# Mobile Users Facing Olympics Scams and Malicious Android Applications According to GFI Software

Submitted by: GFI Software
Wednesday, 8 August 2012

---

OpFake and Boxer malware families continue to evolve and infect smartphones and tablets

London, UK – August 8, 2012 – GFI Software™ today released its VIPRE® Report for July 2012, a collection of the 10 most prevalent threat detections (http://www.gfi.com/) encountered last month. In July, GFI threat researchers observed a number of malware attacks targeting mobile users, including fake applications exploiting consumers' interest in the official app for the 2012 Summer Olympic Games (http://www.gfi.com/blog/scammers-prey-on-london-2012-mobile-game-players/) as well as mobile Web browsers such as Firefox® (http://www.gfi.com/blog/boxer-sms-scam-poses-as-firefox-for-android/) and Opera Mini™ (http://www.gfi.com/blog/new-android-malware-comes-bundled-with-real-opera-mini/).

"Mobile malware is a relatively new frontier for cybercriminals, but that does not mean that their attacks are any less sophisticated or dangerous," said Christopher Boyd, senior threat researcher at GFI Software. "Many users are not aware of the fact that cybercriminals have created malware specifically for Android™ devices (http://www.vipremobile.com/) and are rushing to download apps before ensuring that they are legitimate."

Just days ahead of the 2012 Summer Olympics opening ceremonies in London, GFI researchers uncovered Russian websites hosting Trojans posing as the London 2012 Official Mobile Game (http://www.gfi.com/blog/scammers-prey-on-london-2012-mobile-game-players/) app. The websites were designed to mimic the official Google Play™ app market in order to trick users into downloading the application. GFI also discovered a spam email campaign falsely promising victims a chance to win free airline tickets to the London Olympics (http://www.gfi.com/blog/survey-spam-also-bank-on-2012-olympics-fever/) in exchange for filling out a survey and supplying personal information.

Users also encountered a phony version of Firefox for Android exploiting the recent release of the official Web browser on Google Play in June. The application is part of the Boxer malware family, which normally tricks users into agreeing to send premium SMS messages before directing them to the official Firefox website. This version of the app goes a step further and installs the application without notice, covertly sends premium SMS messages and directs users to the Google™ homepage. GFI researchers believe that this may be a tactic used to convince users that the app was not installed properly, thus returning to the scam website and going through the process multiple times.

Mobile users interested in the Android version of the Opera Web browser were in danger of coming across the OpFake family of Trojans, which often pose as the Opera Mini application. Like victims of the Boxer Trojans, users who fell for this scam had their phones send SMS messages to premium-rate numbers without their knowledge. The version of OpFake uncovered by GFI also installs the real Opera Mini Web browser in order to trick users into thinking that they have installed the correct application. Victims of this scam would not realise anything was amiss until they receive their monthly phone bill.

Secure Smartphones and Tablets

GFI Software recently released GFI VIPRE® Mobile Security Premium (http://www.vipremobile.com/upgrade), one of the most comprehensive mobile protection applications for Android phones and tablets. The app combines GFI Software's award-winning VIPRE antivirus technology with lost device features, parental controls and automatic backup capabilities. This powerful combination enables consumers to use their devices freely without having to worry about mobile viruses, identity theft, data loss or unsupervised activity. To learn more about GFI VIPRE Mobile Security Premium, visit www.vipremobile.com.

Top 10 Threat Detections for July

GFI's top 10 threat detection list is compiled from collected scan data of tens of thousands of GFI VIPRE Antivirus (http://www.vipreantivirus.com/) customers who are part of GFI's ThreatNet™ automated threat tracking system. ThreatNet statistics revealed that adware dominated the list, taking half of the top 10 spots.

| Detection | Type | Percent |
|---|---|---|
| Trojan.Win32.Generic | Trojan | 33.24 |
| GamePlayLabs | Browser Plug-in | 5.43 |
| Yontoo (v) | Adware | 2.47 |
| GameVance | Adware (General) | 2.95 |
| Intellidownload | Adware Installer | 1.01 |
| Wajam | Adware (General) | 0.98 |
| Worm.Win32.Downad.Gen (v) | Worm.W32 | 0.97 |
| Facetheme | Adware (General) | 0.95 |
| INF.Autorun (v) | Trojan | 0.86 |
| Virus.Win32.Sality.at (v) | Virus.W32 | 0.75 |

About GFI Labs

GFI Labs specialises in the discovery and analysis of dangerous vulnerabilities and malware. The team of dedicated security specialists actively researches new malware outbreaks, creating new threat definitions on a constant basis for the VIPRE home and business antivirus products.

About GFI

GFI Software provides web and mail security, archiving and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMB) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMBs, GFI satisfies the IT needs of organisations on a global scale. The company has offices in the United States, UK, Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold ISV Partner.

For more information:

GFI Software
Please email David Kelleher at dkelleher@gfi.com
GFI - Malta: Tel: +356 2205 2000; Fax: +356 21382419.
URL: http://www.gfi.com.

Davies Murphy Group
Please email Chris Green at gfi@daviesmurphy.com
Tel: +44 1256 807360