



Q2

2012

**AVG Community
Powered
Threat Report**

Contents

Introduction	2
Welcome to the AVG Q2 Community Powered Threat Report.....	2
Executive summary: Q2 2012 Highlights	3
Key points for Q2 2012	3
Q2 2012 Top Trends and Insights from AVG Threat Labs.....	4
Web Risks & Threats	4
Mobile Risks & Threats	5
The AVG Q2 2012 Community Powered Threat Report Top Trends	7
About the Community Threat Report.....	8
Quarterly Key Metrics: April – June 2012	9
Web Threats	9
Mobile Threats	11
Email Threats	12
Part 1: Web Risks and Threats	14
Sex and fear: two human vulnerabilities cybercriminals are exploiting for cash	14
Flame and Stuxnet: the end of antivirus?	18
The China connection for a critical rated Microsoft vulnerability	19
Spoof FBI legal action ransomware demands fine for alleged PC misdemeanors	22
Part 2: Mobile Device Risks and Threats	23
Trigger-happy consumers are the target of new Android malware	23
Rovio's 'Angry Birds Space' gets a Trojan makeover on Google Play	26
Part 3: Inside the AVG Threat Labs	28
Hacker back-chat: when AVG met Hacker during a real-time debugging.....	28
Part 4: Appendix	29
Other reports from AVG Technologies	29
About AVG	30
About the AVG Community	30

Introduction



Welcome to the AVG Q2 Community Powered Threat Report

This quarter, we identified scenarios where users are tempted to click on video links promising celebrity sex or where victims were frightened into installing malicious code which purported to be antivirus software that had identified malware on their computer.

We also saw how social engineering techniques have been used to evolve an existing threat, giving it an additional lease of life with users who may have been caught in the past and therefore, are more wary today. In this case, the malware no longer needed to persuade a user to download anything – it is now enough just to get them onto the website and the payload automatically executes. Clever, and concerning.

In our [Q1 Community Powered Threat Report](#), we highlighted how mobile was fast becoming an attack vector for cybercriminals. The trend has only increased in the last three months with the prime target still the Android platform which maintains its popularity, holding 59 percent of the market share worldwide according to [recent IDC figures](#).

In our experience, a platform only needs to have 10 percent market share to become sufficiently worthwhile to malware authors so it's no surprise that Android is attractive. While mobile as an attack channel may not be as lucrative as the PC, in the future, this is likely to change with the proliferation of connected mobile devices.

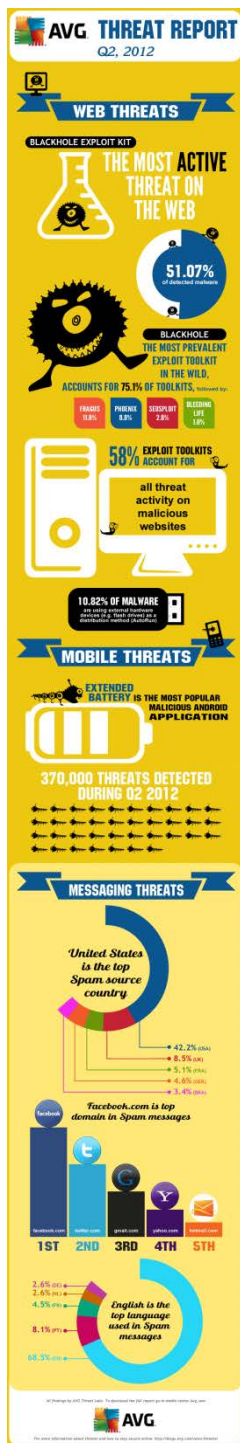
We also noted a significant increase in malware originating in China. China is now the world's [top smartphone market](#), with over one million mobile web users which would explain the emergence of mobile based threats, but we also saw an upsurge in malicious email spam targeting other markets as well, including Japan, South Korea, Taiwan and the US.

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: Q2 2012 Highlights



Key points for Q2 2012

The quarterly AVG Community Powered Threat Report for Q2 2012 was released on 25 July.

Social engineering: this quarter saw an uplift in socially engineered attacks which deceive mobile device users into downloading and then enabling malware to run as root. This has the effect of turning a mobile device into a zombie and providing full control over it to the malware author. PC-based malware that was socially engineered was also identified, including an email scam targeting Asian markets and the US, as well as a mass injection SQL attack using celebrity sex videos and fake antivirus to entrap people. Socially engineered attacks are more sophisticated in their approach, making even users who may have been victims in the past likely to fall prey again.

Mobile: cybercriminals continued their focus on the Android operating system for smartphones this quarter. Given Android now holds 59 percent of the market share, according to the [latest IDC figures](#), it will increasingly become a lucrative attack vector. Mobile users were tricked into downloading malware which was hidden in seemingly legitimate applications such as 'Angry Birds Space'. This then allows the hacker to monetize from the infected device as they wish, and to download additional malicious code or connect the device to a botnet.

Threat geography: one notable theme in the last three months was the amount of malware originating from China. Email scams and malicious Android applications uploaded to third party application markets were just two of the threats identified. These targeted China and in some cases, neighboring countries including Japan, South Korea, Taiwan and the United States.

Executive summary:

Q2 2012 Highlights

Flame as code is not very special. It doesn't appear to have a very sophisticated payload or use remarkable spying methods.

Q2 2012 Top Trends and Insights from AVG Threat Labs

Web Risks & Threats

Sex and fear: two human vulnerabilities cybercriminals are exploiting for cash

In the last quarter, AVG security labs prevented more than 3 million incidents related to rogue software. Rogue software (rogueware) is a form of internet fraud using computer malware (malicious software) that deceives or misleads users into paying for fake or simulated removal of malware, but instead introduces malware to the computer. Fake antivirus and rogue security software are now well known, so rogueware creators initiated a SQL mass injection attack that spreads through web pages. The attack uses different tactics depending on the web browser:

- **Mozilla Firefox:** the user is presented with 'never-before-seen' celebrity sex videos but when they click on the 'play' button, they are told to update their Flash installation in order to see the video. The user will never get to see the video because it's fake and will only install a Trojan disguised as a Flash update.
- **Microsoft Internet Explorer:** a link to a fake antivirus product will pop up, claiming to have identified lots of security threats on the user's PC. This attack is enabled simply by the user landing on a fake antivirus website where the rogue malware downloads and then 'installs' the fake software to purportedly clean it up. The user is then prompted for payment to purchase the fake antivirus, which merely removes the rogue.

Flame and Stuxnet: the end of antivirus?

From a technical point of view, Stuxnet is a piece of art in the world of malware development. Although it was to be expected that cyber-attacks at some point would be used as discreet weapons, the level of sophistication within Stuxnet was nonetheless impressively high. Flame as code, on the other hand, is not very special. It doesn't appear to have a very sophisticated payload or use remarkable spying methods. Despite a lot of speculation, it may never be certain who was behind either Flame or Stuxnet; however, it is increasingly becoming clear that the intended victims for both types of attack are not the average consumer.

Executive summary:

Q2 2012 Highlights

It is almost becoming a fact of life that malware creators release new malicious code following Microsoft Patch Tuesday.

Some commentators have suggested that Stuxnet and Flame demonstrate that the days of antivirus solutions are numbered. The reality is that traditional signature detection is now just one layer of protection within a multi-layered security solution that is being continually developed to keep pace with new trends. With all the spectacular headlines, it is easy to forget that the real risk for consumers today mainly comes from Blackhole exploit kits that attack unsuspecting users visiting the sites they trust.

The China connection for a critical rated Microsoft vulnerability

AVG's Asian Threat and Research team noticed a higher than usual amount of malware being spammed out to a very specific geography: China, Japan, South Korea, Taiwan and USA. In the past few weeks, we collected more than 25 unique malicious Microsoft Office attachments that were distributed to thousands of users via spammed e-mail messages. The email message text usually contains some recent political news or regional incident.

It is almost becoming fact of life that malware creators release new malicious code following Microsoft Patch Tuesday. These malware outbreaks were using the recent vulnerability known as CVE-2012-0158. Windows patches were released in April's issue of Microsoft's Security Bulletin MS12-027¹. This vulnerability can be triggered by opening a specially crafted document file in one of the affected Microsoft products. Once the document is opened in the host application, it crashes and the malware payload is executed. The Trojan collects sensitive user information such as username and passwords for various website services and applications. It then sends this data to the attacker's server.

Spoof FBI legal action ransomware demands fine for alleged PC misdemeanors

In June 2012, AVG found a new ransomware page delivered by the Blackhole exploit kit which claims to be a legal action by the U.S. Federal Bureau of Investigation (FBI). The malware locks up the machine's Windows operating system, claiming the affected PC has been used to violate copyright laws, view pornographic content, or has been infected with malware and violates a fictional "Neglectful Use of Personal Computer article 210 of the Criminal Code". It demands a payment of \$100 through an untraceable money transfer to unlock the PC.

¹ <http://technet.microsoft.com/en-us/security/bulletin/ms12-027>

Executive summary:

Q2 2012 Highlights

Since DKFbootkit adds itself to part of the boot sequence, it is considered to be the first Android bootkit, springing into life as soon as the device is activated. This means it will become a serious threat to Android users as it spreads.

Mobile Risks & Threats

Trigger-happy consumers are the target for new Android malware

Following our investigation of mobile as an attack vector in our [Q1 Community Threat Report](#), AVG has seen continued focus on the Android platform for smartphones, which is now the leading operating system for devices with 59 percent market share, according to the latest figures from IDC². The malware is spread over the third party application market (and not the official Google Play) in China.

The malware, known as 'DKFbootkit', masquerades as a fake version of a legitimate application and seeks to damage the Android phone's Linux kernel code, which in turn gives the malware full control over the device for monetization purposes. Since DKFbootkit adds itself to part of the boot sequence, it is considered to be the first Android bootkit, springing into life as soon as the device is activated, which means it will become a serious threat to Android users as it spreads.

Rovio's 'Angry Birds Space' gets a Trojan makeover on Google Play

AVG's Mobilation™ research team identified a Trojan-infected version of the hugely popular Android application 'Angry Birds Space' which was uploaded to unofficial Android application stores. In addition to having a similar name, icon and graphics to the legitimate application, the Trojan is fully functional which fools users who believe it is the real thing and will therefore be less likely to become aware of its sinister activities.

Its malicious functionality contains usage of the GingerBreak exploit to gain root access privileges; Command & Control communication whereby the Trojan communicates with the remote server to download and install additional malware onto the smart phone device; botnet functionality; and the modification of files, among other things.

For the latest AVG news on threats, please visit:

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

² <http://www.engadget.com/2012/05/24/idc-q1-2012-world-smartphone-share/>

Executive summary: Q2 2012 Highlights

~370,000 mobile threats detected during Q2 2012.

The AVG Q2 2012 Community Powered Threat Report Top Trends

Web Threats

Blackhole Exploit Kit	The most active threat on the web, 51.07% of detected malware
Blackhole	The most prevalent exploit toolkit in the wild, accounts for 75.1% of toolkits
58%	Exploit toolkits account for 58% of all threat activity on malicious websites
10.82%	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
~370,000	Threats detected during Q2 2012

Messaging Threats (Spam)

United States	Is the top spam source country
42.2%	Of spam messages originated from the USA, followed by the UK with 8.5%
Facebook.com	Top domain in spam messages
English	Is the top language used in spam messages (68.5%)

Executive summary: Q2 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

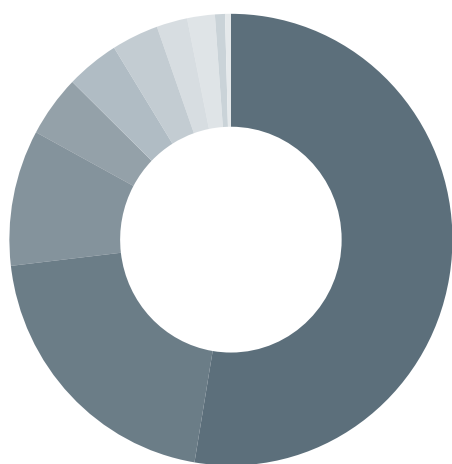
The AVG Community Protection Network is an online neighborhood watch where community members work to protect each other. Information about the latest threats is collected from customers who participate in the product improvement program and shared with the community to make sure everyone receives the 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: April – June 2012

**Top 10 Web Threats
Prevalence Chart Q2 2012**



Blackhole Exploit Kit	51.07
Rogue Scanner	19.91
Facebook Scam	9.45
Script Injection	4.29
Link to Exploit Site	3.74
Pharmacy Spam Site	3.32
Phoenix Exploit Kit	2.18
Fragness Nulled Exploit Kit	1.96
WMP Exploit	0.71
Redirect to Rogue Scanner	0.41

Web Threats

Top 10 Web Threats Prevalence Table Q2 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
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
Link to Exploit Site	These pages contain links to known exploit sites. In some cases, malicious code is automatically downloaded without any user intervention
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
WMP exploit	Exploit in Windows Media Player which leads to remote code execution
Redirect to Rogue Scanner	Injected code which redirect the visitor to a malicious site that tries to install Rogueware

Quarterly Key Metrics: April – June 2012

**Top 10 Web Threats
Prevalence Chart Q2 2012 (%)**



Worm/AutoRun	10.82
Win32/Heur	8.82
Worm/Downadup	7.58
Win32/Cryptor	3.56
SWF/Downloader	3.00
Generic20.GJD	2.81
Worm/Generic_c.ZS	2.69
HTML/Framer	2.69
Win32/Sality	2.19
Win32/Virut	2.19

Top 10 Malware Threats Prevalence Table Q2 2012

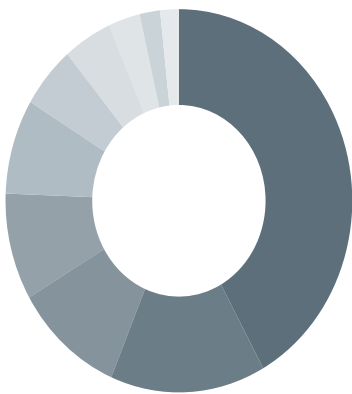
This table presents top traditional malware as detected by AVG Threat Labs

Worm/Autorun	10.82%
Win32/Heur	8.82%
Worm/Downadup	7.58%
Win32/Crptor	3.56%
SWF/Downloader	3.00%
Generic20.GJD	2.81%
Worm/Generic_c.ZS	2.69%
HTML/Framer	2.69%
Win32/Sality	2.19%
Win32/Virut	2.19%

Quarterly Key Metrics: April – June 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 Q2 2012**



Trojan	39.57
Adware/Spyware	13.65
Adware	9.63
Downloader	8.52
Virus	7.56
Malware	4.96
Potentially Unwanted Application	4.26
Network Worm	2.81
Backdoor	1.80
Worm	1.64

Top Exploit Toolkits Seen in Q2 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	75.1%
2	Fragus	11.8%
3	Phoenix	8.8%
4	Seosploit	2.8%
5	Bleeding Life	1.0%

Mobile Threats

Distribution of Android Threats Q2 2012 (%)






Malware	63
Hacking Tools	11
Rooting Tools	26

Quarterly Key Metrics: April – June 2012

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

Email Threats

Top Domains in Spam Messages Q2 2012

1		No domains in messages	11.2%
2		Facebook.com	4.3%
3		Twitter.com	2.9%
4		Gmail.com	1.7%
5		Yahoo.com	1.5%
6		Hotmail.com	1.2%
7		Amazonaws.com	1.2%
8		Linkedin.com	0.9%
9		Tumblr.com	0.9%
10		Constantcontact.com	0.9%










Top 5 Languages Spam Messages Q2 2012

1		English	68.5%
2		Portuguese	8.1%
3		French	4.5%
4		Dutch	2.6%
5		German	2.6%

Quarterly Key Metrics: April – June 2012

The United Kingdom is the second most common spam source country after the United States which comes top.

Top Countries of Spam Senders Q2 2012

1		United States	42.2%
2		United Kingdom	8.5%
3		France	5.1%
4		Germany	4.6%
5		Brazil	3.4%
6		Australia	3.1%
7		Netherlands	2.2%
8		Canada	1.8%
9		Italy	1.5%
10		South Africa	1.1%

Part 1: Web Risks and Threats

In the case of the fake antivirus, this new attack is much more sophisticated as it targets users who may have been a victim once and seeks to fool them again.

Sex and fear: two human vulnerabilities cybercriminals are exploiting for cash

In the last quarter, AVG security labs detected more than three million incidents related to rogue software. Rogue software (rogueware) is a form of internet fraud using computer malware (malicious software) that deceives or misleads users into paying for fake or simulated removal of malware or claims to get rid of malware, but instead introduces it to the computer.

Rogueware mainly relies on social engineering to lure end users into downloading the malware. Initial execution was through fake antivirus sites that distributed rogue antivirus software. Rogues often proxied the victims' internet traffic, only allowing them to visit a payment page to pay the ransom; but when victims did pay up, all the rogue would do was remove itself.

Fake antivirus and rogue security software are now well-known as users have begun to educate themselves and have stopped falling for the scam. So rogueware creators needed to find new ways to ensnare people and extend the lifetime of the attack to improve monetization – and they did so by initiating a mass SQL injection campaign.

Drive-by downloads

When a highly automated, mass injection SQL attack first appeared in early 2011, it affected thousands of web pages with out-of-date or inadequate security, earning the name 'LizaMoon' after the first website it took down. One year on, the recent SQL injection attack is most probably related to LizaMoon but has evolved through social engineering so that it spreads through pages that pretend to offer 'never-before-seen' sexual content or fake antivirus products.

In the case of the fake antivirus, this new attack is much more sophisticated as it targets users who may have been a victim once and seeks to fool them again. Where an attack could originally have been prevented by exiting the malicious website without downloading anything, now a victim need only visit a fake antivirus site to be attacked. This sneaky tactic is known as a 'drive-by download' and closing the browser window will offer no protection since the exploit has already run and any vulnerable system will subsequently become infected.

Part 1: Web Risks and Threats

Cybercriminals have used social engineering tactics to evolve threats by tapping into topics and interest areas that are most likely to get a response.

Anatomy of a SQL injection attack

The purpose of this SQL injection attack is to target the database at the backend of a website and execute unauthorized commands by injecting malicious code onto otherwise legitimate websites and taking advantage of insecure code. The malware then redirects visitors from the legitimate websites to those that have malicious script injected into their HTML code, which in turn redirects visitors to sites that lead to malicious pages. The potential victims' machines go through multiple redirects before landing on the web page that delivers a fake antivirus program or a fake Flash update, depending on which browser they are using. The injection attacks hide iframes on the pages and those lead to the exploits.

The attacks have commonly used vulnerabilities in (outdated) client-side installations of the Java Platform Standard Edition, Adobe Reader and Adobe Acrobat. The i.html iframes load exploits that take advantage of the vulnerabilities described in CVE-2010-0188 and CVE-2012-0507. Hackers took advantage of these vulnerabilities and issued SQL commands to input their injections into webpages on servers running Microsoft SQL Server 2000, 2005 and 2008. Specifically, the vulnerabilities exploited are:

- [CVE-2010-0188](#)
- CVE-2010-0188: [Adobe-issued patches](#) for Adobe reader 9.3 and Acrobat 9.3 (patched February 16, 2010)
- [CVE-2012-0507](#)
- [CVE-2012-0507](#): (Oracle-issued a critical patch for Java SE February, 2012)

Standard tactics such as those used in the LizaMoon SQL attack last year included telling users they are infected (when they were not) and dazzling them with graphics or flash animation in the hope they will click on 'install' and pay the fee without realizing genuine antivirus products usually cost less than the rogue variety. Today's more wary user is much less likely to respond to such blatant attempts to hoax them, which has generated a problem for cybercriminals – how do you make money from users who are now sufficiently technology-aware to avoid the basic tricks?

The latest version of these SQL mass injection attacks began to emerge in April 2012 as a clever response to this dilemma. Cybercriminals have used social engineering tactics to evolve threats by tapping into topics and interest areas that are most likely to get a response. In addition, they have increased the

Part 1: Web Risks and Threats

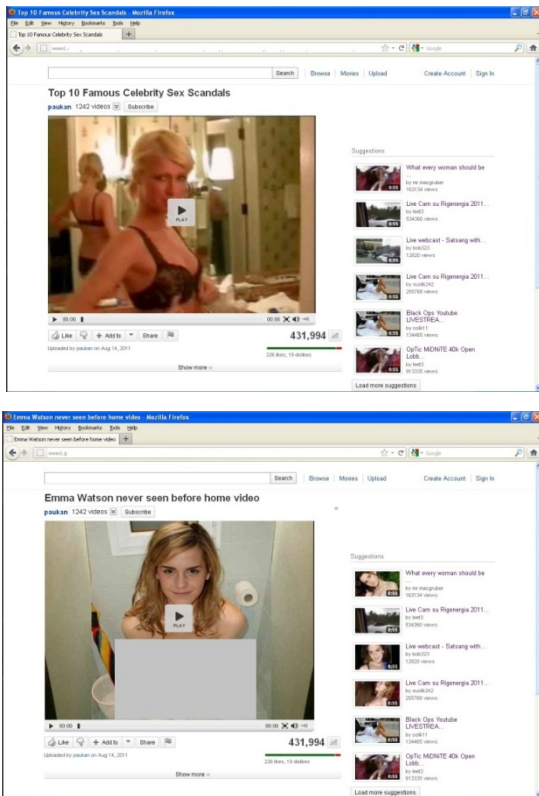


Figure 1: Two examples of the trap set for unwary YouTube visitors

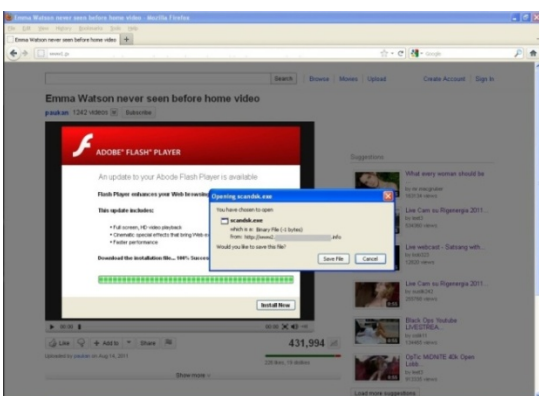


Figure 2: User is given the option to install the malware which pretends to be an Adobe update

sophistication of the malware by making it much harder to detect from the outset and, once the infection is complete, rendering it almost invisible so that security software is required to find and remove it.

We will take a closer look at these two attacks.

A. Sexual content

This type of attack is seen via Mozilla's Firefox browser, driven by fake videos and phony Adobe updates. Most often, these are seen in pages that pretend to offer celebrity sex videos which trigger fake Adobe updates that download the malicious code.

AVG has identified two versions recently where the victim lands on a fake Flash update page and is offered the option to click on a video to view: one features socialite Paris Hilton and the other, actress Emma Watson.

However, when visitors click on the 'play' button, they are told they need to update their Flash installation in order to see the video. The user will never get to see the video because it's fake and will only install a Trojan disguised as a Flash update.

B. Scare-mongering

Rogue security products that mimic legitimate AV products continue to be prevalent as victims are still tricked into purchasing them. The latest, more sophisticated attack is enabled simply by the user landing on a fake antivirus website where the rogue malware downloads and makes a show of 'detecting' numbers of fake viruses, Trojans and malware and then 'installs' the fake software to purportedly clean it up.

If the potential victim clicks 'Remove all', the rogue downloads further malware which eventually leads to a payment screen. If the victim has installed the rogue on his or her machine then declines to purchase it, nag screens will continue to pop up until the rogue is cleaned from the machine. Both the fake antivirus site and the fake Flash update site both offer a file named scandisk.exe, indicating they are part of the same attack.

Part 1: Web Risks and Threats

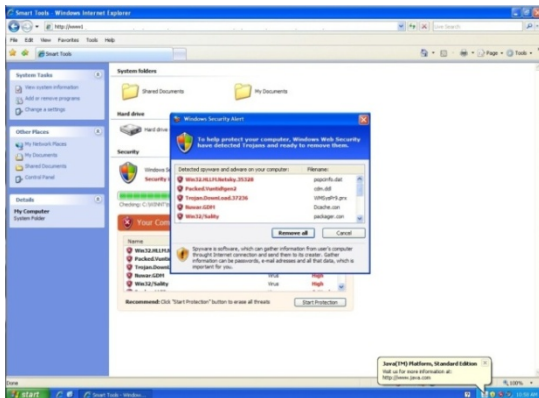


Figure 3: Malicious code is installed by selecting the 'Remove all' function

Recommendations

Countermeasures that web managers can take:

- Web masters should make sure that all applications installed on the web server are constantly updated.
- Keeping alert to unexpected changes in back-end databases also can help spot malicious activity and the installation of the malware.

Countermeasures that web users can take:

- Install security software that detects malware and/or links to malicious web sites.
- Promptly update Adobe Acrobat and Reader installations.
- Promptly update the Java Runtime Environment.

Part 1: Web Risks and Threats



Flame and Stuxnet: the end of antivirus?

The discovery of Stuxnet in 2010 caused considerable uproar, not only among security professionals but also among the wider public. The alleged high-level political dimension to cybercrime made exciting headlines. From a technical point of view, Stuxnet is a piece of art in the world of malware development. Although it was to be expected that cyber-attacks at some point would be used as discreet weapons, the level of sophistication within Stuxnet was nonetheless impressively high.

That Stuxnet went seemingly undetected for a considerable time caused some commentators to suggest that the days of antivirus solutions are numbered. The reality is that the security industry has already adapted to the unexpected nature of threats. Traditional signature detection is now just one layer of protection within a multi-layered security solution that is being continually developed over the years to keep pace with new trends.

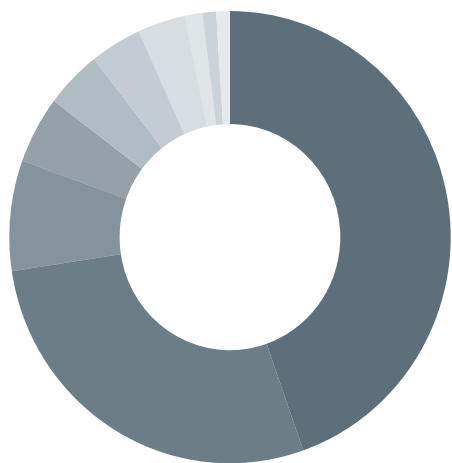
The topic re-emerged with the appearance of Flame in the last quarter. However, if Stuxnet is a work of art, Flame is not so much. Stuxnet employs some very sophisticated techniques, particularly in the payload. Flame as code, on the other hand, is not very special. It doesn't appear to have a very sophisticated payload or use remarkable spying methods. There is one main thing that stands out, though: it uses a very complex cryptographic collision to make it appear as if the malware is signed by Microsoft, and finding that collision will have required considerable resources.

Nonetheless, despite the hype, in both of these attacks, the average consumer is not a target. Despite a lot of speculation, it may never be certain who was behind either Flame or Stuxnet. However, it is increasingly becoming clear that the intended victims for both types of attack are not the average consumer. It might even be in the interest of the makers not to cause harm to ordinary systems to limit the chance of discovery and stay under the radar.

With all the spectacular headlines, it is easy to forget that the real risk for consumers still comes from Blackhole exploit kits that attack unsuspecting users when they visit the websites they trust.

Part 1: Web Risks and Threats

To stay protected from these risks, people should make sure their systems are kept up-to-date and that they have multiple-layered security software installed, up-to-date and active.



Blackhole Exploit Kit	43.55
Rogue Scanner	27.32
Pharmacy Spam Site	7.71
Facebook Scam	4.7
Script Injection	4.03
Phoenix Exploit Kit	3.69
Link to Exploit Site	3.40
Blackhat SEO	1.27
Fake Codec	0.98
Invisible / Frame Injection	0.98

The China connection for a critical rated Microsoft vulnerability

During May 2012, AVG's Asian Threat and Research team noticed a higher than usual amount of malware being spammed out to a very specific geography: China, Japan, South Korea, Taiwan and USA. In the past few weeks, we collected more than 25 unique malicious Microsoft Office attachments that were distributed to thousands of users via spammed e-mail messages. The email message text usually contains some recent political hot news or specific regional incident. In this example, we will look at a malicious spam campaign that is trying to leverage political issues related to Tibet.

The malware needs to convince the user to visit the fake website through a link in the email message, for example, or to encourage them to open an email attachment which contains the malicious file. This is where social engineering techniques are used to make the spam sufficiently persuasive that the user will act on it.

This is important as the total of worldwide software piracy rate for PC software is 42%³ and the majority of PCs worldwide now run a version of a Windows OS⁴. This means that potentially around 200 million people do not have a genuine license, cannot update their system and therefore, are vulnerable to new attacks like this.

The affected products are:

- Microsoft Office 2003 SP3, 2007 SP3
- Microsoft Office 2010 SP1
- Microsoft SQL Server 2000 SP4
- Microsoft SQL Server 2005 Express edition SP4
- Microsoft SQL Server 2008 SP2
- Microsoft BizTalk server SP1 and Microsoft Commerce server 2002/2007/2009
- Microsoft Visual FoxPro 8.0 SP1/9.0 SP2
- Visual Basic 6.0 Runtime

³http://portal.bsa.org/globalpiracy2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf

⁴http://news.cnet.com/8301-1045_3-57464649/windows-7-on-majority-of-pcs-for-the-first-time/?tag=mncol;txt

Part 1: Web Risks and Threats

As soon as knowledge of a vulnerability becomes public, hackers and malware creators race to release their malware as they know that the patching processes take some time and the 'window of opportunity' this provides is therefore quite wide.

Patch Tuesday and the race against time

All of the malware outbreaks were using the recent vulnerability of Microsoft's ActiveX MSCOMCTL.OCX component, part of Windows common controls. This vulnerability is known as CVE-2012-0158 and Microsoft has classified it as 'critical' because it could allow a remote attacker to execute on arbitrary code. Windows patches were released in April's issue of Microsoft's Security Bulletin MS12-027⁵ to address this vulnerability.

It is almost becoming fact of life that malware creators release new malicious code following Microsoft Patch Tuesday. As soon as a fresh vulnerability becomes public, hackers and malware creators race to release their malware as they know that the patching processes (by end users and network administrators) take some time and the 'window of opportunity' this provides is therefore quite wide.

Patching the systems should happen automatically, yet, in the real world, this is not always the case. According to Secunia's research⁶, Windows users need to patch their systems on average every five days to stay ahead of security vulnerabilities. With many applications used by home users and different update mechanisms applied by differing suppliers, this means that most users are not even in the race against time.

This vulnerability can be triggered by opening a specially crafted document file in one of the affected Microsoft products. Once the document is opened in the host application it crashes and the malware payload is executed, downloading a Trojan that then collects sensitive user information such as username and passwords for various website services and applications and sends this data to the attacker's server. It is also able to download another malware to allow a key logger facility or to get a new Trojan configuration (new host to report). AVG detects this malware proactively as variant of Win32/DH{ADUP} or as a variant of Trojan horse Generic and Agent family.

So far, we have registered Microsoft Office exploit-crafted documents to be the most prevalent in-the-wild. These documents (either DOC/DOCX or RTF format) were spammed via email as

⁵<http://technet.microsoft.com/en-us/security/bulletin/ms12-027>

⁶https://secunia.com/gfx/pdf/Secunia_RSA_Software_Portfolio_Security_Exposure.pdf

Part 1: Web Risks and Threats

According to Secunia's research, Windows users need to patch their systems on average every five days to stay ahead of security vulnerabilities.

attachments. We have collected a sample that was spammed as "Inside Information.doc" email attachment:



This exploited document has an embedded encrypted executable file. After opening the document, Microsoft Word crashes and the executable file is dropped and executed. The malicious executable is encrypted using a simple XOR encryption with the **OxAC** key. After decrypting and extracting the file, we can do payload analysis:

1. Document is opened and the file "wcntfy.exe" is dropped to user profile folder and executed.
2. Wcntfy.exe then drops another file "scrss.exe" to a TEMP folder and executes it.
3. Scrss.exe adds itself into registry \Run key with value "IMJPMIG8.1SA" to ensure its start after system restart.
4. Wcntfy.exe drops another file - a Word document - into a user TEMP folder and starts it. This file is harmless.
5. CVE-2012-0158 analysis.

Recommendations

The Windows Data Execution Prevention (DEP) feature is designed to prevent similar stack/heap overflow exploitations but DEP is disabled for Microsoft Office by default. So if a computer is set up to protect Office executables by DEP, it is not affected by this vulnerability.

Part 1: Web Risks and Threats

However, if your computer is not set up in this way, there are some very simple steps that will help protect from this exploit:

- Do not open Microsoft Office and WordPad documents from sources you do not know or trust, or that you receive unexpectedly from trusted sources.
- Enable Windows Data Execution Prevention feature: this feature is designed to prevent similar stack/heap overflow exploitations (disabled for Microsoft Office by default).
- Have your Antivirus application up-to-date so it can proactively detect this type of malware.

Spoof FBI legal action ransomware demands fine for alleged PC misdemeanors

In June 2012, AVG found a new ransomware page delivered by the Blackhole exploit kit which claims to be a legal action by the U.S. Federal Bureau of Investigation (FBI). The malware locks up the machine's Windows operating system and demands payment of a 'fine' to unlock it.

The graphic, which includes a fake video, demands a payment of \$100 through an untraceable money transfer. Since the text cites the fine as "100\$," this is an indication that the demand isn't really from the FBI. Another giveaway that this is fake lies in the text that says the affected PC has been used to violate copyright laws, view pornographic content, or has been infected with malware and violates a fictional "Neglectful Use of Personal Computer article 210 of the Criminal Code."

The ransomware instructs victims to pay their 'fine' with a MoneyPak card, which can be purchased from any of the following well-known U.S. retail chain stores: 7-Eleven, CVS/Pharmacy, Kmart, Rite Aid, Walgreens and Walmart. MoneyPak is a payment system that allows users to reload the card by paying at an approved partner site where it can then be used to pay other merchants. The MoneyPak company has a page on its [web site](#) offering *6 Tips on How to Protect Yourself from Fraud*.

AVG's LinkScanner detects the exploit kit that downloads and executes the ransomware as Exploit, 2182, Blackhole Exploit Kit (type 2182).



Figure 4: Fake demand for payment of a 'fine' delivered via SSL on port 443

Part 2: Mobile Device Risks and Threats

Mobile devices continue to be an evergreen market for malware.

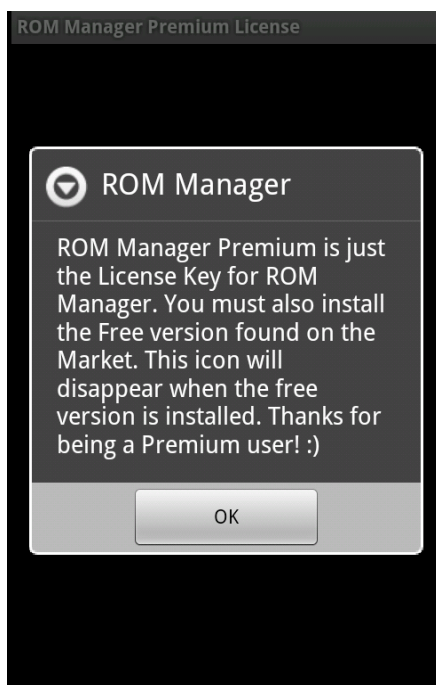


Figure 5: The malware author wants the application to be kept on the device, so tricks the user into enabling the malicious functionality

Trigger-happy consumers are the target of new Android malware

The rapid adoption of mobile technology, new generation multi-function devices and user engagement features such as apps and gadgets has established an evergreen market for malware. Following our investigation of mobile as an attack vector in our [Q1 Community Threat Report](#), AVG has seen continued focus on the Android platform for smartphones, which is now the leading operating system for devices with 59 percent market share, according to the latest figures from IDC⁷. The malware is spread over the third party application market (and not the official Google Play) in China.

The malware, known as 'DKFbootkit', also exploits general user lack of understanding of the technical subtleties by intentionally masquerading as a fake version of a legitimate application, distinguished only by small differences in the package name. The application can be disguised in many ways – the one we identified consisted of a large collection of videos.

The goal of the malware is to damage the Android phone's Linux kernel code by replacing some components with malicious ones, which in turn gives the malware full control over the device for monetization purposes. Since DKFbootkit adds itself to part of the boot sequence, it is considered to be the first Android bootkit, springing into life as soon as the device is activated, which means it will become a serious threat to Android users as it spreads.

It is the latest example of using social engineering to spread infected applications by tricking users to willingly download and accept the payload. Appearing as a bona fide application, it uses a series of standard prompts that encourage users to be complicit in their own hoodwinking by asking them to click on 'OK' in order to confirm the download and to allow the application access. Even more concerning, the average user is unlikely to be aware that anything is wrong as the malware operates at a highly technical level and is therefore exceptionally difficult to spot.

Quick-fingered people can be so used to these notifications that they risk being trigger-happy and not checking first what exactly the application is asking permission to do. And once the device is rooted, it becomes a zombie over which the malware

⁷<http://www.engadget.com/2012/05/24/idc-q1-2012-world-smartphone-share/>

Part 2: Mobile Device Risks and Threats

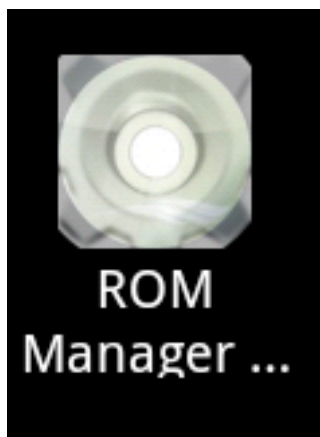


Figure 6: Initiates approval request sequence

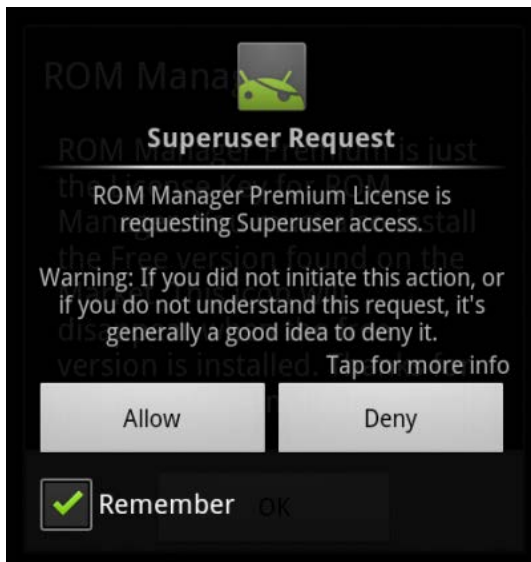


Figure 5: If the user presses "Allow", the native payload will be executed, and the Linux kernel of the user's Android phone will be modified

author has ultimate control. The cybercriminals then use the malware to siphon small amounts of money from the user's account, for example, by SMS; these are usually such small amounts that consumers are unlikely to notice it on their bills. Mobile connected devices are sitting ducks when it comes to this type of crime as they are already linked to a payment method that requires no additional approval or authentication.

Rooting an Android device

To activate, DKFBootkit needs root privileges as those are necessary to replace native binary files. If a user's Android phone is not rooted, its Linux kernel will be safe; however, once the user's device is 'rooted', the malware author is able to do whatever he wants. When the application is installed on an Android device, the user can see the icon below which, when clicked, launches the request for installing the license key. This is then followed by another request, this time for 'Superuser' access, to enable its malicious capabilities.

In the sample analyzed by AVG, the name was 'com.atools.rommanager.license'. This fact by itself is suspicious as the creators of ROM Manager applications, ClockworkMod, use the following structures: com.koushikdutta.rommanager and com.koushikdutta.rommanager.license. The malware author tries to deceive the user into thinking it's the legitimate application by giving it a very similar package name. The malware next requests the permissions that will allow it to initiate a number of actions:

- Allow applications to open network sockets.
- Allow applications to access information about networks
- Allow applications to access information about Wi-Fi networks
- Allow read only access to phone state.
- Allow an application to access coarse (e.g., Cell-ID, WiFi) location

The malware also uses intent filters. A filter object that an application declares in its manifest file is used to tell the system what types of intents each of its components is willing to accept and within which criteria. Through an intent filter, an application can express interest in specific data types, intent actions, URI formats, and so on. The intents declared are used by the malware to understand when the device boots and is active again and also for getting information about the current applications installed.

Part 2: Mobile Device Risks and Threats



Figure 8: adv3 workflow diagram

When we look at the 'running services' tab, we can also see that the malware uses the following service to load a library named 'adv3':

On analyzing the libadv3.so file, we can extract the APK (Android application file). The file is located in the lib folder which has nine export functions; one of these, '_bindata', points to an ELF file that contains a lot of the encrypted strings that the author hoped would obfuscate his purpose. But, those strings can be decrypted and from this, we can see the main purpose of the loader functionality is threefold: to decrypt string data; to run 'su' to request root privileges; and to run payload. The malware is also able to change and modify libraries used by the operating system and writes its configuration information into the target files.

It also changes the service controller, Svc, which auto starts services at boot as the malware author wants it to start working as early as possible. The init.d directory contains a number of start/stop scripts for various services on the phone's system, for example containing initialization and termination scripts for changing init states. In order to control any of the scripts in init.d manually, you have to have root (or sudo) access hence the malware using an exploit to root the device. Again, those changes require root permissions. The malware is also able to download files and after it is installed, users can see a link in the notification area which they press on to activate the application.

Recommendations

- Prior to installing any application, carry out a background check on the developer and the application, especially when downloading from Android markets which are not the official Google Play.
- Only download apps from application stores, sites and developers whom you trust, and always check the application star rating, developer information and user reviews to make sure you know what you are downloading. Or set your Android device to download applications from Google Play only.
- Think before you click 'OK!' When installing new apps to your Android device, always look at the permissions application requests to approve and make sure they seem appropriate.
- Install a mobile security program to protect against malicious applications. Uninstalling DKFrootkit is very difficult so you will need an expert to fix it; therefore avoidance is better than remediation.
- Know your own activity and monitor your bills carefully: look for any anomalous small amounts for which you cannot account as these could indicate your handset has been rooted.

Part 2: Mobile Device Risks and Threats



Figure 9: the game is played as seen in the legitimate application

Rovio's 'Angry Birds Space' gets a Trojan makeover on Google Play

Malware creators are always looking to exploit the 'human factor', which is the weakest link in any malware authoring. AVG's Mobilation™ research team identified a Trojan-infected version, uploaded to unofficial Android app stores, of the hugely popular Android application 'Angry Birds Space', developed by Angry Birds creator Rovio [in conjunction with NASA](#). In addition, to having a similar name, icon and graphics to the legitimate application, the Trojan is fully functional which fools users who install it believing it is the real thing and will therefore be less likely to become aware of its malicious activities.

When the application is installed on an Android device, the user can see the following icon which, when pressed, enables the user to play the game as seen in the legitimate application.

The application has been active since January 2012 but real impact only began to be seen in April. Its malicious functionality contains usage of the GingerBreak exploit to gain root access privileges; Command & Control communication where the Trojan communicates with the remote server to download and install additional malware onto the smart phone device; botnet functionality; and the modification of files, amongst other activities.

The malware has a package name of 'com.rovio.new.ads'. This is suspicious as the Angry Birds applications family, released by Rovio, only features the following type of structures:
com.rovio.angrybirdsspaceHDcom
rovio.angrybirdsspace.ads
com.rovio.angrybirdsrio

The malware then requests permissions that allow it to carry out the following actions:

- Allow applications to access information about networks.
- Allow an application to write to external storage.
- Allow applications to access information about Wi-Fi networks.
- Allow an application to access coarse (e.g., Cell-ID, WiFi) location.
- Allow applications to open network sockets.
- Allow read only access to phone state.
- Allow an application to read the low-level system log files.

Part 2: Mobile Device Risks and Threats

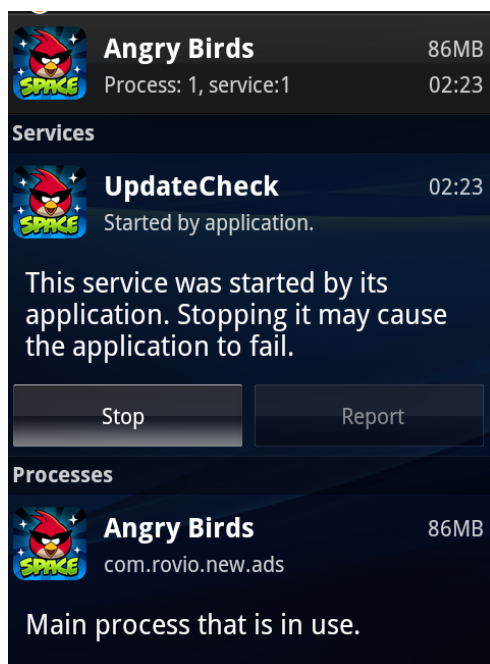


Figure 10: the 'UpdateCheck' service can be seen in the 'running services' tab after the game is activated

The payload of the malware can be found hidden inside a JPG image file named 'mylogo' found in assets folder inside the APK; inside the image, two malicious ELF files can be found.

The malware then uses the 'UpdateCheck' service declared in the AndroidManifest.xml file and this service can be seen in the 'running services' tab after the game is activated:

The service takes care of handling the ELF files hidden in the image and related to the exploitation process. We can see the malware using the IMEI of the device ('getDeviceId'), 'chmod' command that changes the file system mode and the 'exec' command which executes the specified command and its arguments in a separate native process.

Decrypting the strings inside the ELF files can help us to identify the functionality of the working of the Trojan. The malware has bot payload capabilities and functionality to connect remote Command & Control servers. As seen in the decrypted strings above, we could spot Command & Control servers. The malware is also able to change and modify libraries used by the operating system and uses an exploit to gain root privileges. Once the device is rooted, the malware has the power to do what it wants such as be able to download and install additional components from the remote website.

Once again, users should be careful about what applications they download, where they originate, and be vigilant to requests that any application may make for permission.

Part 3: Inside the AVG Threat Labs

The hacker was telling the truth - this backdoor has powerful functions like monitoring the victim's screen, mouse controlling, viewing process and modules, and even camera controlling.

Hacker back-chat: when AVG met Hacker during a real-time debugging

The AVG Threat team was recently researching key loggers for Diablo III as many game players playing this game found their accounts stolen; a sample is found in battle .net in Taiwan. The hacker had posted a topic entitled "How to farm Izual in Inferno" (Izual is a boss in Diablo III ACT 4), and provided a link in the content which pointed to a demonstration video. The video is a RAR archive actually containing two executable files; these two files are almost the same except for the icon.

The malware executes by connecting to a remote server via TCP port 80 and downloading a new file packed by Themida. That's very simple Downloader/Backdoor behavior and we were only interested in looking for key logging code for Diablo III, so we didn't pay much attention to it.

But then ... a chatting dialog popped up with a message:

Hacker: *What are you doing? Why are you researching my Trojan? What do you want from it?*

This dialog is not from any software installed in AVG's virtual machine. On the contrary, it's an integrated function of the backdoor and the message is sent from the hacker who wrote the Trojan. It seems that the hacker was online and he realized that we were debugging his baby.

AVG: *I didn't know you can see my screen.*

Hacker: *I would like to see your face, but what a pity you don't have a camera.*

The hacker was telling the truth - this backdoor has powerful functions like monitoring the victim's screen, mouse controlling, viewing process and modules, and even camera controlling. No Diablo III key logging code was captured as what it really wants to steal is dial up connection's username and password. The malware and its components were detected by AVG as Trojan horse BackDoor.Generic variants.

We chatted with the hacker for some time, pretending that we were new to this and would like to buy some malware from him. But during the course of the conversation, it became clear this hacker was not foolish enough to tell us everything and he ended the conversation by shutting down our system remotely.

Part 4: Appendix

Other reports from AVG Technologies

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 4: 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 114 million active users as of March 31, 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>