TREND MICRO | Securing Your Journey to the Cloud

RESEARCHBRIEF

Fake Apps, Russia, and the Mobile Web

Making the SMS Fraud Connection

Paul Pajares and Max Goncharov

News of an SMS fraud service affecting many countries first broke out in Russia in 2010. It has since put users at risk through popular online activities like social networking and downloading content.

These fraud services are known as "premium service abusers," mobile malware that subscribe users to premium-rated short message services. Some of them also connect to premium numbers without the user's consent, which leads to additional and unwanted charges.

Premium service abusers may favor malicious domains as hosts but they can also spread as fake apps downloaded from third-party or legitimate app stores. Users often get them from poisoned search engine results that lead to fake app download sites, which then install malware.

Premium service abusers comprise over 40% of the global threats to Android devices. They not only affect Android, but also the Java Micro Edition (formerly J2ME) platform. Users of the iOS platform are also at risk, as shown by a rogue Angry Birds Star Wars app that tricks them into giving out their mobile numbers via browser-based social engineering tactics.

Premium service abusers prove the active dynamics of mobile cybercrime, which grows alongside the increasing mobile traffic. Seeing that mobile threats can be agile, jumping from PCs to mobile devices, it is only wise for individuals and companies alike to use comprehensive solutions that protect both.

Why Russia?

Premium service abusers primarily target Russia. This is partly due to the lack of standard app stores in the country, which makes third-party app stores popular. With over 2,800 unique infections from November 2012 to May 2013 alone, the threat aggravates the risks in the Russian mobile landscape.

Other top targets include Russian-speaking countries, Ukraine and Uzbekistan.

Figure 1 shows that more people are downloading malicious .APK and .JAR files. These are mostly hosted in the Czech Republic and Germany. Still, research suggests that there are only a couple of servers that dominate most domains. This indicates that only a handful of players control the large fraud services market.

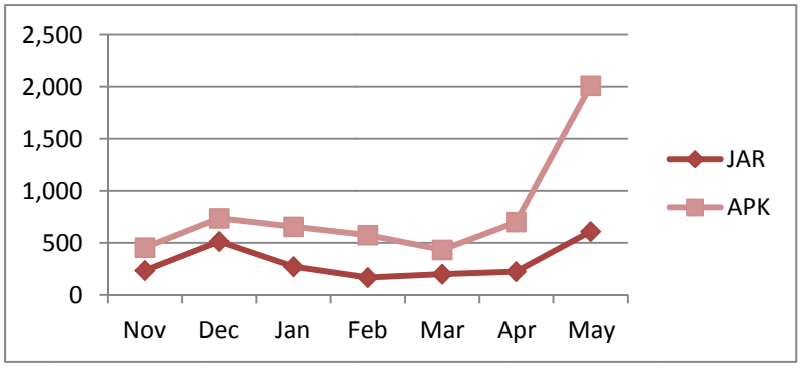

Figure 1: Distribution of .APK and .JAR files downloaded from November 2012 to May 2013

Figure 2: Top SMS fraud host countries most affected by SMS fraud

Figure 3: Countries most affected by SMS fraud

"Free Content" Search Leads to Malware

Fake apps are often obtained when users get redirected to file download sites. The sites use blackhat search engine optimization (SEO) to appear as top search results for popular keywords like "Bad Piggies" and "Download Flash for Android."

These download sites are either constructed blog sites with Russian text, a fake Google Play site, rogue app stores, or specific download sites for apps usually defined on the host name.

Cybercriminals usually trick users to subscribe to free content then charge exorbitant or recurring payments.

Figure 4: Fake Adobe® Flash® Player for Android tricks users into downloading malware

They use advertising network affiliates to push malicious links via mobile apps, providers, sites, SMS, QR codes, and links in spam. They then get paid via these affiliate networks without the users' consent.

Some apps also gather device information like International Mobile Station Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) number, brand, model, manufacturer, and OS software development kit (SDK) version.

Mobile numbers and other personal information are then sold in the underground cybercrime market.

MOBILE DATA	PRICE
1M numbers	US$70
10K numbers	US$10
Customized database with personal data	US$35 for 1,000 numbers

Table 1: Underground prices of collected mobile numbers from Russian network operators

TYPES OF MALICIOUS DOWNLOAD SITES		
		
Malicious apps in a constructed blog site with Russian text	Rogue Google Play app store	Specific app download site

Table 2: Types of malicious download sites

Permissions, Privacy, and a Little Push

Most premium service abusers exploit app permissions for malicious activities like sending, receiving, and reading text messages as well as obtaining access to contacts and locations. The proliferation of FAKE and BOXER malware, meanwhile, show the prevalence of Russian SMS fraud services in the overall mobile threat landscape.

Push notifications can also be dangerous for users, as many malware and high-risk apps push ads that can lead to malicious downloads. Aggressive adware like ARPUSH and LEADBLT variants use push notifications to victimize mobile users as well.

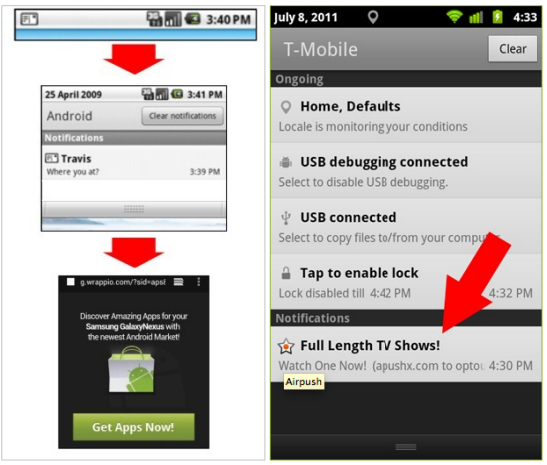

Figure 5: Sample push notification that can be used to redirect users to malicious mobile sites

What Can Users Do?

Russian SMS fraud services and malicious apps from legitimate and/or third-party app stores can cause users to suffer financial losses from sending messages to premium numbers.

Similarly, user privacy and reputation are put at risk with the amount of access that malicious apps can obtain and use for cybercriminal activities.

But they can be effectively fought off with a robust and comprehensive threat solution anchored on reliable, global threat intelligence.

Individuals and businesses can both benefit from using accurate web and IP reputation technologies that can correlate threats and block access to malicious app sources like standalone websites and third-party app stores.

It is also important to collect mobile threat intelligence and use a mobile app reputation technology to identify malicious and high-risk apps.

Proper discretion should be applied when searching for and downloading seemingly malicious and high-risk apps. Check app permissions and only download from official app stores. Look at the routines of the apps you download as well and exercise caution when it comes to push ads that appear as notifications.

More importantly, user devices can be further protected by threat solutions that not only proactively block threats on a single device type but across all possible threat vectors.

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003