STATE OF INTERNET SECURITY

Q107 Focus:

Protecting Enterprise Systems

webroot
SOFTWARE, INC.

TABLE OF CONTENTS

INTRODUCTION

The State of Internet Security report provides an in-depth review and analysis of the most pressing computer and data security related concerns. Based on research conducted by Webroot Software, Inc., each quarterly report will focus on a specific aspect of Internet security.

The focus for the first quarter of 2007 is *Protecting Enterprise Systems*. This report provides industry data, trends, best practices and an evaluation of the threat landscape.

Future reports will concentrate on the Internet security topics of the day that impact Webroot's consumer and business customers around the globe.

O V E R V I E W

Since the very beginning of commerce, businesses large and small have needed to secure and protect their assets. For many years, a safe inside strong walls with a locked door, or perhaps a fence and a vicious dog, were all perfectly adequate solutions. Of course, with the advent of computer technology the world has changed significantly in recent decades.

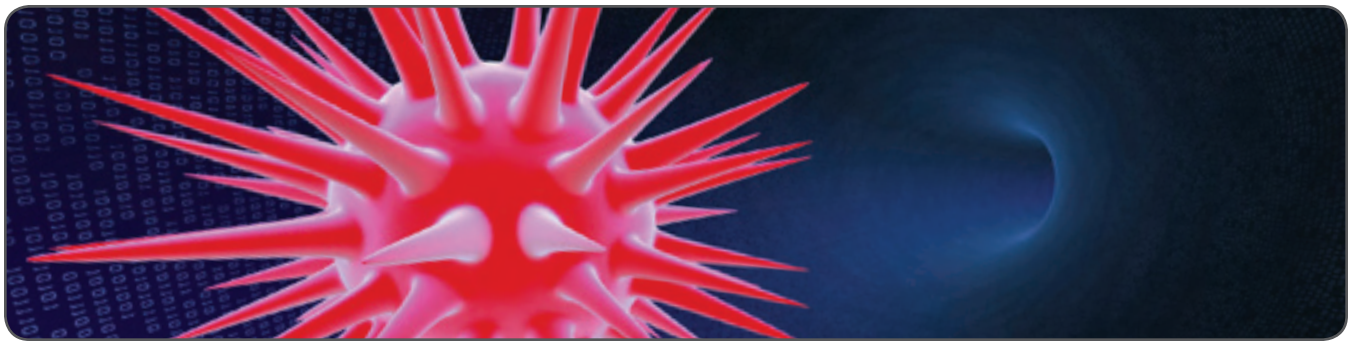
Today, the vast majority of intellectual property, customer information and trade secrets are created and stored in the form of 1s and 0s – making data security a top priority for every company. Loss of physical assets such as laptops and storage media that can contain highly sensitive and valuable data, as well as intentional criminal or malicious activities from within the organization caused by a disgruntled employee, remain significant risks to data security that need to be addressed in a company's approach to protecting information assets.

Additionally, with the arrival of the Internet the number of external people who can potentially make their way "inside the company's walls" has multiplied exponentially. Online perpetrators are well-paid to extract information such as social security numbers, credit card numbers, bank account numbers, user names and passwords from company files. Internet security deals specifically with risks that arise from network connectivity to the world, including spyware, viruses, Trojan horses, system monitors, rootkits, keyloggers, phishing, pharming, adware and spam.

These economically motivated efforts to infiltrate a company's network present significant costs and liabilities. In addition to the risk of direct losses, there are also significant impacts to staff productivity. Furthermore, companies are increasingly held accountable by government agencies and shareholders for properly securing the consumer data they retain. Failure to do so can result in legal charges, fines and a damaged reputation.

This report explores the most prevalent Internet security threats, their impacts, and what companies need to do to protect their most valuable business assets.

SECURITY THREATS



Internet Security Threats Impacting Enterprise Systems

Companies hold valuable information in the form of customer data, proprietary information and trade secrets in their computers, networks, servers and storage devices. As a consequence, company IT systems are under constant attack driven by the potential for monetary gains. Greed breeds creativity in the methods used to steal enterprise data. This is evidenced by the "wolf in sheep's clothing" approach that ties lower risk threats to critical risk threats, as well as the increasing complexity of the threats invading IT systems.

The Threat Food Chain

Industry analyst firm IDC's Enterprise Security Survey for 2006 identifies the top five threats to enterprise security as:

- Trojans, viruses, worms, and other malicious code
- Spyware
- Spam
- Employees
- Application vulnerabilities

These categories are closely intertwined. Spam can be the delivery mechanism for spyware, and spyware's primary payload is often a Trojan horse, which disguises the real or secondary payload. A Trojan can download multiple pieces of spyware, or contain spyware bots (web robots that run automated tasks) used for spam, backdoors, or keyloggers to record user keystrokes.

Spam can be the delivery mechanism for spyware, and spyware's primary payload is often a Trojan horse, which disguises the real or secondary payload.

Too often adware and spam have been categorized as mere nuisances and not considered truly damaging. That trend is clearly changing. Recently, the New York State Attorney General reached a settlement with three well-known online advertisers, Travelocity, Priceline and Cingular Wireless, for promoting products and services on the Internet through deceptively installed adware programs. This is just one example of government action based on the view that adware can cause material harm.

Beyond the incessant inflow of spam and adware, spyware writers will be relentless in their efforts to penetrate the enterprise because it is their business. They are parasites in the corporate IT environment that survive at the expense of the systems they infiltrate. Successful spyware writers reap significant financial rewards, usually in the form of bank passwords and personal information, such as social security numbers, credit card information, as well as Web site and e-mail usernames and passwords.

Beyond individuals chasing these financial gains, there has also been greater involvement from organized crime groups in recent years. While at a cybercrime conference in London, Christopher Painter, deputy chief of the computer crimes and intellectual property section of the U.S. Department of Justice, told reporters, "There are still instances of 'lone-gunman' hackers but more and more we are seeing organized criminal groups." In an interview with ComputerWorld magazine, Andrew Arena, special agent in charge of the U.S. Federal Bureau of Investigation's criminal division in New York, stated that cybercrime is the number three overall priority at the FBI (only behind counter-terrorism and counter-intelligence) as it overlaps organized crime, as well as state-sponsored and terrorist organizations.

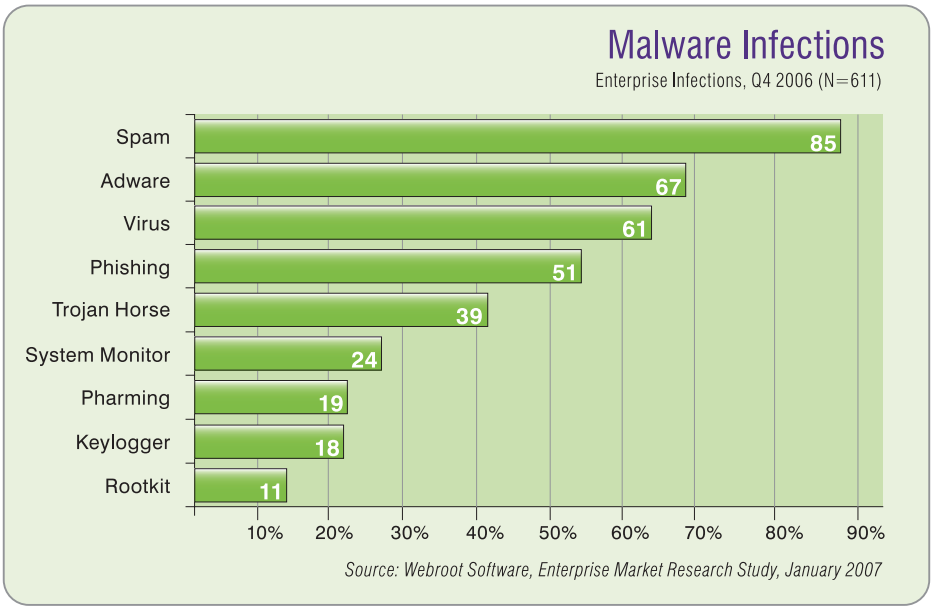
Increasing Complexity of Threats

The United Kingdom's Department of Trade and Industry (DTI) commissioned PricewaterhouseCoopers LLP to conduct an Information Security Breaches survey in 2006 that found 99 percent of companies are connected to the Internet, and over 80 percent of the large companies surveyed suffered a security incident within the preceding year. Web sites continue to be a leading source for malware infections. The Threat Research Team at Webroot Software identified exploits on over 3 million web sites in 2006. An exploit takes advantage of malicious code present on a Web site to force a Web browser to install spyware or other malware on a user's machine without his or her knowledge or consent.

Cyber-crime is the number three overall priority at the FBI, only behind counter-terrorism and counter-intelligence.

For years now, spyware and other unwanted programs have often been able to bypass traditional security defenses like firewalls and other perimeter solutions because the malicious programs are disguised as legitimate traffic entering through well-established ports left open on firewalls. Once installed on a system, many spyware applications disguise themselves as trusted programs, allowing them to communicate freely with the Internet over TCP ports that are commonly left unprotected.

According to a market research study conducted by Webroot Software in January of 2007, over one-third of enterprises surveyed dealt with Trojan horse attacks (39 percent) and almost one-fourth dealt with system monitor attacks (24 percent).



Significantly compounding the challenges posed by these programs is how they are programmed to evade detection. Today's spies are more complex and dangerous, infecting machines with more registry entries and files to make removal more difficult. Further complicating removal efforts, many pieces of spyware use watcher processes, which monitor each other so that when removal is attempted the malicious code will be repopulated or new components will be downloaded from the Internet.

Most alarming is the continuous trend towards more advanced techniques. Just a couple years ago, rootkits, Trojans, and polymorphic code (capable of mutating while keeping the original functionality intact) were the most advanced methods being used; these are now becoming common ways to evade detection. Today's spyware programs create permissions to gain network access, alter security settings and modify system properties and preferences.

In 2006, there were increasing incidents of even more sinister ways to infiltrate and capture PC data, including what has become referred to as ransomware. In these cases, once installed on the computer, the code encrypts data holding it hostage. Then a ransom to be paid via an online payment service is requested to recover the files. Businesses are often the targets of these types of attacks. The requested amount is generally low enough that many simply pay "the ransom" and do not report the crime to law enforcement so that access to the information can be recovered as quickly as possible.

The chart below summarizes how the distribution and infection methods, as well as the removal techniques required, have evolved since 2004.

The Evolution of Threat Complexity

	2004	2005	2006
Type	• Benign Adware • Randomized Hijacks	• Malicious Adware • Trojans	• Targeted/Custom Trojans • Phishing Trojans
Distribution	• Web sites	• BitTorrent • Peer-to-Peer (P2P) • Bundles • Piggybacking	• Email • Internal Hacking
Infection	• File Placement and Naming	• DLL Injection • Browser Helper Object (BHO)	• Modifying Executables
Removal	• Deleting on Disk • Deleting Registry Keys	• File Neutering • Correlation Removal	• Driver-based Removal • Dynamic Conditional Removal

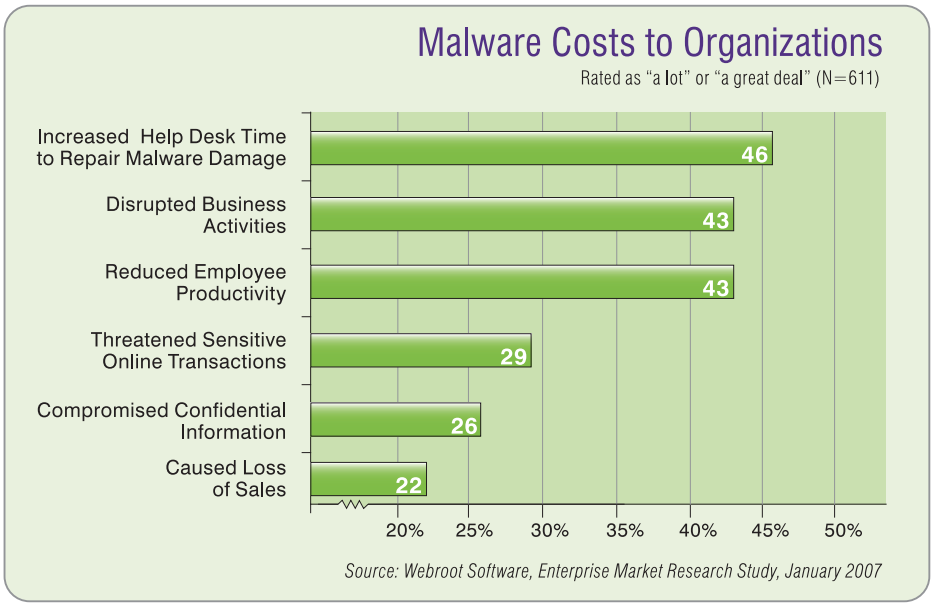
Source: Webroot Software Threat Research Department

COST IMPLICATIONS

Cost Implications for the Enterprise

These unrelenting attacks on enterprise networks have significant cost implications. Based on an industry survey conducted by Webroot in January 2007, almost half of the companies had incurred the costs of increased help desk time to repair spyware damage, disrupted business activities and reduced employee productivity. In addition, more than a quarter of the companies stated that confidential information had been compromised as a result of spyware. Beyond the direct costs and impacts to employee productivity, failure to adequately protect enterprise IT systems from Internet security threats can also expose the company to legal liabilities.

Almost half the companies surveyed had incurred the costs of increased help desk time to repair spyware damage.



Repairs and Support

Based on Webroot's experience with thousands of enterprise customers, a profile of an "average" company's experience with malware issues is described in the table below. Webroot prepared this case study analysis of the repair, support and productivity costs for a company with 14,000 workstations.

Malware Cost Analysis: Company X with 14,000 Workstations				
Help Desk Costs				
Average percent of users with a malware-related call each month	Average number of malware-related calls per month	Average cost per call	Monthly Cost	Annual Cost
7.5%	1,050	$20	$21,000	$252,000
IT Support Costs for Machine Re-Imaging				
Average number of machines re-imaged per day	Average hours needed for each re-image	Average hourly rate for employee time	Monthly Cost	Annual Cost
3	3	$50	$9,000	$108,000
Lost Productivity of Employee (user) with Affected Machine				
Average number of employees with affected machines per day	Average hours of lost productivity while machine is being re-imaged	Average hourly rate for employee time	Monthly Cost	Annual Cost
3	3	$50	$9,000	$108,000
		Total Costs:	**Per Month**	**Per Year**
			$39,000	**$468,000**
Source: Webroot Software Threat Research Department				

While these costs will vary from company to company, the multiplying effect of the sheer volume of incidents that enterprise IT departments must remedy remains the same. These direct support and productivity costs are themselves significant, yet they are only a part of the impact felt by enterprises infected with spyware and other Internet threats.

Information Security Breaches

The 2006 Information Security Breaches survey issued by the United Kingdom's Department of Trade and Industry (DTI) found that the average cost of a UK company's worst data security incident of the year was roughly $23,000. The breaches in large businesses were seven times more expensive, with the average cost of the worst incident reaching $175,000. Based on the survey, DTI has said that the overall cost of data security breaches incurred by UK companies is in excess of $19.5 billion per annum.

In the U.S., the Small Business Technology Institute conducted a study called *Small Business Information Security Readiness* covering the same time period that reported more than half of all small businesses experienced a security breach. In spite of these incidents, nearly one-fifth of the companies were not using virus-scanning software for e-mail, over 60 percent did not protect their wireless networks with encryption, and two-thirds did not have an information security plan. The costs of a serious incident could have an even more significant impact on a smaller company, yet many small businesses make reactive purchase decisions only after suffering an information security incident.

The overall cost of data security breaches incurred by UK companies is in excess of $19.5 billion per annum.

Beyond the direct costs associated with resolving incidents, there are significant intangible costs associated with brand and reputation damage when government action is taken following a data breach. In the United States, government offices responsible for protecting consumer interests, such as the U.S. Federal Trade Commission (FTC) and several state Attorneys General have become increasingly proactive in filing complaints against companies for lax computer security measures.

For example, in 2006, the Federal Trade Commission (FTC) approved a final consent order with DSW, Inc. (FTC File No. 052-3096). The complaint filed by the FTC stated that DSW, Inc. had created unnecessary risks to the personal information collected about consumers in its stores by failing to use readily available security measures to protect its computer networks, nor employing sufficient measures to detect unauthorized access. As result of the consent decree, DSW was required to establish and implement "a comprehensive information security program that is reasonably designed to protect the security, confidentiality and integrity of personal information collected from or about consumers." Similar findings and requirements have been included in other FTC consent decrees, such as in the BJ Wholesale case in 2005 (FTC File No. 042-3160).

In spite of these and other highly visible cases in the past couple years, significant data breach stories continue to surface. In January 2007, reports emerged that hackers used a Trojan to access customer information from TJX Companies, possibly for as long as three years. Stolen was credit card, debit card, check and merchandise return transaction information for customers of T.J. Maxx, Marshalls, Homegoods and A.J. Wright stores in the United States and Puerto Rico; Winners and HomeSense stores in Canada; and possibly T.K. Maxx stores in the United Kingdom and Ireland. The breach has already generated consumer lawsuits against TJX, the first of which was filed in U.S. federal court in Boston. The case, which may become a class action suit on behalf of anyone who had their personal information stolen, claims that TJX failed to have adequate security in place to safeguard customers' data, and failed to notify customers of the breach as soon as it was discovered, constituting negligence.

Legal and Regulatory Compliance

Over the past decade, in an effort to protect citizens' data from misappropriation and fraud, governments in many parts of the world have instituted additional data protection measures. While legal and regulatory compliance can often be expensive, it is a cost of doing business in that given jurisdiction. Even more costly is the potential liability for a company that fails to comply with the appropriate legal requirements to safeguard sensitive information.

One of the most well known laws in this regard is the European Union's Data Protection Directive. This Directive sets out the guidelines on which European countries have crafted their laws. Article 17 of the Directive requires:

> *Member States shall provide that the (data) controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, alteration, unauthorized disclosure or access, in particular where processing involves the transmission of data over a network.*

Most European countries have now implemented this Directive in country-specific laws very similar to the language used in Section 31 of the Italian Personal Data Protection Code to address security requirements. It states:

> *Personal data undergoing processing shall be kept and controlled, also in consideration of technological innovations, of their nature and the specific features of the processing, in such a way as to minimize, by means of suitable preventative security measures, the risk of their destruction or loss, whether by accident or not, of unauthorized access to the data …*

The United States also has several laws that set out data protection requirements. For example, the U.S. Health Insurance Portability and Accountability Act (HIPAA) requires that the privacy of medical records be adequately protected against unauthorized access and misuse. In the financial sector, the Gramm-Leach-Bliley Act requires that organizations which maintain credit information for customers be held accountable if that data is accessed or compromised by an unauthorized third party. All public companies must comply with Sarbanes-Oxley (SOX) which includes attesting to the risk assessment and audit controls required by the Act. Incidents of unauthorized network access, system monitors and Trojans can bring the authenticity of reporting into question, and will raise concerns of SOX non-compliance.

Beyond country laws, there are international governing bodies and industry organizations that have set certain relevant requirements. For example, the Basel Committee on Banking Supervision provides a forum for regular cooperation on banking supervisory matters, and over recent years, it has developed increasingly into a standard-setting body. The Committee, whose members come from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom and the United States, is best known for its international standards on capital adequacy. Risk management is a significant factor in determining a bank's required capital reserves. In turn, this becomes a factor in a bank's review of business loan applications. Planned for implementation by this year, the Basel Committee issued a revised Framework referred to as Basel II to "promote the adoption of stronger risk management practices by the banking industry." Basel II defines operational risk as "the risk of loss resulting from inadequate or failed internal processes, people or systems, or from external events."

Many U.S. companies that do business in Europe have struggled to comply with European directives since they can be a significantly higher standard than in the U.S. Rules and regulations in different countries can overlap or conflict, creating a complex challenge for security executives responsible for aligning security strategy across the globe. In the face of these diverse laws, rules and regulations, some organizations find themselves overwhelmed and unsure about how to achieve compliance. To complicate matters further, the often-ambiguous language of the laws causes some businesses to suffer from 'analysis paralysis' and ultimately – they end up doing nothing at all.

Rules and regulations in different countries can overlap or conflict, creating a complex challenge for security executives responsible for aligning security strategy across the globe.

PROTECTING THE ENTERPRISE

Protecting the Enterprise

One of the biggest challenges enterprises face in dealing with Internet security is the apparent pot of gold available to the perpetrators. Malware writers can be paid large sums for each Trojan planted on a computer. This creates some very strong incentives that undermine a company's ability to protect enterprise IT systems.

Another development complicating the job of corporate IT departments is the ever-growing number of network access points and wireless network support. As employees are increasingly mobile, relying on laptops and remote access to connect to the corporate network, the ability to ensure those machines are malware free is critical. Network-level controls are insufficient. Every machine needs to be secure as well.

In order to effectively protect the enterprise against Internet security threats, companies require a multifaceted approach. Fortunately, there has been a great deal of attention paid to these concerns in recent years, and there are both guidelines and technologies that companies can implement to help assure the security of their information.

Failure to protect enterprise IT systems from Internet security threats can expose a company to legal liabilitites.

Policy and Process Best Practices for Securing Enterprise Information

Company efforts to secure enterprise information must include appropriate corporate policies for information handling that are strongly enforced, along with significant employee education.

Based on the widely accepted British Standard BS 7799 for information security management, the International Standards Organization issued ISO/IEC 27001 that specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System. It specifies requirements for the implementation of security controls customized to the needs of individual organizations. This along with other guidelines and standards provide tools for companies to assess and implement appropriate information security programs.

Another reliable directive is the globally recognized Payment Card Industry (PCI) Data Security Standard, which was created as guidance for all companies that process any credit card information whether from consumer or businesses customers. It states that companies should:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

The PCI standard provides details about how to best fulfill each of these objectives. Specific elements of the standard, such as ensuring that anti-virus programs can protect against other forms of malicious code such as spyware and adware, are important guidance for all companies, even those that do not accept credit cards as a form of payment.

Along these same lines, some government regulatory bodies have issued advisories to the entities which they oversee in an attempt to avoid preventable security breaches. For example, the U.S. Federal Deposit Insurance Corporation (FDIC) issued an official letter of guidance to financial institutions that recommends:

- Restricting users from downloading software not previously approved by the bank.
- Expanding the risk-assessment process to consider threats from spyware.
- Expanding security and Internet use policies to include risks associated with spyware and acceptable user behavior.
- Taking steps to enforce these policies and reprimand staff who fail to comply.
- Installing and configuring firewalls to monitor both inbound and outbound traffic. If possible, block outbound ports that are not necessary for business functions.
- Implementing tools to scan e-mail for spam and either block the e-mail or designate it as spam.
- Implementing tools to restrict or prevent pop-up windows.

While aimed specifically at U.S. banks, there are policies and processes that all enterprises will benefit from following. Implementing strong Internet security policies and processes is critical to ensure that the technological tools utilized are fully effective.

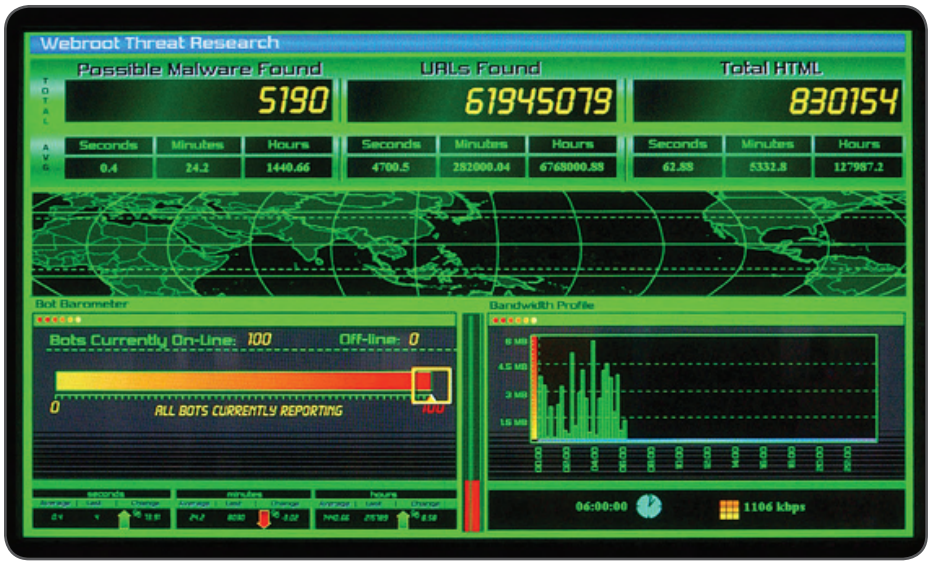
Technology Best Practices to Secure Enterprise Information

The U.S. Government Accountability Office provided government departments with these criteria for the consideration, selection and implementation of cybersecurity technologies that are equally applicable to private enterprises:

- Implement technologies through a layered, defense-in-depth strategy.
- Consider the (organization's) unique information technology infrastructure.
- Utilize results of independent testing when assessing the technologies' capabilities.
- Train staff on the secure implementation and utilization of the technologies.
- Ensure that technologies are securely configured.

Most important for the enterprise Internet security infrastructure are solutions that provide accurate threat detection that minimize false positives and provide comprehensive removal in real-time. Enterprises require seamless, scalable deployments that provide centralized, customizable user management, including coverage for laptops and remote employees. Most importantly, advances in technology need to provide proactive defenses.

One such proactive system is Phileas™, a ground-breaking online research system developed by Webroot Software that uses patent-pending technology to scour the entire Web discovering spyware on the Internet faster and more efficiently than any other research method. Developed to automate the search and discovery of new threats, Phileas consists of servers that control "bots" to detect web pages with characteristics of exploits, suspicious application code or suspected new spyware threats. One Phileas bot is able to scan 10 URLs per second, completing in one hour the equivalent of 80 hours of manual research. The bot architecture used by Phileas is also highly scalable to keep pace with the growing volume of Internet threats.



Phileas scours the entire Web discovering malware faster and more efficiently than any other research method.

Its innovative, pattern-matching technology allows Phileas to identify known and unknown exploits, plus any changes to existing spyware variants. New URL targets identified by Phileas are sent to Webroot's threat research team, who use proprietary algorithms to evaluate the URLs and create definitions for each new signature or variant. Since its inception in October 2004, Phileas has found over 8 billion URLs, scanned 250 million URLs, and identified 4.2 million malicious URLs.

This proactive approach to seeking, finding and disabling malicious malware is a revolutionary advancement that takes the burden off the user or IT director and places it confidently on the shoulders of the technology itself. Webroot was the first security company to develop and use this proactive technology in the fight against spyware.

C O N C L U S I O N

What the Future Holds

If there is a silver lining in the dark cloud that looms over Internet security, it is that awareness about the problem has greatly increased over the past couple of years. Spyware, system monitors and Trojans have become a part of the lexicon within enterprise IT departments. One of the biggest risks going forward is that this increased familiarity with the problem could breed complacency. We cannot mistake attentiveness for vigilance.

The assault on the enterprise will continue. According to eWEEK magazine, hackers are now being paid up to $50,000 to find vulnerabilities in Microsoft's new Vista operating system. IDC's "Key Forecast Assumptions for the Worldwide Software Market, 2006-2010" found that:

> *Software is becoming much more dangerous… The ability to bury malware within other software will become a dangerous trend that will lead to improved spyware software, and increase the need for software and application security tools…*

66 percent of enterprises will increase spending on security equipment and services this year.

As would be expected, companies will continue to make Internet security one of their highest priorities. In her December 2006 paper "State of Security in SMBs and Enterprises," Forrester analyst Natalie Lambert found that "66 percent of enterprises will increase spending on security equipment and services this year."

Certainly it bodes well that enterprise IT departments will continue to invest in procuring security tools to protect valuable company and customer data. At the same time, growing network security budgets will also attract newcomers into the security market that lack the experience and expertise held by the companies who have been on the front lines for years. Effectively protecting enterprise systems will require more than simply increasing spending.

Parsing the multitude of devices, software and service options will no doubt present challenges for enterprise IT managers. Most effective will be those companies that remain focused on their priorities, and select industry-leading solutions to address these needs:

- Prevent the installation of unauthorized software.
- Monitor network use and abuse.
- Block inappropriate content on the Web.
- Remove useless files to free up disk space (temp files, memory dumps).
- Set custom policies to manage employee Internet, network, and application use.

While the marauders will continue their attacks, the enterprise can be protected by continuing to widen the moat, raising the walls and placing the best trained sentries at the posts.

Additional Information

Webroot is one of the founding members of the Anti-Spyware Coalition (ASC) based in Washington, D.C., which is another source of educational resources, including:

ASC Definitions (June 2006)
http://www.antispywarecoalition.org/documents/DefinitionsJune292006.htm
ASC Glossary (June 2006)
http://www.antispywarecoalition.org/documents/GlossaryJune292006.htm
Protecting Your Network: Mitigating Spyware in Organizations (April 2006)
http://www.antispywarecoalition.org/documents/documents/ProtectingYourNetworkflyerA4.pdf

About Webroot Software

Webroot Software, Inc. provides industry leading security software for consumers, enterprises and small and medium-sized businesses worldwide. Globally recognized for its award-winning Spy Sweeper® line of anti-spyware products, Webroot recently incorporated anti-virus protection into two new products for consumers and SMBs, respectively: Spy Sweeper® with AntiVirus and Webroot® SME Security. The company also recently expanded into the parental controls software market with the introduction of Webroot® Child Safe®. The Boulder, Colorado based company is privately held and backed by some of the industry's leading venture capital firms, including Technology Crossover Ventures, Accel Partners and Mayfield.

Webroot's software consistently receives top review ratings by respected third-party media and has been adopted by millions globally. Available as either branded solutions or on an OEM basis, Webroot products can be found at www.webroot.com and on the shelves of leading retailers worldwide.

To find out more about Webroot, visit www.webroot.com or call 1-800-772-9383.

Certain data is available upon request.

Sources

Government-Issued Documents:

Directive 95/46/EC of the European Parliament and of the Council (The 'Data Protection Directive')
Official Journal of the European Communities
Brussels, Belgium – October 1995
http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

Decision and Order in the Matter of BJ's Wholesale Club, Inc.
File Number 042-3160
Federal Trade Commission
Washington, D.C. USA – September 2005
http://www.ftc.gov/os/caselist/0423160/092305do0423160.pdf

Decision and Order in the Matter of DSW, Inc.
File Number 052-3096
Federal Trade Commission
Washington, D.C. USA – March 2006
http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWDecisionandOrder.pdf

German Federal Data Protection Act (English translation)
The Federal Ministry of the Interior
Berlin, Germany – February 2002
http://www.iuscomp.org/gla/statutes/BDSG.htm

Gramm-Leach-Bliley Act of 1999
Public Law 106-102
U.S. Congress
Washington, D.C. USA – November 1999
http://banking.senate.gov/conf/confrpt.htm

Guide for Assessing the Security Controls in Federal Information Systems
Ron Ross, Arnold Johnson, Stu Katzke, Patricia Toth, George Rogers
National Institute of Standards and Technology
U.S. Department of Commerce
Washington, D.C. USA – April 2006
http://csrc.nist.gov/publications/drafts/SP800-53A-spd.pdf

Health Care Insurance Portability and Accountability Act of 1996 (HIPAA)
Public Law 104-191
U.S. Congress
Washington, D.C. USA – August 1996
http://aspe.hhs.gov/admnsimp/pl104191.htm

Information Security Breaches Survey 2006
Prepared by PriceWaterhouseCoopers LLP
UK Department of Trade and Industry (DTI)
London, United Kingdom – April 2006
http://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults06.pdf

Medical Privacy – National Standards to Protect the Privacy of Personal Health Information
Office for Civil Rights
U.S. Department of Health and Human Services
Washington, D.C. USA
http://www.hhs.gov/ocr/hipaa/

Press Release: Groundbreaking Settlements Hold Online Advertisers Responsible For Displaying Ads Through Deceptively Installed "Adware" Programs
Office of the New York State Attorney General
Albany, New York USA – January 2007
http://www.oag.state.ny.us/press/2007/jan/jan29b_07.html

Press Release: Massachusetts Attorney General Martha Coakley Leads Multi-State Investigation Into TJX Security Practices
Office of the Massachusetts State Attorney General
Boston, Massachusetts USA – February 2007
http://www.ago.state.ma.us/sp.cfm?pageid=986&id=1812

Personal Data Protection Code (English Translation)
Legislative Decree no. 196
Italian Parliament
Rome, Italy –June 2003
http://www.garanteprivacy.it/garante/doc.jsp?ID=311113

Recommended Security Controls for Federal Information Systems
Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, George Rogers, Annabelle Lee
National Institute of Standards and Technology
U.S. Department of Commerce
Washington, D.C. USA – February 2005
http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

Sarbanes-Oxley Act of 2002
Public Law 107-204
U.S. Congress
Washington, D.C. USA – July 2002
http://corporate.findlaw.com/industry/corporate/docs/publ107.204.pdf

Security Controls for Information Systems
Shirley Radack, Editor
NIST Information Technology Laboratory Bulletin
U.S. Department of Commerce
Washington, D.C. USA – January 2007
http://csrc.nist.gov/publications/nistbul/b-01-07.pdf

The 60 Minute Network Security Guide (First Steps Towards a Secure Network Environment)
Systems and Network Attack Center
U.S. National Security Agency
Fort Meade, Maryland USA –May 2006
http://www.nsa.gov/snac/support/I33-011R-2006.pdf

Industry Analyst White Papers:

2007 Enterprise IT Budget Outlook: North America
G. Oliver Young, Forrester Research, Inc.
Cambridge, Massachusetts USA – February, 2007
http://www.forrester.com/Research/Document/Excerpt/0,7211,41034,00.html

Corporate Anti-Spyware Market: 2006-2010
Matt Anderson and Sara Radicati
The Radicati Group, Inc.
Palo Alto, California USA –March 2006
http://www.radicati.com/reports/single.asp

Enterprise Security Survey 2006: The Rise of the Insider Threat
Brian Burke, Rose Ryan, Sally Hudson, Charles Kolodgy, Allan Carey
IDC
Framingham, Massachusetts USA – December 2006
http://www.idc.com/getdoc.jsp?containerId=204807

Worldwide Anti-Spyware 2006-2010 Forecast and Analysis: Boom or Bust?
Brian Burke
IDC
Framingham, Massachusetts USA – June 2006
http://www.idc.com/getdoc.jsp?containerId=202020

Industry Organization Studies:

Small Business Information Security Readiness
Andrea Peiro, Patrick Cook, Hassan Beydoun
Small Business Technology Institute
Santa Jose, California USA – July 2005
http://www.sbtechnologyinstitute.org/mi/research/readReport.php?codeId=1172605709&targetFile=security.pdf

Standards Related Documents:

BS 7799-3:2006 Information Security Management Systems
British Standards Institute
London, United Kingdom – March 2006
http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030125022&recid=2568

International Conversion of Capital Measurement and Capital Standards
Basel Committee on Banking Supervision
Basel, Switzerland –June 2004
(for implementation by 2007)
http://www.federalreserve.gov/BoardDocs/press/bcreg/2004/20040626/attachment.pdf

ISO/IEC 27001 Information Security Management Systems
International Standards Organization
Geneva, Switzerland –October 2005
http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103

Payment Card Industry (PCI) Data Security Standard
PCI Security Standards Council, LLC
Wakefield, Massachusetts USA – September 2006
https://www.pcisecuritystandards.org/tech/

News Articles:

"DOJ Prosecutor: Criminals Teaming Up With hackers"
By Jeremy Kirk
InfoWorld – September 14, 2006
http://www.infoworld.com/article/06/09/14/HNdojhackers_1.html?VIRUSES%20AND%20WORMS

"Q&A: Making a Federal Case – How the FBI Collars Cyber Criminals… and What Companies Can do to Avoid Being Victims"
By Robert Mitchell
ComputerWorld – July 28, 2006
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002069&intsrc=article_more_bot

"TJX Faces Class Action Lawsuit in Data Breach"
By Jenn Abelson
Boston Globe –January 30, 2007
http://www.boston.com/business/globe/articles/2007/01/30/tjx_faces_class_action_lawsuit_in_data_breach/

webroot

SOFTWARE, INC.

Webroot Software, Inc.
P.O. Box 19816
Boulder, CO 80308-2816
USA
www.webroot.com
Phone: 303.442.3813
Fax: 303.442.3846
Corporate Sales & Support: 800.870.8102
Consumer Sales & Support: www.webroot.com/support