

Lloyd Borrett from AVG (AU/NZ) Predicts Internet Security Threats for 2010

Internet Security Predictions for 2010

by Lloyd Borrett, Marketing Manager, AVG (AU/NZ)

Every year most of the security vendors' forecasts predict dramatic spikes in volumes of spam, phishing, botnet activity, and malware. And unfortunately, every year these predictions come true. While we prefer not to be sowing seeds of fear, uncertainty and doubt, the cyber criminals are succeeding on such a scale and making so much money, that each year they are able to invest in better and more automated ways to run their rapidly expanding and increasingly sophisticated operations. So once again we can safely predict that in 2010 the threat environment will look pretty much like this year except that it will have more of everything and be even more transient, agile and organised!

More diverse, automatically generated malware

Today malicious code is written with more variants. The bad guys can now automatically create hundreds of thousands of unique pieces of malware a day, much of which has no unique signature and can bypass old-fashioned signature-based virus detection software. This makes it increasingly important for people to have more than just anti-virus protection on their computer.

More people will buy complete protection

The good news is that reputable security vendors like AVG now provide full Internet security suites with multiple layers of protection. The majority of people that pay for security software now buy the full suite, complete protection solution instead of entry-level solutions. This trend continued through 2009, in spite of tougher economic times, and we expect it to be maintained in 2010.

The bad guys still want your money, identity and/or resources

For many years now most malicious code and web sites have been directly or indirectly about stealing your money, identity, computer resources, or some combination of these. In simple terms the cyber criminals:

Trick you to hand over money to them via social engineering and phishing scams. Yes, people still believe they can help that relative of a despot in Nigeria who needs their help to access squillions of dollars. They believe they've won a lottery they never entered. Or they believe that there really is a long lost, hugely wealthy, dead relative they've never heard of and that the kind and diligent lawyer will help them to get access to the estate.

Trick you into providing, or steal off of your computer, enough of your personal details so as to build up a dossier of information about you that is sufficient to trick someone else into providing them with money, goods or services. Expect to see even more legitimate-looking and personalised phishing attacks impersonating your bank or other businesses you have accounts with. Once the bad guys have your details they buy online using your credit card details and trick the merchant into providing them with goods or services. They steal online gaming usernames and passwords to gain access to your winnings in your favourite game world.

Make your computer into a part of their botnet. Then they can use your computer resources and Internet bandwidth to send out spam, host poisoned web pages, host downloads of illegal software, movies, music, xxx adult images, child pornography etc.

Cyber criminals in the cloud

To keep ahead of the computer security industry's efforts to thwart their activities, the bad guys have become quite agile. They are using in the cloud technologies in far more sophisticated and effective ways than most legitimate businesses. It was recently discovered that Google's AppEngine had been tapped to act as the master control channel to feed commands to large networks of infected computers in a botnet. (Google shut down the rogue app shortly after being notified of it.) We can expect more of sort of activity in 2010.

Highly transient web threats

In 2010 we will see the cyber criminals continue to improve the speed with which they are able to move their campaigns from domain to domain, server to server. This is partly in response to improved detection and blocking methods deployed in updated security products like AVG LinkScanner. In recent times we've been increasingly seeing the bad guys set up hundreds of thousands of new web sites and pages per day, well in advance of using them for nasty purposes. This enables them over a period of a week or so to gain a good rating in the reputation-based security networks being used by some security vendors. Then the bad guys change their innocent web pages and go live with their malicious payloads on those same web pages. In early 2009, AVG researchers reported that 60% of these poisoned web threats were active for less than a day and 75% for less than 30 days. By the time the reputation-based networks and blacklists are flagging these poisonous web sites and pages as bad, the cyber criminals have shut them down and moved them on to another domain or server.

Exploitation of major events, news and gossip

Some of these gangs of thieves have also recently enjoyed success in manipulating the popular online search services. They are clearly now investing more effort in such activities so they can, almost at the drop of a hat get search results at or near the top of the first page of results. Should a celebrity die, an election be fought, some video clip go viral, the bad guys quickly exploit the blossoming interest in that topic. The cyber criminals hijack search results into clicks on links to their malicious web pages. This is all a part of the bad guys moving away from spray and pray attacks into more premeditated attacks with specific objectives. Expect to see more highly targeted, convincing attacks with custom malware in 2010.

Web two-point-uh-oh

But that's all so Web 1.0. What about social media and Web 2.0 that's where things are at now. Of course, the bad guys have not failed to notice this either and have been improving their own Web 2.0 skills while checking out the opportunities afforded by Web two-point-uh-oh. The Koobface worm has been rattling around Facebook and a worrying number of its users for a while now. Along the way support has been added for MySpace, several other social networking sites and more recently Twitter and LinkedIn. Attacks that impersonate social networking sites or spoof contacts from your friends list, are more likely to be clicked on. So the bad guys exploit this trust. This approach seems to have a good return on investment for the financially motivated crooks behind it, and it's likely we'll see a great deal more of this kind of thing in 2010.

Emerging nations go online with poor security

The number of computers and number of people connected to the Internet is still growing fast. More and more people in places like China, India, Brazil etc. are going online with improved connection speeds. Unfortunately many of them are using pirated software that can't be kept up to date with security patches. This makes it easy for the bad guys to target those computers, get control of them and start using them as resources to power their criminal activities. We expect to see a big increase in threats being delivered via emerging countries in 2010.

Global economic crisis impacts security

Although the effects of the current economic downturn are quite unequally distributed, employment in the USA and some parts of Europe and Asia has taken a particularly hard hit. This can have a flow on effect.

Firstly, while there is no good data that I'm aware of to support the following suggestion, it is commonly accepted that violent and property crime rates rise during hard economic times. Its quite likely that more people will be tempted into becoming cyber criminals, especially as more organised underground channels are opened up.

Secondly, it seems likely that otherwise decent people facing increasingly desperate economic conditions, may be more likely to fall for the quick-money appeal of the Nigerian prince offering 40% of his fortune, or to ignore what in better times would be the obvious telltale signs of the too good to be true work from home scams and the like, favoured by so many cyber criminals to effect their money laundering schemes. Or as a form of retribution, those who have lost their jobs will take valuable data with them, or details of how to access company resources, and it ends up in the hands of the cyber criminals.

Business still too complacent

If business IT and security managers have ensured that the workstations and servers the business uses are properly up-to-date and protected, that staff understand the threat landscape and know what to do as they move about with notebooks, then they too can be safe. It just requires constant vigilance and contingency planning. Sadly, events in 2009 showed that many businesses simply werent properly protected.

The success of the exploits used to penetrate and establish Conficker into business and enterprise networks early in 2009 was largely because of complacency. The attitude common among certain business IT and security people is "we have a firewall to keep out worms and other network vulnerability-based attacks, and content filters to stop employees browsing porn, gaming and other 'dubious' sites".

This attitude means many businesses have poor update policies, which leave their networks well out of date on OS and application patches. These weaknesses are the stock-in-trade of the drive-by download exploits commonly used by the cyber criminals.

It also means business is ignoring the fact that the cyber criminals buy professional advertising served by legitimate ad-serving networks, and yes, even the biggest ad networks. These ads then appear on perfectly legitimate websites that employees are quite likely to access to do their work. So we can expect to see more business damaged as the bad guys expand the use of this attack vector.

It will get worse before it gets better

Sadly, the security threats in 2010 are likely to be nastier than ever, more targeted and more frequent. With malware and cybercrime now being almost exclusively driven by organised crime running on a business model, changes are largely driven by criminal cost/benefit analysis of opportunities and risks.

The good news is that people dont need to worry if they understand the nature and purpose of the threats, can see through the scams and the too good to be true offers, have good Internet security protection on their computers and keep all of their software up-to-date.

Do you measure up for a safe 2010?

About AVG (AU/NZ) Pty Ltd: www.avg.com.au

Based in Melbourne, AVG (AU/NZ) Pty Ltd distributes the AVG range of Anti-Virus and Internet Security products in Australia, New Zealand and the South Pacific. AVG software solutions provides comprehensive real-time protection against everything from viruses, spam, spyware, adware, worms, Trojans, phishing and exploits to cyber-criminals, hackers, scammers and identity thieves. AVG provides outstanding technical solutions and exceptional value for home, small to medium business and enterprise clients. AVG delivers always-on, always up-to-date protection across desktops, servers and e-mail in the home plus corporations, government agencies, utilities and educational institutions.

AVG products actively protect more than 80 million users worldwide, including more than three million users in Australia and New Zealand.

AVG (AU/NZ) has more than 2500 resellers across Australia, New Zealand and the South Pacific.

For more detailed information please contact:

Lloyd Borrett AVG (AU/NZ) 03 9581 0807

Shuna Boyd BoydPR 02 9418 8100

Media resources, including logos, box shots, screen shots etc., are available online at: www.avg.com.au/media/