

# The Future of Enterprise Hacker Attacks: How to Secure Network Endpoint PCs

A White Paper Presented by Zone Labs



Smarter Security™



As CEO and co-founder of Zone Labs, Gregor Freund brings his impressive experience as a technologist and entrepreneur to the company. In addition to holding eleven software patents, Freund provided the vision for Zone Labs enterprise security solution Integrity™ and the award-winning ZoneAlarm® and ZoneAlarm Pro personal firewalls.

Prior to founding Zone Labs, Gregor's accomplishments include helping to found Starfish Software, later acquired by Motorola, with noted software visionary Philippe Kahn as well as founding Borland International's first independent German and Italian distribution and development companies. Gregor also worked as a principal software architect for Borland.



### **In addition to the loss**

of business continuity, inconspicuous hybrid attacks can deliver a crippling financial blow to enterprises through theft of competitive, customer, and financial data or other valuable information.

## **SQL Slammer: A Warning Sign to Enterprises**

“The recent SQL Slammer attack comes as a warning to enterprises,” says Gregor Freund, CEO and co-founder of Zone Labs, a San Francisco-based company known for its best-of-breed, endpoint security solutions. In January 2003, the malicious SQL Slammer worm spread rapidly across the Internet—infesting millions of servers and PCs. Although the worm was relatively benign, it could have destroyed data easily and viciously.

Exploiting a buffer overflow vulnerability on Microsoft SQL Servers (and on any PC that ran applications with embedded SQL Server versions; otherwise known as MSDE), Slammer self-propagated by repeatedly probing port 1434/UDP, on any machine it could communicate with, in search of other vulnerable SQL Servers or SQL Server-equipped PCs. During its continued quest for unprotected PCs, SQL Slammer created a network traffic deluge that resulted in an effective denial of service for many enterprises.

The SQL Slammer worm illustrates how quickly an attack can infiltrate a network and spread to other systems. The Independent Digital reported that the worm “spread worldwide in 10 minutes,” and in its early stages, the worm doubled the number of machines it infected “every 8.5 seconds.” SQL Slammer’s rapid progress led the Cooperative Association for Internet Data Analysis (CAIDA) to conclude that if the worm “had carried a malicious payload, had attacked a more widespread vulnerability, or had targeted a more popular service, the effects would likely have been far more severe.”

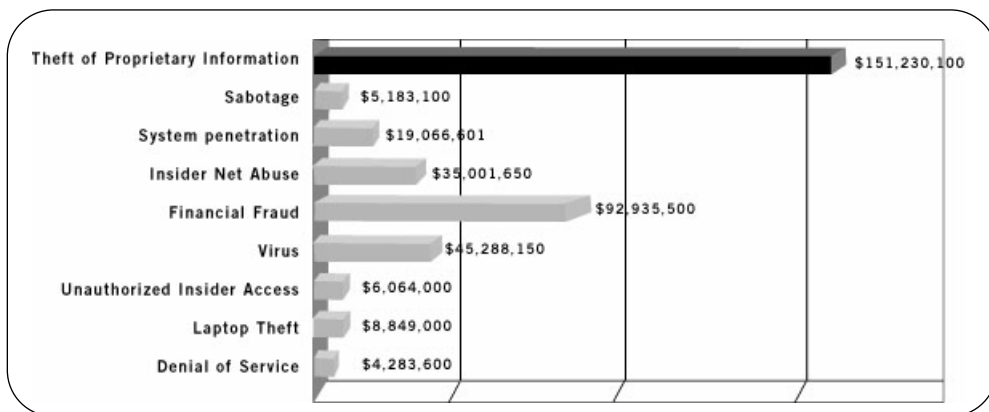
“This time, the worm didn’t deliver a payload, but had it combined its propagation technology with a Trojan, it would have become a next-generation, hybrid attack.” notes Freund. And, if SQL Slammer had been a hybrid attack, it could have done much more than interrupt business continuity. It could have, for example, propagated itself and then deployed spyware to broadcast sensitive enterprise data online; or a virus to deface or erase valuable data entirely; or, if combined with RAT technology, to give the hacker unregulated access to proprietary enterprise data accessible by the infected machines—information that could be stolen for profit.

Once any hybrid attack infects network PCs, it has the means and the opportunity to deliver a destructive or malicious payload. In addition to the loss of business continuity, these often inconspicuous hybrid attacks can deliver a crippling, financial blow to enterprises through theft of competitive, customer, and financial data or other valuable information. “Enterprises have real secrets, and they have real enemies who want to steal their data. The threat to all enterprises is, in other words, clear and present. Our enterprise customers have a vested interest in thwarting these next-generation, targeted attacks against their networks,” says Gregor Freund.

### Targeted Hacker Attacks: The Danger of Trojan Horses

Recognizing this threat and understanding its implications, Gregor Freund deems it critical that enterprises view SQL Slammer as a harbinger of next-generation, targeted attacks. Based on recent events, it's clear that "Hackers' motivations have changed. Instead of demonstrating their technical prowess by defacement or destruction, they're now hacking for dollars," he says.

With such profit-driven motivation, the attacks are likely to increase—in sophistication, frequency, and severity. Already, the consequences are staggering: a recent CSI/FBI survey found that two-thirds of all financial losses can be traced to data theft. Today's hacker is a technological thief who understands that proprietary enterprise information



*In 2002, according to the CSI and FBI Computer Crime and Security Survey, security breaches resulting in data theft accounted for 2/3 of all financial losses—far outstripping the costs associated with destructive viruses or worms.*

has become worth staggering sums to the right people. The intent of a targeted attack, in other words, is usually criminal, and any enterprise can become a target.

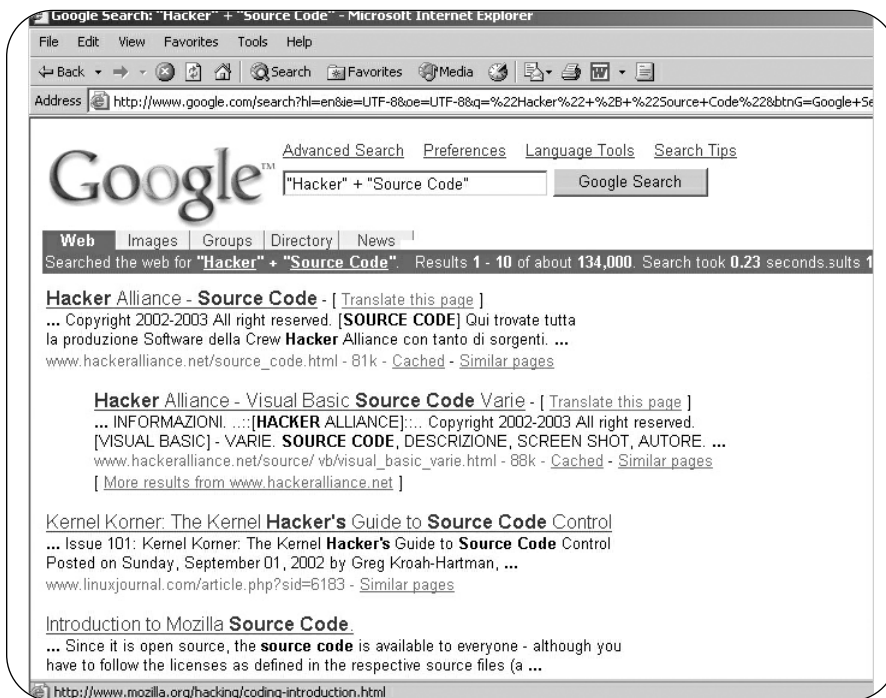
These next-generation attacks incorporate Trojan horses. Whereas the spread of SQL Slammer worm was noisy and obvious in its slowing of networks, a Trojan horse sneaks into a network surreptitiously. When successful, it draws little attention to itself; its goal is to infiltrate the enterprise, capture information, and send it back to a hacker—or, in the case of a remote-access Trojan horse, to give a hacker remote control of a computer—all as quietly as possible. With a Slammer-type attack, enterprises know almost immediately when they've been hit; with a Trojan horse, an enterprise may discover the extent of the damage only after it is too late.

Compounding the threat of next-generation attacks is a confluence of contributing factors. New worms are extremely adept at propagation and infiltration, and the Internet facilitates their spread. Also, because hacking-tool source code and pre-packaged scripts for Trojan horses are readily available online, all a hacker needs is a little knowledge of system vulnerabilities and a willingness to exploit those attributes for financial or personal gain. And because companies often publish system vulnerabilities in an attempt to protect or warn their customers, their revelations can then become

“Without question, the easiest way of targeting an enterprise is through its network endpoints—especially its remote and mobile PCs.”

- Gregor Freund

attack maps for hackers exploiting these same vulnerabilities. “The line between telling people how to protect themselves and educating hackers is a very fine line,” says Gregor Freund. Once a hacker is armed with tools and motivation, it isn’t long before an enterprise becomes the victim of a targeted attack.



Unfortunately, dangerous hacker tools are readily available. For example, any search engine query will result in over 134,000 sites with sophisticated hacker tools designed to assist criminals in targeted data theft and corporate espionage.

### The Enterprise Vulnerability: Endpoint PCs

“Without question, the easiest way of targeting an enterprise is through its network endpoints—especially its remote and mobile PCs,” says Gregor Freund. With this in mind, it becomes essential for enterprises to protect their vulnerable endpoints against next-generation attacks.

Hackers find remote and mobile PCs extremely attractive targets because they reside outside the corporate firewall but have access to the enterprise. As such, these computers offer a convenient entry point. Aiding the hackers is the fact that telecommuters or mobile professionals often access their enterprise networks using insecure connections, such as dial-up, broadband, wireless, or third-party networks. At the same time, on-site employees often leave work with their laptops and return to their enterprises the next morning—only to re-dock behind the corporate firewall. PCs behind the perimeter firewall are at risk as well. Employees use their work PCs for personal use, so they have access to their POP3 mail accounts via their mail client or Web browser. They also may participate in peer-to-peer file sharing, instant messaging, and file downloading, and all these activities could potentially bring a Trojan horse directly into the heart of an enterprise network.

**Nearly 90 percent**  
of companies use  
perimeter firewalls and  
antivirus software, but  
85 percent still  
succumbed to attacks  
last year.

—2002 CSI/FBI  
*Computer Crime and  
Security Survey*

Unfortunately, existing security technologies—which many enterprises have deployed—do not effectively mitigate these risks or seal these vulnerabilities; as a result, endpoint PCs become convenient targets for today’s hackers.

Traditional antivirus security measures rely upon databases of known viruses, which make them reactive by nature. Also, antivirus measures are burdened by latency of signature; by the fact that they only acknowledge known viruses; and by the fact that they do not recognize custom viruses. And no antivirus database can be updated quickly enough to halt a worm that spreads to every Internet host within 10 minutes. Although host- and network-based intrusion detection and prevention systems can be more proactive, they also depend upon a database of known attack patterns, network traffic, and host-intrusion attempts. Perimeter firewalls can stop some inbound attacks at the gateway, but they must remain open for ports and protocols that bear network inbound and outbound traffic. IT professionals using perimeter firewalls cannot view the source of outbound traffic and therefore can’t differentiate between valid port 80 ‘http’ traffic generated by a browser and similar traffic generated by an insidious Trojan horse. In fact, nearly 90 percent of companies use perimeter firewalls and antivirus software, but 85 percent still succumbed to attacks last year, according to the 2002 CSI/FBI Computer Crime and Security Survey. The fact is: perimeter-centric security systems alone cannot offer the necessary protection against new and unknown hacker attacks.

The sophistication of today’s targeted, next-generation attacks demands an aggressive, intelligent solution—that of endpoint security.

**Integrity: The Proactive Solution for Vulnerable Endpoints**

With Integrity, vulnerable endpoint PCs are protected by a multi-layered security system that enables enterprises to block new and unknown attacks automatically. As a result, IT departments can mitigate the impact of malicious worms and can defend their enterprises against costly Trojan horse attacks.

Integrity is built upon patented technology that has been field-tested across industries on more than 20 million consumer PCs and throughout countless enterprises. Zone Labs TrueVector® technology takes a unique, guilty-until-proven-innocent approach to security, and it allows enterprises to control and extend security down to the application level. Application control is critical in securing network endpoints because it ensures that only checksum-verified applications enter the network, thereby keeping enterprises safer from targeted hacker attacks.

“Technology, no matter how advanced, needs a strong management complement for the system to operate seamlessly and effectively,” says Gregor Freund. Using centralized, Web-based management combined with agents on each endpoint, Integrity enables efficient network management so an IT professional can quickly create, deploy, and enforce flexible policy assignments across the network from a single location. As a whole, the multi-layered security approach of Integrity, with its advanced management component, minimizes the risk of vicious targeted hacker attacks and malicious worms.



**“A solution is to install centrally managed personal firewall software on all PCs across the enterprise, including tower desktop PCs...such as Zone Labs.”**

*- John Pescatore,  
The Gartner Group*

### **Three Steps for Securing Enterprise Systems Now—with Zone Labs Integrity**

“SQL Slammer illustrated how hard it is for enterprises to constantly follow up on patches and deal with all the system vulnerabilities,” Freund says. Indeed, in a perfect world, all systems would be updated immediately and continuously. New patches would be installed as soon as they are released. System-wide implementation would happen routinely. But reality dictates differently. At any given time, a significant number of enterprise endpoints do not reflect the most current security measures. With shrinking staffs and increasing responsibilities, today’s IT professionals struggle to perform basic network maintenance. With a fleet of thousands of PCs and laptops, ongoing administrative tasks create a huge burden on IT departments. There is no question that the time involved in researching each patch and updating every computer is formidable. But obsolete security or insufficient security make network endpoints even more vulnerable, and hackers bank on this.

Zone Labs has designed its Integrity management tools to address this very problem and to help IT departments gain control of their enterprise networks. Once an IT department has a solid PC firewall in place, it can then set proactive and reactive policies to mitigate system vulnerabilities. And once system vulnerabilities are locked down, the enterprise becomes more secure against worms and targeted hacker attacks.

#### **Step 1: Deploy a PC Firewall**

The mandate is stunningly simple: for immediate protection, IT departments can deploy a PC firewall on each network endpoint. By putting the machines in “stealth” mode, administrators ensure that enterprise PCs are invisible to hackers; if these machines cannot be seen, they cannot be hacked.

Now administrators have the tools to establish an enterprise-wide firewall with minimum effort. Integrity ships with pre-configured policy templates, so an IT administrator can immediately pick a template that is appropriate for the level of security he wants to apply—and then deploy that policy across the entire network. Unlike traditional ‘port and protocol’ firewalls, Integrity offers an immediate solution that does not require complex configuration. The process is simple, and within minutes, an IT department can have a solid firewall policy set and deployed on all of its PCs.

#### **Step 2: Create and Enforce Proactive Policy**

Once an IT department has its firewall policy in place for immediate protection, it can begin to think about shaping a proactive policy. Policy serves an important function: closing off known system vulnerabilities. By creating and deploying role-appropriate policies throughout the enterprise, IT departments ensure that only authorized applications can access the enterprise network. At the same time, IT administrators can minimize the risk inherent in applications such as peer-to-peer file sharing, outdated browser versions, or instant messaging programs.

Once these flexible policies are created, an administrator can deploy and assign them in a number of ways, depending on the needs of the enterprise. For example, an IT administrator may set policy by users or groups (syncing with existing active directory, LDAP or Radius management systems), connection type (VPN, dial-in, wireless LAN), or by IP address.



Enterprises also need to ensure that endpoint antivirus software is current when employees access the network. Integrity's exclusive Cooperative Enforcement™ technology quickly audits each PC before it accesses the network. If the endpoint does not comply with the latest antivirus software, the user is directed to upgrade. Cooperative Enforcement also integrates with select VPNs to prohibit remote-access connections until the user is in compliance. Cooperative Enforcement technology integrates within the existing IT infrastructure to close gaps and harden overall network security.

### Step 3: Deploy a Reactive Option

At some point, despite the best measures, an IT department might discover that its security policy parameters were too lenient and that a threat has infiltrated its enterprise. When this occurs, Integrity provides the ability to set an immediate, reactive policy so that an IT department can respond to the threat in real time. In the midst of an attack, for example, an enterprise can block ports or applications and effectively put the network in lockdown while assessing the situation. In this way, Integrity gives IT departments a measure of control over the attack; more importantly, Integrity reduces the extent of an attack's damage.

### Conclusion

SQL Slammer was relatively innocent this time, but this worm should be seen as a harbinger of future attacks. Next-generation attacks will combine the spread and reach of a worm with the payload of Trojan horse technology.

It is an unfortunate truth that calculated, targeted attacks are part of today's enterprise landscape. Inevitably, almost every enterprise will be attacked at some point. The response to such dangerous, but as yet unknown, attacks is "to work at developing security solutions that effectively mitigate the risk," says Gregor Freund.

At the same time, a confluence of factors contributes to danger of these insidious attacks: the Internet facilitates the fast spread of threats; system and software vulnerabilities are well known and easily exploited; vendors have emphasized access and productivity over security; and, tomorrow's hackers are criminal: they are driven by theft and destruction and are motivated by profit.

Until now, enterprise security administrators have not had access to effective tools to secure their networks. Now, IT professionals can use Integrity, which allows enterprises to assess risk and then create and enforce proactive policies across the organization. "We have designed Integrity," Freund says, "with the IT professional in mind. IT departments need maximum yet flexible security that is easily managed and easily deployed."

Integrity is a proven, best-in-class solution that offers superior security and easy administration. It has been designed to protect an enterprise's most vulnerable areas—namely, its endpoint PCs. As a result, the entire enterprise network becomes more protected. Integrity is the solution of choice for enterprises that are committed to mitigating the risk of next-generation attacks.

To learn more about how Integrity can minimize your risk of new and unknown hacker attacks, contact a Zone Labs representative at 1-877-876-4960.

### **About Zone Labs**

Zone Labs, Inc. is a leading creator of endpoint security solutions that millions of customers trust to protect their PCs from the risk posed by hackers and data theft. Zone Labs' proven technology is deployed by global enterprises, service providers, small business and consumers.

**For additional information, please contact a Zone Labs representative at 1-877-876-4960 or visit our Web site at [www.zonelabs.com](http://www.zonelabs.com).**

#### **US Headquarters**

Zone Labs, Inc.  
1060 Howard Street  
San Francisco, CA 94103  
tel (415) 341-8200  
fax (415) 341-8299

#### **European Headquarters**

Zone Labs, Inc.  
Düsseldorfer Str.  
65760 Eschborn, Germany  
tel +49 6196 773 670  
fax +49 6196 773 6777

© 2003 Zone Labs Inc. All rights reserved. All trademarks of Zone Labs, Inc. used herein (including but not limited to TrueVector, ZoneAlarm, Zone Labs, the Zone Labs logo, AlertAdvisor, Cooperative Enforcement, Policy Lifecycle Management, Zone Labs Integrity and Smarter Security) are trademarks or registered trademarks of Zone Labs, Inc. in the United States and other countries. All other trademarks are the property of their respective owners. v032703

