



BEHAVIOUR-BASED TECHNOLOGY



Pop-up plague

Behind every pop-up may lurk a virus or spyware and with many users suffering from 'OK addiction', it's time to tighten security

Marketing companies spend money on pop-up boxes to advertise and drive traffic to their web site, simply because they work. For every person who closes down, or blocks, pop-up boxes, there is one who obediently clicks on 'OK' without a second thought. It's what we at Finjan call 'OK addiction'.

Today people have been conditioned to click on 'OK' – leaving businesses vulnerable. What are they 'okay-ing'? A free report or a virus? Membership to a new magazine or some spyware? Tackling 'OK addiction' is increasingly a security priority, but what can be done?

With the introduction of spyware, malicious code can stay hidden on a PC for as long as criminals need in order to steal information or cause damage.

As a result, spyware embedded in the Active Content in pop-up advertising is a growing threat. Active Content refers to software components that are

"People have been conditioned to click on 'OK', leaving businesses vulnerable. Tackling 'OK addiction' is increasingly a security priority"

hidden within an electronic document such as a pop-up window or advertisement, which can carry out or trigger actions automatically (and dynamically), often without the user's consent or even knowledge.

Active Content is 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. Active Content can also be delivered via e-mail, file transfers, instant messaging and other means of communication.

In a business environment people will often click on a web link or attachment with less caution than they exercise at home, because they assume the company's security protects them. This compulsive clicking on appealing 'special offers' provides organised crime gangs with an open door to critical networks.

As cyber criminals become increasingly educated, security firms can no longer rely on producing fixes based on spotting the characteristic of a virus. Criminals are writing code to try to target specific networks and organisations. These targeted attacks are difficult to detect using network monitoring applications, allowing criminals to achieve maximum gain and then disappear unnoticed.

Enterprises require highly intelligent and behaviour-based security solutions that can analyse Active Content and block only the malicious or inappropriate content. At the same time, this level of proactive security must be achieved without compromising the productivity or performance of the enterprise.

Modern hackers are crafting their malicious code to 'outsmart' traditional security systems, such as firewalls. To differentiate legitimate Active Content, used in applications such as web conferencing, e-commerce, and webmail, from malware, security solutions must analyse behaviour at the Active Content level.

Behaviour-based technology is used by security vendors to inspect the application level traffic that might carry the malicious mobile code which can infect the computers, and to analyse the behaviour of the code itself – before it even arrives and begins to run on the target computer.

This technology identifies the combinations 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. In accordance with each organisation's specific security policy, the security system decides whether to pass, block or neutralise the content.

Only when organisations employ this kind of technology will they be able to keep their networks safe from the prying eyes of the outside world. <

Yuva Ben Itzhak is CTO at Finjan. You can reach him at edtoral@server-management.co.uk. Finjan is exhibiting at Infosecurity Europe 2006 on 25–27 April 2006. For details see p8.