AVG Community Powered Threat Report

Q2 2011

Contents

Introduction

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

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

With more than 110 million users using AVG's various solutions, AVG provides strong community protection. Each new user who chooses to participate increases the security level of all of us as a whole.

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.

Q2 2011 Highlights

Web Threats	
Rogue AV Scanner	The most active threat on the Web, **35.79%** of detected malware
Blackhole	The most prevalent exploit toolkit in the wild, accounts for 75.83% of toolkits
37%	Exploit Toolkits account for **37%** of all threat activity on malicious websites
11.3%	Of malware are using external hardware devices (e.g. flash drives) as a distribution method (AutoRun)
Mobile Threats	
com.noshufou.android.su	The most popular malicious Android application
997,362	Malicious SMS messages were detected
298,339	Malicious mobile applications were detected
Messaging Threats (Spam)	
USA	Is the top Spam source country
32.9%	Of Spam messages originated from the USA followed by the United Kingdom with 3.9%
bit.ly	Is the most exploited URL shortening service which is abused to spread Spam messages
English	Is the top language used in Spam messages

Key Points – Q2 2011

The trend in Q2 2011 could be characterized as '**the shift**'. As cybercriminals are shifting some of their efforts to better monetize having the increased popularity of new computer platforms there is also a shift in responsibility of cybercrime damages to the victims. This quarter we noticed that cybercriminals are utilizing the knowledge, experience and tactics to explore 'new markets' to increase revenue from their operation. These criminals are performing even more sophisticated attacks in order to steal assets that can later be used to simplify other, more sophisticated, attacks. Although we have not seen any specific technical innovation by these criminals this quarter, we did find business innovation and creativity that are not less important for them. As we mentioned in the past, and will probably be said in the future, cybercrime is growing and will continue to grow with great financial success for the criminals operating it.

The main stories spotted by AVG Threats labs during Q2/2011:

(1) Stealing the *keys to the house* becomes easier than *breaking the Windows* – the rise of **Trusted Malware:** As digitally signed code unlocks 'doors' to enable binary code to execute on a PC, hackers increased their efforts in stealing digital certificates to sign their malware with it. Starting 2011, and more specifically in Q2, AVG Threat Lab has seen a rise of stolen digital certificates being used to sign malware before it is being distributed by hackers. We have detected 53,834 pieces of signed malware in the first 5 months of the year comparing to 39,102 during the whole 2010, indicating an increase of **over 300%**. Although in the last few years we have seen many faked digital certificates in use by cybercriminals, the use of stolen legitimate keys is a major trend these days.
These stolen digital signatures are used to "sign" a malware application in order to trick the Windows OS security mechanism and the end users since a "signed" file is considered to be trusted. Stolen certificates made the headlines recently with the highly publicized Stuxnet worm that used valid stolen certificates and the RSA hack in March, which is claimed to be related to the Lockheed Martin network breach of last month. In this report, we present some examples of malware using legitimate digital signatures as detected and analyzed by AVG Threat Labs.

(2) It is the 'Business' of the Business to be protected from online banking malware - **A Spy on the SpyEye Operation: Having the recent publication on a US court ruling of a case where money was stolen from a business as a result of a malware,** AVG Threats Labs shares some insights on the most investigated piece of online banking malware in the past few years - SpyEye. AVG Threat labs investigated 702 Command & Control servers in the first half of 2011, together they collect online banking credentials from hundreds of thousands of people and businesses worldwide. United States holds the lead of Command & Control servers with 30% 'market share', the runner up is Ukraine with 22% 'market share'.

(3) Mac users, welcome to the world of targeted Cyber attacks - **New Dog, Same Old Tricks – Mac Attack:** Like any other business that is constantly looking to increase its operation and revenue, **cybercriminals identified the rise of Mac users and are starting to target them**. What Windows users have known for a while, Mac users are starting to get acquainted with. Criminals are targeting Mac OS using the same old tricks well known to Windows users – social engineering.

(4) Mobile cybercriminals monetize via fake Apps and premium SMS - **Mobile Malware**: Cyber criminals utilize monetization techniques that are much easier to operate than the ones in use on PC. Spamming users to download Apps or simply posting them on online stores/Markets make the software distribution easy and scalable. This was clearly demonstrated by the continued effort by Google to clean its Android Market and IM spam messages sent to mobile users. **Leveraging premium SMS services** that can be sent from any mobile device, they monetize their activity worldwide.
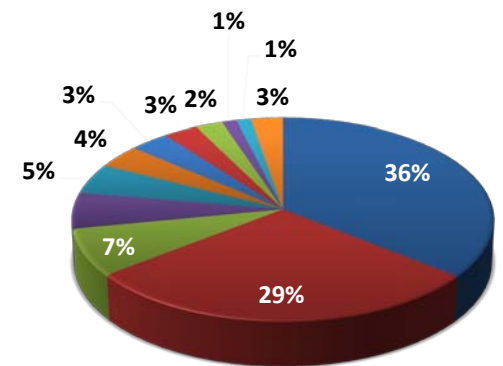
Quarterly Key Metrics: April – June 2011

Metrics -Web Threats

Top 10 Web Threats Prevalence Table Q2 2011

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

Rogue Scanner	35.79%	Pages containing fake virus scanners, or appear to be pages pushing fake antivirus products. Such pages intend either (or both) to lure end user to buy worthless software, or to install malware under the cover of seemingly useful software
Blackhole Exploit Kit	28.66%	Pages containing script code characteristics of the Blackhole exploit kit, which is used to install a range of malware
Fragus nulled exploit kit	7.48%	Exploit toolkit which is used to install a range of malware
Social Engineering	5.73%	These pages contain a code/information which tries to lure people into downloading malicious code
Pharmacy Spam Site	3.75%	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
Link to Exploit Site	3.34%	These pages contain links to known exploit sites. In some cases, malicious code is automatically downloaded without any user intervention
Facebook Clickjacking	2.92%	Facebook Clickjacking Worm
Rogue Spyware Scanner	2.29%	Pages containing fake anti-spyware scanners, or appear to be pages pushing fake anti-spyware products. Such pages intend either (or both) to lure end user to buy worthless software, or to install malware under the cover of apparently useful software
Fake Codec	1.23%	Malicious Trojan disguised as a video codec
NeoSploit Exploit Kit	1.22%	Crimeware toolkit which is used to install a range of malware

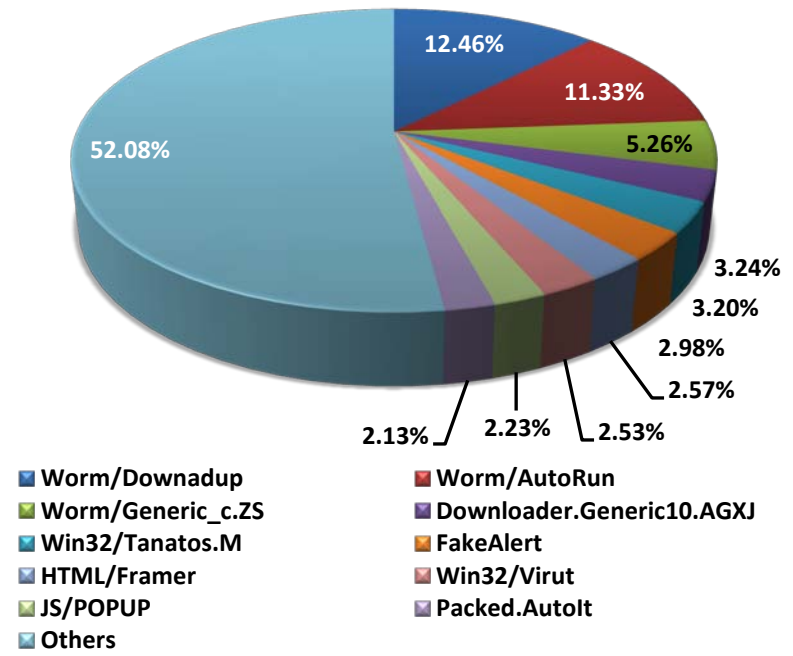**Top 10 Web Threats Prevalence Chart Q2 2011**

- Rogue Scanner
- Blackhole Exploit Kit
- Fragus nulled exploit kit
- Social Engineering
- JavaScript Obfuscation
- Pharmacy Spam Site
- Link to Exploit Site
- Facebook Clickjacking
- Rogue Spyware Scanner
- Fake Codec
- NeoSploit Exploit Kit
- Others

Top 10 Malware Threat Prevalence Table Q2 2011

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

Worm/Downadup	12.46%
Worm/AutoRun	11.33%
Worm/Generic_c.ZS	5.26%
Downloader.Generic10.AGX	3.24%
Win32/Tanatos.M	3.20%
FakeAlert	2.98%
HTML/Framer	2.57%
Win32/Virut	2.53%
JS/POPUP	2.23%
Packed.AutoIt	2.13%

Top 10 Malware Prevalence Chart Q2 2011

- Worm/Downadup
- Worm/AutoRun
- Worm/Generic_c.ZS
- Downloader.Generic10.AGXJ
- Win32/Tanatos.M
- FakeAlert
- HTML/Framer
- Win32/Virut
- JS/POPUP
- Packed.AutoIt
- Others

Behavior Categories Chart Q2 2011

This table presents threats prevalence as detected by AVG 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 of files and prevents their execution
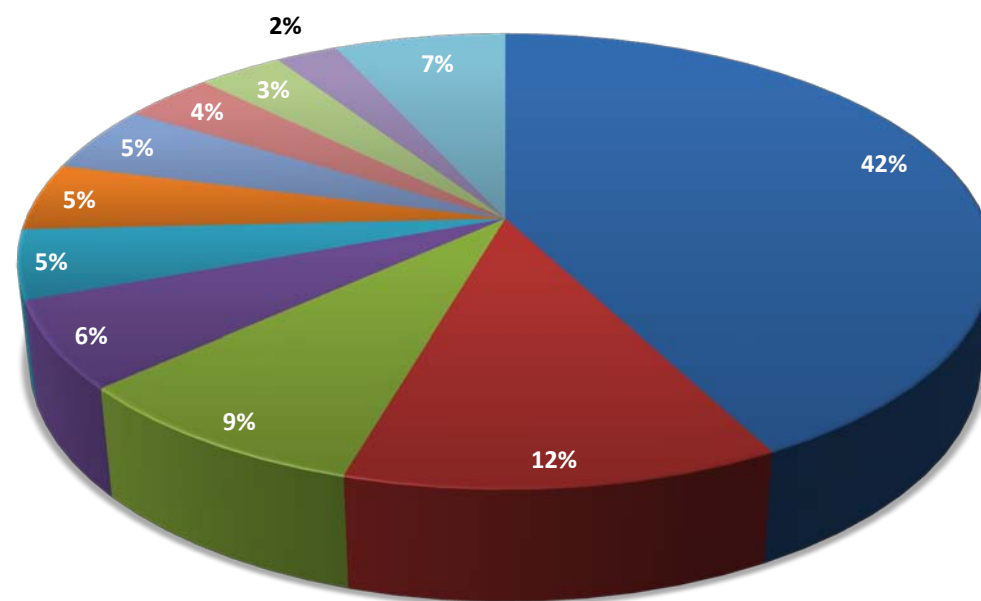
- Trojan
- Adware/Spyware
- Downloader
- Adware
- signed
- Virus
- PUA - Potentially Unwanted Application
- Network Worm
- Malware
- Backdoor
- Others

Top Exploit Toolkits Seen in Q2 2011

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

1	**Blackhole**	**75.83%**
2	**Fragus**	**19.75%**
3	**Neosploit**	**3.22%**
4	**WebAttacker**	**0.58%**
5	**Siberia**	**0.16%**

Metrics - Mobile Threats

Top Malicious Android Applications Q2 2011

Top malicious Android applications as detected by AVG Threat Labs	
com.noshufou.android.su	52.92%
android.tether	10.41%
com.z4mod.z4root	7.23%
com.corner23.android.universalandroot	2.29%
com.android.tethering	1.84%

Metrics - Email Threats

Top 10 Domains in Spam Messages Q2 2011

		Top domains used in Spam messages	
1		kore.us	1.3%
2		amazon.com	1.2%
3		bit.ly	1.2%
4		hotmail.com	0.9%
5		facebook.com	0.7%
6		walmart.com	0.6%
7		gmail.com	0.6%
8		6pm.com	0.6%
9		mail.ru	0.5%
10		dieneme.com	0.5%

Top 5 Languages in Spam Messages Q2 2011

		Top languages used in global Spam messages	
1		English	81.2%
2		Unknown	6.6%
3		Portuguese	2.6%
4		Spanish	2.1%
5		German	1.7%

Top Countries of Spam Senders Q2 2011

		Top Spam source countries	
1		United States	32.9%
2		United Kingdom	3.9%
3		Brazil	3.8%
4		India	2.8%
5		Russian Federation	2.5%
6		Germany	2.3%
7		France	1.7%
8		Vietnam	1.6%
9		Republic of Korea	1.5%
10		China	1.5%

Web Risks & Threats

Trusted Malware?

Digital certificates were introduced to provide a method to declare, by a known and trusted authority, that a given file was created by a known and trusted provider. Using this method one can trust the authorities to issue certificates and benefit from the chain of trusts for all signed files of their trusted providers. Nowadays, digital certificates are widely used in modern operating systems to unlock protection layers and allow files to be executed, knowing a trusted authority confirmed the legitimacy of the file. Many companies sign their software products with such digital certificates so they can be easily recognized as trusted by security components.

Does it mean that signed equals trustworthiness'? Not necessarily. We currently see a rising trend of stolen digital certificates used by malware authors. Compared to 2010, we have witnessed a three-fold rise in the number of malware signed with a stolen certificate in 2011. The advantages of using stolen certificates for hackers are clear: 1) Signed files are considered to be more trustworthy. 2) In order to install certain types of software on Windows Operating Systems (Vista & Win 7), the file has to be properly signed with a trusted certificate. This means the file gets installed without the end user getting OS warnings and, in case someone checks the signature, they will see a trusted company name. Although almost anyone can obtain a valid certificate from the CA (Certificate Authority), this certificate cannot hold the name of a known trusted company. By stealing the certificate of a trusted vendor, malware writers minimize the chance of their malicious software being detected quickly.

We anticipate that 'stolen keys' such as digital certificates, tokens and passwords will eventually become a significant problem. They are likely to be utilized by high revenue generating malware such as Zeus or being used by countries/organizations as part of their cyber war, political agenda or industrial espionage. We have already seen the examples of this recently with Stuxnet and the RSA hack, which might lead to the Lockheed Martin breach and other examples. Other popular examples are the use of stolen certificates by malware toolkits to automatically generate signed malware.

Let's look at two examples of (ab)use of digital certificate theft:

Case #1: Qbot variant signed by BlackBaud Inc.

The first case is the Qbot aka QakBot aka PinkSlipbot worm variant. Qbot is what is known as a **Trojan Banker**. A Trojan Banker aims to steal information such as bank accounts, usernames, passwords and credit card details from your computer and sends it to the attackers. In this example, it also has the capabilities to steal digital certificates and upload them to an FTP server.

Qbot uses well known ways to spread itself such as open/system shares and thumb drives. Qbot's capabilities are:

- IRC backdoor with self-update functionality
- Command & control support
- Credential and password stealing/logging and reporting capability
- HTTP/HTTPS communication interception and monitoring
- Multi-component body
- Security software solution termination
- Self-protection and hiding
- Rootkit capability (API hooking)
- Stolen digital certificate usage

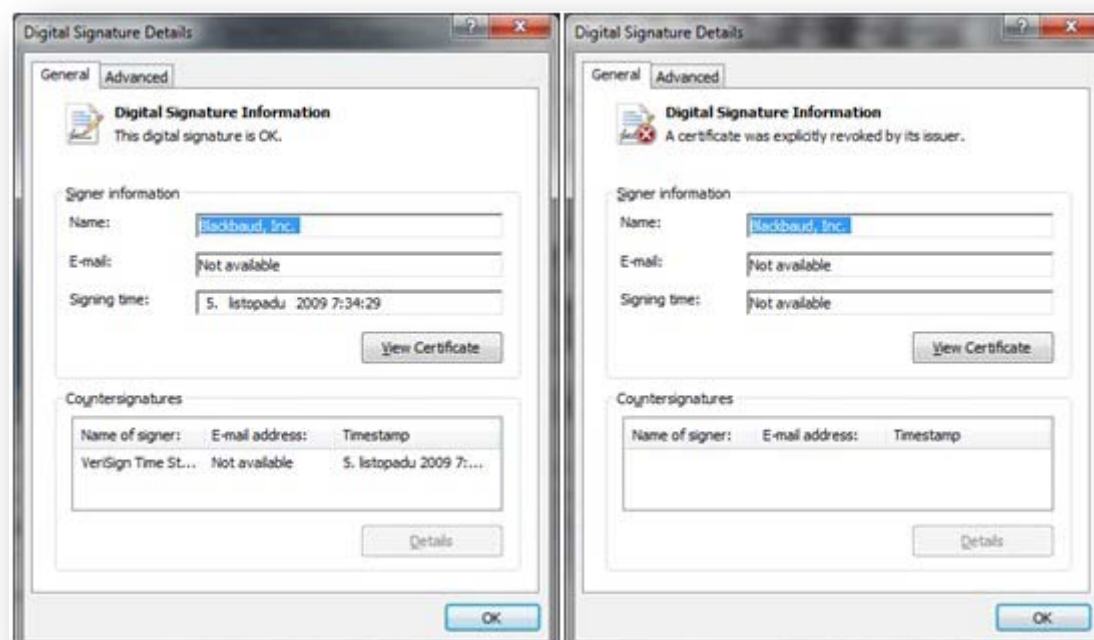When looking at Qbot's digital signature we can see the following:

As seen on above screenshots, both files are signed by Blackbaud, Inc. At the time of writing the certificate was already revoked by its issuer thanks to a proactive report.

- The Qbot initial infection is usually via drive-by-downloads on various exploited websites.
- Qbot uses an interesting, and innovative way of starting itself after a computer restart: It "emulates" an existing \Run registry item by adding the original executable path as parameter to the new malware path. In our case it takes the "AVG_TRAY" item and overwrites its value with the "emulated" one.
- The main executable, DLL component and all folders with Qbot files are hidden using an API hook technique. Functions from advapi32.dll, kernel32.dll, user32.dll, ws2_32.dll and others **are hooked to evade Anti-virus tools and system tools to track them down**.
- Qbot is targeting the following banking domains:
  - sovereignbank.com, cunet.org, amegybank.com, synovus.com, suntrust.com, bankofamerica.com, usbank.com, bokf.com
  - ibanking-services.com, web-cashplus.com
  - frostbank.com, pncbank.com, jpmorgan.com, ktt.key.com, premierview.membersunited.org
  - directline4biz.com, webcashmgmt.com, moneymanagergps.com, klikbca.com, express.53.com
  - itreasurypr.regions.com, goldleafach.com
  - wachovia.com, wellsfargo.com
- Qbot also tries to eliminate/block a long list of security solutions:
  - Agnitum, ahnlab, arcabit, avast, avg, avira, avp, bitdefender, bit9, castlecops, centralcommand, clamav, comodo, computerassociates, cpsecure, defender, drweb, emsisoft, esafe, .eset, etrust, ewido, fortinet, f-prot, f-secure, gdata, grisoft, hacksoft, hauri, ikarus, jotti, k7computing, kaspersky, malware, mcafee, networkassociates, nod32, norman, norton, panda, pctools, prevx, quickheal, rising, rootkit, securecomputing, sophos, spamhaus, spyware, sunbelt, symantec, threatexpert, trendmicro, virus, wilderssecurity, windowsupdate, webroot.

As you can see above, we are looking at a well-crafted piece of malware with advanced features and functionality. And we are sure more will come with more features and more improvements, so we all must be prepared.

Case #2: ZXShell backdoor signed by Gameforge Productions

Another digital certificate theft case involves the certificate of the Gameforge Productions GmbH software company. All parts of the Trojan horse are signed with a valid but stolen digital certificates. Let's have a look at the certificate details first:

Figure 2-Which one is bad? (Hint -malware is on the left)
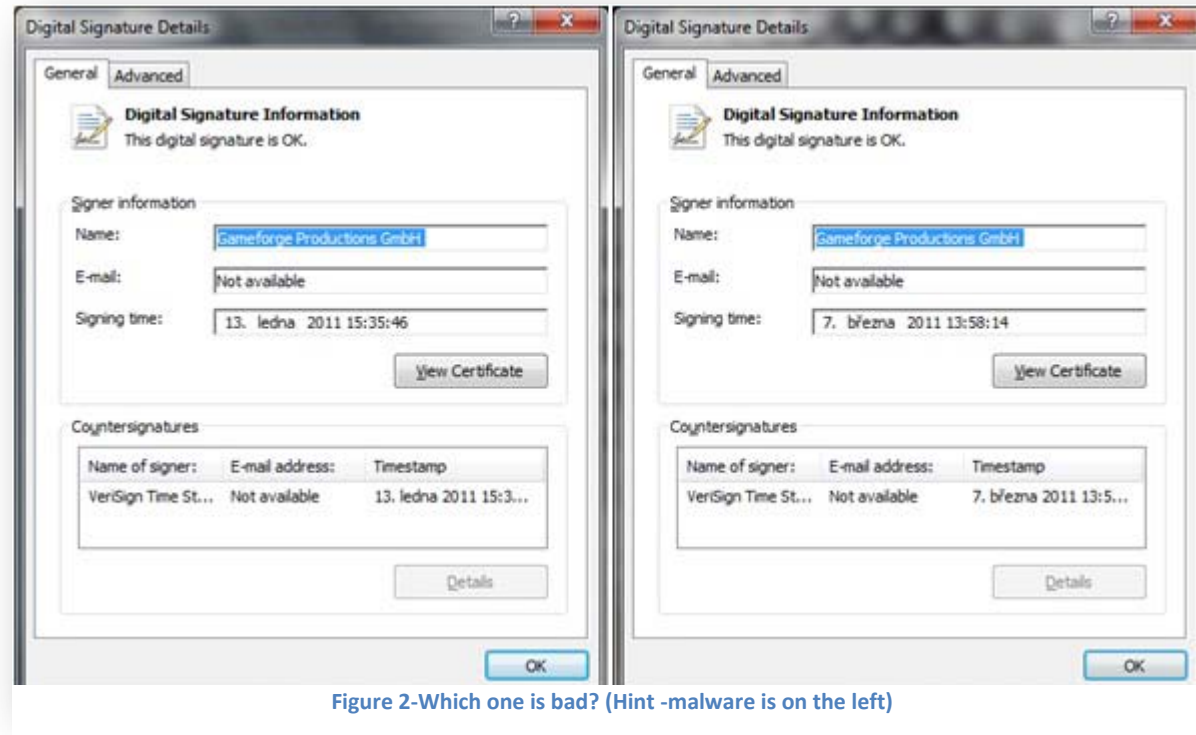
As you can see the bad certificate is still valid even though it was reported to the vendor a couple of weeks ago by AVG.

The main component of this Trojan is a remote administration tool, a client executable of Chinese origin. The Trojan is capable of doing the following:

- Remote control terminal
- Remote desktop monitoring
- File management
- Port mapping
- Socks proxy server
- Direct command line access support
- Security software termination and evading

Another interesting part of this sample is that the main dropper has two versions of the ZXShell backdoor in its Resource section: one for the x86 OS architecture and one for x64 OS support:
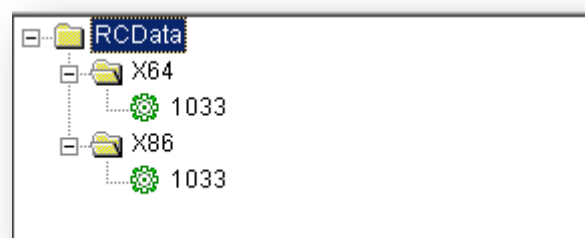
Resources tree

Upon execution of any of the DLL components, the rootkit component is dropped into the System folder; **The rootkit component is responsible for termination of various security solutions such as 360Safe, AVP, AVG, IceSword and others** (the list depends on the malware variant).

The malware authors also attempted to use authentic and trustful VersionInfo description in all their binaries.

![AVG logo]

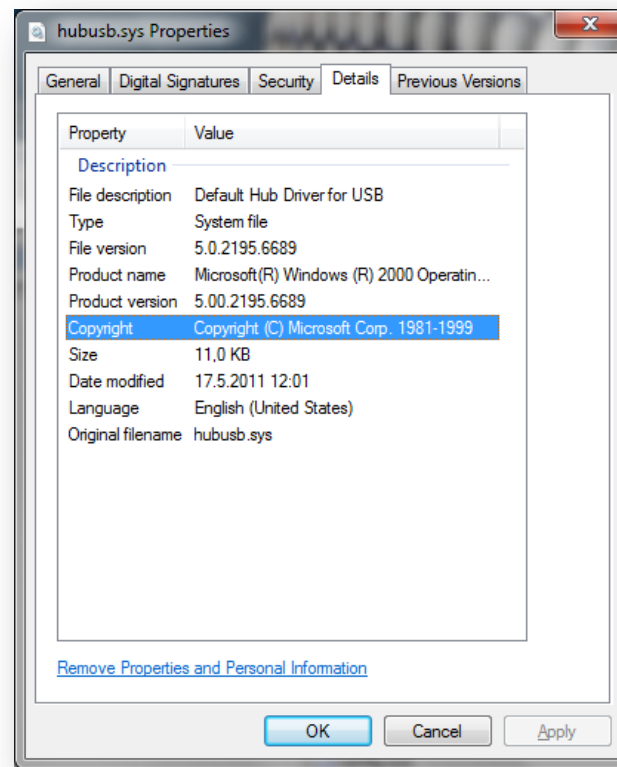The problem is that files described as Microsoft files should not be signed by Gameforge Productions GmbH:

Figure 3-This looks OK … but it is not!

Once the DLL component is executed, it contacts the master server bot.timewalk.me on the port 80 and waits for commands to be passed on. These are the essential ZXShell commands:

- CloseFW – shutdown Windows Firewall
- Execute – start program
- FindPass/FindDialPass – list password of the given system/dial-up account
- SYNFlood – SYN DoS attack
- ZXHttpProxy/ZXHttpServer/XFTPServer – configure particular server

Recommendations

- Take precautions when handling a signed file, code signing does not come with any guarantee about what the code does or whether it's malware-free.
- Security vendors, especially Anti-virus vendors, should not automatically assume that validly signed files indicate it can be trusted. The automatic whitelisting approach of digitally signed code should be evaluated.
- The need for AV companies to have their own trusted certificate list and not just rely on the certificate issuer is almost a requirement these days.

A Spy on the SpyEye Operation

The last few years, security researchers from all around the world have been investigating the two most interesting pieces of malware targeting online banking users worldwide: SpyEye & Zeus.

Research documents, videos, headlines and security products were released to help raise awareness and fight this malware.

The criminal activities of the people involved in making and using this malware were also documented. A few arrests were made by law enforcement organizations, and a few Internet Service Providers were cut off to help stop such activities.

Large command and control (C&C) servers helping in the operation of such malware were investigated in detail by security researchers, and their reports were published in public and closed forums.

Having the increased interest and volume of such malware operations, dedicated Zeus & SpyEye tracking sites emerged to help the security community fight against these criminals' activities.

The malware managed to consume lots of attention and resources from the security community to track them down. This is probably indicative of the size of the criminal organization(s) behind them.

Despite their large operational size and known financial damages to individuals and businesses, many people question who should be held responsible and recover financial losses as a result of these criminal attacks. Until recently, there was the belief that banks are responsible for money stolen by these criminals. However a recent US court ruling has changed that belief – it is the business of the Business to protect itself from such attacks and losses.

In this report, we share some statistics about the magnitude of such SpyEye criminal operation. We investigated over 700 C&C servers operated by cybercriminals during the first half of 2011.

C&C servers under research

AVG's people-powered-protection network includes millions of users installing and running our software on their PCs while connected online. Utilizing our multi-layered security engines, we managed to detect and report back to our Cloud-based data center on any suspicious malware activities.

By analyzing such activities, AVG's smart engines successfully identified 702 C&C servers around the world supporting the criminal operation of SpyEye during the first half of 2011. Some of these servers had been running for a while, and others just started at the current month.

Geographic distribution of the C&C servers under research:
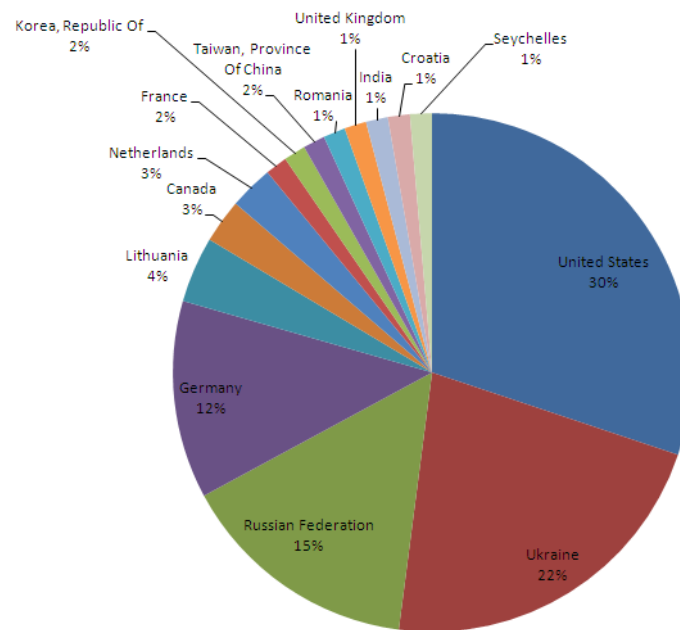
Geo Distribution of Spyeye C&C

We also noticed that some of the servers were running multiple C&C instances using different DNS names. Some IP addresses resolved to 84 different DNS records in use by criminals, indicating potential fast-flux hosting methods to protect their servers from detection and blacklisting.

Geographic distribution of the servers running more than one instance of the C&C:
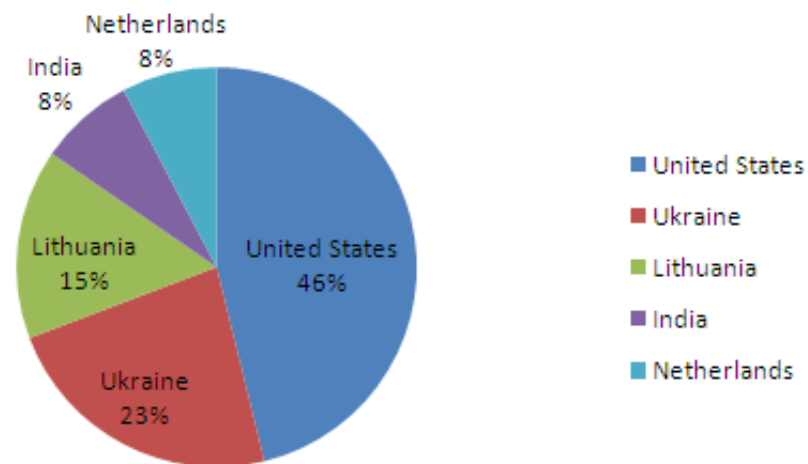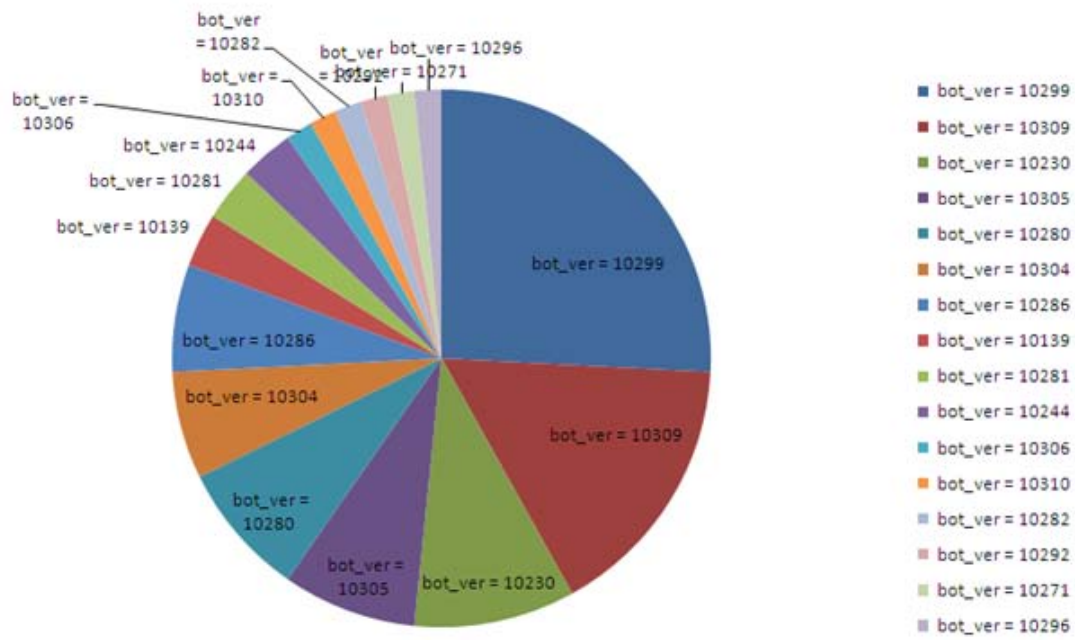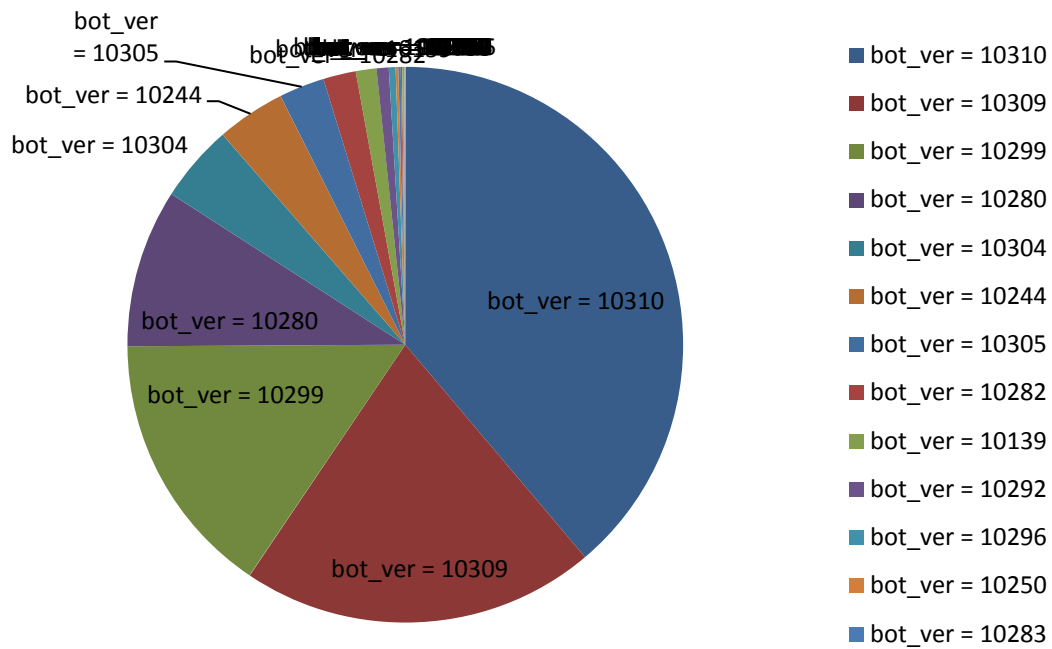
SpyEye bot versions under research

Analyzing data collected from the C&C servers included in our research, we identified over 30 malware versions involved in the attacks:

Oldest malware version: 1.1.39 ; Newest malware version: 1.3.10

Top malware versions used in Q1:

Top malware versions used in Q2:

As each C&C serves a different SpyEye malware binary, we were also interested to find how many unique binaries were involved. Our research uncovered over 140,000 different MD5 hashes being used by the servers under research.

While some of the C&C servers were using more than a hundred MD5s, others were using just a few.

By looking at the number of infected PCs per C&C, we found a few managing over 100K users while most of the C&C manage around 25K PCs on average. Surprisingly, the most active C&C server (with over 900M interactions with its managed infected PCs) was not the largest operation but more near the average size of 25K.

- The World-wide-web might as well be re-branded the World-**wild**-web. Our research indicated hundreds of live servers operating all around the world and active 24x7 to steal users' credentials for online banking and other private assets. While our research focused on just a single type of malware, we know many other types are in use by cybercriminals. The volume of criminal activities on the Web today can justify to be named the World-**wild**-web.
- As hackers are constantly improving their attack techniques, AVG believes that a security product to protect against these types of threats should include multiple layers of protection utilizing various detection technologies: signature-based, heuristics-based, and behavior-based for both network and content inspection. This is why we armed our AVG2011 product with all such layers to provide our users with an ultimate protection.
- When you go online, make sure you are secured and protected as it is wild out there.

Mobile Devices Risks & Threats

New Dog, Same Old Tricks – Mac Attacks

Recently, we have seen an attack targeting Mac Operating System using same old tricks. There is nothing new under the sun when it comes to the recently discovered Fake /Rogue Anti Virus (MAC Defender rogue antivirus) and crimeware Toolkits targeting Mac OSX and iOS.

Although Mac users are not as used to it, Windows users have long been targets of Rogue Anti Virus and crimeware toolkits. If Mac users believe that they are protected from these attacks, they should think again.

As AVG stated in the past, it is only a matter of market share, above a certain level any platform becomes a target. Cyber criminals pick their targets according to the expected revenue stream through monetization, hackers are where people are. Since Mac OS and iOS are becoming more popular, it was to be expected they would become a target.

The unwritten rule in security research says the 5% and 10% market share levels indicate when a product/OS becomes interesting enough for certain hackers to target and when the volume of attacks is expected to soar.
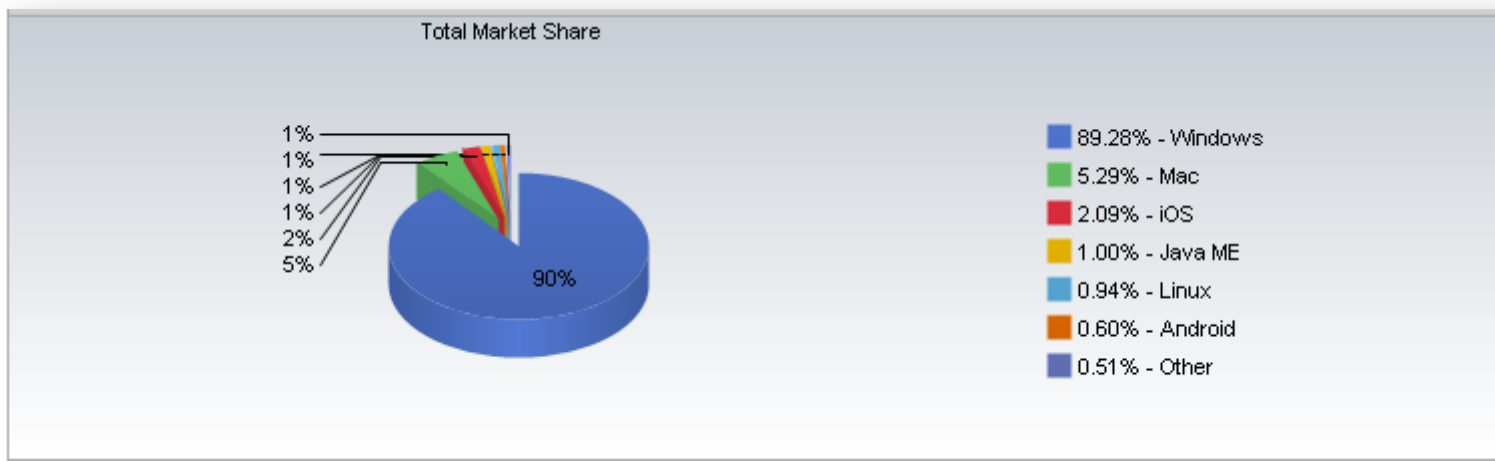

Figure 4 - Operating Systems Market Share (source: https://marketshare.hitslink.com/)

According to Net Applications (marketshare.hitslink.com), iOS and Mac together have 7.38% market share – indicating these platforms will be on the radar of hackers and will see initial mass attacks emerging. Once the 10% mark is crossed, we expect to find more such attacks to happen.
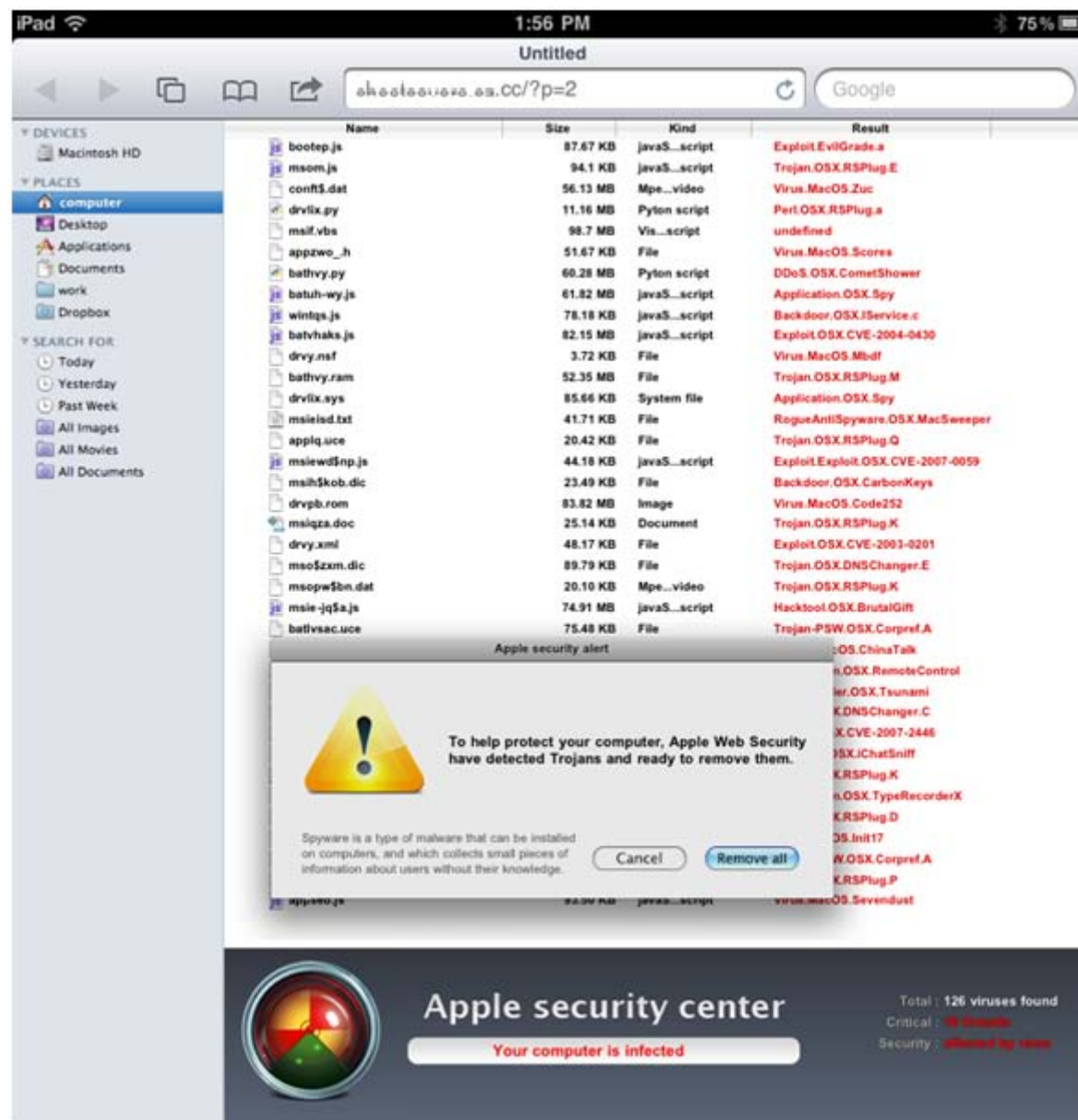

Figure 5 – A screenshot of the message used by the criminals as captured on iPad

The first major wave for Mac users is a rogue AV, the main reason is that it is the quickest and easiest way to monetize.
However, a new element to this fake AV is that it attacks both Mac OS, iOS (mobile devices) and Windows. **A Cross platform attack**.
This particular piece of malware was distributed using a massive SEO poisoning attack on Google; Google's search results act as the referrer.
It acts as any other Rogue AV we have seen before, first the user is presented with a fake anti-virus scanning screen, which presents fictitious infections and then asks the users to purchase a copy of the software to 'remove' these infections. Anything a victim clicks on will leads to a server serving malware.

AVG Threat labs have seen close to 2,000,000 hits during May, during the peak days we have seen more than 150,000 hits a day.
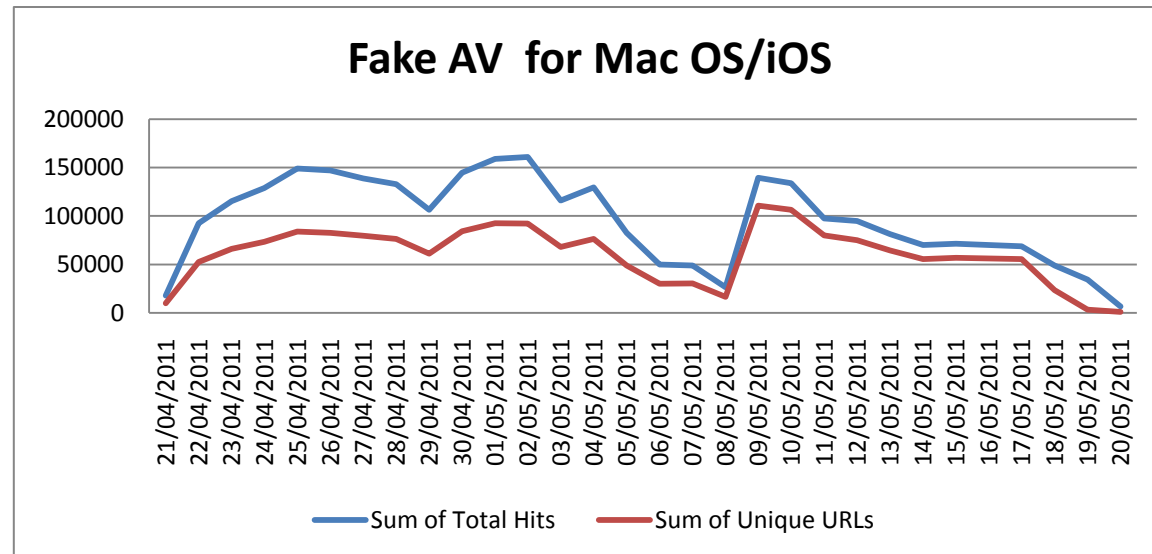
Recommendations

- For Mac users, it is a good time for a re-think. Their devices were "secure" as long as the market share was way below the Windows OS market share. However, with the exponential growth of iOS market share resulting from the popularity of the iPhone & iPad. They are appearing on the criminal's radar and should expect to find that your devices are not as secure as they might think.
- For Mac users, it is also a good time to look for anti malware solutions for their Mac, iPad and iPhone if they wish to protect their devices. However, they should be careful and avoid the fake ones out there.
- AVG provides a FREE protection – AVG Linkscanner for Mac – to protect OS X users from these attacks

Mobile Malware

As anticipated in our last report, this year mobile malware is going to make the headlines. A lot of this may be explained by the massive and practically defenseless target posed by the exploding number of smart phones, tablets and other advanced mobile devices.

Gartner foresees that the total mobile communication devices' sales to the end user will reach ~413 million devices – this is an 'attractive' target for hackers.

Responding to this development we noticed that cyber criminals are shifting more resources from PC to mobile. The current low security awareness among mobile users opens the door for cyber criminal to monetize quickly.

Additionally, the fact that there is no need to go through the evolution of malware development which was necessary for PC targeted attacks, the knowledge and the tricks are already there. Cyber criminals just have to execute.

AVG Threat labs have spotted various monetization methods criminals are using on mobile platforms. The most popular being Premium SMS. All they need to do is persuade a user to download an App that they think they need. When installed it sends an SMS to a premium number to monetize that victim.

Below is one example out of many we found this quarter.

China mobile is considered the world largest phone operator with more than 70% of the Chinese domestic market and 518 million subscribers (source: Guardian.co.uk).

1. The chosen attack vector was a text message to China Mobile subscribers.
2. It used a phishing attack, disguised as coming from China Mobile, trying to lure users to believe that this is coming from 10086 and China Mobile. The message contained a link to a phishing site.
3. The cyber criminals used a domain name which is similar to the legitimate site, 1oo86.cn instead of the real 10086.cn (using the letter "O" instead of the digit zero) which is difficult to notice by a novice user.

Figure 6- Translated SMS Content

4. When clicking on the link, an App was downloaded and the user would not suspect anything because they expect that an update will be downloaded and installed. The attacker gets another advantage here – if the user sees nothing on their device, they forget about it and leave the malware untouched.
5. The criminals developed two variants, one for Android and one for Symbian OS.

6. When installed, it performs the following activities:
   a. It downloads a configuration file.
   b. It sends out device information (as IMEI number, phone model, and SDK version)

c. It writes to a log file
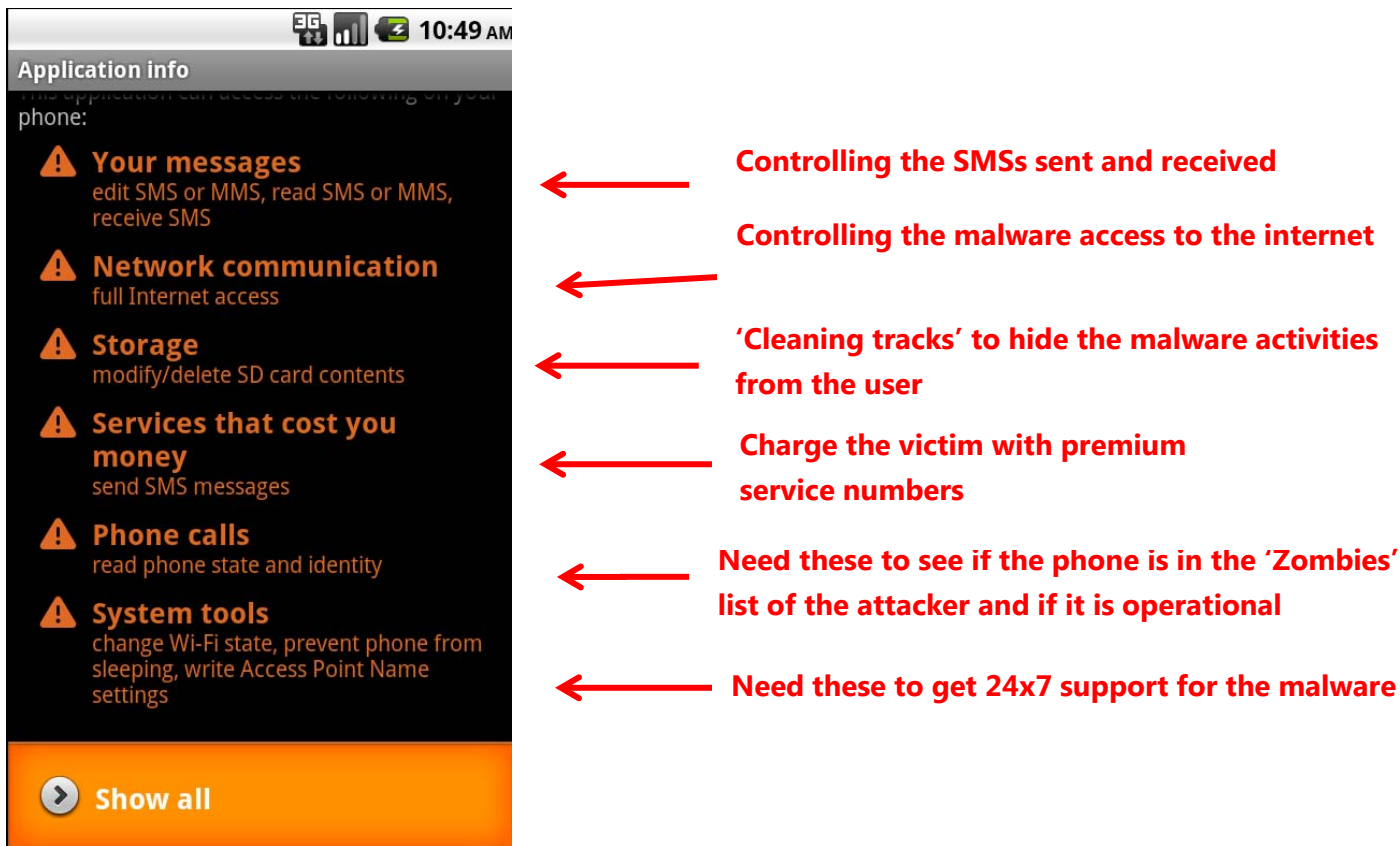d. It allows remote control / monitor the device.

Figure 7 - Android Variant

e. Update mechanism

The crown jewels of this piece of malware are the "premium SMS charges". The malware is sending text messages to premium rate numbers. Premium Messaging is where a user is subscribed to receive content and is billed by a third party. The charges can be one-time or recurring. The subscribing processed is being monitored by the cyber criminals.

The user is being charged premium prices, and their phone bill is increasing. The malware can hide these activities from the user by not listing the send/received text messages.

Up until now, the main tactic used by hackers is by uploading malicious application to the Android Market place. Google, for the second time in the past three months, had to remove dozens of malicious applications from the Google market. Some of these apps were pirated legitimate programs that had been modified with malicious code and uploaded to the Google Market.

However, as seen by AVG Threats Labs lately, a phishing method is being used by sending Text messaging or Instant Messaging or Emails with content which tries to lure users into installing malware to their mobile. Cyber Criminals are using Social Engineering tactics when targeting mobile users as done to PC users. Cyber criminals know they can be successful bytargeting the weakest link in the chain, the human part! Social Engineering attacks are more difficult to protect against.

As with the above example, the criminals' mobile monetization is mainly coming via premium paid services such as SMS Trojans, which send text messages to premium rate numbers or by applications that initiate calls to highly rated numbers.

Mobile malware reached the sophistication and complexity of PC malware. Most mobile malware is using Command & Control to support and to update the malware remotely. This is done to maximize the profit for the criminals. With the C&C, the attacker can monitor any activity performed on the mobile device.

Recommendations
- Any mobile device should be equipped with security measures.
- AVG provides 'AVG Mobilation', free software for Android to protect users from such threats
- Become security aware, expect being a target for criminal activity
- Be cautious in what you download to your device.
- Monitor your device activities
- The most important task is… check your phone bills.

About AVG Technologies

AVG Technologies is a global leader in security software, protecting more than 110 million consumers and small business computer users in 170 countries. Headquartered in Amsterdam, AVG is the fourth largest vendor of anti-virus software and employs close to 600 people worldwide with corporate offices in the US, the UK, the Netherlands, the Czech Republic, and Germany.

AVG has nearly two decades of experience in combating cyber crime and operates one of the world's most advanced laboratories for detecting, pre-empting and combating web-borne threats from around the globe for both businesses and home customers.

The company boasts one of the most extensive self-help communities on the Internet, having established its technology credentials early on amongst technically savvy consumers.

www.avg.com