# Why Traditional Anti-Malware Solutions Are No Longer Enough

## An overview of the threat landscape and how AVG 9.0 can help keep you and your business safe online

# Contents

## 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 paper provides an overview of the current threat landscape, explains why your current security solution is not enough, and demonstrates how AVG 9.0 can close the gap.

## 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 MPack[1] 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 Storm[2]. 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 Conficker[3] – have already emerged to take its place.

## Your identity: a 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

> "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 2008[6]

a large amount of personal information - and that makes them an extremely attractive target for criminals. If your computer is compromised or its communications intercepted, an attacker may be able to establish your:

- Date of birth
- Social Security or other national identity number
- Online banking information and passwords
- Email address and passwords
- Mailing address
- Telephone number
- Employment details

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

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 2008[4]. 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 in general – and social networks in particular - 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 75 announced vulnerabilities in the last two years. The so-called "social web" provides attackers with new mechanisms for attack such as cross-site scripting in AJAX and RSS/Atom injection.

> "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

Compounding the problem is the fact that no website can be considered safe. Established and popular websites which users would usually trust 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 websites[7]. 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 visitors[8].

## 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. More than half of such sites are live for less than 24 hours, but nonetheless they are 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. Metamorphic[10] and polymorphic[11] 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. Research undertaken by CoreTrace in the summer of 2009 found that more than 50% of companies consider signature-based protection to be inadequate against today's threats.

## AVG's three layers of protection

Imagine your valuable data is stored on a square of card and that AVG's three layers of protection are slices of Swiss cheese.

The first layer of protection is traditional anti-virus, which keeps known viruses, worms, spyware, and the like out of your system by matching them to a database. The holes in this first layer of cheese are where unknown viruses and here-today, gone-tomorrow web threats get in, because they're not detected by the signatures in your anti-virus. In AVG 9, signature-based scanning has been speeded up by marking files as safe or potentially unsafe during the initial scan, which enables the scanner to skip the safe files in future scans unless the file structure changes. As a result, scan time is dramatically reduced– by up to 50 percent depending on system configuration. AVG 9 also demonstrates improvements of 10 to 15 percent in both boot times and memory usage.

The second layer of protection is represented by AVG's LinkScanner® safe-surfing and safe-searching technology. LinkScanner takes care of the here-today, gone tomorrow threats on the web by understanding and blocking the distribution methods the

bad guys use. It's the only software to check the safety of a web page you're about to go to at the only time that matters - right at the time you're going to go there.

Other programs will only tell you whether the web site in question was clean the last time they checked it – which might be weeks or even months ago. Not too helpful when over 60% of web-based infections stay on the same site for less than 24 hours.

In AVG 9, LinkScanner delivers improved anti-phishing detection by more quickly and accurately determining whether or not a web page is hosting a phishing attack. This is accomplished by allowing the software to apply more than 100 different potential threat indicators to a page. If the result is inconclusive, LinkScanner then makes a call to the cloud to check a multitude of phishing feeds plugged into the AVG research network to make a final determination regarding threat potential.

Now there are fewer holes.

The third and final layer is unique to AVG 9 and keeps your data safe against new and unknown threats. It does this through co-operation between our Resident Shield, firewall, and identity protection modules, using cutting-edge technologies like behavioral analysis, in-the-cloud testing, and application whitelisting. This co-operation enables the modules to share malware information with each other, increasing our ability to detect and remove threats for which signatures have not yet been issued.

Now all the holes are overlapped and nothing can get past your PC protection.

"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 behavioral 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 behaviors, 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 behavioral 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.

Benefits of Identity Protection's behavioral analysis include:

- 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 behavior-based products

In AVG 9, Identity Protection is further enhanced by the ability to track malware installs through hi-jacked processes, which significantly improves removal results, together with new behavior to detect malware that copies itself all over the machine.

Like LinkScanner, 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.

## Why the third layer is so crucial today

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.

As noted earlier, AVG 9 now combines cutting-edge security technologies – behavioral, in-the-cloud, and whitelisting – to optimize protection against today's here-today, gone-tomorrow threats. These technologies come together through co-operation between the Resident Shield, firewall, and identity protection modules. These modules communicate with each other to provide malware information to each other, increasing the software's ability to detect and remove threats for which signature-based solutions along have not yet issued detections.

Here's how it works.

The firewall has been completely redesigned to make use of application whitelisting, which reduces intrusive firewall alerts by 50%. The new firewall communicates behind the scenes with the behavioral detection technology in the identity protection module to deliver the most accurate detection of new and unknown threats. AVG estimates that this approach delivers 90% fewer false alarms than other products that are attempting to implement this approach. This enhanced protection level is particularly effective against phishing threats through the use of "in-the-cloud" automated testing to detect tell-tale signs that indicate the presence of a new threat. Because the earlier the software can detect a threat, the more effectively it can protect you.

### Combined Firewall, IDP, and AV Signature detections

Each detection technology uses its own techniques for detecting potential threats; combining this information improves overall detection. Here are some of the interactions and benefits:

#### Firewall and IDP

Whenever the firewall detects an attempted connection, it consults with IDP. If IDP has determined that this process is trusted it will let the firewall know and thus not require the user to respond to a pop-up question. If IDP has determined that the process is malicious, it automatically instructs the firewall to block all communications, thus reducing the chance of any information leaking from the PC before the threat is quarantined. The process also works in reverse, when the communication is used by IDP to help make a behavioral analysis.

#### Resident Shield and IDP

If Resident Shield detects a malicious file being installed, it passes that information to IDP. IDP uses this information to determine whether any related components that might not be detected by Resident Shield are malicious and, if so, remove them. Essentially, being associated with known malware is used as a behavioral characteristic, similar to the concept of guilt by association.

#### In-the-Cloud Check Server and White Lists

Basically, whenever a process performs an activity deemed suspicious but with insufficient evidence to confirm it as malware, that process is checked against the in-the-cloud service, which returns back whether this is a trusted, malicious, or unknown process. If the process is trusted or malicious, appropriate actions are taken. If it's unknown, the process continues to do what

it was doing, until such time as enough suspicious activity has accumulated to trigger detection. As and when that transpires, the user will be asked to make a decision. If the user approves, the process will be submitted for additional analysis which will in turn mark it as malicious or trusted. That information is then sent to the check service, so that all AVG customers' PCs that perform checks against this process will be notified immediately. This does several things. It allows for the detection of malware before it gets too far in its activity, as well as preventing any false positives. The trust information is added to the internal configuration, which is then distributed to all the agents as a configuration update, which is distributed periodically to all agents.

## AVG 9: Choose Your Security

### For personal use

**AVG Internet Security**

*Complete protection for everything you do*

We know the things users like to do on their computers - surfing, shopping, banking, downloading and chatting with their friends - so we developed AVG Internet Security to give them the multiple layers of protection they need to stay safe online. Internet Security is constantly on alert, so they don't have to be. Includes LinkScanner and Identity Protection.

**AVG Anti-Virus**

*Essential protection that won't get in your way*

AVG Anti-Virus makes sure users' computers stay free of viruses, spyware, and other malware. It includes AVG's unique LinkScanner technology to keep them safe from harmful web pages by scanning those pages right as users go to them.

**AVG Identity Protection**

*Up-to-the-minute protection for online banking and shopping*

The more time users spend online, the more important it is for them to keep their personal information secure. Anti-virus alone is no longer enough to keep users safe when they're shopping and banking online; whatever anti-virus they use, they need the added security of AVG Identity Protection.

AVG LinkScanner and a less-automated, unsupported version of AVG Anti-Virus are available at no cost for home users unwilling or unable to purchase the commercial products. Licenses are for one year.

## For business use

### AVG Internet Security Business Edition

*Complete protection for your business*

Internet Security Business Edition is faster, smarter security that won't slow businesses down. AVG's most advanced protection, Internet Security 9.0 merges ground-breaking online threat prevention techniques with enhanced anti-virus and firewall technologies to deliver proactive protection that's second to none. Includes new Rescue CD network recovery toolkit.

### AVG Anti-Virus Business Edition

*Essential protection for your business*

With AVG Anti-Virus Business Edition, companies get high-performance, next-generation scanning that doesn't get in the way of doing business. Plus, they get LinkScanner and enhanced phishing and firewall protection to keep the business safe while employees are online. It's easy to set up, easy to manage, and includes the new Rescue CD network recovery toolkit.

### AVG File Server Edition

For businesses that already have anti-virus protection on their workstations but need protection for their file server, this is the solution. Includes enhanced anti-virus scanner, LinkScanner web threat protection, and improved phishing detection.

### AVG Email Server Edition

For businesses that already have anti-virus protection on their workstations and file server but need protection for their email server, this is the solution. Includes enhanced anti-virus scanner, LinkScanner web threat protection, centralized spam prevention, and improved phishing detection.

### AVG Server Edition for Linux/FreeBSD

For any organization operating a Linux/FreeBSD Server, particularly for email, this is flexible, scalable protection against infected email and attachments, including on the server itself. AVG supports all leading Linux and FreeBSD e-mail server applications, including PostFix, QMail, Sendmail and Exim. Includes free client software.

## 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**.

## AVG on the Web

For up-to-the-minute news on the latest cyberthreats:

- Subscribe to AVG Chief Research Officer Roger Thompson's blog at http://thompson.blog.avg.com/

For general AVG updates:

- Join our Facebook community at http://www.facebook.com/avgfree
- Follow AVG on Twitter www.twitter.com/officialavgnews
- Register at www.avgnews.com

## References

[1] MPack:
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/pumpdump.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.jhtml?articleID=208803810

## Corporate offices

**AVG Technologies CZ, s.r.o.**

Lidická 31, 602 00 Brno
Czech Republic
www.avg.cz

**AVG Technologies USA, Inc.**

1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA
www.avg.com

**AVG Technologies UK, Ltd.**

Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
United Kingdom
www.avg.co.uk

**AVG Technologies GER GmbH**

Bernhard-Wicki-Str. 7
80636 München
Deutschland
www.avg.de

**AVG Technologies CY Ltd.**

Arch. Makariou III.
2-4 Capital Centre
1505, Nicosia, Cyprus
Fax: +357 224 100 33
www.avg.com