* vulnerability to work.

Apart from malware infection, mobile device users are also at risk of the dangers phishing attacks pose. An independent security researcher demonstrated a proof-of-concept (POC) attack against iPhones that causes *Safari* to hide the real address bar after a page finishes loading. This vulnerability can be used by cybercriminals to mask the URL of a bogus page, which may be useful in phishing attacks.

▶ Apart from malware infection, mobile device users are also at risk of the dangers phishing attacks pose.

According to a [2010 Computerworld report](#), 75 percent of the total number of organizations surveyed allowed the use of personally owned mobile devices. Moreover, 41 percent of the total number of IT professionals surveyed said that some unauthorized devices also accessed their office networks.

Mobile device management (MDM) of employee-owned devices that are not properly configured for enterprise-oriented platforms should be enhanced. Employees who lack threat awareness should not be left on their own with regard to setting security policies, as this may lead to corporate data leakage. IT administrators should ensure that the personally owned mobile devices that access their corporate networks comply with their MDM policies to avoid the serious security implications of not doing so.

According to a [Pew Research Center study](#), most of the mobile device users are younger adults. They exhaust every feature available on their mobile devices. They surf the Web, send email, and chat with their contacts. They also heavily access social networking sites using their mobile phones, which exposes them to the same threats targeting computers.

Securing the Mobile World

The increasing use of mobile devices to access the Internet unfortunately translates to a rise in the number of Web threats targeting this platform. In fact, Trend Micro's [2011 prediction for the mobile threat landscape](#) is already coming true. As early as January, we saw a mobile malware detected as **JAVA_JIFAKE.SMA** that **specifically targets Russian users**. As in previous cases, it purports to be a legitimate mobile app.

A month after, we spotted a *Symbian OS* malware detected as **SYMBOS_ZBOT.B** that steals banking authentication codes. It also compromises a mobile device's security, clearly showing that mobile threats are slowly but surely becoming more prevalent.

Users can, however, arm themselves against mobile threats by being wary of what they download from app stores. Trend Micro advises users to never install apps from unknown sources. Mobile threats often come disguised as legitimate apps. It is also best that users remain vigilant when it comes to Web threats and to stay abreast of the latest social engineering tactics. Those who access social networking sites via their mobile devices should refrain from clicking suspicious-looking links even if prompted by their trusted contacts. Make sure to only access legitimate sites and to divulge information to known and trusted contacts.



Employees who use their personal mobile devices while at or for work should also comply with the security policies set by their companies' IT departments so as not to contribute, albeit unknowingly, to data leakage or to find themselves the originators of malware infection. They should avoid accessing their office networks using unauthorized devices. Furthermore, they should only access sites that have been approved by their IT departments. Finally, Trend Micro highly recommends that users install **security software** that can stop the execution of malicious files on their mobile devices.

References:

- 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 March 2011).
- 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 March 2011).
- Bernadette Irinco. (August 8, 2009). *TrendLabs Malware Blog*. "Mobile Users Unfazed by Web Threats." <http://blog.trendmicro.com/mobile-users-unfazed-by-web-threats/> (Retrieved March 2011).
- Bernadette Irinco. (March 6, 2008). *TrendLabs Malware Blog*. "WinCE Worms Itself to Windows Mobile." <http://blog.trendmicro.com/wince-worms-itself-to-windows-mobile/> (Retrieved March 2011).
- Dianne Lagrimas. (January 24, 2008). *TrendLabs Malware Blog*. "Symbian Malware Gives Love (Beauty, and Sex) a Bad Name." <http://blog.trendmicro.com/symbian-malware-gives-love-and-beauty-and-sex-a-bad-name/> (Retrieved March 2011).
- Dianne Lagrimas. (May 24, 2007). *TrendLabs Malware Blog*. "New Symbian Malware on the Block." <http://blog.trendmicro.com/new-symbian-malware-on-the-block/> (Retrieved March 2011).
- Jake Soriano. (November 22, 2008). *TrendLabs Malware Blog*. "WinCE Malware Blackens Phone Wallpapers." <http://blog.trendmicro.com/wince-malware-blackens-phone-wallpapers/> (Retrieved March 2011).
- Jonathan Leopando. (November 30, 2010). *TrendLabs Malware Blog*. "Mobile UI Spoofing—Another Reason for Smart Surfing." <http://blog.trendmicro.com/mobile-ui-spoofing%E2%80%93another-reason-for-smart-surfing/> (Retrieved March 2011).
- 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 March 2011).
- Jonathan Leopando. (July 15, 2009). *TrendLabs Malware Blog*. "Signed Malware Coming to a Phone Near You?" <http://blog.trendmicro.com/signed-malware-coming-to-a-phone-near-you/> (Retrieved March 2011).

- Kathryn Cheng. (March 17, 2007). *TrendLabs Malware Blog*. "Target: UIQ + Symbian Mobile Devices." <http://blog.trendmicro.com/target3a-uiq-2b-symbian-mobile-devices/> (Retrieved March 2011).
- Kathryn Zickuhr. (February 3, 2011). *PewInternet*. "Generations and Their Gadgets." <http://www.pewinternet.org/Reports/2011/Generations-and-gadgets.aspx> (Retrieved March 2011).
- Leena Rao. (February 9, 2011). *TechCrunch*. "Gartner: Android OS Sales Trump iOS and RIM, Grew 888 Percent in 2010." <http://techcrunch.com/2011/02/09/gartner-android-os-sales-trumps-ios-and-rim-grew-888-percent-in-2010/> (Retrieved March 2011).
- Scot Finnie. (November 9, 2010). *Computerworld*. "Getting IT Set for Mobile." http://www.pcworld.com/businesscenter/article/210079/getting_it_set_for_mobile.html (Retrieved March 2011).
- Trend Micro Incorporated. (February 2011). *Threat Encyclopedia*. "ANDROIDOS_ADRD.A." http://about-threats.trendmicro.com/Malware.aspx?language=us&name=ANDROIDOS_ADRD.A (Retrieved March 2011).
- Trend Micro Incorporated. (February 2011). *Threat Encyclopedia*. "SYMBOS_ZBOT.B." http://about-threats.trendmicro.com/Malware.aspx?language=us&name=SYMBOS_ZBOT.B (Retrieved March 2011).
- Trend Micro Incorporated. (December 2010). *Threat Encyclopedia*. "JAVA_JIFAKE.SMA." http://about-threats.trendmicro.com/Malware.aspx?language=us&name=JAVA_JIFAKE.SMA (Retrieved March 2011).
- Trend Micro Incorporated. (December 9, 2010). *TrendWatch*. "Trend Micro Threat Predictions for 2011." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/trend_micro_2011_threat_predictions.pdf (Retrieved March 2011).
- Trend Micro Incorporated. (August 2010). *Threat Encyclopedia*. "ANDROIDOS_DROIDSMS.A." http://about-threats.trendmicro.com/Malware.aspx?language=us&name=ANDROIDOS_DROIDSMS.A (Retrieved March 2011).
- Trend Micro Incorporated. (June 2010). *Threat Encyclopedia*. "SYMBOS_FLOCK.I." http://about-threats.trendmicro.com/Malware.aspx?language=us&name=SYMBOS_FLOCK.I (Retrieved March 2011).
- Trend Micro Incorporated. (July 22, 2009). *Threat Encyclopedia*. "SYMBOS_YXES.B." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=SYMBOS_YXES.B (Retrieved March 2011).
- Trend Micro Incorporated. (November 18, 2008). *Threat Encyclopedia*. "WINCE_CRYPTIC.A." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=WINCE_CRYPTIC.A (Retrieved March 2011).

- Trend Micro Incorporated. (March 4, 2008). *Threat Encyclopedia*. "WINCE_INFOJACK.A." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=WINCE_INFOJACK.A (Retrieved March 2011).
- Trend Micro Incorporated. (January 23, 2008). *Threat Encyclopedia*. "SYMBOS_BESELO.A." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=SYMBOS_BESELO.A (Retrieved March 2011).
- Trend Micro Incorporated. (May 21, 2007). *Threat Encyclopedia*. "SYMBOS_VIVER.A." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=SYMBOS_VIVER.A (Retrieved March 2011).
- Trend Micro Incorporated. (March 11, 2007). *Threat Encyclopedia*. "SYMBOS_FEAKS.A." http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=SYMBOS_FEAKS.A (Retrieved March 2011).
- Valerie Boquiron. (February 23, 2011). *TrendLabs Malware Blog*. "From RSA 2011: Mobile Security in Today's Threat Landscape." <http://blog.trendmicro.com/from-rsa-2011-mobile-security-in-today%e2%80%99s-threat-landscape/> (Retrieved March 2011).
- Warren Tsai. (January 17, 2011). *TrendLabs Malware Blog*. "The 'Consumerization' of Mobile IT: Risks and Rewards." <http://blog.trendmicro.com/the-consumerization-of-mobile-it-risks-and-rewards/> (Retrieved March 2011).