Cybercrime Hits Users at Home and On-The-Go in September, According to GFI Software

Submitted by: GFI Software
Tuesday, 9 October 2012

Users encounter spam and malware at every turn on social networking sites and mobile browsers

London, UK – 9 October 2012 – GFI Software™ today released its VIPRE® Report for September 2012, a collection of the 10 most prevalent threat detections (http://www.gfi.com/) encountered last month. In September, GFI threat researchers documented a number of cybercrime campaigns directed at users of various social networking sites including direct message spam (http://www.gfi.com/blog/twitter-video-facebook-app-rogue-dms-fake-flash-umbra-loaders/) on Twitter® and a phony Pinterest application (http://www.gfi.com/blog/fake-pinterest-app-homes-in-on-pinners/). Users of Android™ smartphones and tablets also encountered mobile malware under the guise of Grand Theft Auto® (http://www.gfi.com/blog/gta-vice-city-android-game-installs-sms-sending-boxer-variant/) and lingering Olympics 2012 (http://www.gfi.com/blog/the-olympics-are-over-fake-android-apps-are-still-going-for-gold/) applications.

“With the emergence of smartphones and widespread access to the Internet, today’s consumers have an ever-growing demand for constant, reliable connectivity at all times. However, constant connectivity to social networks, websites and email goes hand-in-hand with constant threats of malware, spam and phishing attacks,” said Christopher Boyd, senior threat researcher at GFI Software. “The convenience of being connected 24 hours a day requires constant vigilance if the user wants to keep their personal devices and sensitive information safe from cybercriminals.”

Many Twitter users received direct messages linking them to a phony login page for the “Twitter Video” application on Facebook. Users who entered their Twitter account credentials had their own accounts hijacked for direct message spam campaigns and were directed to download an Umbra Loader Botnet building tool disguised as a Flash Player update. Pinterest users looking for a way to quickly and easily view full-sized images without having to click through to individual pages were also targeted with the fake “Pin Photo Zoom” application which infected their system with adware.

Mobile users using Android devices continued to be at risk of downloading malicious programs last month including a fake “Results for the Olympics” application which sent premium text messages from the victim’s phone. Mobile gamers were also targeted with a phony Android version of the popular video game Grand Theft Auto: Vice City containing a Boxer Trojan disguised as a Flash Player.

Securing PCs and Mobile Devices
This month, GFI Software released VIPRE Antivirus 2013 (http://www.vipreantivirus.com/VIPRE-antivirus/) and VIPRE Internet Security 2013 (http://www.vipreantivirus.com/VIPRE-internet-security/) for PC users. Annual subscriptions for each product include threat definition updates, software upgrades, free tech support and a 100% money-back guarantee within 30 days of purchase. GFI Software also offers GFI VIPRE Mobile Security Premium (http://www.vipremobile.com/), one of the most comprehensive mobile protection applications for Android phones and tablets.

To learn more about VIPRE Antivirus 2013 or GFI Internet Security 2013, please visit

http://www.vipreantivirus.com or click here to download a free 30-day, full-featured trial.

To learn more about GFI VIPRE Mobile Security Premium, visit www.vipremobile.com.

Top 10 Threat Detections for September
GFI's top 10 threat detection list is compiled from collected scan data of tens of thousands of GFI VIPRE Antivirus customers who are part of GFI's ThreatNet™ automated threat tracking system. ThreatNet statistics revealed that adware took half of the top 10 spots this month.

Detection	Type	Percent
Trojan.Win32.Generic	Trojan	25.89
Yontoo(v)	Adware (General)	4.11
Trojan.Win32.Sirefef	Trojan	8.81
GamePlayLabs	Adware (General)	6.40
GameVance	Adware (General)	2.79
Wajam	Adware (General)	2.28
LooksLike.HTML.Blacole.a (v)	Trojan	1.05
Click run software (v)	Adware (General)	0.89
INF.Autorun (v)	Trojan	0.83
InstallBrain (fs)	Misc (General)	0.77

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, United Kingdom, 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 Janne Virtanen at gfi@daviesmurphy.com
Tel: +44 1256 807360