AVG Community Powered Threat Report for Q1 2012 – Executive Summary

The quarterly AVG Community Powered Threat Report for Q1 2012 was released on 27 April.

Key Points – Q1 2012

- Consumers are going mobile and so are cyber criminals. Social media platforms accessed via mobile devices have become hugely popular and cyber criminals have realized that through social networks, they can reach a large number of potential victims that can be converted into profitable source of income. A quick way to generate high revenue is by using malware which is designed to send text messages to premium rate services. Android, with its significant market share, is the main target for cyber criminals but, across the board, social networks are an increasingly popular avenue of attack.

- Cyber criminals are adopting an increasingly professional attitude by marketing of 'commercial' crimeware kits. These kits are available to purchase online and effectively give anyone the tools to become a cyber criminal.

- This quarter, other commercial crimeware kits lost market share to the most advanced crimeware offering, the Blackhole exploit kit. Its creators are using a 'planned obsolescence' business model to guarantee their income stream and to reduce the effects of piracy.

About the report

The AVG Community Protection Network is an online neighborhood watch, where community members work to protect each other. Information about the latest threats is collected from customers who participate in the product improvement program and shared with the community to make sure everyone receives the best possible protection.

The AVG Community Powered Threat Report is based on the Community Protection Network traffic and data collected from participating AVG users over a three-month period, followed by analysis by AVG. It provides an overview of web, mobile devices, spam risks and threats. All statistics referenced are obtained from the AVG Community Protection Network.

AVG has focused on building communities that help millions of online participants support each other on computer security issues and actively contribute to AVG's research efforts.

Q1 2012 Top Trends and Insights from AVG Threat Labs

Mobile Threats – Increase Use of Social Networks to Infect Android Devices

The trend of malware targeting Android devices continues to grow, with social networks in particular becoming an important attack vector.

- There are over 300 million Android phones already activated and over 850,000 phones and tablets are added per day[1].
- Twitter has more than 140 million active users[2], Facebook has over 845 million users[3] and, as reported by comScore[4], 34% of mobile users access social networking sites or blogs.

Cyber criminals know their audience, know what people are looking for and take advantage of it by posting tweets with links to malicious sites that include popular keywords. For example, if they see that many mobile users are searching for news, the content of the tweets will be changed accordingly.

Mobile devices are easier to monetize so they are a popular target for cyber criminals. It can therefore be expected that the combination of social networks and mobile platforms will be an attractive target for cyber criminals to launch attacks. Mobile devices are increasingly used to access news and social networks. This makes this an increasingly lucrative way to attack mobile users. Examples of how this works include:

- Facebook: all it takes for a cyber criminal to attack is to set up a fake profile which downloads malware to a device and randomly invites Facebook users.
- Twitter: a cyber criminal creates a spam profile and then posts tweets containing shortened hyperlinks to malware using trending hashtags. The way in which Twitter works makes sure the tweet appears on the top of many people's Twitter feed.

Web Threats – "Planned Obsolescence" as a Business Model of Blackhole Crimeware

AVG research shows that the Blackhole toolkit was most popular and the toolkit of choice for cyber criminals, with AVG research showing that on average 70 per cent of attacks were performed by variants of Blackhole.

Blackhole is a sophisticated and powerful exploit kit, mainly due to its ability to adapt (it is polymorphic) and in that its code being heavily concealed (obfuscated) to evade detection by anti-malware solutions. These are the main reasons it has a high success rate.

---

[1] https://plus.google.com/u/0/112599748506977857728/posts/Btey7rJBaLF
[2] http://blog.twitter.com/2012/03/twitter-turns-six.html
[3] http://newsroom.fb.com/content/default.aspx?NewsAreaId=22
[4] http://www.comscore.com/Press_Events/Press_Releases/2012/3/comScore_Reports_January_2012_U.S._Mobile_Subscriber_Market_Share

The AVG Q1 2012 Community Powered Threat Report key findings:

Web Threats	
Blackhole Exploit Kit	The most active threat on the Web, **43.55%** of detected malware
Blackhole	The most prevalent exploit toolkit in the wild; accounts for 39.4% of toolkits
45%	Percentage of exploit toolkits that account for 58% of all threat activity on malicious websites
10.6%	Percentage of malware uses external hardware devices (e.g. flash drives) as a distribution method (AutoRun)
Mobile Threats	
tp5x.WGt12	The most popular malicious Android™ application
360,000	Number of malicious events detected during Q1 2012
Messaging Threats (Spam)	
United States	The top spam source country
48.3%	Number of spam messages originated from the USA, followed by the UK with 9.7%
Facebook.com	The top domain in spam messages
English	The top language used in spam messages (69.3%)

###

Download the full Q1 2012 Community Powered Threat Report at:
www.avg.com/filedir/news/AVG_Community_Powered_Threat_Report_Q1_2012.pdf