

# Network Immunity – Is It Possible?

by Mike Englebrecht  
National Director of Networking & Security Solutions

Networks worldwide are being threatened, attacked and subjected to a variety of threats including viruses, worms, Trojan horse and internal attacks. These attacks are coming from individuals that are no longer looking for playful logins, but for more devious and damaging results.

According to the 2006 CSI/FBI Computer Crime and Security Survey, more than half of the organizations surveyed – including U.S. corporations, government agencies, financial institutions, medical institutions and universities – experienced computer security incidents during the previous year. Of those that experienced incidents, nearly 25% reported six or more attacks during the year.

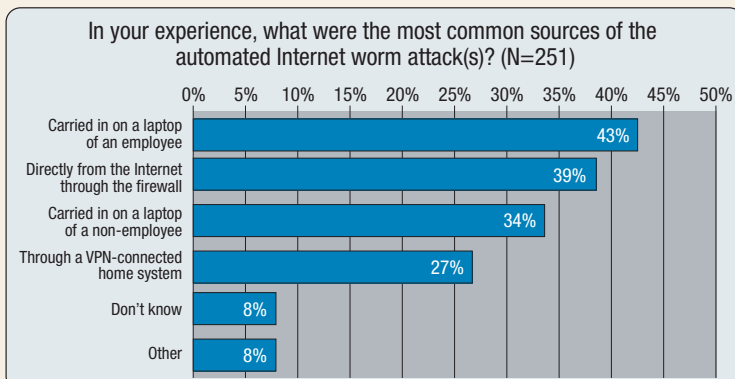
The reported losses are significant: \$52 million for the 313 respondents, an average of \$167,000 per respondent. More importantly, only half of the total survey respondents actually reported their losses, due to concern about public reporting of attacks and losses, and so it is difficult to accurately gauge the actual losses. One thing is certain, network attacks are far more widespread than had been imagined.

Today's security concerns are pushing companies to implement stronger measures to protect the organization's assets. Hackers are creating more sophisticated worms and viruses that exploit clients as they move to a more mobile workforce. Companies are losing millions of dollars in damage due to these more sophisticated viruses and Regulatory Compliances are forcing business to rethink their security measures. A single attack can cause an unexpected and unwanted downtime, forcing IT departments to rethink their current position on network security. Today's firewalls, Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS) and corporate VPNs have helped prevent attacks from external sources and these measures have been effective in preventing attacks in the past. Today's viruses are attacking corporate assets from inside the protection of the firewalls with infected laptop and desktop clients and bypassing many of the security solutions put in place.

Today's viruses, like Slammer, Sasser, Blaster and Code Red, show Internal attacks (ones from companies own client PCs) and are an even a larger threat and shown to be even more difficult to defend against. With companies using more mobile devices, trusting user's ability to bring in these threats are even greater. These users could be partners, contractors, or employees. With these new threats, companies today need a solution that is part of the network, can detect know and unknown threats, and react to minimize the impact of the virus attack on the network and users. Network administrators also need to be concerned about the amount of additional management traffic that is created to secure the network from these threats.

Attacks are on the rise on vulnerable network operating systems as well as network applications. Applications and operating systems from companies like Microsoft and others remain a primary target of "day zero" attacks as hackers continue to find and exploit their network vulnerability. A day zero attack is a virus or worm that attacks the weakness of these networked solutions before one of the antivirus solutions has a fingerprint for the virus or the application vendor has a fix or patch. Day zero virus's can spread quickly, infecting an organization's servers, clients and other user devices across an organization's LAN and WAN infrastructure causing a disruption and loss of business. With increased sophistication these viruses are rapidly creating staggering losses within an organization.

## PCs and Employees Are Often Responsible for Malware Proliferation



Source: "The New Network Security Architecture" by the Enterprise Strategy Group, June 2006

Historically, threats were looked at as being externally oriented. In order to protect the organization, firewalls and intrusion detection solutions were used to protect the internal corporate LAN from the external world. This approach assumed the source of the attack was from the outside environment. Today's new virus and worms depend on users being more mobile, where clients bring their infected laptop or handhelds into the protected environment. In addition, disgruntled employees releasing viruses or acting maliciously inside the corporate LAN circumvents the protection of the firewall and other security solutions. These threats spread faster since most of the safeguards have already been bypassed.

Anti-virus solutions depend on pattern matching or recognition of a previously identified virus or worm to be effective. Day zero attacks release a new virus or worm that has not previously been identified or fingerprinted, and until a patch or signature is created, the clients and servers remain vulnerable. Day zero attacks must be looked at in a different way, since the traffic cannot be identified by its "pattern," but rather needs the "behavior" of the network or traffic analyzed.

offending port to an optional IDS/IPS. Further deep packet inspection can be done by the IDS/IPS and additional behavioral and pattern checks can be performed and evaluated. Security alerts from the IDS/IPS can be received by NIM with the appropriate action then taken. These actions are configured and automatically applied as inappropriate behavior is identified.

Other solutions, like the Symantec Security Information Manager (SSIM), work with network event correlation. The SSIM appliance collects data not only locally, but also looks at information collected by Symantec globally and applies policy compliance and vulnerability assessment from data collected around the world. SSIM uses log consolidation, event management and security intelligence correlation, delivering a comprehensive threat management solution. This solution allows customers to identify, prioritize, respond to and review incidents and threats in their environment. By providing real time updates from the Symantec Global Intelligence Network, security response teams can raise their security level and save time by more efficiently managing threats and responding with built in remediation instructions. SSIM minimizes deployment and management costs

**Day Zero Virus Timeline**



Solutions like, ProCurve's Network Immunity Manger Solution, look at the behavior of the network rather than the actual information inside the data stream packets. ProCurve Network Immunity Manager (NIM) solution along with the security features built into the ProCurve infrastructure devices (switches, routers and access points using s-Flow) and an optional IDS solution can provide a comprehensive threat detection and mitigation solution across a wired and wireless infrastructure. The s-Flow solution delivers a scalable security solution. The ProCurve NIM solution receives sampled traffic from around the network and its devices. The ProCurve NIM solution then evaluates the traffic looking for offending behavior. When an improper activity is detected, appropriate action is determined and automatically applied including mirroring the

through a self-maintaining infrastructure, which minimizes additional staffing and expertise.

Symantec's customizable dashboard allows a user to monitor the incoming events and view the current threat assessment from a single pane of glass. The desktop management tool will also allow the user to configure, control and monitor the response, as well as control the response of the current risks.

SARCOM can provide a number of security solutions including products from ProCurve and Symantec that will provide customers with a comprehensive security solution. SARCOM can also provide security assessments solutions and implementations that will deliver a turnkey solution, meeting their needs and delivering a high return on their investment.