Not A Patch On The New Breed Of Cyber-Criminal
by Nick Ray - CEO of Prevx - Monday, 8 November 2004.

The cyber-criminal is getting smarter and more organised and alongside this as have their methods of attack. Whereas 2 years ago the watchword was computer viruses, now new and infinitely more advanced attack methods exist. New and unknown ‘Zero-day’ attacks, such as worms and Trojans, seem to have the measure of traditional signature-based security technologies and a determined hacker can bypass even the most stringently configured company firewall to access system files and the registry. Also, attackers now seek to run targeted scams that are kept purposely low enough profile to not raise awareness with AV and spyware vendors.

Whatever the reason for a malicious cyber-attack, whether it be for financial gain, espionage or just for the sheer hell of it, companies must protect against unwarranted incursion into their system. However, with these new methods of attack it is becoming increasingly difficult to ensure that they don’t penetrate computer systems because when they do the effects can range from the defacement of websites to the fraudulent extortion of vast sums of money. The recent attacks Bluesquare are a case in point of how far hackers are willing to take extortion.

So what can be done to ensure a sufficient level of protection against attack from these sources? Clearly, patching is not working because of the speed with which these attacks strike and propagate to other computers. A PC worm may be similar to a virus, in that it spreads from computer to computer, but where the worm differs is the speed of self-propagation. Worms use the basic transport mechanisms of any computer or network to spread as quickly as possible, allowing attackers to take control of systems and execute malicious behaviour. Normally this happens before a patch has had a chance to be created, let alone implemented, meaning worms can march through the globe’s computer systems at an incredible rate. Sasser and Blaster are examples of how devastating they can be.

The traditional signature-based approach still favoured by many companies to detect malicious attacks is based on patches, updated at regular intervals, and is inherently reactionary and out-of-date to stop zero-day attacks. Until a worm or Trojan is known and a signature created and updated, the antivirus program cannot provide protection against the malicious code as it does not recognise it as a threat. Even when the signature for these is known, if a worm executes itself from memory and not from the file system, a lot of antivirus programs are not capable of protecting a system from it. A lot of this type of code also hides in less accessed system directories which will only be processed by AV software during a full file scan. Which means that in most cases AV will help clean up the worm only after it infects the machine or network, and probably infected many other systems.

So how do we protect against this new breed of attack that is seemingly marching through unprepared systems? Intrusion detection software does not rely on signatures but highlights when malicious code has accessed critical areas such as memory, file system, OS, registry and applications. However closer to the mark this is it is still a case of closing the gate once the horse has bolted – surely prevention is better than cure. This is where Host Intrusion Prevention Software (HIPS) enters the fray.

HIPS recognizes anomalies in exactly the same way that intrusion detection software does – crucially, however, it does so before these have had a chance to access critical systems. Sitting just behind the firewall, HIPS recognizes all the traits of a zero-day attack by understanding the methods used to launch such an attack and blocking them. HIPS requires no patches, no signature updates or rules to work because it identifies the characteristics of the attack behaviour and stops the action taking place. A security guard trained to recognize the faces of wanted criminals is no good if they cannot work out for themselves when a masked man is breaking in.

Data is now the most important commodity that many companies have. This data needs to stay protected from outsiders whilst at the same time continually available to those who it is intended for. Malicious attacks seek to undermine both of these objectives using progressively more advanced hacking techniques. It is up to the corporate world to adapt to this and employ progressive IT security capable of addressing the problems of zero-day hacker attacks. Whilst HIPS may not be a silver bullet, employed in-line with AV software it will catch and destroy any attempt to enter your system propagated by these new attacks - providing the last man standing where signature-based security has failed.