GFI Labs Observes Cybercriminals Targeting Users of Major Social Networking Sites in April

Submitted by: GFI Software
Tuesday, 8 May 2012

GFI® Software urges users to be vigilant as they browse for content on popular social networking sites

Clearwater, Fla. – May 8, 2012 – GFI Software today released its VIPRE® Report for April 2012, a collection of the 10 most prevalent threat detections encountered last month. In April, cybercriminals were seen exploiting users of major social networking sites including Facebook® (http://www.gfi.com/blog/facebook-profile-viewer-shenanigans/) , Twitter® (http://www.gfi.com/blog/spam-leads-to-exploits-and-fake-av-on-twitter/), Tumblr® (http://www.gfi.com/blog/tumblr-tublr/) and Pinterest (http://www.gfi.com/blog/pinterest-visa-giftcard-spamrun-on-twitter/) in order to spread malware and spam surveys.

“In the same way that the popularity of social networking sites makes them a widely accepted tool for businesses to reach customers and elevate brand awareness, it also appeals to cybercriminals seeking a large pool of captive users to be targeted for malware and spam attacks,” said Christopher Boyd, senior threat researcher at GFI Software. “Established sites like Facebook and Twitter have long been a breeding ground for new cyber-attacks, but now we are seeing scammers taking an interest in the popularity of newer sites like Pinterest in order to catch victims off guard and trick them into clicking on something they shouldn’t.”

Twitter users were the quarry of cybercriminals looking to distribute fake antivirus (http://malwareprotectioncenter.com/) applications during a particularly vicious spam run, which tweeted a link labeled “must-see” from numerous compromised accounts and spam-bots. Followers unlucky enough to click on the links were directed to a site infected with a fake antivirus program. Once installed, the program constantly alerted users that their machine was infected and requested payment to clean up the system. The next day, additional links used the Blackhole exploit kit to infect victims’ machines with malware before automatically sending them to a site that was hosting another scareware program called “Windows Antivirus Patch (http://malwareprotectioncenter.com/2012/05/07/how-to-remove-the-windows-advanced-user-patch-rogue/).”

Twitter was also used as a platform to take advantage of users on Pinterest, a social networking site which is rapidly gaining popularity. A spam campaign using the account “Pinterestdep” claimed to be offering Visa® gift cards to users willing to provide their opinions about Pinterest. Instead of being directed to a user feedback form, victims were sent to a site which required them to complete up to 11 reward offers and to refer three friends to do so as well. Scammers also took advantage of Tumblr users who mistakenly entered “Tublr” into their web browser when attempting to access the popular micro-blogging site and redirected them to a message that claimed the victim had been selected as a “daily winner.” Like the scam on Pinterest, the victim was then asked to fill out surveys or complete other offers in order to claim the prize.

In a rehash of a popular lure used previously on Facebook and MySpace, scammers tricked users into installing a fake application which promised to show them a list of people who had viewed their profile.

The application did little more than tag the victim’s friends in a spam image in order to spread the fake application among their network and serve them with surveys that generate affiliate cash for the scammer.

“With countless studies being released which point to the regularity with which users are visiting their favorite social networking sites, it should come as no surprise that cybercriminals see these sites as prime targets for their attacks as they look to reach as many people as possible,” continued Boyd.

Top 10 Threat Detections for April

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 Trojans remained the most used attack method in April 2012, taking four of the top 10 spots.

Detection	Type	Percent
Trojan.Win32.Generic	Trojan	31.78
Trojan.Win32.Fakealert.cn (v)	Trojan	3.04
Yontoo	Adware	2.58
GamePlayLabs	Browser Plug-in	4.24
INF.Autorun (v)	Trojan	1.25
Worm.Win32.Downad.Gen (v)	Worm.W32	1.14
Trojan.Win32.Ramnit.c (v)	Trojan	1.11
GameVance	Adware (General)	1.04
iBryte	Adware (General)	0.99
Virus.Win32.Sality.at (v)	Virus.W32	0.92

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 Janne Virtanen or Martin Brindley at gfi@daviesmurphy.com
GFI – UK: Tel: +44 1256 807 360

Disclaimer

To the best of our knowledge, all details were correct at the time of publishing; this information is subject to change without notice