AVG Community Powered Threat Report

Q1 2012

Contents

Introduction

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 Highlights

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%)

Key Points – Q1 2012

Consumers are going mobile and so are cyber criminals; social media platforms on mobile devices have become hugely popular and cyber criminals are waiting around the corner. Cyber criminals watch the trends closely and adjust their attack methods accordingly.

- Cyber criminals have realized that through social networks, they have access to a large number of potential victims that can be converted into a considerable amount of income.
- A quick way to generate substantial revenue is by using malware which is designed to send text messages to premium rate services. Android™, with its significant market share, is the clear focus for cyber criminals.
- Cyber criminals are adopting an increasingly professional attitude through the marketing of 'commercial' crimeware kits.
- Other commercial crimeware kits lost market share to the most advanced crimeware, the Blackhole exploit kit.

The main stories spotted by AVG Threat Labs during Q1/2012 were:

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 on average 70 per cent of attacks performed by variants of Blackhole. Blackhole is a sophisticated and powerful exploit kit, mainly due to its polymorphic nature, and it is heavily obfuscated to evade detection by anti-malware solutions. These are the main reasons why it has a high success rate.

Blackhole's creators 'commercialized' their product by providing a subscription-based service. The people who purchase the Blackhole exploit kit from the creators are criminals themselves and will try to recover the cost by selling it on to others. However, Blackhole's creators have found a unique way to keep the money stream by releasing many updates to paying customers only and, along the way, reducing the numbers of non-paying customers.

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

The trend of malware targeting Android devices continues to grow, with social networks becoming an important attack vector. There are over 300 million Android phones already activated (over 850,000 phones and tablets per day[1]). Meanwhile, Twitter® has more than 140 million active users[2], Facebook® has over 845 million users[3] and, as reported by comScore[4], 34 per cent of mobile users access social networking sites or blogs. Because mobile devices are easier to monetize they are a popular target for cyber criminals. So it is to be expected that the combination of social networks and mobile platforms will be used by cyber criminals to launch attacks.

In this report, we'll show examples of methods that use both Twitter and Facebook to lure device owners into installing malicious applications.

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. It appears that cyber criminals are tracking mobile usage trends, and if they see that many mobile users are searching for news, for example, the content of the tweets will be changed accordingly. In the EU's five biggest markets (France, Germany, Italy, Spain, United Kingdom), smartphone owners accessing news sites via an application or browser at least once a month increased 74 per cent to 39.5 million during the three-month average ending January 2012[5].

[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
[5] http://www.comscore.com/Press_Events/Press_Releases/2012/3/Number_of_European_Smartphone_Users_Accessing_News_Surges_74_Percent_Over_Past_Year

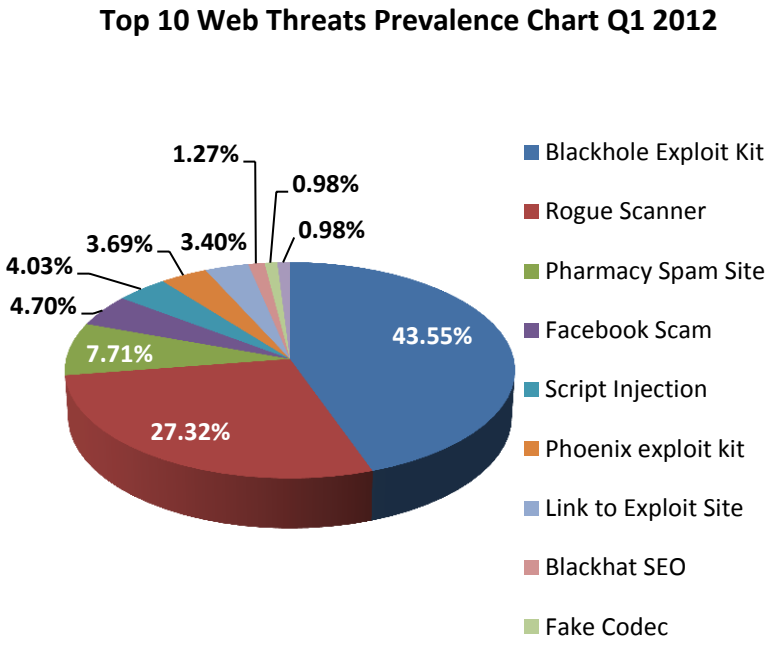
Quarterly Key Metrics: January-March 2012

Metrics - Web Threats

Top 10 Web Threats Prevalence Table Q1 2012

This prevalence table shows the top web threats as reported by the AVG community

Blackhole Exploit Kit	Pages containing script code characteristics of the Blackhole exploit kit which is used to install a range of malware
Rogue Scanner	Pages containing fake virus scanners, or appear to be pages pushing fake antivirus products. Such pages intend either (or both) to lure end user to buy worthless software, or to install malware under the cover of seemingly useful software
Pharmacy Spam Site	The Pharmacy Spam sites appear to be legitimate online pharmacies, but usually are facsimiles of real sites. These fake pharmacies often supply generic, or even fake, drugs rather than the brands advertised, and reportedly often deliver no drugs at all
Facebook Scam	A scam targeting users of Facebook
Script Injection	Injection of code by an attacker, into a computer program to change the course of execution
Phoenix Exploit Kit	Exploit toolkit which is used to install a range of malware
Link to Exploit Site	These pages contain links to known exploit sites. In some cases, malicious code is automatically downloaded without any user intervention
Blackhat SEO	Unethical or frowned upon Search Engine Optimization techniques
Fake Codec	An attempt to trick users into installing malware by suggesting they need to install a codec to watch a particular video
Invisible IFrame Injection	Malicious code injected into legitimate sites but invisible to normal users

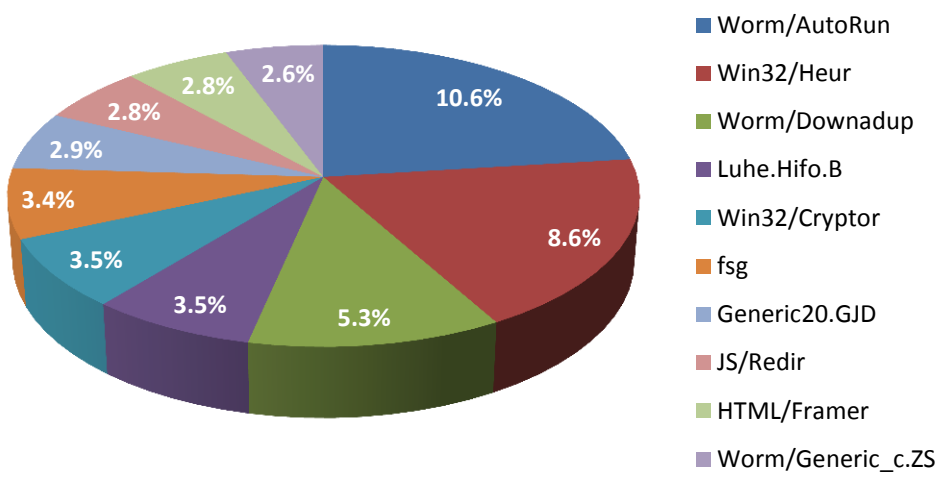


Top 10 Malware Threats Prevalence Table Q1 2012

This table presents top traditional malware as detected by AVG Threat Labs

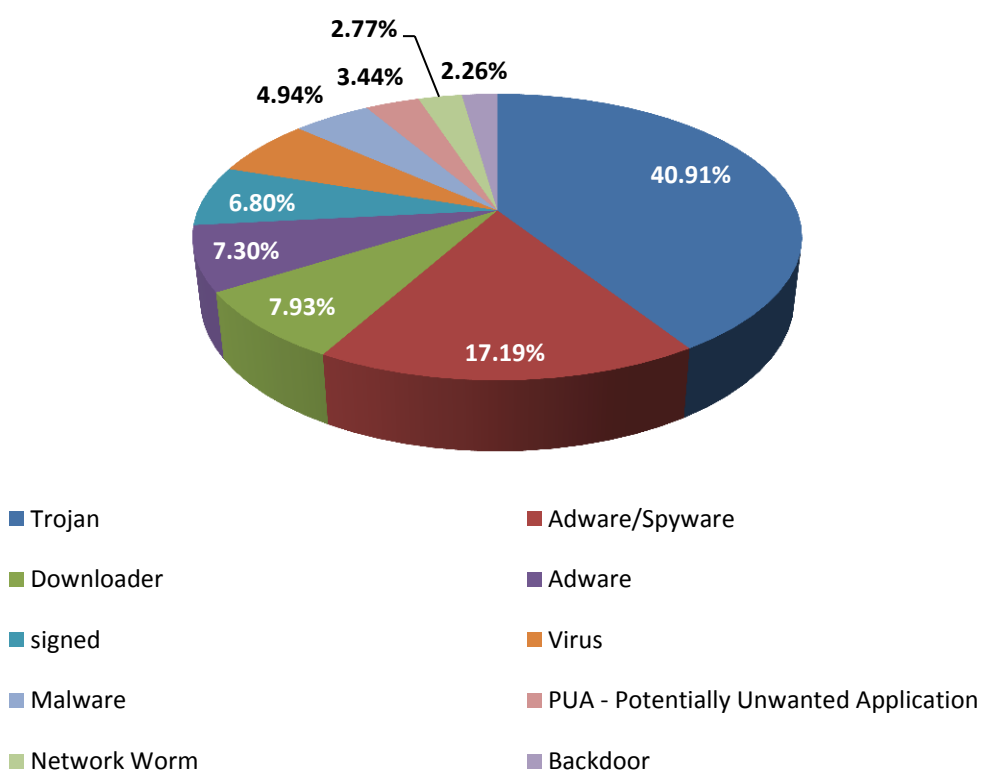
Worm/AutoRun	10.6%
Win32/Heur	8.6%
Worm/Downadup	5.3%
Luhe.Hifo.B	3.5%
Win32/Cryptor	3.5%
Fsg	3.4%
Generic20.GJD	2.9%
JS/Redir	2.8%
HTML/Framer	2.8%
Worm/Generic_c.ZS	2.6%

Top 10 Malware Prevalence Chart Q1 2012



Behavior Categories Chart Q1 2012

This table presents threats prevalence as detected by the patent-pending technology in AVG's Identity Protection engine. Using various classifiers and advanced algorithms, this technology determines the hostile behavior of files and prevents their execution



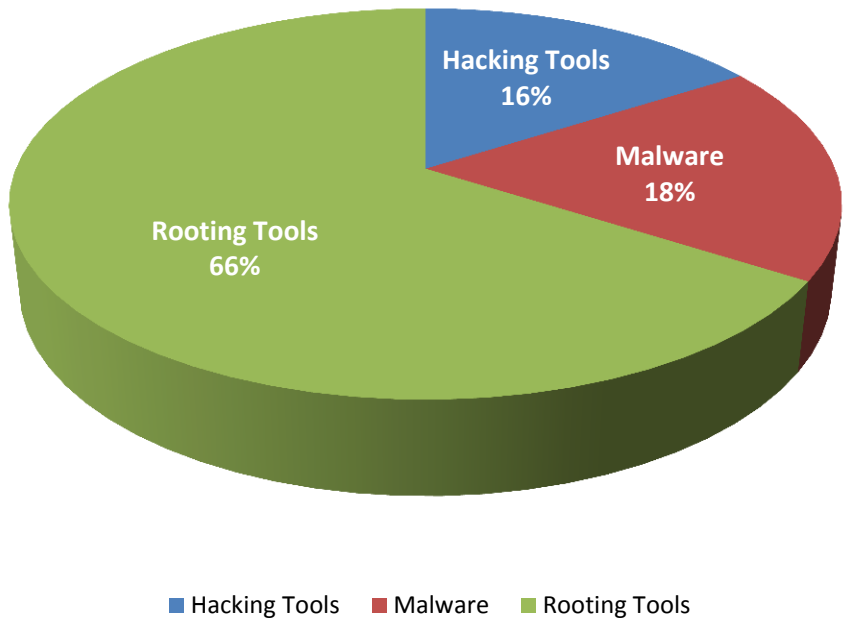
Top Exploit Toolkits Seen in Q1 2012

These metrics present the top five exploit toolkits in terms of malicious web activities. Criminals are increasingly utilizing toolkits to carry out cyber attacks. In many cases, using these attack toolkits does not require technical expertise

1	Blackhole	39.4%
2	Phoenix	32.6%
3	Fragus	18.5%
4	Seosploit	8.2%
5	Bleeding Life	1.2%

Metrics - Mobile Threats

Distribution of Android Threats Q1 2012



Metrics - Email Threats

Top Domains in Spam Messages Q1 2012

Top domains used in spam messages

1	No domains in message	18.5%
2	facebook.com	6.8%
3	twitter.com	4.9%
4	gmail.com	2.6%
5	yahoo.com	2.4%
6	hotmail.com	2.2%
7	chtah.com	2.0%
8	emv3.com	1.7%
9	linkedin.com	1.7%
10	doubleclick.net	1.5%

Top 5 Languages in Spam Messages Q1 2012

Top languages used in global spam messages

1	English	69.3%
2	Portuguese	7.5%
3	French	5.2%
4	Dutch	3.1%
5	German	2.4%

Top Countries of Spam Senders Q1 2012

Top spam source countries

1	United States	48.3%
2	United Kingdom	9.7%
3	France	5.3%
4	Germany	4.5%
5	Brazil	3.3%
6	Netherlands	3.1%
7	Australia	2.8%
8	Canada	2.2%
9	Italy	1.8%
10	South Africa	1.5%

Web Risks & Threats

Blackhole Exploit Toolkit

The Blackhole crimeware toolkit dominated the malware scene over the past year. From the moment it appeared, it quickly gained 'market share'. As AVG presented in our reports at that time, Blackhole's market share in the global malware market is on average 35 per cent, and its market share among the crimeware toolkits is on average 70 per cent. Blackhole is a sophisticated and powerful exploit kit, mainly due to its polymorphic nature; it is heavily obfuscated to evade detection by anti-malware solutions.

A crimeware toolkit is a "commercial" software program that can be used by novices and experts alike to facilitate the launch of widespread attacks on networked computers. With the attack toolkit, the cyber criminals can easily launch an attack using pre-written malicious code that exploits a number of vulnerabilities in popular applications. These attacks often target un-patched security bugs in widely used products such as Adobe® Flash® Player, Adobe® Reader, Internet Explorer® and the Java Runtime Environment.

The ease of use and accessibility of these toolkits gaining popularity in recent years have opened the doors to more cyber criminals who would otherwise lack the required technical expertise to succeed in the cybercrime underground.

In the past, cyber criminals had to write their own malicious code from scratch, so the field was dominated by more technically savvy criminals. Quite quickly, they realized that they could 'monetize' their efforts by selling toolkits to less savvy individuals who would pay good money for them. The Blackhole creators have taken that commercialization one step further by ensuring users of the exploit kit need to keep paying the creators to receive the most recent and effective versions. The success of the kit lies in its straightforward user interface, sophisticated design, encryption, and seemingly successful marketing model. As a crimeware toolkit, Blackhole is developed and maintained by cyber criminals but sold just like legitimate software.

Blackhole and Vulnerable TimThumb Utility on WordPress sites

WordPress™ is a popular blogging tool and publishing platform. Free to install and use, WordPress is used by over 14.7% of the Internet's 'top 1 million' websites, according to Alexa, and, as of August 2011, manages 22 per cent of all new websites[6]. WordPress is currently the most popular Content Management System in use on the Internet[7] and has a large community of developers producing themes and plug-ins. Over the years, many WordPress installations have been vulnerable to compromises making it possible to serve malware to unsuspecting users[8].

At this point, we will discuss the TimThumb image utility. TimThumb is a simple, flexible PHP script that resizes images. The php script has a series of parameters passed to it through a query string. While TimThumb has found a home in WordPress themes, it is by no means limited to them; TimThumb can be used on any website to resize almost any image[9]. The reason that TimThumb poses a risk is because it writes files to a directory when it fetches images from a remote server and resizes them, and this directory can be accessed by the site's visitors and used to launch web attacks. TimThumb versions prior to 2.0 were included in many WordPress theme kits. These older versions do not correctly manage long file names or site names and provide an opportunity for cyber criminals to upload and execute a malicious piece of code in the cache directory by taking advantage of TimThumb flaw and using a Blackhole toolkit to exploit it.

TimThumb is important here because if vulnerability is fixed in the official code but that code is not updated in third-party plugins and themes, the vulnerability persists on many WordPress installations. Many WordPress users are customizing their themes and therefore using external plug-ins and scripts; consequently, TimThumb has become widely distributed. The majority of WordPress sites are maintained by ordinary users, not by security experts, and those users do not necessarily have the skills to analyze compromised machines and to diagnose the problem. Moreover, a piecemeal approach by replacing one file that appears to be compromised may not fix the problem. A thorough approach would include a backup of the content database, removal of the entire site, installation of the latest WordPress version with *only* the needed plug-ins.

It is recommended WordPress users follow these security measures:

- Install updates promptly
- Backup database and files regularly (especially the .htaccess file)
- Run through one of the WordPress security checklists
- Install a security-checking plug-in, available from WordPress, to remove unnecessary files (such as sample sites and test files)
- Strengthen passwords (especially the admin) and change default ones (especially the admin)
- Use the "limit login attempts" plug-in
- Prevent the disclosure of the WordPress version number with the functions.php file of the theme
- Do not use FTP for access; use SSL to connect with the dashboard
- Do not allow guests to post content
- Do not allow guests to register (settings tab -> 'membership' area -> uncheck 'anyone can register')
- Use the .htaccess file to disallow directory listing and limit access to the wp-config.php file
- Ban undesirable users and bots with a 'deny' entry in .htaccess
- WordPress can use shared databases, which creates a security exposure; create a database just for WordPress, limit access to SQL commands and create a strong database password

[6] http://techcrunch.com/2011/08/19/wordpress-now-powers-22-percent-of-new-active-websites-in-the-us/
[7] http://en.wikipedia.org/wiki/WordPress
[8] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wordpress
[9] http://www.binarymoon.co.uk/2010/08/timthumb/

The Dominance of Blackhole in the Exploit Kit Scene

The Blackhole kit is sold on a subscription basis to customers who install it on malicious or compromised web sites to download a wide variety of malware onto victims' machines. Money drives this business model, and the customers purchase the Blackhole kit from its creators. These customers can then use it to make money themselves through credit card and banking frauds and by installing rogue security products or through ransomware and other payloads.

Blackhole is one crimeware toolkit among many others including: Phoenix, Fragus, SEOSploit, BleedingLife, Aurora, CRiMEPACK, Eleonore, NeoSploit, WebAttacker and more. AVG research shows that Blackhole is the most popular and widely used, and during 2011, achieved on average 70 per cent of attacks were performed by variants of Blackhole (Figure 2).

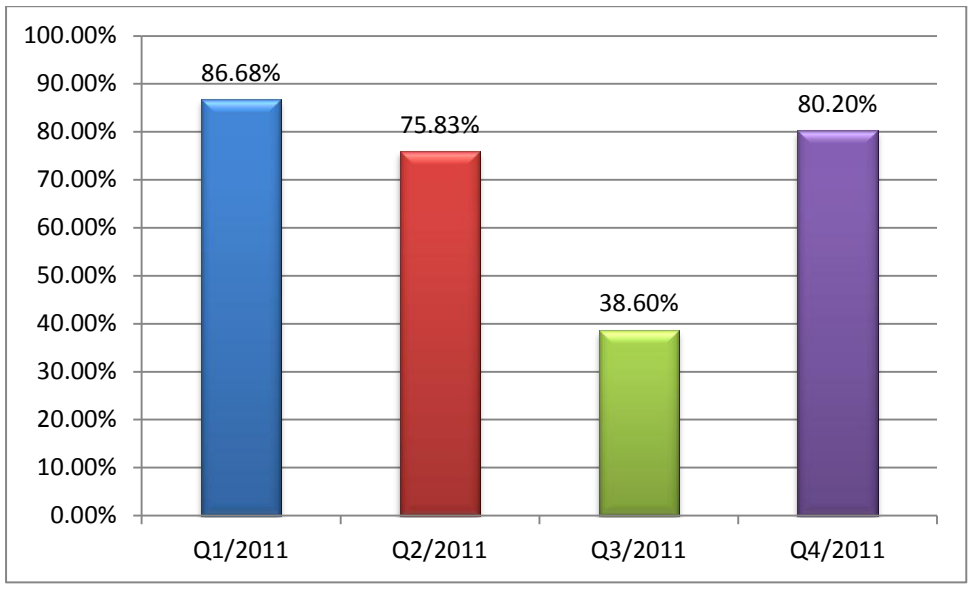


Figure 1 - Blackhole "Market Share" Among the Crimeware Toolkits

Blackhole came to the attention of researchers in January 2011, though it was already in circulation in late 2010 as samples of the code showed unique encryption techniques. Some of the values used in decrypting were derived from a formula based on the current date. Resulting values were used to decrypt a fairly unremarkable multisploit that used MDAC, malicious Java .jar files and malicious .PDF files.

Researchers found variants on public sites that would not work after the end of year 2010. From these samples, it was obvious that the Blackhole exploit kit was active at least as early as end 2010. The creators of older exploit kits clearly spent an enormous amount of time writing code to avoid detection as new numbered versions of the kits emerge every few months. Most disappear after a while, although the Phoenix exploit kit continues to circulate. Blackhole has been different, though, with fresh variants that started emerging at an accelerating rate at the beginning of 2011. By the autumn of 2011, researchers were seeing three to five new Blackhole variants each week.

The Blackhole Kit is mainly an encryption tool. It is designed using very odd though valid and predictable javascript to hide its workings. Initially, researchers saw Blackhole encryption hiding multiple exploits, like the older NeoSploit tool kit did (while it was active). Blackhole code would first try a MDAC-based exploit, then perhaps one based on Windows® Help, followed by an attack using a malicious .pdf and a Java .jar file with a malicious .class in it.

At one point, the Blackhole writers switched to code that obfuscates redirects to malicious servers. That strategy allowed injected Blackhole script to be hidden on compromised mainstream websites where, due to its size, it has more chances to escape notice. Most recently (as explained above), AVG Threat Labs have detected numerous sites using WordPress blogging software infected with Blackhole. WordPress tool scripts have been injected with relatively small Blackhole encrypted scripts, when decrypted they redirect to sites that serving malware.

'Planned Obsolescence' as a Business Model

Due to the illegality of the practice, it is reasonable to assume that the Blackhole creators expect some of their customers to redistribute or resell copies of the tool kit that they purchased. This is akin to software piracy.

We cannot rule out the possibility that the Blackhole creators don't try hard to encrypt the exploit code. Decrypting Blackhole isn't particularly difficult for anti-virus researchers. The ease of decryption of the code by the security industry provide sort of 'planned obsolescence' of their product. Any version of the kit which is more than a few days old would be useless. This means that the creators can create a revenue stream from new versions, and they can release updates only to paying subscribers.

With the planned obsolescence business model, Blackhole creators are assuring themselves of a recurring stream of revenue from their subscribers.

Blackhole Ever Changing Attack Methods

The Blackhole exploit kit has used a wide range of vulnerabilities to install itself and do its work. Below is a list of exploits the Blackhole admin panel records in order to show how successful infections rates. As you can see, the Java exploits have a better rate of infecting a victim's computer (Figure 3). Each version includes a different set of un-patched vulnerabilities (Figure 4).

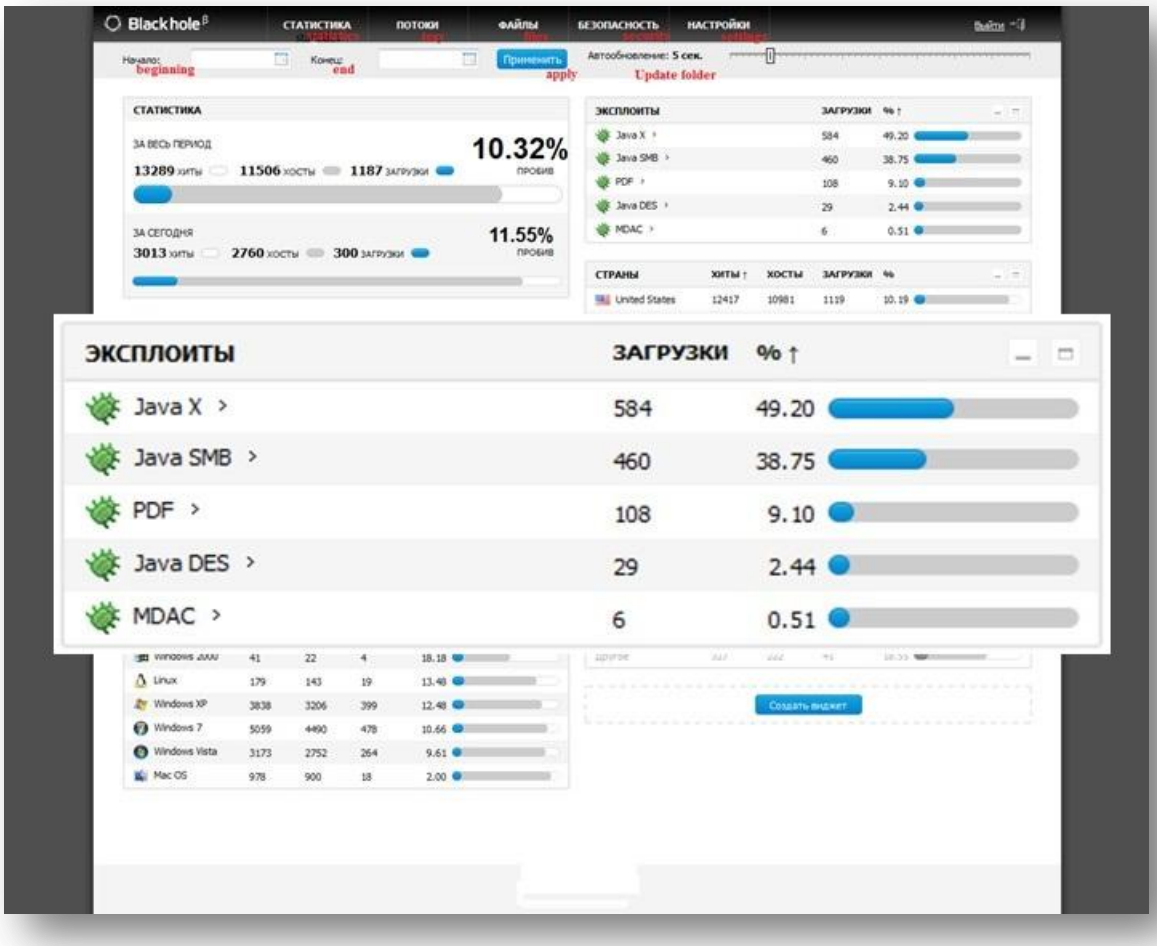


Figure 2 - Blackhole Admin Panel

September 2010	February 2011 Version 1.0.0	August 2011 Version 1.1.0	December 2011 Version 1.2.1	February 2012 Version 1.2.2
Java X	Java X	JAVA SKYLINE	Java Rhino	Java Pack
PDF	Java SMB	Java OBE	MDAC	PDF LIBTIFF
Java DES	PDF	PDF LIBTIFF	PDF ALL	PDF ALL
Java SMB **MDAC**	Java DES	Java Trust	PDF LIBTIFF	HCP
	MDAC	PDF ALL	HCP	MDAC
		Java SMB	Java OBE	FLASH

Figure 3 - Blackhole Targeted Zero Day Vulnerabilities

An analysis of Blackhole's malicious mechanisms and encryption in the last year shows a steady change of techniques that its creators have used to evade detection and analysis by security researchers and to infect victim machines:

February, 2011

- Loads a .jar without trying to hide it
- Contains a multisploit (in cyphertext) containing an MDAC, PDF and possibly a SWF exploit. The ciphertext is a comma-delimited list of character codes in a hidden textarea element. It uses document.getElementsByTagName("textarea") to access it. It also fetches "String.fromCharCode" from a stylesheet. These strategies are very familiar even a year later
- The "Page Is Loading" message isn't present yet
- The eval at the end is fairly easy to spot, despite eval being put in a variable "zmkvq". This makes decryption relatively simple
- The decrypted string is stored in the easy-to-spot variable named "s"

May 2011 (File: serpbe_net)

- The java exploit (.jar) is hidden in ciphertext
- The victim will see a 404 error page in his or her browser. Later it will display "Page Is Loading"
- The ciphertext is stored in a section in the page .html code instead of a <textarea>. It is still hidden
- Key-like information is stored in another , and a paragraph tag. All hidden from the user
- The decryptor script is formatted, making it easier to read and to identify the call to eval at the end (now "hidden" in a variable named"e")
- The decrypted string to execute is still stored in the file named "s"

August 2011 File: adenpshabvf_com

- The decrypt is mostly the same as May, with different URLs and names for the downloaded files
- Decryption is much simpler and easier to decode: the eval and ciphertext arrays are not hidden. The code writers simply call "eval(String.fromCharCode)" on the array, which isn't even in a variable. Decoding is trivial
- The code subtracts a variable named "z" (in this case 5) from every element in the array. This is clearly a move to thwart scanners, not decryptors

November 2011 File: kkkkkkkkkl_coom_in

- The fake 404 error message has been replaced with "Please wait while loading..." (see figure 5)
- There's a .jar file loaded plainly at the top of the page, not in the ciphertext
- An SWF exploit seems to have been added to the ciphertext
- The ciphertext array is within another array, within an object definition, but the eval is easier to spot than ever - literally 'window["eval"]'. The decryptor is still nicely formatted as well. The coders continue to make no effort to avoid decryption, just detection
- The creators also split "fromCharCode" into "fromCharCo"+"d"+'e', presumably to avoid a particular signature

March 2012 File: kmkndkbc_findhere_org

- The decrypt seems essentially identical to the one from kkkkkkkkkl_coom_in in November. Obfuscation has changed significantly
- The .jar file is loaded in the same way as November, though with different filenames
- The major difference in the code development is that the ciphertext (in a paragraph tag this time) is delimited by the character "p" instead of commas.
- The decryptor is slightly more complicated as a result, but still neatly indented
- The code writers are intentionally failing "try" statements to run code in the "catch" sections. This doesn't seem like it would slow decryption, but it makes new anti-virus scanner signatures necessary
- The code writers continue to split strings with quote-plus-quote

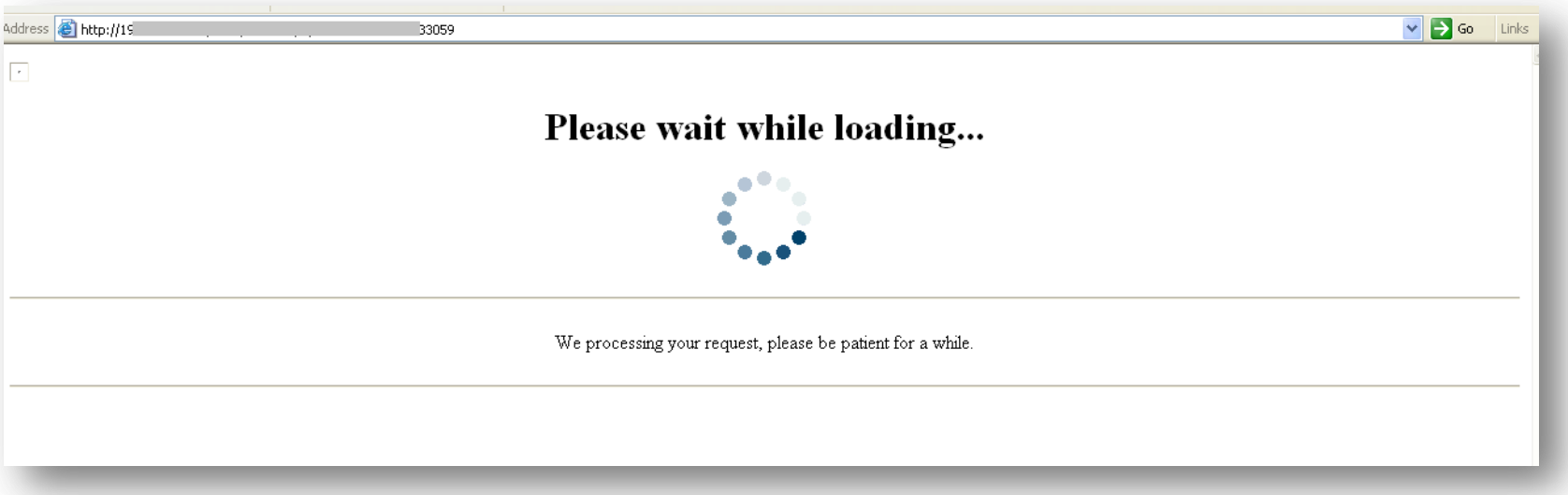


Figure 4 - Blackhole 11/2011 version

You can read more about Blackhole on AVG Threat Labs reports:

- http://blogs.avg.com/news-threats/avg-web-threat-update-week-12/
- http://blogs.avg.com/news-threats/weekly-threat-update-week-14/
- http://aa-download.avg.com/filedir/press/AVG_Community_Powered_Threat_Report_Q3_2011.pdf

Mobile Devices Risks & Threats

Android Malware is Spread via Facebook or Twitter

For malware authors, most users are an easy target; if you follow your target closely, you can predict its moves. Malware authors know how to catch users when they pay less attention or when they are too curious. This is why social engineering techniques are so powerful.

Malware authors follow trends and change their techniques accordingly. Therefore, the combination of smart phones and social networks have become a malware author's playground.

Recently, we have witnessed an increase in techniques used to spread malware among Android users via Facebook and Twitter applications.

How Facebook is Used to Spread Malware

It is not uncommon to receive a friend request on Facebook from people we don't know. As the proverb states 'curiosity killed the cat', curiosity is a human nature which is taken advantage by the malware's authors.

Even if we don't know that person, curiosity takes over, and we are tempted to know more about this specific person. But one errant click and the malicious application gets downloaded to our Smartphone. However, the malicious application is downloaded but not automatically installed, which is especially dangerous for the novice user who does not check permissions before installing an application. The malware's authors can then trick these users into installing the application (Figure 6). As said above, the malware authors know exactly what the 'victim' will do next and just wait around the corner.

In this specific case, the link to the malware web page was included in the requestor's Facebook profile, the first place to look for more information about the requestor. When clicking on the link, it redirects the browser to a website that automatically downloads an application to the Android device. After the application has been installed by the user, it can send text messages to premium rate services. The downloaded application pretends to be a legitimate opera browser.

Figure 5 - Automatic Application Download

How Twitter is Used to Spread Malware

The method selected by malware authors is simple; they create many bogus Twitter accounts. Using these accounts, malware authors post multiple tweets (figure 8) using a combination of URL shortening services and a use of popular keywords which combined, direct to malicious sites. Popular keywords or hashtags are used to categorize a message (tweet) like #Iran, #Egypt or popular topics like porn, diet, computers, mobile etc.

When a victim searches for information on one of these popular topics, they can potentially infect their mobile devices with malware since, unlike search engine results, the most recent tweets appear at the top of the search results. Cyber criminals do not have to invest in SEO, for that matter.

When clicking on the link, the victim is redirected to the malicious website. This website contains a malicious Android application which in some cases is being automatically downloaded to the victim's device and in other cases, disguises itself as a legitimate application such as Opera Mini browser and lures the victim to download and install the application. These applications send SMS or call to premium rate services.

It is hard for a novice user to figure out which links are malicious since the links are masked behind URL shortening services.

Below is an example of a Twitter account spreading malware (Figure 7):

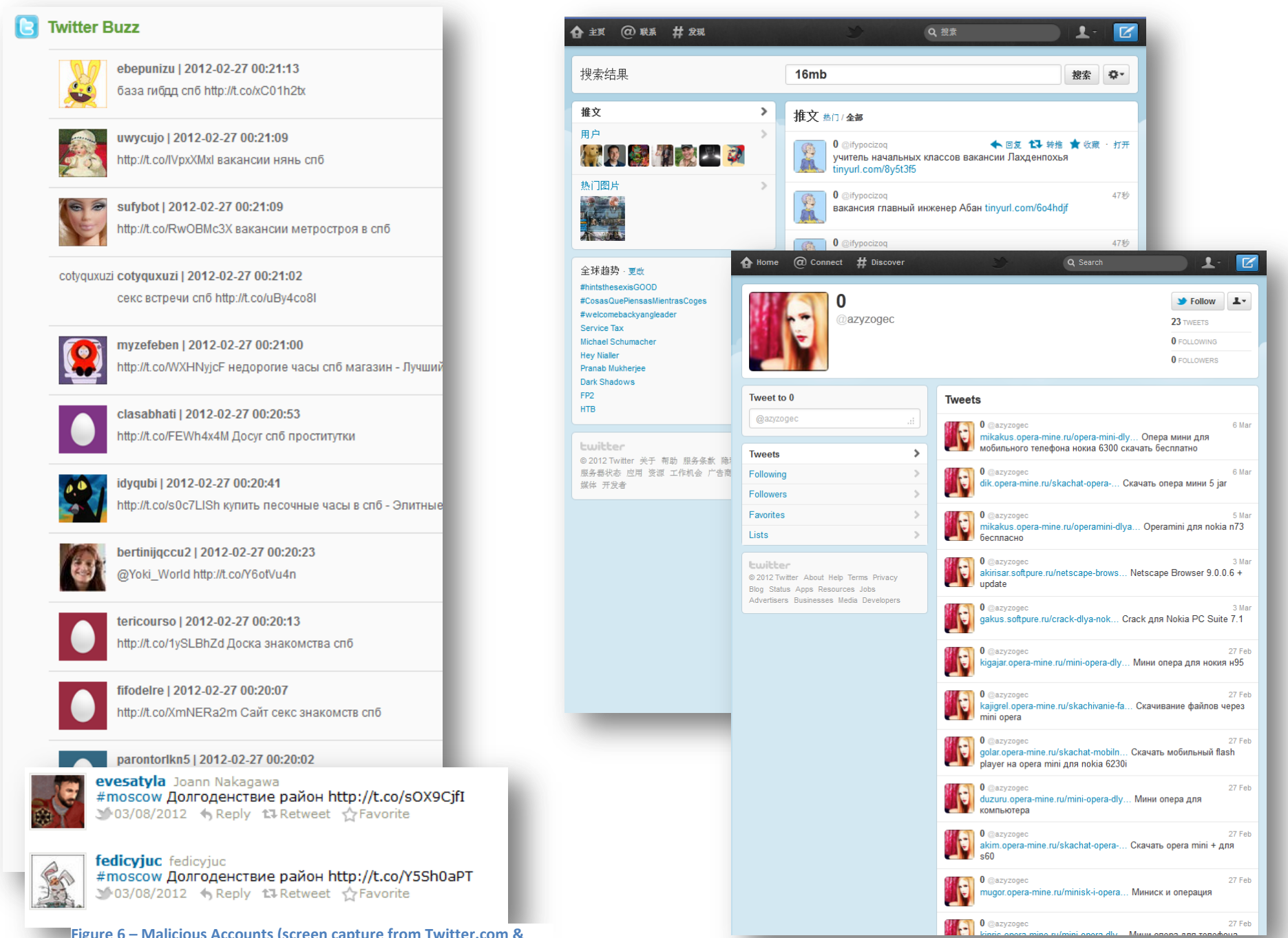


Figure 6 – Malicious Accounts (screen capture from Twitter.com & Topsy.com)

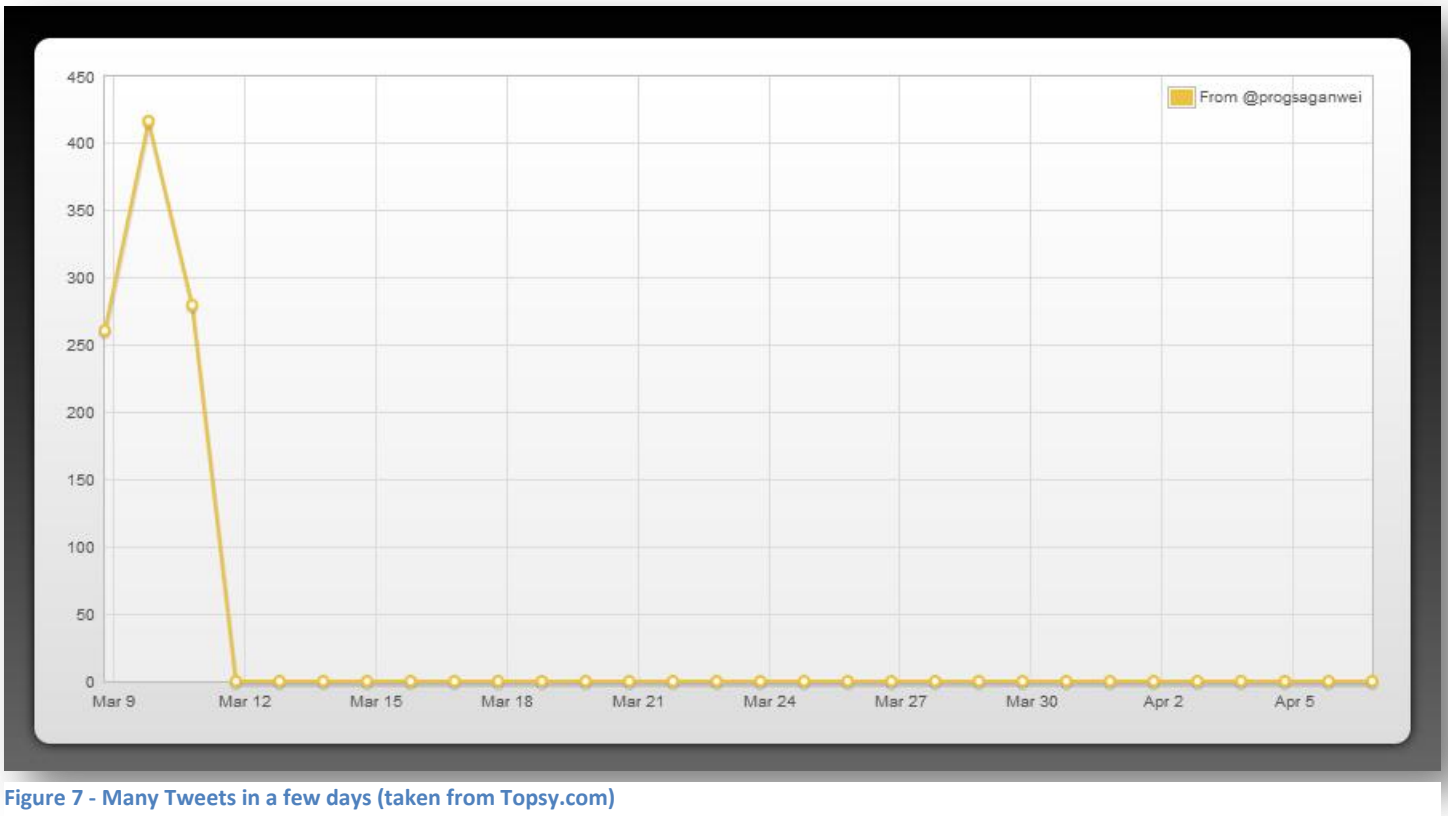


Figure 7 - Many Tweets in a few days (taken from Topsy.com)

Recommendations:

- Prior to installing any application, carry out a background check on the developer and the application, especially when downloading it from Android markets other than the official Google Play™.
- When installing new apps to your Android device, always look at the permissions application requests to approve and make sure the list seems appropriate.
- Only download apps from trusted application stores, sites and developers, and always check the app's star rating, developer information and user reviews to make sure you know what you are downloading.
- If you receive a Facebook invitation from a person you don't know, don't be tempted but treat it with suspicion.
- Twitter background check prior to clicking on any link:
    - Usually bogus Twitter users do not have any followers.
    - Usually they do send lots of similar tweets in a short period of time (few days).
- Set your Android device to download apps from Google Play only.
- Keep your device protected by installing an anti-virus application such as AVG Mobilation™.
- Discovered a spam account? Report it to Twitter[10].

[10] http://support.twitter.com/articles/64986-how-to-report-spam-on-twitter

Other reports from AVG Technologies

AVG and Ponemon Institute: 'Smartphone Security - Survey of U.S. consumers' – March 2011
http://aa-download.avg.com/filedir/other/Smartphone.pdf

Anatomy of a major Blackhole attack – March 2011
http://www.avg.com/filedir/other/blackhole.pdf

AVG Community Powered Threat Report Q1 2011 – April 2011
http://www.avg.com/press-releases-news.ndi-129

AVG Community Powered Threat Report Q2 2011 – June 2011
http://www.avg.com/press-releases-news.ndi-1563

AVG and Future Laboratories: 'Cybercrime Futures' – September 2011
http://www.avg.com/press-releases-news.ndi-1953

AVG and GfK: 'AVG SMB Market Landscape Report 2011' – September 2011
http://download.avg.com/filedir/news/AVG_SMB_Market_Landscape_Report_2011.pdf

AVG Community Powered Threat Report Q3 2011 – October 2011
http://www.avg.com/press-releases-news.ndi-2323

AVG Community Powered Threat Report Q4 2011 – January 2012
http://www.avg.com/press-releases-news.ndi-3723

About AVG Technologies (NYSE: AVG)

AVG's mission is to simplify, optimize and secure the Internet experience, providing peace of mind to a connected world. AVG's powerful yet easy-to-use software and online services put users in control of their Internet experience. By choosing AVG's software and services, users become part of a trusted global community that benefits from inherent network effects, mutual protection and support. AVG has grown its user base to approximately 108 million active users as of December 31, 2011 and offers a product portfolio that targets the consumer and small business markets and includes Internet security, PC performance optimization, online backup, mobile security, identity protection and family safety software.

www.avg.com