Computing Security
Secure systems, secure data, secure people, secure business

NEWS
OPINION
INDUSTRY
COMMENT
CASE STUDIES
PRODUCT REVIEWS

Malware - and Malpractices

David Fertell, Pearl Software: Web filtering services are a powerful way to fight Bots

Despite the potential threats, as many as 25% of all PCs remain unprotected. Why is there such a poor attitude to security in some quarters? Computing Security finds out

When you consider the huge volume of malware spreading instantly via the Internet, it's foolish not to protect your PC. Yet despite the potential threats, many of which make national headlines, Microsoft's Security Intelligence Report tells us almost 25% of all PCs remain unprotected, including PCs owned by both consumers and businesses. There really is no excuse for this negligence."

NOT 'IF', BUT 'WHEN'!
Such is the view of George Anderson, senior product marketing manager for enterprise at Webroot, who adds this rider: "So why are PCs left unprotected? For consumers, it may be because the PC came equipped with a free 30-day AV trial at purchase, so the user just doesn't understand the risks or assumes it will never happen to them. It will. It's not a matter of 'if', but 'when', your PC gets infected. For businesses, it could be because people are not sure whose responsibility it is to protect PCs - is it the CIO, the IT team or the individual user?"

However, a more likely cause is the actual nature of modern PC malware, he states. "Simply put, it is no longer 'noisy'. By that, I mean it doesn't make its presence known, even when it has full control. Malware writers are looking to make their gains silently, so they don't get caught. The Trojan that makes your PC part of a botnet to attack websites and infect others; or that uses your PC as a low volume spam relay; or has a Keylogger primed to steal your online banking, credit card and other personal details without you knowing is there - it's just you don't know it is and, in this case, ignorance isn't bliss.

"For a consumer, this means the risk of financial loss or performance issues on PCs. For businesses, such a security problem could be even more catastrophic - valuable business data in the wrong hands could damage the company's finances, reputation and even future success."

THE GOOD NEWS
There is good news behind all these dire warnings, however, says Anderson. "If consumers and businesses do take steps to protect their PCs, modern endpoint security does detect these threats and stop them. If it's one of the new generations of real-time detection and prevention antimalware solutions, it does so without slowing your device down or even needing daily detection updates. Next-generation AV stops the threats from files and processes within MS Office documents and PDFs, too. These programs are dangerous, as it's easy to embed macros and scripts, plus Internet access is a part of their make-up. This means they can run malware easily alongside their apparently legitimate purpose.

"Yet malicious variants will behave in ways legitimate Word, Excel or PDF files don't and make system changes they shouldn't. Any decent AV should detect and stop such actions immediately and, if it's a next-generation AV, it will also roll back any of the changes made by the malware to automatically remediate any damage that was done."

INSIDE STORY
So, all positive stuff overall. But let's look inside what some of those threats represent for a deep understanding of what your systems, and organisation, are up against when malware strikes. Take the much feared Bot Net, for example.

"This is a group of Internet-enabled computers that have been surreptitiously configured to forward spam and viruses to other computers on the Internet," explains David Fertell, president, Pearl Software. "A Bot Net operator sends out viruses or worms, infecting computers with a Trojan application. The Trojan, or Bot, then logs into a particular master web or chat server where instructions can then be sent to the Bot to send out spam or viruses to mail servers."

And the solution? "Web filtering services are a powerful way to fight Bots, since users are blocked from suspicious web sites. Many IT administrators don't realise that, while they successfully fight the onslaught of inbound spam, their own systems may be compromised to the point of being the conduit for outbound spam and virus attacks. Comprehensive web filtering allows administrators to set specific access rules to web pages, based on the pages' categorised content."

BLENDING APPROACH

Typically, automatic updates to the URL database are done using various proprietary search algorithms to scour over web content looking for inappropriate or harmful content including malicious Bot Net sites. "Our company's web filtering algorithms take a blending approach to categorising content, including scanning the target sites for viruses in setup files, zip files and executable files," adds Fertell. "If viruses are found, the site is added to one of our malware categories to prevent a seemingly harmless site from launching a drive-by install of malicious code or providing a fake hardware driver. There have been instances where we have identified over 10,000 such sites in less than a month."

Stopping malware at its source is often not the first approach his customers have tried, rather opting for retroactive anti-virus and spyware removal tools. "One of our healthcare customers was repeatedly being hit by open spam relays and viruses," he says. "Our Internet monitoring and filtering tools were deployed to stem the tide of constantly repairing their virus-stricken network. In addition, this hospital was able to identify where the problems were originating, in order to educate end users about downloading files with dangerous attachments." CS