Drive-by downloads attack where least expected

The web is still the greatest attack surface and largest entry point for malicious code. Attacks usually happen via drive-by downloads, in which malware is downloaded and executed without the user even realising.

Image: www.freedigitalphotos.net

"These threats make use of exploits, or tools that find and use vulnerabilities in the target user's system," explained Lutz Blaeser, MD of Intact Software Distribution. "Unfortunately, it is not only dubious websites that can infect users; today the vast majority of drive-by download attacks happen via legitimate and trusted sites."

He said that popular sites for news, lifestyle and specialist magazines, career sites, and daily newspapers most often fall victim. "Because these sites are legitimate, safe surfing behaviour is an ineffective measure against these attacks. In addition, keeping your anti-malware protection up to date, although helpful, is no silver bullet. Of course, making sure that all patches are installed and applied increases security; however it is almost impossible to have a 100% up-to-date machine. Think of over 100 patches, for a multitude of applications from several vendors, and even then you are assuming patches are issued almost instantly, which is not always the case."

Over and above these myriad patches, you should bear in mind that many software packages are preinstalled by the vendor that manufactured the machine, he added. "Because of this, the user is often completely in the dark and has no idea that the software on his machine might be vulnerable. Moreover, because there are sometimes compatibility issues or an expired service it might also not be possible for any updates to be installed."

Zero-day vulnerabilities

He said that experts say that approximately 40% of computers out there are vulnerable to exploits on the internet. "In reality, however, there is no such thing as a totally secure computer that does not have any security holes. Each and every piece of software has vulnerabilities that have not yet been discovered and, therefore, no patch will exist. These zero-day vulnerabilities are frequently exploited by cyber criminals who discover the vulnerability before the vendor does."

Zero-day attacks are usually only identified by the software vendors after they have occurred. "The lack of a patch for this type of vulnerability presents an enormous threat to companies and individuals alike, as they can easily slip through the net

of purely signature-based solutions until a patch is released. Their stealthy and unexpected nature is a serious concern, particularly as they can be employed in more serious, targeted attacks as well as the propagation of malicious code."

He said that to prevent falling foul of these attacks, good preventive security practices are essential. "This includes installing a firewall and rigidly maintaining its policies. In addition, keep anti-virus up to date, to block any harmful attachments and keep systems patched against all known threats. Add intrusion prevention to the security mix, and have well-thought-out incident-response measures in place, just in case."