

Country: HK

Date: September 30 2008

Publication: South China Morning Post

Section: Special Report: Antivirus & Security

Article 1 headline:

“Businesses are becoming much more vulnerable”

# Businesses are becoming much more vulnerable

‘15,000 webpages infected with malware daily’ and firms are falling behind in safeguarding their networks. Reports by **Jason Krupp**

For most companies, the internet has become an indispensable means of doing business, whether it is to run an ERP system or an e-commerce platform, or simply as a communications channel and information source.

But with these benefits come dangers, with the ever-present threat of hackers, viruses and spam.

As a result, many organisations have installed antivirus packages and firewalls to protect themselves.

Now, with the advent of Web 2.0 platforms, mobile internet, third-party devices, external network access, social networking and a host of other technologies many companies are finding that their security infrastructure is woefully inadequate for the task of protecting their networks.

“The biggest change to traditional security measures has been the Web. There are 15,000 new webpages infected with malware every day. That is one every five seconds.

“And the scary part is that 90 per cent of the malware is being found on legitimate sites,” said Jim Dowling, director of Asian sales at security vendor Sophos.

“The environment has changed. It is no longer just about how many times your antivirus updates its definitions per hour. You can’t just have gateway applications and think that your network is secure.”

This has created a massive challenge for many companies from the enterprise level down, because maintaining a secure infrastructure is becoming more and more time-consuming and resource-intensive.

“Messaging security, antivirus, anti-spam, filtering, anti-spyware ... the list of required technologies just keeps getting longer, which can be particularly troubling for smaller-

sized businesses trying to keep pace,” said Jens Andreassen, vice-president for Asia-Pacific sales at Fortinet.

“Regulatory and best-practice guidelines place an enormous due diligence burden on information technology (IT) executives. Not only must the latest technologies be implemented for dealing with potential attacks, but executives must prove that all is being done to protect sensitive data and networks.

“To add to the burden, traffic and events must be logged for audits to prove compliance and also for forensic operations, which are critical to discerning and quickly remedying weaknesses in the network security regime.”

Many businesses are now looking to outsource their security to managed-security service providers.

As a result of this increased demand, the market has boomed in recent years, with a number of dedicated providers sprouting up, including the likes of BT Global Services, IBM Internet Security, Paladion and growing numbers of regional players.

In the United States for example, the International Data Group said the managed-security services market was valued at about US\$1.3 billion last year, an increase of 19.6 per cent over 2006. This figure is expected to increase to US\$2.8 billion by 2012, representing a compound annual growth rate of 17.2 per cent.

The Asia-Pacific region is expected to follow suit. Global research firm Gartner forecasts a 12 per cent compound annual growth rate for managed-security services through to 2011.

For the companies themselves, managed-security services offered a number of appealing advantages, said Michael Gazeley, managing

director of Hong Kong-based managed-security service provider Network Box.

The first of these is that companies can now get on with their core business, knowing that their security function is being handled by dedicated professionals.



**Michael Gazeley:** botnets are constantly scanning for weaknesses

“A lot of companies have general IT staff who are not security experts. They will buy a solution and hope for the best. This doesn’t cut it when you have massive botnets out there constantly probing your network for vulnerabilities,” Mr Gazeley said.

Another advantage of outsourcing is that clients, provided they choose a good provider, get the benefit of the latest security technologies without having to invest in hardware or integration with existing systems, once the initial set-up has been done.

An example of the new technologies available is unified threat management, a next-generation firewall technology that combats threats including hackers, bots, viruses, worms, trojans, spam and phishing.

In addition, network access-control technologies proactively scan traffic to and from the network, remove possibly infected data and prevent malware from infected sites compromising corporate networks. These solutions combine with standard end-point technologies to offer companies a comprehensive security package.

However, outsourcing was not the silver-bullet solution for every company, Mr Dowling said. His company’s service is for the most part aimed at small- and medium-sized businesses, where IT infrastructure spending is traditionally tight.

“It depends on the level of risk your company is willing to take, because you are outsourcing a vital function to a third party. For some, particularly financial organisations, this is just too risky and they’d rather handle security in-house.”

Article 2 headline:

“Good antivirus package can help prevent stealth attacks”

# Good antivirus package can help prevent stealth attacks

Ten years ago you knew you had been hacked when a large portion of your disk drive suddenly went missing. Today experts say it is not that simple, with hackers and botnet-herders employing increasingly sophisticated techniques to keep their presence on your computer a secret.

“Hackers don’t want you to know they have compromised your network, and some malware programs are so sophisticated that they can crash your antivirus so that you won’t be alerted to the infection,” said Gerald Hong, director of Hong Kong-based Lapcom.

So how do you know if your computer has been breached?

“There are three signs to watch out for if you suspect your computer has become a botnet zombie,” Mr

Hong said. “The first is that the computer hard disk keeps running all the time even when the machine is idle. The second is when your contacts start complaining that you keep sending them spam. And last, your machine performs slowly for no reason.”

The solution for home users was simple, Mr Hong said. “Just install a good antivirus package with quarantine capabilities and make sure it has a self-protect function to prevent it from being shutdown in the future.”

However, if you are on a network, it becomes more serious.

Derek Manky, security researcher at [Fortinet](#), said: “They should treat it as a very serious matter. Network activity should be ceased. But in a large corporate environment this is not always a

possibility. Infected machines should be located and quarantined until the infection has been cleaned.

“Credentials and system passwords should be reset. Any other information that may have been at risk should also be dealt with in an appropriate manner. If this risk involves data belonging to third parties or employees, the information should be immediately relayed so that they can deal with it appropriately.

“Finally, the origin of the infection should be investigated and resolved so that it does not occur again. Employees should be educated, and a proper layered security system ... should be put in place.

“Understanding the origin of these threats goes a long way to preventing future vulnerabilities.”

Article 3 headline:

“Education and IT policy can provide safeguards”

# Education and IT policy can provide safeguards

**Jason Krupp**

Ask any information technology (IT) professional from the help desk operator to the chief technology officer in any company, and they will tell you that security is one of their primary concerns.

You can almost be guaranteed that they will rattle off a list of exotic titles in your direction, with words like intrusion detection systems, anti-spam, firewalls, antivirus and reverse proxies being bandied about as a measure of how secure their IT infrastructure is.

However, one area that many IT departments neglected to factor in when they crafted their security strategy was the human factor, security experts said.

“Security in a large enterprise can be analogous to a chain – if there is one weak link [through an employee], the enterprise may be at risk,” said Derek Manky, a security researcher for Fortinet. “This may be through an innocent mistake – as most cases are – or through actual malicious intent.”

The answer to this was education and a solid IT security policy, experts said.

Michael Gazeley, managing director of Network Box, a managed security service provider, said it was a matter of time before the sheer volume of spam, viruses, worms and trojan horses hitting corporate networks every day compromised even the most robust security system.

He said user education and a clear IT policy played a vital role in preventing a small breach from infecting the whole system.

“No matter what security system you put in place, it goes hand in hand with how powerful that policy is,” Mr Gazeley said.

“For example, teaching a user about the dangers of spam may stop them from clicking on a link that redirects to a compromised site which hosts malware that launches SQL attacks.”

Likewise, a clear security policy, which specifically covers all sanctioned uses of the IT infrastructure from software to hardware, may prevent a user from

engaging in behaviour that could expose a company to a security breach. The emphasis is on making this as comprehensive as possible.

“Many network layers may be built up for security settings, but if administrative policies do not exist, such as control over physical access, security breaches may occur. This includes corporate laptops being removed and re-introduced into an internal network, where malware may spread,” Mr Manky said.

“Other such physical objects include USB keys that contain malware; in particular worms which can quickly spread from such a third party medium.”

**Security in a large enterprise can be analogous to a chain - if there is one weak link [through an employee], the enterprise may be at risk**

**DEREK MANKY**  
SECURITY RESEARCHER, FORTINET

The problem for many companies is that security-focused user education and IT policy are time consuming and resource intensive. Instead of creating and maintaining a comprehensive document very often these were simply downloaded from the net, Mr Gazeley said.

Similarly, these documents can become so dense and technical that they become completely inaccessible to the average user who might just want to take some files home to work on.

The serious message from the industry is this makes businesses that ignore security policy and

training responsible for user-related security breaches.

“As a managed security service we can only recommend examples of good IT policies to our customers,” Mr Gazeley said. “It is up to them to adapt these to their needs and police them. We have seen cases where IT policy is completely ignored.”

At a recent security conference in Hong Kong, IBM’s security and risk evangelist Pierre Noel identified a number of ways organisations could act to ensure they avoided these pitfalls.

Firstly, he advocated making it a process that wasn’t driven purely by IT. “Having the best team of technology people is irrelevant,” Mr Noel said. “Sometimes it is often detrimental because they will look at it from a technology-only perspective and not focus on user policies and good education.

“Technology is important, knowledge is more important and education is even more important. Companies must educate people on their policies and the right way to behave.”

Secondly, he stressed the need to keep in mind not only the security needs of the network but the business requirements – often the kneejerk reaction of IT departments was to say no to new technologies that could stifle innovation.

Thirdly, Mr Noel said that making a single person responsible for security was an effective means of ensuring security policy and education was created and conducted thoroughly.

“In every organisation you want there to be one person who has a difficult night sleeping because it is their problem. If it is diluted, no one is responsible and you will have another incident,” he said. This trend is increasing today in many enterprise-level companies, where the role of the chief security officer at a board level has emerged.

The final step, Mr Noel said, was constructing the policy so that it was aligned to the corporate culture. “Policy must match your culture or it will not resonate with the users,” he warned.

Article 4 headline:

“New criminal tactic takes advantage of users’ concerns over security”

# New criminal tactic takes advantage of users’ concerns over security

**Gilmore Cheung**

Cyber criminals are sending out false security applications as users become more conscious of the need for safeguards, a leading provider of unified threat management solutions warns.

The tactic was highlighted in the latest report on the level of threats to systems by Fortinet. Malware W32/Multidr.JD!tr and HTML/Agent.HFZ!phish, disguised as security software Antivirus XP 2008 and XP Security Center, claimed the top two positions in Fortinet’s top 10, accounting for nearly 20 per cent of suspect activities last month.

Rogue mass mailer Netsky was dislodged from its dominating spot by W32/Multidr.JD after a one-day onslaught late last month when it was sent to users disguised as a vital UPS document.

“Cyber criminals are clearly trying to take advantage of users’ security concerns with an intense campaign for rogue security applications this past month,” said Derek Manky, security researcher for Fortinet.

“This is a popular, emerging area that provides a new social engineering approach – black hats posing as white hats.”

Fortinet’s FortiGuard global security research team compiled this report based on data from FortiGate multithreat security systems in production worldwide.

The company said customers who used FortiGuard were already protected against the threats outlined in the report.

Other malware trends observed during this period included Virut.A, a persistent virus that infects executable files, which has been in the top five position for seven

consecutive months. Though Mytob and Pushdo mass mailers were no longer on the top 10 list, experts warned they still remained a threat. Iframe traffic redirectors also remained a strong threat with indications that it could become more prevalent.

“Since Web-borne attacks are frequent and often involve hijacking and redirecting traffic through such iframes, we will likely see this trend continue,” a report by FortiGuard stated.

## Know your foe

### Top 10 individual threats

	Name	Type	% of detections
1	<b>W32 Multidr.JD!tr</b>	Trojan	10.02
2	<b>HTML Agent.HFZ!phish</b>	Trojan	8.15
3	<b>W32 Netskytsimilar</b>	Mass mailer	5.95
4	<b>JS Agent.WMA!tr.dldr</b>	Trojan	5.9
5	<b>W32 Virut.A</b>	Virus	4.65
6	<b>JS Iframe.DR</b>	Trojan	4.19
7	<b>W32 Agent.KG!tr</b>	Trojan	3.36
8	<b>HTML Iframe.DN!tr.dldr</b>	Trojan	2.59
9	<b>HTML Iframe.CID!exploit</b>	Exploit	2.12
10	<b>JW32 Agent.HKR!tr</b>	Trojan	1.98

SCMP GRAPHIC

### Top five malware families

	Family	%
1	<b>Netsky</b>	9.5
2	<b>OnlineGames</b>	7.7
3	<b>MyTob</b>	5.8
4	<b>Virut</b>	5.4
5	<b>Pushdo</b>	3.0

SOURCE: FORTIGUARD