



Q3

2012

**AVG Community
Powered
Threat Report**

Contents

<u>Introduction</u>	2
Welcome to the AVG Technologies Q3 Community Threat Report	2
<u>Executive Summary</u>	3
Key points for Q3 2012	3
Q3 2012 Top Trends and Insights from AVG Threat Labs	4
Mobile Risks & Threats	4
Web Risks & Threats	5
The AVG Q3 2012 Community Powered Threat Report Top Trends	6
About the Community Threat Report	7
<u>Quarterly Key Metrics: July – September 2012</u>	8
Web Threats	8
Mobile Threats	10
Email Threats	11
<u>Part 1: Mobile Risks & Threats</u>	12
Mobile banking under attack	13
<u>Part 2: Web Risks & Threats</u>	15
‘Commercialised’ malware, the Blackhole Toolkit, continues its upwards trajectory	15
Social network users hit by bad ads	17
Hiding in plain sight – the Trojanization of an image file	18
Tricks of the cybercriminal trade	20
Czechs experiment with malware development	21
<u>Appendix</u>	22
Other reports from AVG Technologies	22
About AVG	23
About the AVG Community	23

Introduction



Welcome to the AVG Q3 Community Powered Threat Report

This quarter, we saw the continued rise of malware targeting mobile devices, especially those using the popular Android platform. In particular, mobile banking services were targeted with social engineering techniques that allow cybercriminals to circumvent the two-factor authentication process many banks have in place to secure their online banking services. The continuing prevalence of Blackhole Toolkit exploits was also noted this quarter, with several inventive campaigns providing security researchers with fresh challenges.

In our [Q2 Community Powered Threat Report](#), we discussed the creation of the first Android Rootkit and its potential to make Android-targeting malware more sophisticated. IDC figures now put the Android OS market share figure at 68.1%, nearly a ten percent increase on last quarter and we can see cybercriminals using social engineering malware to reach that expanding user base. In this case, the goal was to lure the bank account owner into revealing their password and credentials to install a Trojan on the mobile device which then intercepts all text messages, including those sent by the bank.

This is concerning because, according to a 2012 [PriceWaterhouseCoopers' report](#), digital banking is projected to become the norm globally by 2015. The malware we are seeing target existing m-banking users today is therefore only the tip of the iceberg compared to what we can expect to evolve, exploiting consumers who come new to online banking services.

'Commercial' toolkit, Blackhole, continues to rule the malware market with 63 percent market share. With the 'release' of Blackhole Exploit Toolkit 2.0 in September, we can expect in future months to see an upsurge in large-scale attacks. These will likely be more aggressive as a result of the new evasion techniques introduced in this latest version.

Finally, we also saw malware originating from the Czech Republic designed to install a Trojan to lock the user's desktop and then demanding a small sum of money to release it. Overall, however, this localized threat it was neither very innovative nor particularly successful.

I hope that you enjoy reading this quarter's Threat Report.

You can keep up to date with our regular threat bulletins on the [AVG News & Threats](#) blog.

Yuval Ben-Itzhak, CTO, AVG Technologies

Executive summary:

Q3 2012 Highlights



Key points for Q3 2012

The quarterly AVG Community Powered Threat Report for Q3 2012 was released on 24 October.

Mobile banking targeted for attack

- Zitmo, known as the “Man- in-the- Mobile” malware (aka Zeus-in-the-Mobile) is malware targeting online banking aiming to bypass the two-factor authentication process used by many online banking services globally. This report covers a new version of the Zitmo malware that was spotted recently.

Commercializing malware with the Blackhole Toolkit:

- Blackhole continues to rule the malware market with a 63 percent malware market share. Blackhole creators have ‘commercialized’ their product by providing a subscription-based service. The Blackhole toolkit is available to purchase online and effectively gives anyone the tools to become a cybercriminal.
- With the release of Blackhole Exploit kit 2.0 in mid-September 2012, we can expect to see new waves of large scale attacks come in our direction. These attacks will be more aggressive since new methods of evasion techniques were introduced in the latest version.
- Exploits include:
 - Social networks overwhelmed by malicious advertising from compromised ad servers
 - Seemingly normal graphics images containing malicious script
 - Tricks to trap experienced website owners and administrators

Executive summary:

Q3 2012 Highlights

With mobile banking projected to be the next big thing, we can expect to see increasing amounts of targeted malware in the next few years.

Q3 2012 Top Trends and Insights from AVG Threat Labs

Mobile Risks & Threats

Mobile banking under attack

Over the past 12 months, it appears that targeting mobile devices has been sufficiently lucrative for cybercriminals to make this a key focus for malware development. Cybercrime has evolved from digital vandalism for fun to digital burglary for financial gain. If stealing money is the objective, today's sophisticated smartphones make the ideal target. Mobile phones are usually tied into billing systems and therefore installing a piece of malware and sending one expensive premium SMS a week in the middle of the night can go unnoticed for a considerable period of time.

However, the increasing popularity of smartphones has given some criminals more ambitious goals. By installing malware on the phones of people who use internet banking, cybercriminals can steal large sums in a single transaction. By the time the victim becomes aware of the theft, their bank account could have already be emptied. This method of attack may sound familiar and that's because it was originally targeted to PC users; as consumers are shifting to use mobile devices to undertake the same activities they would previously have carried out on a desktop, so cybercriminals are shifting their malware over to mobile as well.

Earlier this year, PricewaterhouseCoopers [predicted digital banking will be the norm in 2015](#) and the [US Federal Reserve research](#) found that nearly 21 percent of mobile phone users have used mobile banking in the past 12 months. Moreover, among those consumers who do not currently use mobile banking, 11 percent reported that they will "definitely" or "probably" use mobile banking in the next 12 months. Strategy Analytics also released figures showing that in the third quarter of 2012, the number of smartphones in use worldwide [surpassed the 1 billion-unit mark](#) for the first time ever.

As mobile banking services evolve, so does the sophistication of cybercriminals, and this trend is an indication that the stakes are becoming increasingly high.

Executive summary:

Q3 2012 Highlights

Blackhole is effectively the first 'commercial' toolkit, accounting for 63 percent share of the malware market and 73 percent of the toolkits market.

Web Risks & Threats

'Commercialized' Malware, the Blackhole Toolkit, continues its upward trajectory

For those interested in becoming a sophisticated cybercriminal, the notorious Blackhole Toolkit seems to have been the kit of choice for the last few years. Available as a subscription-based service, Blackhole is effectively the first 'commercial' toolkit, so to speak, and now accounts for 63 percent of the malware market and almost 76 percent of the toolkits market.

Social network users hit by bad ads

In August, AVG Threat Labs identified an explosion of attacks using the notorious Blackhole Exploit kit that targeted popular social networks. The attack left users unable to log-on to their accounts or access any games or apps. Cybercriminals coordinated the attacks from multiple external advertising servers, which generated an exceptional increase from 250,000 attacks to over 1.6m recorded events within an eight hour period.

Hiding in plain sight – the 'Trojanization' of an image file

Malicious activity is obviously most successful if it goes unnoticed. And where better to hide the presence of malicious code from the system administrator by doing it in plain sight. This disturbing technique has been seen where normal graphics files – such as.gif, .jpg and .png – are effectively converted into Trojans. They still have their full original image functionality intact so the user doesn't suspect that, underneath, the file allows parsing malicious PHP scripts on their compromised server.

Tricks of the cybercriminal trade

The main problem that webmasters face is actually finding malicious code on the web page as often it is well hidden and can be easily missed. This quarter we look at the most recent examples of how cybercriminals obfuscate malicious code to ensure their ruses are successful.

Czechs experiment with malware development

This quarter, AVG security researchers noticed a local piece of malware in the wild called "Lock Screen" targeting Czech users. It was quite primitive in terms of technique and not very successful.

For the latest AVG news on threats, please visit:

<http://blogs.avg.com/news-threats/>

Executive summary:

Q3 2012 Highlights

~320,000 mobile threats detected during Q3 2012.

The AVG Q3 2012 Community Powered Threat Report Top Trends

Web Threats

Blackhole Exploit Kit	The most active threat on the web, 63.2% of detected malware
Blackhole	The most prevalent exploit toolkit in the wild, accounts for 75.8% of toolkits
49%	Exploit toolkits account for 49% of all threat activity on malicious websites
11.41%	Of malware are using external hardware devices (e.g. flash drives) as a distribution method (AutoRun)

Mobile Threats

extend.battery	The most popular malicious Android application
~320,000	Threats detected during Q3 2012

Messaging Threats (Spam)

United States	Is the top spam source country
41.7%	Of spam messages originated from the USA, followed by the UK with 7.9%
Facebook.com	Top domain in spam messages
English	Is the top language used in spam messages (65.65%)

Executive summary:

Q3 2012 Highlights

The AVG Community Protection Network is an online neighborhood watch, where community members work to protect each other.

About the Community Threat 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.

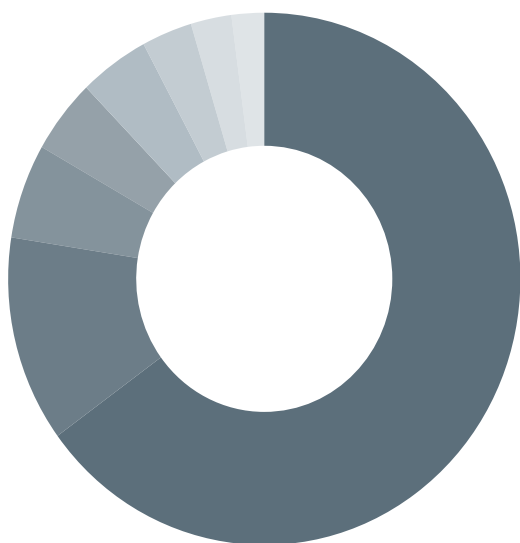
The AVG Community Powered Threat Report is based on the Community Protection Network traffic and data collected from participating AVG users over a three-month period, followed by analysis by AVG. It provides an overview of web, mobile devices, spam risks and threats. All statistics referenced are obtained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

Quarterly Key Metrics:

July – September 2012

Top 10 Web Threats Prevalence Chart Q3 2012



Blackhole Exploit Kit	63.2
Rogue Scanner	12.2
Redkit Exploit Kit	5.6
Parallels Plesk Panel compromise	4.4
Redirect to Rogue Scanner	4.3
Facebook Scam	3.1
Script Injection	2.5
Pharmacy Spam Site	2

Web Threats

Top 10 Web Threats Prevalence Table Q3 2012

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

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 the end user to buy worthless software, or to install malware undercover of seemingly useful software
Redkit Exploit Kit Detection	Exploit toolkit which is used to install a range of malware
Parallels Plesk Panel Compromise	Parallels Plesk Panel is website control panel software widely used by web hosting companies. The vulnerability was discovered in older versions (using plain text to store password data), and allows cybercriminals to extract all website account details
Redirect to Rogue Scanner	Injected code which redirect the visitor to a malicious site that tries to install Rogueware
Facebook Scam	Utilizing Facebook to scam people into revealing personal data (personal or financial data)
Script Injection	Injection of code by an attacker into a computer program to change the course of execution
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
Phoenix Exploit Kit	Exploit toolkit which is used to install a range of malware
Fragus Nulled Exploit Kit	Exploit toolkit which is used to install a range of malware

Quarterly Key Metrics:

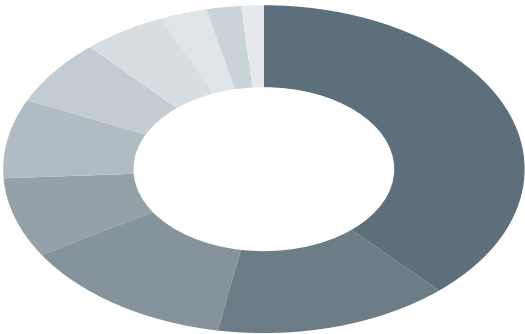
July – September 2012

Top 10 Malware Threat
Prevalence Table Q3 2012

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

Worm/Autorun	11.41%
Worm/Downadup	10.04%
Win32/Heur	9.84%
Win32/Cryptor	4.09%
HTML/Framer	3.17%
Worm/Generic_c.ZS	2.74%
Win32/Sality	2.6%
Generic20.GJD	2.61%
Crack.CO	2.41%
Win32/Virut	2.35%

Behavior Categories
Chart Q3 2012



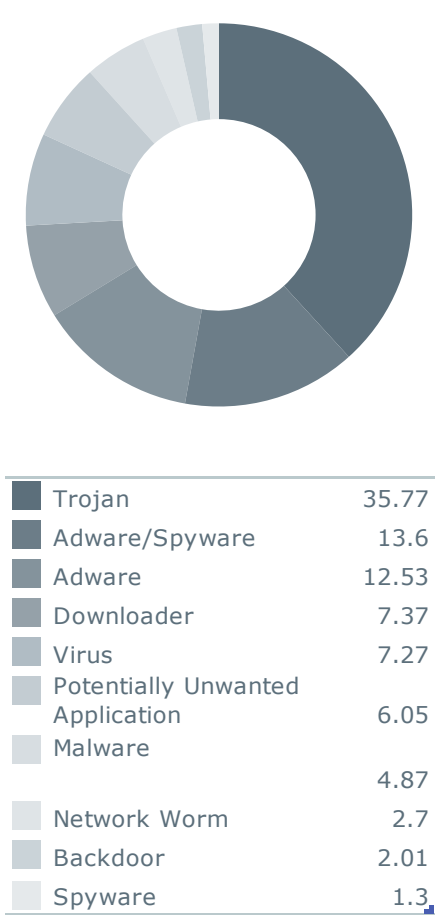
Trojan	35.77
Adware/Spyware	13.6
Adware	12.53
Downloader	7.37
Virus	7.27
Potentially Unwanted Application	6.05
Malware	4.87
Network Worm	2.7
Backdoor	2.01
Spyware	1.3

Quarterly Key Metrics:

July – September 2012

This table presents threats prevalence as detected by AVG's Identity Protection engine. This patent-pending technology looks at what the software does during execution. Using various classifiers and advanced algorithms, this technology determines the hostile behavior.

Behavior Categories
Chart Q3 2012



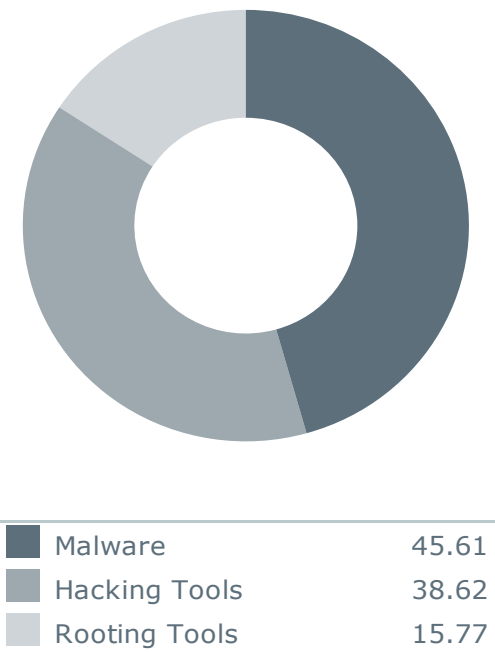
Top Exploit Toolkits Seen in Q3 2012

These metrics represent 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	75.77%
2	Fragus	12.16%
3	Phoenix	9.15%
4	Bleeding Life	1.15%
5	Seosploit	1.13%

Mobile Threats

Distribution of Android Threats Q3 2012 (%)













Quarterly Key Metrics: July – September 2012

Spanish is the second most used language in spam messages after English, which is most common.

Email Threats

Top Domains in Spam Messages Q3 2012

1		No domains in messages	9.0%
2		Facebook.com	4.8%
3		Twitter.com	3.2%
4		Bit.ly	2.0%
5		Gmail.com	1.6%
6		Hotmail.com	1.2%
7		YouTube.com	1.1%
8		Amazonaws.com	1.1%
9		t.co	1.1%
10		Linkedin.com	1.0%

Top 5 Languages Spam Messages Q3 2012

1		English	65.6%
2		Spanish	8.5%
3		Portuguese	5.9%
4		Dutch	3.2%
5		Chinese	2.6%

Quarterly Key Metrics: July – September 2012

The United Kingdom is the second most common spam source country after the United States, which continues to come top.

Top Countries of Spam Senders Q3 2012

1		United States	41.7%
2	m 	United Kingdom	7.9%
3		France	5.4%
4		Germany	4.4%
5		Brazil	4.1%
6		Australia	3.6%
7		Netherlands	2.7%
8		Canada	1.9%
9		South Africa	1.1%
10		Italy	1.0%

Part 1: Mobile Risks and Threats

It is now clear that some criminals have more ambitious goals. By installing malware on the phones of people who use internet banking, cybercriminals can steal large sums in a single transaction.

Mobile banking under attack

Over the past 12 months, it has become clear that targeting mobile devices has been sufficiently lucrative for cybercriminals to make this a key focus for malware development. Cybercrime has evolved from digital vandalism for fun to digital burglary for financial gain. If stealing money is the objective, today's sophisticated smartphones make the ideal target. Mobile phones are usually tied into billing systems and therefore installing a piece of malware and sending one expensive premium SMS a week in the middle of the night can go unnoticed for a considerable period of time.

However, the increasing popularity of smartphones has given some criminals more ambitious goals. By installing malware on the phones of people who use internet banking, cybercriminals can steal large sums in a single transaction. By the time the victim becomes aware of the theft, their bank account could have already be emptied. This method of attack may sound familiar and that's because it was originally targeted to PC users; as consumers are shifting to use mobile devices to undertake the same activities they would previously have carried out on a desktop, so cybercriminals are shifting their malware over to mobile as well.

Earlier this year, PricewaterhouseCoopers [predicted digital banking will be the norm in 2015](#) and the [US Federal Reserve research](#) found that nearly 21 percent of mobile phone users have used mobile banking in the past 12 months. Moreover, among those consumers who do not currently use mobile banking, 11 percent reported that they will "definitely" or "probably" use mobile banking in the next 12 months. Strategy Analytics also released figures showing that in the third quarter of 2012, the number of smartphones in use worldwide [surpassed the 1 billion-unit mark](#) for the first time ever.

So with mobile banking projected to be the next big thing, AVG expects mobile banking malware to be the next wave of malware.

As banking evolves, so does the sophistication of cybercriminals, and this threat is an indication that the stakes are increasingly high.

Part 1: Mobile Risks and Threats

In both scenarios, the user is now asked to provide his mobile phone number for "security reasons," and once this is provided, the cybercriminal can get to work.

Zitmo: a "Man-in-the-Mobile" Attack

Zitmo (aka Zeus-in-the-Mobile) is malware targeting online banking aiming to bypass the two-factor authentication process used by some online banking services. A new version of the Zitmo malware was spotted recently in which hackers extended the botnet commands they can send and receive from the infected device to their Command & Control. The user base targeted by hackers for this new attack was focused on Germany.

In this process, a Transaction Authentication Number (TAN) is used as a one-time password to authorize financial transactions. TAN is used as a second level of security on top of the traditional user and password which means that in order to perform the financial transaction, criminals need to obtain both the TAN and the user/password as holding just one of them is useless.

This mobile TAN (mTAN) system is used by banks in many countries including Austria, Germany, New Zealand, Russia, Spain, Switzerland, the United Kingdom, the United States and more. When the user initiates a transaction, a TAN is generated by the bank and sent to the user's mobile phone by SMS. The SMS may also include transaction data, allowing the user to verify that the transaction has not been modified in transmission to the bank¹.

Cybercriminals have already succeeded in obtaining online banking account information (e.g. username and password) with phishing or by luring users to access a malicious page which manages to download and install malware on the machine of an unsuspected user, such as 'Zeus on PC', for example. In both scenarios, the user is now asked to provide his mobile phone number for "security reasons," and once this is provided, the cybercriminal can get to work.

¹https://en.wikipedia.org/wiki/Transaction_authentication_number#Mobile_TAN .28mTAN.29

Part 1: Mobile Risks and Threats



Figure 1: The 'security

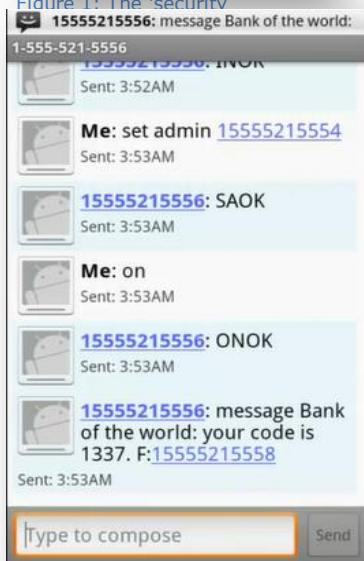


Figure 2: Hidden correspondence between attacker and user's phone

How Zitmo works

When Zitmo is installed, an SMS is sent from the user device to the Command and Control (C&C) device (the attacker) with SMS content 'INOK' to notify the attacker that there's a device with the Zitmo installed ready and active.

The attacker then sends an SMS command which tells the user's device to expect commands from the administrator. The SMS correspondence between the users and the attacker devices are hidden; the user knows nothing about it.

Command & Control gets approval that the victim device got his command (SAOK) and in response sends the command 'on' to the victim's device, telling it to intercept every incoming SMS and forward the incoming SMS to the C&C. C&C then receives a confirmation message back (ONOK).

When a user logs-in to the online banking and tries to perform a financial transaction, the bank sends mTAN to his mobile; this message will never be received by the victim's device but will instead be intercepted and forwarded to the attacker who then can perform any financial transaction from the victim's bank account to any other bank account.

Following an "off" message sent by the attacker, Zitmo stops intercepting SMS messages. The victim will now receive any message sent to him by the bank and other sources, but the damage is already done.

Part 2: Web Risks and Threats

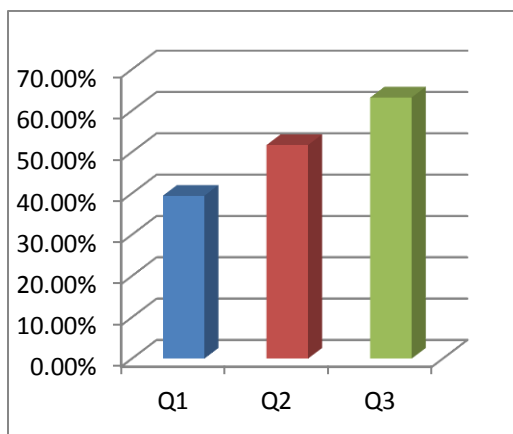


Figure 3: Blackhole malware 'market share' 2012

'Commercialized' Malware, the Blackhole Toolkit, continues its upward trajectory

For those who are interested in becoming a sophisticated cybercriminal, the notorious Blackhole Toolkit has been the kit of choice for the last few years. Available as a subscription-based service, Blackhole is effectively the first 'commercial' toolkit, so to speak, and now accounts for 63 percent of the malware market and almost 76 percent of the toolkits market.

Blackhole's creator, nicknamed 'Paunch', has further improved the toolkit with the release of version 2.0 in mid-September 2012, which includes a raft of new features and evasion techniques that will generate increasingly massive and aggressive attacks. This new version aims to fly under the radar of security researchers in order to prevent them from either getting hold of the new exploits or reverse-engineering the toolkit.

We will take a look at how some of these new features have manifested themselves recently and the risks they pose to unwary internet users.

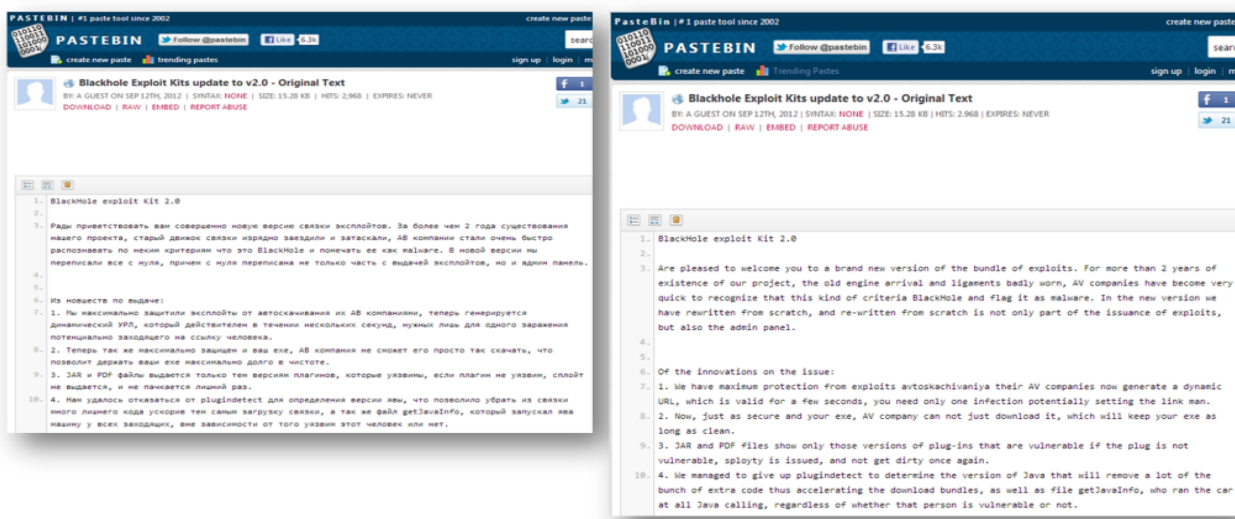


Figure 4: Blackhole 'launch' announcement on PasteBin

Part 2: Web Risks and Threats



Figure 5: Spike in Blackhole Exploit-based attacks

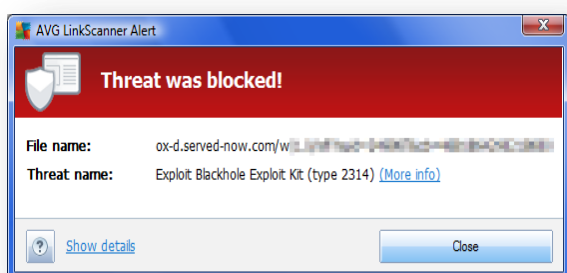


Figure 6: AVG LinkScanner Alert



Figure 7: Examples of some of the ads on legitimate web pages that had been tampered with by the cybercriminals

1. Social network users hit by bad ads

In August, AVG Threat Labs identified an explosion of attacks using the notorious Blackhole Exploit kit that targeted key social networks including Facebook. The attack left users unable to log-on to their accounts or access any games or apps. Cybercriminals coordinated the attacks from multiple external advertising servers, which generated an exceptional increase from 250,000 attacks to over 1.6m recorded events within an eight hour period.

The actual detections of the Blackhole Exploit Kit were a result of these malicious ads passed along by an advertising service which was appearing on Facebook's pages and those of other affected websites. The cybercriminals coordinating the attack had also designed some of their infected ads with graphical features, color and typefaces that imitated the style of the social network targeted.

The advertising server supplying the ads had been compromised by cybercriminals who installed the Blackhole Exploit Toolkit, whose code injects malicious JavaScript into pages served from the compromised web server. Typically, JavaScript associated with Blackhole grabs other malicious scripting from yet another server in order to compromise the security of web users visiting the site – this is known as a drive-by malware attack, which we discussed at length in our [AVG Q2 Community Threat Report](#). In this case, the compromised server provided the content of advertisements to various other web sites, delivering the intended ads plus the Blackhole exploit script.

No user intervention is required in order to trigger the malicious code in a drive-by scenario. Instead, simply visiting a page where such ads are displayed is enough. The malware binaries included bots and backdoors and were designed to lead to the installation of various nasty software pieces on the user's computer, enable identity theft or credit card fraud. One of the widest circulating ads was for a fake antivirus called 'Security Shield'.

Detecting and blocking such attacks require real-time web security technologies, like AVG LinkScanner that scans the oncoming web content before it is being served to the browser.

Part 2: Web Risks and Threats

This disturbing technique has been seen where normal graphics files – such as .gif, .jpg and .png – are effectively converted into Trojans.



Blackhole exploits also targeted website owners. Some of the recent methods spotted in the wild during Q3 left webmasters struggling to identify how their website was compromised and are outlined below.

2. Hiding in plain sight – the 'Trojanization' of an image file

Malicious activity is obviously most successful if it goes unnoticed. And where better to hide the presence of malicious code from the system administrator than in plain sight. The graphics files still have their full original image functionality intact so the user doesn't suspect that, underneath, the file allows parsing malicious PHP scripts on their compromised server.

Not only are ordinary users very likely not to notice anything, but even experienced system administrators can be easily fooled by this technique, making it likely for it to go undetected for a long period of time. Website owners should check their image files and not just their script files when their website is reported to be compromised.

Since server software must be reconfigured to allow the script interpreter to run the image files, it means that a script masquerading as an image is always the result of site compromise.

How the Trojanized image file works

The file is made up of three main function blocks but the first two only run if specific conditions are met. The third block is known as the 'fall through' process and deals with what happens if neither of the specifically checked conditions is met so is likely to be the most common functionality.

For example, this file is an icon of the US flag. The code preserves the Trojanized file's normal functionality through a web browser that requests a URL (in this case, [http://\[server\]/images/flag-icon-us.gif](http://[server]/images/flag-icon-us.gif)) which when referenced in pages on the compromised server, receives and therefore displays the correct image.

Part 2: Web Risks and Threats

[illegible]

Figure 8: PHP code of a Trojanized .gif file

We can also look at how the first two blocks function, if the right conditions are met.

The first block:

- This gives the cybercriminal the ability to check remotely (and almost invisibly) that their malicious image/script is in place. The script operates by testing to see if the request for the URL was accompanied by a cookie which is named 'a' and whose value is set to 'check'. If so, the script sends the 'content-type' HTTP response header set to 'text/plain' followed by the word 'alive'.
- The script then exits without running other code. If the Trojanized image has replaced the original image, the response won't be 'alive' but rather a stream of image data. As the image file is part of a regular web page, an administrator looking at server logs would not be surprised to see requests for the image file – this request would be considered normal, even commonplace.

The second block:

- This sends an HTTP 'content-type' response header but it is set to 'text/javascript' whose purpose is to inject a JavaScript element into the HEAD section of the web page that requested the URL. However, this URL looks like an image URL so why would JavaScript content be accepted and run by a web browser from what was presumably expected to be an image? It is not entirely unheard of but in most typical websites, it would not be standard to call an image via a URL with parameters such as JavaScript.

This gives a hint that something unusual is happening but may not stand out on casual inspection of the server logs; in fact, webmasters may just think that the antivirus product is showing a false position on normally harmless graphics files.

Part 2: Web Risks and Threats

Malicious code can be hidden from website owners through a number of simple techniques that aren't immediately obvious even to the experienced webmaster.

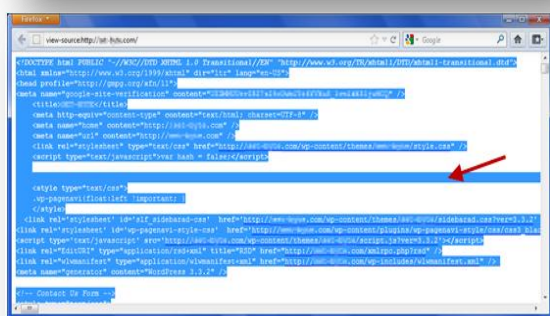
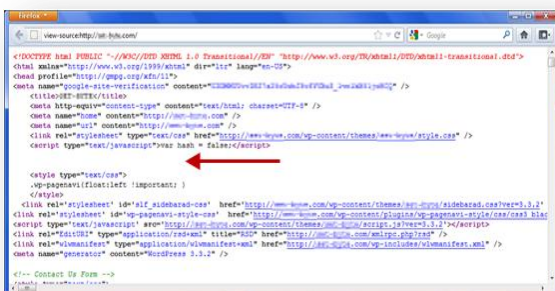


Figure 9: Revealing hidden malicious script

3. Tricks of the cybercriminal trade

The main problem that webmasters face is actually finding malicious code on the web page as often it is well hidden and can be easily missed. This quarter we look at three of the most recent examples of how cybercriminals obfuscate malicious code to ensure their ruses are successful.

Search engines as channels of malicious code:

- This involves the HTTP Referer (sic) header in that exploit scripts will only be injected into pages served from a compromised server if the Referer header accompanying the URL request is from a specific location, or more commonly, if the Referer is from one of the top search engines, such as Google, live.com, Baidu, or Yandex.
- Website owners and administrators checking complaints from site visitors whom their antivirus or internet security software blocked pages from the site should keep all these kinds of tricks in mind while investigating their own sites.

Heavily indented malicious code:

- When we use the 'view-source' option to look at source code on a malicious page, at first glance no malicious code seems to appear. However, if we 'select-all', it is clear that line 12 (formerly empty) contains content, as shown in Figure 9.

'Served once' malicious code:

- This is where malicious code is being served only once to a specific IP. The compromised server is loaded with server-side scripts that make sure the malicious client-side JavaScript it injects into pages is only served on a 'once-per-IP' basis. Some malicious client-side JavaScripts set cookies that the server-side script uses to stop repeated injections of malicious JavaScript into the pages it serves.
- In practice, we see the list of IP addresses already served is either dropped or the entries on it age-out approximately every 24 hours. Most website administrators visit their pages often so by the time they get a complaint from a visitor, most will have already put their IP address(es) into the server-side script's block list on their own servers, meaning they will not be served the malicious code.

Part 2: Web Risks and Threats

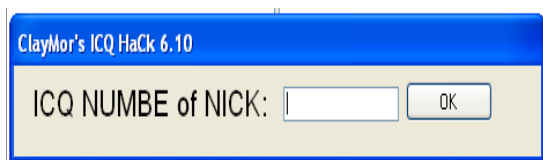


Figure 10: Initial dialog box of the malware

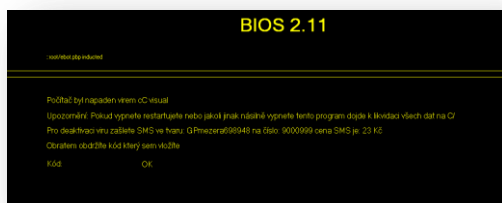


Figure 11: Hijacked desktop

4. Czechs experiment with malware development

This quarter, AVG security researchers spotted a local (Czech-born) piece of malware in the wild called "Lock Screen".

This kind of malware is known for its user-desktop-hijacking and exploiting behavior. It works on a very simple premise: once this Trojan is installed, it locks the user's desktop and demands a small sum of money to be paid in order to unlock it back. Payment is usually requested via PayPal or similar services. Our sample requires sending a Premium SMS which costs 79 Czech crowns (~3 Euros).

The malware is distributed via a public download sharing centers, Torrent servers and Czech game forums, aimed at targeting Czech users. The sample below was "promoted" as a game cheating and hacking tool using the following filenames:

- "Call-of-duty-4-Multi-hack-Undetected.exe"
- "Diablo-3-Fully-working-crack.exe"
- "Counterstrike-Multi-hack-Fully-undetected.exe"
- "ICQ-6.1-Hack-patch.exe"

When downloading and running the file, the following dialog appears requesting to enter either a game or ICQ nickname. When clicking on the OK button, the malware displays a full-screen text indicating the computer was infected by cC visual virus. The malware author then asks the user to send a Premium SMS to a Premium rate phone number 9000999 which includes the text GP_698948. Using this trick, the attacker can buy virtual money on Czech gaming server Gamepark.cz.

After sending the SMS, the victim should receive an unlock code. The text also claims that if the machine is rebooted, the data on the computer will be deleted; fortunately, it is not true as there is no code that would perform this operation, and the full-screen application can be easily bypassed.

This malware is detected by the latest version of AVG as variant of Trojan horse Ransomer. We disassembled and reverse engineered the malware, which quickly revealed the correct unlock code. The unlock-code is "SoNNy" is a nickname used by one of the players registered on the game server mentioned above so it appears that someone was trying to cheat and gain virtual money from competitors.

Part 3: Appendix

Other reports from AVG Technologies

AVG Community Powered Threat Report Q2 2012 – July 2012

<http://www.avg.com/press-releases-news.ndi-7062>

<http://mediacenter.avg.com/en/press-tools/avg-threat-reports/avg-community-powered-threat-report-q2-2012.html>

AVG Community Powered Threat Report Q1 2012 – April 2012

<http://www.avg.com/press-releases-news.ndi-4711>

AVG Community Powered Threat Report Q4 2011 – January 2012

<http://www.avg.com/press-releases-news.ndi-3723>

AVG Community Powered Threat Report Q3 2011 – October 2011

<http://www.avg.com/press-releases-news.ndi-2323>

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 and Future Laboratories: 'Cybercrime Futures' – September 2011

<http://www.avg.com/press-releases-news.ndi-1953>

AVG Community Powered Threat Report Q2 2011 – June 2011

<http://www.avg.com/press-releases-news.ndi-1563>

AVG Community Powered Threat Report Q1 2011 – April 2011

<http://www.avg.com/press-releases-news.ndi-129>

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>

Part 3: Appendix

About 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 128 million active users as of June 30, 2012 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.

For more information, please visit:
<http://mediacenter.avg.com/>

About the AVG Community

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.

You can read more about the threats featured in this report at: <http://blogs.avg.com/news-threats/>