



AVG: Protecting you from today's rapidly evolving, Web-borne threats

Contents

Why you should read this paper	3
The evolution of malware	3
The Web becomes an attack vector	6
The risk window	8
AVG: closing the risk window	8
Conclusion	10
About AVG Technologies	11
About the authors	11
References	12

Why you should read this paper

The challenge for personal and business computer users alike today, is to stay ahead of the rapidly evolving array of viruses, spyware, phishing scams and other threats collectively referred to as malware that can wreak havoc on their lives. This paper explains how AVG Technologies' products reduce the risk, by providing real-time protection against existing and emerging threats.

The evolution of malware

The battle between malware authors and security vendors has been ongoing for years. When a new threat emerges, security vendors update their products to counter that threat. In response, malware authors release attack variants, or seek out fresh vulnerabilities to exploit. But the security landscape has changed notably during recent years. In the past, malware was primarily created by mischievous script kiddies intent on random vandalism. Today, the script kiddies have been dethroned and a significant proportion of malware is generated by organised criminals intent on stealing money and/or information.

The fact that malware authors are now motivated by profits has served to up the ante considerably. This has led to the creation of a completely new underground economy in which both malware and stolen information can be bought, sold, rented and traded. Furthermore, it has also led to an increase in both the frequency and sophistication of attacks.

- Criminals can rent time on networks of compromised home computers (botnets¹) that can be used to send enormous volumes of spam, launch denial-of-service (DoS) attacks², commit click fraud³ and distribute malware without either the knowledge or consent of the owners of the computers. In September

"Phishing attacks are becoming more surreptitious and are often designed to drop malware that steals user credentials and sensitive information from consumer desktops. Anti-phishing detection and prevention solutions are available but not utilized widely enough to stop the damage. These must be deployed and combined with solutions that also proactively detect and stop malware-based attacks."

Avivah Litan, vice president and distinguished analyst, Gartner

2007, it was estimated that up to 50 million computers had been co-opted into the Storm Worm Botnet⁴ and that the botnet had enough power to be able to force entire countries off the Internet — as the Estonian government discovered when a number of their websites were forced offline by a series of DoS attacks⁵. The botnet has since been segmented, with each segment being either sold off or rented out.

- Spam has become a global pandemic that costs businesses more than \$100 billion per year⁶ — and about 90% of it is routed through botnets. While spam is still used as a marketing tool for various lotions and potions, it is also used for far more sophisticated schemes. In pump-and-dump scams, for example, spam is used to distribute “hot tips” that are intended to either increase or decrease the stock of a particular company⁷, enabling the spammer to buy low and sell high. In the US, eleven people have recently been indicted over their participation in a pump-and-dump scam which netted the perpetrators around \$3 million⁸.
- Phishing scams⁹ in which victims are led to a spoofed website and asked to provide personal information are becoming increasingly commonplace — and increasingly costly. According to Gartner, “3.6 million adults lost money in phishing attacks in the 12 months ending in August 2007, as compared with the 2.3 million who did so the year before¹⁰.” Furthermore, Gartner found that “Of consumers who received phishing e-mails in 2007, 3.3 percent say they lost money because of the attack, compared with 2.3 percent who lost money in 2006¹⁰.”
- In the past, malware tended to be aimed at a wide and random audience. Today, attacks are often targeted at specific individuals or organisations. Targeted attacks draw on publicly available information to construct credible sounding emails that are used to deliver malicious payloads. In 2006, the US State Department’s network was compromised by a socially engineered email¹¹. The email contained a Microsoft Word Document attachment that had malicious code embedded. When opened, the code in the attachment established hidden and unauthorised communications outside of the Department’s network.

In addition to driving an increase in the frequency and sophistication of attacks, the commercialisation of the malware industry and its enormous potential for profits have also caused malware authors to step up their efforts in finding new methods to bypass security — and finding new vulnerabilities to exploit. In the past, e-mail was the most commonly used method of propagating malware, but malware authors have now discovered a new and far more flexible attack vector — the Web.

The Web becomes an attack vector

As the majority of computer users are now reasonably well protected against e-mail threats, malware authors have turned their attention to the Web — and found it to be the ideal attack vector. The vulnerabilities discovered in Web browsers leave computers wide open to exploitation. Additionally, vulnerabilities in browser plug-ins such as Adobe Flash Player and Apple

QuickTime open more doors through which private and confidential information can be compromised. Such is the extent of the problem that the SANS Technology Institute listed malicious websites that seek to exploit vulnerabilities at number one on its “Top Ten Cyber Security Menaces for 2008” list¹².

"Parts of the UK's Critical National Infrastructure (CNI)¹ are being targeted by an ongoing series of email-borne electronic attacks. While the majority of the observed attacks have been against central Government, other UK organisations, companies and individuals are also at risk. The emails use social engineering to appear credible, with subject lines often referring to news articles that would be of interest to the recipient. In fact they are 'spoofed', making them appear to originate from trusted contacts, news agencies or Government departments."

National Infrastructure Security Co-ordination
Centre

"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 one or two 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 utilise packaged modules that can effectively disguise their payloads."

SANS Technology Institute

The emergence of Web 2.0 — the name given to the collection of technologies that enables people to interact with the information held on the Web — has also resulted in new opportunities for exploitation; opportunities that the creators of worms such as Yamanner¹³ and Samy¹⁴ have already seized. Similarly, technologies such as RSS and ATOM present yet another channel that could potentially be exploited¹⁵.

To get malware onto users' computers, a wide range of techniques may be deployed. Emails or links on websites are used to lure people to sites which have been configured to exploit a vulnerability to silently download and install malware ("drive-by downloads"¹⁶). Web search results can be poisoned to lead users to booby-trapped websites¹⁷. Vulnerable web servers can be

"Parts of the UK's Critical National Infrastructure (CNI)¹ are being targeted by an ongoing series of email-borne electronic attacks. While the majority of the observed attacks have been against central Government, other UK organisations, companies and individuals are also at risk. The emails use social engineering to appear credible, with subject lines often referring to news articles that would be of interest to the recipient. In fact they are 'spoofed', making them appear to originate from trusted contacts, news agencies or Government departments."

National Infrastructure Security Co-ordination Centre

compromised using tools such as MPack¹⁸ enabling the legitimate websites that they host to be hijacked and used as delivery agents for malware¹⁹. Malware can also be served via banner ads on legitimate websites.

In 2006, up to one million MySpace users were infected by banners ads which silently installed malware by exploiting a vulnerability in the Windows Graphics Rendering Engine²⁰. The malware was relatively harmless and simply caused the computers to display pop-up ads, but it could just as easily have been a password-stealing Trojan that fed bank account information back to those responsible for the hack.

Compounding the problems, Web attacks have also become increasingly sophisticated and attempt to exploit multiple vulnerabilities simultaneously while using complex obfuscation techniques to conceal the payload from anti-virus and anti-spyware scanners.

People who visit a hacked or malicious website may find that their computer is co-opted into a botnet and used like a drug-smuggling "mule" to traffic spam, that their bank account details and other personal information have been stolen by a keystroke logger²¹ or that their computer is suddenly displaying unwanted popup advertisements.

The risk window

Once a user has patched their computer against a particular vulnerability, the computer is then immune to malware that seeks to exploit that vulnerability. The problem is that patches cannot be immediately delivered: vendors must analyse a vulnerability and develop and extensively test a patch that remedies it — and then push the patch out to users. This is not a speedy process. The delay between the discovery of a vulnerability and the release of a patch can often run to more than 50 days²² — and this creates a risk window during which any user running the vulnerable application can be exploited.

The challenge facing security companies is how to close that risk window — and it is a challenge that is far from easy.

Anti-virus and anti-spyware vendors face a similar problem to that outlined above — they need to analyse hostile code in order to be able to develop, test and distribute a fix. While they are usually able to do this considerably faster than application and operating system vendors can release a patch for a vulnerability, there is nonetheless some delay and, accordingly, still a window of risk.

The heuristic detection (“behaviour analysis”) capabilities built in to many anti-virus and anti-spyware programs provides some degree of protection against emerging threats, but it is far from complete. Independent testing²³ has shown heuristic detection methods to be far less effective than the traditional signature-based detection methods. Technological advances may well result in heuristic detection eventually becoming much more effective, but at this point in time it is simply too inaccurate to provide reliable protection.

To be able to provide complete protection against emerging and rapidly evolving malware, a product needs to be able to close the risk window by blocking exploits and the sources of exploits as soon as they appear. And that is exactly what AVG does.

AVG: closing the risk window

AVG Technologies recently acquired Exploit Prevention Labs and has incorporated their LinkScanner technology into the AVG product line beginning with Version 8.

Leveraging LinkScanner technologies, AVG gathers information about new and emerging threats — and the sources of those threats:

- The Exploit Intelligence Network (EIN) is a global network of hunting pots, automated probes, search bots and human researchers that perform continuous reconnaissance across the Internet to find new exploits and the websites that are luring unsuspecting users, as well as those delivering both new and known exploits (including phishing websites).
- The Community Intelligence Network (CIN) is a network of AVG users who allow information about any attempted exploitation of their computers to be channelled back to AVG Research.

The information gathered by this “neighbourhood watch on the web” is automatically correlated and immediately fed back to AVG users in the form of updates, enabling AVG to protect against new threats within minutes of their discovery. Furthermore, as AVG blocks users from accidentally visiting websites that are known or suspected delivery agents for malware, it is not limited to blocking only known threats — by blocking the sources of malware, it can also block unknown and undiscovered threats. The entire process — from exploit discovery to update release — is completely automated and transparent to ensure that AVG is able to protect its users within the shortest period of time.

While this may all sound simple, the underlying technology is actually extremely complex. AVG Search-Shield and Surf-Shield components analyse all the traffic passing through port 80 — the port through which computers connect to the Web. The real benefit of this approach is that exploits are blocked before they even reach the computer.

AVG’s real-time scanning has a distinct advantage over static, database-based blocking methods, such as that used by McAfee SiteAdvisor. SiteAdvisor alerts its users to the fact that a website is bad by checking against a database of known bad websites. To find bad websites, McAfee search bots crawl the Web looking for websites that are delivering or hosting malicious content — and any that are found are added to its database. But malware authors know that this happens and so attempt to

hide from the search bots by configuring their websites to only drop their malicious payloads on certain visitors or at certain times of the day. As a result, a website can infect a large number of machines before SiteAdvisor can detect — and warn its users about — the hostile content the website is intermittently serving up. AVG, on the other hand, inspects all content in real-time — as it being delivered — and so is completely immune to such subterfuge. Database-based blocking methods can also harm businesses. In a number of cases, legitimate websites that have been hacked have continued to be blocked by both SiteAdvisor and Google long after the problem was remedied — and for a business that relies on the Web for its custom, that approach could spell disaster.

Threats are evolving more rapidly than ever before. Each and every day, thousands of new and varied exploits emerge and are pushed out by an ever-changing number of websites. By constantly searching the Web for new exploits and new sources of exploits, AVG is able to provide up-to-the-minute protection against the very latest threats, as soon as they are discovered — sometimes even before they are discovered.

Conclusion

The Web has become a dangerous place. During 2007, millions of people lost billions of dollars to phishing scams; malware levels increased by more than 500%²⁴; millions of users found their computers co-opted into enormous botnets and used to send out spam that peddled everything from penny stocks to pornography; and millions had personal information stolen or found that malware brought their computers to a grinding halt.

The integration of LinkScanner technology into the AVG product line has enabled AVG Technologies to make the Web a safer place for its users, by providing them with world-class protection against today's rapidly evolving, Web-borne threats.

About AVG Technologies

Founded in 1991 and headquartered in the Czech Republic, AVG is a leading international developer of Internet threat protection solutions for consumers and SMBs. AVG is one of the fastest growing companies in the industry with more than 70 million active users around the world. The company has regional offices in North America and the United Kingdom, and employs some of the world's leading experts in Internet security, specifically in the areas of threat research, analysis and detection. AVG's award-winning products are distributed globally through resellers and over the Internet as well as via third parties through Software Developer's Kits (SDK).

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

About the authors

Brett Callow and Rhonda Turner are technical consultants providing services to a number of leading international technology companies and have been extensively involved in the planning and development of various industry-standard IT certification examinations. Brett has been awarded Microsoft's Most Valuable Professional (MVP) designation for the last 4 years. MVPs are exceptional technical community leaders from around the world who are awarded for voluntarily sharing their high quality, real world expertise in offline and online technical communities by Microsoft. To contact the authors, e-mail brett@mvps.org.

References

¹Know your Enemy: Tracking Botnets
<http://www.honeynet.org/papers/bots/>

²Denial-of-service attack (Wikipedia)
http://en.wikipedia.org/wiki/Denial-of-service_attack

³Click fraud (Wikipedia)
http://en.wikipedia.org/wiki/Denial-of-service_attack

⁴Storm botnet (Wikipedia)
http://en.wikipedia.org/wiki/Storm_botnet

⁵Bots Hammer Estonia In Cyber Vendetta
<http://www.informationweek.com/internet/showArticle.jhtml?articleID=199602023&pgno=1&queryText>

⁶Industry statistics (Ferris Research)
<http://www.ferris.com/research-library/industry-statistics/>

⁷Pump and Dump Schemes (U.S. Securities and Exchange Commission)
<http://www.sec.gov/answers/pumpedump.htm>

⁸US Indicts 11 Over Pump-and-Dump Stock Spam
<http://www.pcworld.com/article/id,141001-c,spam/article.html>

⁹Phishing (Wikipedia)
<http://en.wikipedia.org/wiki/Phishing>

¹⁰Gartner Survey Shows Phishing Attacks Escalated in 2007; More than \$3 Billion Lost to These Attacks
<http://www.gartner.com/it/page.jsp?id=565125>

¹¹House Committee on Homeland Security Subcommittee on Emerging Threats, Cyber Security, and Science and Technology (statement of Donald R. Reid, Bureau of Diplomatic Security)
<http://homeland.house.gov/SiteDocuments/20070419153111-10569.pdf>

¹²Top Ten Cyber Security Menaces for 2008 (SANS Technology Institute)
<http://www.sans.org/2008menaces>

¹³Web 2.0, AJAX Bring New Era of Threats
<http://www.eweek.com/c/a/Security/Web-20-AJAX-Bring-New-Era-of-Threats/>

¹⁴Samy (XSS) (Wikipedia)
[http://en.wikipedia.org/wiki/Samy_\(XSS\)](http://en.wikipedia.org/wiki/Samy_(XSS))

¹⁵RSS For Hackers?
<http://www.internetnews.com/security/article.php/3624601>

¹⁶Drive-by download
http://en.wikipedia.org/wiki/Drive-by_downloads

¹⁷Hackers hijack web search results
<http://news.bbc.co.uk/1/hi/technology/7118452.stm>

¹⁸MPack (Wikipedia)
http://en.wikipedia.org/wiki/MPack_%28software%29

¹⁹80% of Web malware is hosted on legitimate sites that have been hijacked
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9027925&source=rss_news10

²⁰MySpace Banner Ad Infects Million Users
http://www.cio-today.com/news/MySpace-Banner-Ad-Infects-Million-Users/story.xhtml?story_id=111003TRG55F

²¹Keystroke logging (Wikipedia)
http://en.wikipedia.org/wiki/Keystroke_logger

²²Web browser security summary
<http://www.webdevout.net/browser-security>

²³AV Comparatives
<http://www.av-comparatives.org/>

²⁴Malware Quietly Reaching 'Epidemic' Levels
http://www.darkreading.com/document.asp?doc_id=143424&f_src=drweekly



Headquarters:
AVG Technologies CZ, s.r.o.
Lidická 31
602 00 Brno
Czech Republic
Phone: +420 549 524 011
Fax: +420 549 524 394
www.avg.cz

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

UK & Ireland:
AVG Technologies UK, Ltd.
27B Cartergate
Newark, Notts, NG24 1UA
UK
Phone: +44 016 367 004 96
Fax: +44 016 367 077 38
www.avg.co.com

Sales Department e-mail: sales@avg.com