



AVG: Protecting your computer from tomorrow's threats today

Contents

Why you should read this paper.....	3
The evolution of commercial malware.....	3
Your identity: an extremely valuable commodity in the underground economy	4
The World Wide Web of deceit.....	5
Rapidly evolving and invisible threats: why your current security solution is not enough	6
AVG's proactive, preventive protection	7
Layered security: the best way to keep your computer and data safe	8
AVG Internet Security: complete security - complete peace of mind	9

Why you should read this paper

Security used to be a straightforward matter. Email was the primary attack vector and simply installing an anti-virus product and exercising caution when opening attachments mitigated the majority of threats. When a system did become infected, the consequences were not usually particularly dire; inconvenience and data loss were the most likely consequences. But times have changed. The Web has become the attack vector of choice and today's threats are rapidly evolving, stealthy and almost always motivated by profit.

This white paper provides an overview of the current threat landscape and explains why your current security solution is not enough.

The evolution of commercial malware

A decade ago, viruses and other forms of malware were authored primarily by young, attention-seeking amateur coders (script kiddies or script bunnies) seeking to earn notoriety in underground hacker communities. The sole purpose of their malicious programs was to inconvenience users by scrambling their data and/or making their computers unstable. While some of their creations caused widespread disruption, the majority were relatively unsophisticated and easily detected and blocked.

The security landscape has, however, changed markedly during recent years. Organized criminal gangs realized that there was money to be made from malware and recruited skilled programmers to create malicious programs. These programs were not intended to cause disruption, but to enable the theft of money or data or both. This led to the creation of an underground economy in which criminals can buy and sell both data and the programs that are used to steal that data. Kits such as MPack¹ are sold as commercial software, complete with support and update options, and enable anybody – even people without programming skills – to launch sophisticated attacks against unsuspecting users. Consequently, there has been an exponential increase in both the number of attacks and the number of compromised systems. During 2008 alone, more than 1.5 million new strains of malware were identified – which translates to tens of thousands of samples arriving in security companies' research labs every day.

Security threats have also become increasingly complex and interlinked. For example, in the past spam was used to push little blue pills and counterfeit software; but today it is used to push worms such as Storm².

When infected by the worm, computers would be co-opted into the Storm botnet – a centrally controlled network which, at one time, consisted of up to 50 million similarly compromised computers. Those computers would then be used, without the owner's knowledge, to send out spam emails to which the worm was attached in order to ensure the continued expansion of the botnet. Additionally, criminals could rent time on the botnet and use it to send out their own scam emails. While the Storm botnet may now be dead, others - such as Conficker³ – have already emerged to take its place.

Your identity: an extremely valuable commodity in the underground economy

For millions of people, using a computer to make financial transactions has become as routine as brushing their teeth. Consequently, today's personal computers are used to store and transmit a large amount of personal information - and that makes them an extremely attractive target for cybercriminals. Should your computer be compromised or its communications intercepted, an attacker may be able to establish your:

- Date of birth
- Social Security Number
- Address
- Telephone number
- Online banking information and passwords
- Email address and passwords
- Employment details

In other words, your computer can provide a criminal with enough information to enable your identity to be stolen.

“Web site attacks on browsers are increasingly targeting components, such as Flash and QuickTime, that are not automatically patched when the browser is patched. At the same time, web site attacks have migrated from simple ones based on exploits posted on a web site to more sophisticated attacks based on scripts that cycle through multiple exploits to even more sophisticated attacks that increasingly utilize packaged modules that can effectively disguise their payloads. One of the latest such modules, mpack, produces a claimed 10-25% success rate in exploiting browsers that visit sites infected with the module. While all this is happening, attackers are actively placing exploit code on popular, trusted web sites where users have an expectation of effective security. Placing better attack tools on trusted sites is giving attackers a huge advantage over the unwary public.”

SANS Institute, Top Ten Cyber Security Menaces for 2008⁶

The return on cybercrime is not nickel and dime; on the contrary, it is a multi-billion dollar industry. A study by Javelin Strategy and Research found that 9.9 million Americans lost a total of \$48 billion to identity fraud in 2008⁴. And according to Gartner, a leading research and advisory company, phishing scams alone cost consumers \$3.6 billion during 2007.

The World Wide Web of deceit

The Web has become the attack vector of choice. With email, attackers had only a limited number of ways to compromise a computer: either with an infected attachment or with a link to a website which would deliver a malicious payload. While attackers still use email, they have discovered that the Web provides them with a much broader range of options. Vulnerabilities in web browsers and browser add-ons, such as Flash, QuickTime and Microsoft Silverlight, provide backdoors which enable systems to be infected with keyloggers, password-stealing Trojans and other forms of malware. And there is certainly no shortage of those backdoors: Internet Explorer alone has had more than 70 announced vulnerabilities in the last two years. Web 2.0 technologies provide attackers with new mechanisms for attack such as cross-site scripting in AJAX and RSS/Atom injection.

Compounding the problem is the fact that no website can be considered safe. Established and popular websites which users would usually trust

"The hallmark of today's web-borne infections is 'here today, gone tomorrow'. Unlike LinkScanner, web security products that rely on visiting and scanning websites to deliver a safety rating to users would have to visit every one of the hundreds of millions of sites on the Internet every day to provide protection against these threats – a technological impossibility even with today's supercomputers."

J.R. Smith, CEO, AVG Technologies

can be compromised and used as malware delivery vehicles without the site owner's knowledge. Similarly, advertisements can be designed to exploit vulnerabilities in web browsers and browser add-ons and distributed via advertising networks across numerous websites. Such attacks have become extremely common. During

the second half of 2008, 70 of the world's top 100 websites were found to have either been compromised or to contain links to other malicious websites⁷. In January 2009, thousands of websites – including sites belonging to Fortune 500 companies, federal agencies, embassies, celebrities and even some security companies – were compromised and used to steal data from unsuspecting visitors⁸.

Rapidly evolving and invisible threats: why your current security solution is not enough

In order to be able to successfully extract data and/or money, cybercriminals need their malicious programs to remain on computers undetected and, consequently, the destructive viruses of the past have been superseded by malware that is much more stealthy. Today, simply visiting a trusted website can result in a computer being stripped of its sensitive information without the user having a clue as to what has happened - until, that is, he finds that his online accounts have been compromised or there are unexplained items on his credit card statement. But it is not only detection by users which cybercriminals need to avoid in order for their schemes to succeed; it is detection by security products too – and they are deploying increasingly sophisticated techniques in order to do just that.

To hide from search engines such as Google and from solutions like Site Advisor or phishing filter products – all of which regularly scan the Web in an attempt to seek out and blacklist malicious sites - attackers use temporary websites which are online for only a matter of hours before being taken down and the malicious content moved to a new website. Research by AVG Technologies indicates that between 200,000 and 300,000 new infective websites come online each and every day. While such sites may only be live for a short period of time, they are nonetheless able to infect a substantial number of computers thanks to spam campaigns relayed through botnets and through social networking sites such as Facebook.

To detect malware, traditional security products rely on signatures. These signatures are byte sequences – or code snippets – extracted from the original malware and are pushed out by vendors whenever a new piece of malware is discovered. Security products use these signatures to perform pattern matching. Should a file be found to contain a byte sequence that matches a signature in the security product's database, it is classed as malware and the user notified. Consequently, cybercriminals want to prevent security companies from obtaining their malware as, without a sample, they cannot release a signature – and that means the malware will be able to remain undetected for longer and, accordingly, be able to infect more computers. To keep malware out of the hands of security companies, its creators use a variety of techniques including browser and operating system validation, download threshold restrictions and randomization. This means that

websites can push different content to different visitors: a security company's automated search tools can be served content that is completely harmless, but a person visiting the website with an unpatched browser can be served malicious content.

Even when security companies do obtain a sample of the malware, blocking it can be much harder than it was in the past. Metamorphic¹⁰ and polymorphic¹¹ coding techniques enable the creation of malware which can change its signature upon each new infection. Similarly, some malware is encrypted in order to make it unreadable to anti-virus scanners (in such cases, detection relies on being able to detect the presence of the decrypting module rather than the virus itself).

Today's sophisticated and rapidly evolving malware is beginning to expose the shortcomings of traditional signature-based detection methods – and that's putting users' data at risk. Research by a security company in 2007 highlighted the extent of the problem: 72% of company computers and 23% of home computers that ran signature-based security products were found to be infected by malware.

AVG's proactive, preventive protection

Proactive, preventive protection starts with AVG's LinkScanner technology scanning the packets of code being sent over the trusted web-browsing HTTP channel. While there are millions of different pieces of malware code floating around on the Internet, the number of different types of packages in which they are distributed is in the hundreds. So LinkScanner looks at the packages and, when it spots one that it recognizes, it simply prevents that package from being delivered to the user's PC. So any web page that tries to deliver a drive-by download or other exploitative threat is unable to deliver its infective payload without the need to specifically identify that payload.

"If it looks like a duck, quacks like a duck and waddles like a duck, then it probably is a duck". While this saying may seem completely irrelevant to the subject of malware detection it is, in fact, anything but. In much the same way that a person can identify a duck by its waddle and quack, a security product can identify malware by its behavioural characteristics. The process is known as heuristic detection or heuristic analysis.

To be able to steal user data, malware must perform certain actions that would not normally be performed by a legitimate program. For example,

a legitimate program would not normally attempt to conceal its presence on a computer, inject code into another program, log user keystrokes or access areas of the computer in which passwords are stored. By looking for such behaviours, heuristic security products are able to identify potentially malicious programs and block them before they can cause any harm.

The main advantage of this approach is that the window of opportunity – that is, the time between a new piece of malware being released and a signature for it being released – is completely eliminated. Accordingly, unlike signature-based products, heuristic products are able to protect against both known and unknown threats.

This is the approach taken by AVG Identity Protection. AVG's new behavioural analysis technology detects and deactivates any suspicious activity on your PC before it can cause damage. In addition, it all happens in the background, in real time, and with minimal impact on system performance.

Users benefit from:

- Best of breed identity theft prevention through detection and blocking of new and unknown threats such as rootkits, Trojans, and keyloggers
- An instant layer of continuous proactive protection without the need for signatures or scanning
- A false positive rate that's 10 times lower than other behaviour-based products

AVG Identity Protection does not require other AVG products to be installed and running. However, when run with other AVG products, the combination delivers a highly effective layered security approach.

Layered security: the best way to keep your computer and data safe

No single detection mechanism can provide complete security: neither signature-based nor heuristic products are foolproof. However, by implementing a combination of detection mechanisms, the chances of malware slipping by can be drastically reduced.

Scenario: you receive a spam email which links to a malicious website that will attempt to silently install malware on your computer. If your only security product is a signature-based anti-virus product, you only have a

single line of defence against that malware – and that line of defence will fail if the malware is new and a signature has yet to be released and, as is increasingly likely, that website also may or may not be poisoned, depending on the time of day or the number of people clicking on the link.

But if, on the other hand, you are running a product which offers multiple detection mechanisms, you will have multiple lines of defence against that malware. The email may be blocked by your spam filter, the website may be blocked by your phishing filter, the malware may be blocked by your anti-virus product by its signature if it's a known virus or by its behaviour if it's not, and your safe-surfing protection will block its embedded poisons if they happen to be present when you click.

This is known as layered security – or defence in depth – and is the best way to protect your computer against today's sophisticated and rapidly evolving threats.

AVG Internet Security: complete security - complete peace of mind

In order to provide users with the ultimate in protection, AVG Technologies acquired Sana Security – the developer of an industry-leading heuristic detection product – and have incorporated Sana's technology into AVG Internet Security. Consequently, AVG Internet Security now provides unparalleled protection against the complete range of threats:

- **Anti-virus:** signature-based protection against malware
- **Heuristics:** behaviour-based protection against both known and unknown threats
- **Anti-rootkit:** protection from malicious applications that can hide from other security products
- **Web Shield and LinkScanner:** protection from web threats and malicious websites
- **Anti-spam:** blocks junk and phishing emails in Outlook, Windows Mail and other popular email applications
- **Firewall:** to secure computers against hacking

By combining these features into a single easy-to-use product, AVG simplifies security making it easier for customers to secure their valuable data against the complete range of internet security risks.

Customers using the commercial version of AVG Anti-Virus, the free version of AVG Anti-Virus or another company's anti-virus product can supplement and bolster their current protection by purchasing a standalone version of AVG Identity Protection

About AVG Technologies

AVG is a global security solutions leader protecting more than 80 million consumers and small business computer users in 167 countries from the ever-growing incidence of web threats, viruses, spam, cyber-scams and hackers on the Internet. Headquartered in Amsterdam, AVG has nearly two decades of experience in combating cyber crime and one of the most advanced laboratories for detecting, pre-empting and combating Web-borne threats from around the world. Its free online, downloadable software model allows entry-level users to gain basic anti-virus protection and then to easily and inexpensively upgrade to greater levels of safety and defense in both single and multi-user environments. Nearly 6,000 resellers, partners and distributors team with AVG globally including Amazon.com, CNET, Cisco, Ingram Micro, Play.com, Wal-Mart, and Yahoo!.

To find out more about AVG Technologies and its products, please visit www.avg.com.

References

¹ MPack:

[http://en.wikipedia.org/wiki/MPack_\(software\)](http://en.wikipedia.org/wiki/MPack_(software))

² Storm worm:

http://en.wikipedia.org/wiki/Storm_Worm

³ Conficker:

<http://en.wikipedia.org/wiki/Conficker>

⁴ US '08 identity fraud up in total dollars, victims:

<http://uk.reuters.com/article/marketsNewsUS/idUKN0646389320090209?pageNumber=1>

⁵ Pump and Dump Schemes:

<http://www.sec.gov/answers/pumpedump.htm>

⁶ Top Ten Cyber Security Menaces for 2008

<http://www.sans.org/2008menaces/>

⁷ 70 Of Top 100 Web Sites Spread Malware

<http://www.informationweek.com/news/internet/security/showArticle.jhtml?articleID=212901775>

⁸ Hackers turn Cleveland into malware server

http://www.theregister.co.uk/2008/01/08/malicious_website_redirectors/

⁹ Short-lived stealthy attacks are the new web threats

<http://www.avg.com/press-releases-news.ndi-222533>

¹⁰ Metamorphic code

http://en.wikipedia.org/wiki/Metamorphic_code

¹¹ Polymorphic code

http://en.wikipedia.org/wiki/Polymorphic_code

¹² Malware Quietly Reaching 'Epidemic' Levels

<http://www.darkreading.com/security/vulnerabilities/showArticle.ihtml?articleID=208803810>



Headquarters:
AVG Technologies, NV
Claude Debussylaan 46
NL-1082 MD Amsterdam
The Netherlands

North America:
AVG Technologies USA, Inc.
1901 Summit Tower Blvd.
Orlando, FL 32810, USA
Tel: + 1 (321) 274 1888
Fax: +1 (321) 274 1886
www.avg.com

UK & Ireland:
AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire, NG24 2EG
United Kingdom
Tel: 0844 894 1000
Fax: +44 (0) 1636 682201
www.avg.co.uk

Sales Department e-mail: sales@avg.com