

A WICK HILL & FINJAN WHITE PAPER

TRADITIONAL SECURITY SYSTEMS WILL NOT PROTECT AGAINST ALL WEB-BORNE THREATS

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

Ian Kilpatrick, chairman of security specialist Wick Hill Group, discusses the dangers of malicious active content picked up from web-browsing, and advises on how to protect against this growing risk.

Bullet point summary:

- * Many people are still unaware that simply browsing the web can result in malware (e.g. viruses, trojans, spyware, keyloggers, worms, etc.) being downloaded onto their computers, without their knowledge.
- * Firewalls and other security applications do not necessarily protect against infection from web browsing
- * The danger is from something called 'active content'
- * Definition of 'active content'
- * Why traditional security systems don't necessarily protect against 'active content'. Examination of why firewalls, anti-virus, intrusion detection/prevention and heuristic technology may not protect.
- * How to protect against malicious 'active content'. Why behaviour-based technology provides an answer.
- * Behaviour based solutions from Finjan

Introduction

The time we spend using the web in a work situation has increased hugely and is now part of the daily routine of most companies. Yet, many people are still unaware that simply browsing the web 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. Simply visiting a web site page, can result in acquiring these undesirable additions to your network.

Many people also believe that they are protected against such infection from web browsing because they are using URL filtering, anti-virus or anti-spyware software, or because they have a firewall. Unfortunately, this is not necessarily the case.

One danger on the web 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 and is growing at an extremely rapid rate. 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.

What is active content?

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 even knowledge. This content can be delivered to the user's computer while browsing the web, enabling web sites to provide increased functionality, such as interacting dynamically with visitors, delivering animation and interactive applications, and much more.¹

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. The results of malicious active content can also mean company confidential information is exposed or stolen. Another potential outcome is damage to a company's reputation.

Why not traditional security solutions?

Why aren't traditional security systems effective against active content attacks? The reason is that many systems such as anti-virus and intrusion detection/prevention, are 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.

Firewalls

Firewalls are capable of protecting networks against packet level attacks but may not detect malware or malicious content entering the network via web traffic, and many firewalls cannot analyse how the content will behave as a whole (at the application level) once it reaches the end user. Firewalls are no longer sufficient for preventing today's malicious code.

Spyware and phishing attacks may also bypass firewalls, using open ports in the firewall. The foremost of today's complex threats enter the network via port 80 (HTTP) and port 443 (HTTPS). In most organisations, opening port 80 is vital to the productivity of the users.

Email transportation also opens the door to many threats, and the combination of both web and email transportation is highly exploited by various types of threats, such as phishing. The ineffectiveness of firewalls against such threats is evidenced by the rapid increase in worm penetration despite the extremely wide deployment of firewalls.

Anti-virus

Traditional solutions block known viruses and worms by comparing content against signature databases, which need to be updated each time a new virus is discovered. They do not typically protect against day zero threats. These reactive solutions are not sufficient for combating unknown and targeted attacks such as spyware, phishing, worms, trojans, viruses, or blended threats.

Company networks are at risk from the time a new vulnerability is published or an attack is launched until the time a signature update or patch to combat that virus is delivered and installed. And even with the latest anti-virus update, enterprises are still vulnerable since virus attacks can be modified using compressors, and mutations can be released.

Even once a patch is issued, it may be some time before it is installed. So, it is hardly surprising that companies without proactive protection against new, unknown attacks are in danger of compromising their network security and valuable business assets.

Intrusion detection/prevention systems

Intrusion detection systems and intrusion prevention systems are similarly not effective against complex attacks driven by active content. Because they operate primarily at the packet level, they cannot know how a given web page will behave when loaded into a browser or email application, because they never see the web page - they only see individual packets. This type of security can only be achieved by application-level solutions.

Heuristic technology.

Heuristic-based technologies detect infections by scrutinizing a programme's overall structure, its computer instructions and other data contained in the file. The heuristic scanner then makes an assessment of the likelihood that the program is malicious based on the logic's apparent intent.

Anti-virus engines often use heuristics to identify variations of known viruses. However, since these schemes don't actually observe full execution of the scanned software, they often fail to detect new infections; there are simply too many ways to obfuscate malicious code, and often the only way to know content is malicious is to watch it run in real-time. This accounts for an excessively high rate of false-positives when using some heuristic-based systems.

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.

One company offering a pro-active solution to these issues is Finjan, which has developed its own patented behaviour-based technology. Finjan's solutions 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.

This 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. Another useful benefit is that it can expose the type of malware that tries to extract private information and publish it to the Internet.

Finjan's range includes all-in-one, integrated security appliances, for SMEs through to the largest enterprises. The Vital Security range protects against malicious code and malicious active content, securing corporate networks and users from spyware, viruses, Trojans and other types of web-borne threats. Finjan's pro-active behaviour based content inspection technology is integrated with industry-leading anti-virus and URL filtering components for a comprehensive solution, which reduces business total cost of ownership.

Vital Security solutions include.

- * Patented behaviour-based security engine for detection and blocking of unknown threats
- * Vulnerability Anti.dote™ which performs virtual patching for zero-hour protection against known software vulnerabilities
- * Anti-Spyware engine for stopping costly Spyware attacks at the gateway before they infiltrate corporate PCs
- * Industry-leading Anti-Virus engines for protection against known viruses (optional)
- * Industry-leading URL Filtering engine for full control over your organization's web browsing (optional)
- * SSL Inspection for scanning encrypted content and enforcing certificates (optional)
- * ICAP standard compliance allows inter-operability with third party proxies (e.g. NetCache, Blue Coat) and appliances. Vital Security also features customised reporting and logging which empowers companies to monitor ROI and trends and to accurately adjust security policies as their business evolves. Solutions comply with regulatory initiatives such as HIPPA and GLBA.

At entry level, the NG-5100-S (up to 1000 users) offers a robust, high performance platform providing a cost-effective web security solution that meets the throughput requirements of today's enterprises.

At mid-tier, the NG-6100-S (up to 10,000 users) is for enterprises with high availability requirements. It provides a robust, high availability platform that meets enterprises' stringent performance requirements. It can be used in a centralised manner at the main office, or as a high availability scanning solution for branch offices of large enterprises in conjunction with the NG-8100 at enterprise headquarters.

At the top end, the NG-8100 is tailored to the web security needs of large enterprises and organisations of up to 250,000+ users with multiple chassis. It is a high performance, scalable and high availability integrated blade server appliance, which allows enterprises to scale up cost-effectively by adding scanner blades to the appliance chassis without increasing management overheads. High availability features, including redundant, hot-swappable hardware components, ensure zero downtime. The NG-8100 can be integrated with various load balancing options to ensure compliance with the high performance and availability requirements of large enterprise networks.

For those users who aren't sure if they need a Finjan style behaviour-based system, Finjan can provide, where relevant, an RUSafe Audit. A Finjan security appliance can be placed on the user's network to listen for all HTTP transactions carried out and mirror all Internet traffic. This gives a complete picture of how users in the organisation are accessing the Internet and allows IT staff to make an informed decision about whether unnecessary security risks are occurring; or indeed identify if threats are evading their existing solutions and there is a need to protect the network further. Testing with the Finjan security appliance carries on in the background and does not affect the performance of the user's network.

Finjan also provides a very specific free tool for detecting malicious active content while browsing the web. Finjan Secure Browsing alerts users to potential malicious content hiding behind links of search results, ads and other selected web pages before you visit them. It accesses each of the links and scans the relevant pages in real time using Finjan's patented behaviour based technology, as well as leading anti-virus engines from Sophos and Kaspersky. It then displays a safety rating next to each link it has scanned.

Conclusion

It is in the very nature of computer security that new threats continue to emerge and challenge our defences. The dangers of malicious active content picked up by web browsing is a growing problem which is not adequately dealt with by traditional security solutions such as firewalls, anti-virus, intrusion detection/prevention, anti-spyware, etc. Signature based solutions and patches leave company networks exposed when new malware first emerges.

The effective way to tackle these issues is to install a solution which uses behaviour-based technology and can actually analyse the behaviour of all types of active content coming into the network. That solution should be able to decide, without affecting the efficient running of the business, whether the active content is malicious and should be removed, or benign and allowed in, so business can continue as normal and employees can use the Internet safely.

ENDS

1. Thanks to Finjan for this definition of active content and for some of the other technical material in this article, which was taken from Finjan white papers.

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, web www.wickhill.com. Further press information from Annabelle Brown on 0191 252 8548, email abpublicrelations@btinternet.com