

FEATURE

THINK BEFORE YOU CLICK

By Ian Kilpatrick, chairman of security specialist Wick Hill Group.

Many people are still unaware that simply browsing the web and clicking on a web page can result in picking up malware, a term which covers a multitude of security threats such as Trojans, spyware, key loggers, worms, viruses, phishing, hacking and other forms of malicious activity.

Many people also believe they are protected from any kind of malware because they are using URL filtering, anti-virus or anti-spyware software, or because they have a firewall. Unfortunately, this is often not the case.

The danger comes from something called active content. While active content can be non-malevolent and is used by companies on a daily basis, malicious active content can cause real damage. Companies need to take proactive steps to protect against this type of dangerous active content, whilst ensuring these measures do not hamper the efficient running of the business.

Active content refers to components that are embedded in web pages or documents. These components can carry out or trigger actions automatically and dynamically, often without the user's consent or knowledge.

Non malevolent active content technologies (e.g., Java applets, ActiveX controls, macros, JavaScripts and executable files) are commonly used for regular business practices such as CRM, ERP, web conferencing, e-commerce, webmail, etc. JavaScript and other forms of active content are not always dangerous, but they are commonly used as tools by attackers.

Most web pages contain one or more types of active content, which is sometimes referred to as mobile code. It can also be delivered via email, instant messaging and other means of communication

Attacks by active content using malicious code are growing exponentially and account for the vast majority of today's malware. These attacks can affect a company's profitability, because of the time and resources spent dealing with them, as well as a reduction in productivity and lost revenue. They can also mean company confidential information is exposed or stolen. Another potential outcome is damage to a company's reputation.

Why aren't traditional security systems effective against active content attacks? The reason is that many anti-virus and intrusion detection/prevention systems were designed to protect against known threats and are ineffective against unknown threats and complex blended attacks, which may use multiple technologies to infiltrate your network.

Traditional security solutions were originally designed to protect email attachments from threats which were much less sophisticated than those delivered by active content. Today's new generation of malware attacks take advantage of vulnerabilities in web browsers, which offer more opportunities for malicious or inappropriate behaviour.

Protecting against malicious active content

To protect themselves against malicious active content, companies need solutions that can deal with threats the first time they attempt to strike, not some time after a signature or patch has been issued. An approach is necessary which analyses the actual behaviour of the active content to decide if it is malicious or inappropriate and needs to be blocked; or to decide that it is appropriate and can be allowed in uninterrupted.

There are solutions available which use behaviour-based technology. This can inspect the application-level traffic (i.e., the active content objects) that might carry the malicious mobile code which can infect the network, and analyse the behaviour of the code before it arrives and begins to run on the target computer.

This technology is able to identify the combination of operations, parameters, script manipulations and other exploitation techniques, and can determine that a piece of mobile code is trying to exploit one or more types of vulnerabilities. Then, in line with each organisation's specific security policy, the system decides whether to pass, block or neutralise the content.

Such behaviour-based technology can prevent new and previously unknown viruses, spyware, malicious code and complex attacks from entering the network. It can also reduce the 'false positives' that heuristics-based techniques are prone to. As companies become more aware of the risks they are facing, using this type of system can result in a more educated, better-defined security policy.

ENDS

Bio - Ian Kilpatrick

Ian Kilpatrick is chairman of Wick Hill Group plc, specialists in secure infrastructure solutions. Kilpatrick has been involved with the Group for more than 30 years and is the moving force behind its dynamic growth. Wick Hill is an international organisation supplying most of the Time Top 1000 companies through a network of accredited resellers.

Kilpatrick has an in-depth experience of computing with a strong vision of the future in IT. He looks at computing from a business point-of-view and his approach reflects his philosophy that business benefits and ease-of-use are key factors in IT. He has had numerous articles published in the UK and overseas press, as well as being a regular speaker at IT exhibitions.

Wick Hill contact details for information on how to protect employees from succumbing to malware while surfing the web. 01483 227600, www.wickhill.com. Further press information from Annabelle Brown on 0191 252 8548, email abpublicrelations@btinternet.com