



Computer Associates®

White Paper

Minimizing Liability and Productivity Risks: How to Control the Impacts of Spyware, Hacker Tools and Other Harmful Applications

An eTrust™ PestPatrol® Anti-Spyware Corporate Edition Business White Paper

Roger Thompson
Director, Malicious Content Research

October 2004

Table of Contents

Executive Summary	3
Corporate Liabilities From Spyware	4
Employee Productivity Issues	5
New Vulnerabilities and Entry Methods	7
Evaluating Organization-Wide Pest Prevention Programs	8
Company-Wide Benefits of eTrust™ PestPatrol® Anti-Spyware Corporate Edition	10
References	11

Executive Summary

Companies of all sizes face increasing threats from spyware, adware and other malicious programs commonly known as “pests” or “nonviral malware.” These unwanted applications, which are not detected by antivirus programs, pose an escalating danger to corporate data security and employee productivity. Businesses that wish to reduce potential liability and improve workforce efficiency will benefit from supplementing existing antivirus and other security strategies with comprehensive protection from these malicious programs.

eTrust™ PestPatrol® Anti-Spyware Corporate Edition (eTrust PestPatrol) from Computer Associates International, Inc. (CA) is a powerful, flexible solution for organization-wide protection against nonviral malware. This white paper explains how CA’s unique solution helps companies minimize risk and improve productivity without increasing administrative overhead.

Understanding Spyware, Adware and Other Pests

Today’s computer users are under attack from spyware, adware, hacker tools and other unsolicited applications that are often installed without the user’s permission or knowledge. Collectively known as “pests” or “nonviral malware,” these malicious applications can perform a host of activities ranging from nuisances, such as surreptitiously tracking web-surfing habits and displaying unsolicited advertisements, to potentially devastating actions, such as reconfiguring operating systems and web browsers, monitoring email, logging and transmitting keystrokes (including passwords), and compromising access to confidential data. These applications typically enter a PC through one of the following methods:

- **Automatic web-based downloads or scripts.** Depending on the security settings of an employee’s browser, visiting a spyware — or adware-infested web page can cause these items to be automatically installed on a computer without the employee’s knowledge.
- **Hidden installation alongside a desired application.** Pests can enter an organization when employees open solicited or unsolicited email attachments or intentionally download and install apparently legitimate applications from the Internet. Legitimate applications, including today’s peer-to-peer file sharing programs such as KaZaA and Grokster, often contain adware as part of the installation set. Other more insidious programs

illegally install undocumented malware applications whose presence is not disclosed in the licensing agreement. Additionally, they may compromise data security and integrity for the employee’s system or the company at large.

- **Intentional malicious installation.** Individuals who wish to damage a company or profit from illegally obtaining confidential information can exploit a variety of internal and external vulnerabilities to install malicious applications, such as hacker tools, keyloggers, password crackers and others.

In all of the above cases, spyware, adware and other unwanted applications would in most instances not be stopped by firewalls, intrusion detection systems or antivirus programs. These items appear to be legitimate applications, seemingly approved — expressly or tacitly — by the user.

Corporate Liabilities From Spyware, Adware and Other Non-Viral Malware

When pests enter a business, they have the potential to introduce significant legal liabilities (particularly in regulated industries). In addition, they can compromise trade secrets, damage corporate reputation and reduce employee productivity throughout the organization.

Legal Liabilities. Businesses that maintain any kind of confidential data, such as financial, customer or employee information, are governed by a wide range of regulations regarding data privacy and integrity. Existing legislation includes the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes–Oxley Act (SOX), the Gramm–Leach–Bliley Financial Modernization Act (GLBA), California Senate Bill 1386 and Senate Bill 1, the European Union Data Protection Directive 95/46/EC and others — all of which regulate the privacy, security and integrity of personal, health, financial and other data that a corporation may collect. Because spyware and other unwanted applications make it possible to compromise data security and confidentiality, their presence poses a serious threat to a company’s regulatory compliance.

A few notable cases of companies assuming financial liability for breaches in data confidentiality and security include the following:

- In April 2004, Barnesandnoble.com reached an agreement with the New York Attorney General to pay US\$60,000 in fines and penalties after an Internet security breach exposed customers’ personal information (ComputerWorld, 2004).

- International penalties to date include fines levied by the Spanish Data Protective Authority of 840,000 Euros (approximately US\$900,000) against an organization for inappropriately sharing customer data with a subsidiary, and 1.08 million Euros (approximately US\$1.17 million) for disclosing protected personal information to the public (Morrison and Foerster LLP, 2004).
- After hackers breached the security of Citibank's online credit card application mechanism in Taiwan in November 2003, the Ministry of Finance required that Citibank cease issuing new credit cards for one month, suspend online banking services for three months and allow the Ministry to inspect security before reinstating service (Taipei Times, 2004).

Businesses should be aware that, regardless of their primary location, they are subject to these regulations if they serve customers in the areas governed by these laws. In fact, data privacy and security regulation is so widespread that a single breach could place a company at risk for penalties under any number of state, national and international laws.

Compromised Trade Secrets. Malware, including hacker tools, keyloggers and other security-compromising programs, can provide unauthorized access to confidential data such as intellectual property and customer or price lists and other proprietary information. While no data protected by privacy legislation is affected, such breaches can cause businesses to lose competitive advantage.

Public Relations Issues. Companies that fail to protect data privacy face public relations challenges as well as financial penalties. For example, California Senate Bill 1386 requires businesses to inform customers of security issues in corporate networks, even if customer information has not been definitely compromised. Warning a potentially large group of customers that their data may no longer be private is likely to reduce customer and shareholder confidence and damage the company's image.

In March 2004, Softbank (Japan's largest broadband Internet service provider) disclosed to 4.51 million current and former subscribers that the security of their customer database had been compromised. To regain customer goodwill, Softbank provided \$37.8 million of free services and top executives gave up a portion of their annual salaries (Associated Press, 2004).

For publicly traded companies, the loss of customer goodwill and marketplace reputation may harm more than customer relationships — a general loss of confidence in the company may also be reflected in the company's stock price.

Employee Productivity Issues

Spyware and adware also present serious threats to internal productivity:

- **Reduced employee productivity across the board.** Employee efficiency can be drastically affected by the presence of spyware or adware on a user's computer.

Figure 1 illustrates the results of eTrust PestPatrol controlled comparison tests, indicating startup times for identically configured computers with no adware, one instance of adware and two instances of adware. A computer with two adware applications required 880 seconds, or more than 14 minutes, to boot. Assuming that employees reboot their computers daily and work five days weekly for 50 weeks (250 days), each employee with an affected machine could lose nearly 60 hours a year simply waiting for his or her computers to start. In addition, Microsoft estimates that as many as half of all PC crashes are caused by spyware (*InformationWeek, 2004*).

- **Reduced IT staff productivity.** The presence of spyware and adware in a company also reduces the productivity of IT staff responsible for maintaining employee systems. For example, Dell Inc. estimates that 20 percent of technical support calls from customers are spyware related (eCommerce Times, 2004). Companies that manage their own technical support likely experience similar or even greater numbers of spyware-related complaints. Manually identifying and removing unwanted applications can take up to an hour per computer, directly impacting the amount of time that IT staff can dedicate to strategic business-related projects.

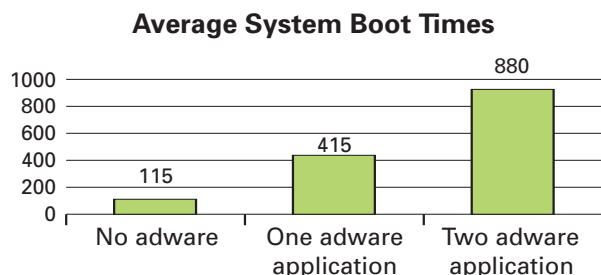


Figure 1. Average system boot times (in seconds) for identical computers with no adware, one adware application and two adware applications.

- **Increased spam.** Because some pests harvest email addresses, their presence most likely contributes to the ever-growing problem of unsolicited commercial email.
- **Wasted bandwidth.** Because spyware, adware and similar applications transmit and receive information across the network, bandwidth that should be available for customers, partners and employees may instead be occupied delivering tracking information to third-party servers and advertisements to desktops.

Proliferation of Spyware, Adware and Other Pests

While statistics vary, one trend is clear: spyware, adware and other pests are on the rise. One recent study conducted by Information Week magazine indicates that nearly one in three computers currently hosts a Trojan horse or an activity-monitoring application; industry experts estimate that the average PC has approximately 28 pieces of spyware installed. The situation is expected to worsen as the number and severity of malicious nonviral applications increase, and as new vulnerabilities and entry methods are identified and exploited.

Growth Trends for Nonviral Malware

Nearly every major category of non-viral malware — spyware, adware, hacker tools and more — has

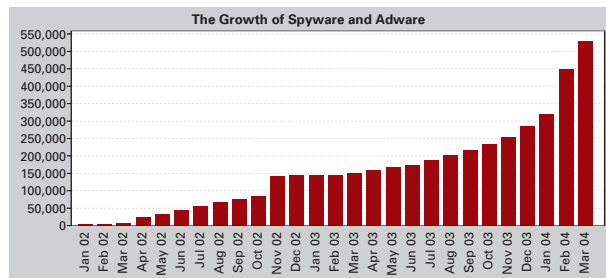


Figure 2. The number of spyware applications increased significantly between 2002 and 2004.

grown exponentially over the past few years. Figure 2 illustrates the growth in documented spyware and adware from January 2002 to March 2004. When reviewing these statistics, it is important to note that the number of spyware and adware applications in existence is not an indicator of the threat they pose; the potential damage that could be caused by a certain kind of spyware entering an organization is a more accurate indicator of risk than the mere number of spyware applications. However, as the number of these unwanted applications increases, the potential harm that they may inflict increases as well.

Hacker tools, password crackers and other applications designed specifically to compromise data privacy and

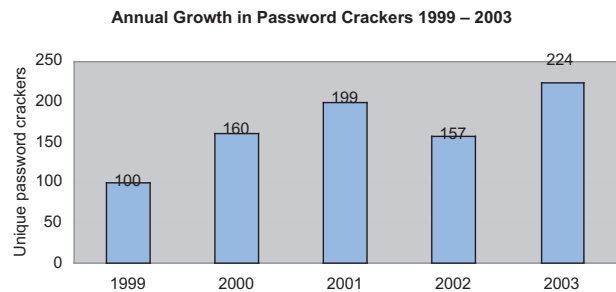


Figure 3: The number of known password-cracking applications has more than doubled since 1999.

integrity increased as well. Figure 3 illustrates the growth of password-cracking applications, one of many kinds of tools used to breach corporate security.

New Vulnerabilities and Entry Methods

New trends in technology and computer usage can also increase the vulnerability of employees' systems and confidential company data. These trends include:

- **Growing numbers of remote workers.** As more employees travel extensively or telecommute, the likelihood of their systems being compromised increases exponentially. The National Cyber Security Alliance estimates that 91 percent of computers used in households with broadband access are infected with spyware (Houston Chronicle, 2004). Home-based workers may use the computer for personal purposes or allow family members to do so, thus creating the opportunity for additional vulnerabilities.
- **Increasing complexity of web scripts.** Because web browsers now support complex scripting and delivery of dynamic applications, it is easy for a misguided or ill-intentioned developer to implement malicious applications that can compromise a system without the user's knowledge through simple web-browsing.
- **Complex desktop management issues.** As computer users demand greater flexibility to customize their working environment, it is increasingly difficult to enforce company-wide policies concerning unauthorized applications. However, the freeware and shareware screen savers, games, file-sharing programs and other applications that individuals may install for work-related and non-work-related purposes can pose a major threat.

Effective Techniques to Combat Spyware and Other Nonviral Malware

Companies that wish to guard against spyware, adware and other unwanted applications will benefit from supplementing traditional protection methods (including firewalls, vulnerability manager, intrusion detection systems and antivirus programs) with new strategies that address the unique characteristics of nonviral malware. A comprehensive, company-wide pest-prevention strategy should incorporate multiple elements:

- **Detailed acceptable use policies (AUPs) for company-owned computers.** An effective company-wide AUP should specifically address the ways in which malware may enter, including browsing to non-work-related sites, opening unsolicited email attachments, and installing unauthorized and/or non-work-related applications. If such activities are allowed, the AUP should establish configuration and usage procedures that would help to protect the company against inadvertent pest installation. While AUPs are an effective employee education method, however, they are not sufficient on their own to protect against intentional or accidental violations.
- **Firewall strategies.** Regularly reviewing and revising firewall policies to help ensure that only authorized outbound traffic is allowed can reduce the likelihood of confidential data being transmitted outside the organization.
- **Threat-specific protection.** No matter how effective the first two techniques are, unauthorized third parties will always find new ways to access forbidden data or resources. As noted previously, antivirus programs do not provide reliable protection against spyware; therefore, dedicated tools are required.

Evaluating Organization-Wide Pest-Prevention Programs

Businesses considering the deployment of organization-wide protection against spyware, adware and other malicious applications will benefit from solutions that:

- Address legal and regulatory issues. As a starting point, an effective strategy should address the local, national and international legislation regarding confidentiality and integrity of customer, financial and employee data.
- Minimize strain on computing resources. The software should provide comprehensive protection against a variety of threats without consuming significant bandwidth or operating resources on servers and client computers.

- Decrease employee interactions. Pest-prevention software should operate transparently so that employees cannot bypass or disable the protection.
- Reduce IT overhead. To free IT staff to focus on more strategic projects, the software should offer automatic deployment, trickle-down updates and centralized reporting and management.
- Enable flexible file handling. Because there may be legitimate business uses for potentially suspect applications such as file-sharing programs and network packet sniffers, administrators should be able to make case-by-case decisions about which kinds of tools may be allowed in specific circumstances.
- Support the improvement of company-wide protection. The protection software should offer comprehensive event logging capabilities so that administrators can spot trends and update AUPs and firewall configurations accordingly.

Introducing eTrust PestPatrol

eTrust PestPatrol offers a powerful, flexible method of protecting Windows-based systems throughout an organization from spyware, adware and other nonviral malware threats. The software complements existing antivirus and firewall installations to protect against the many kinds of nonviral malware that can evade existing security technologies, compromise corporate privacy and consume valuable computing resources



Figure 4. eTrust PestPatrol adds an extra layer of security initiatives.

How eTrust PestPatrol Works

eTrust PestPatrol detects and removes nonviral malicious code that can expose confidential information and diminish the performance of consumer and business PCs by:

- Scanning all or selected file types and directories
- Quarantining or deleting any or all pests detected
- Providing real-time protection by scanning system memory for active pests and terminating associated processes

- Cleaning pests from Windows Registry and startup areas, helping to ensure that “dormant” pests are not activated when the system is rebooted
- Automatically removing cookies before they can capture any sensitive information
- Reporting all activities to a central log
- Automatically downloading and distributing updates

The flexibility of eTrust PestPatrol enables:

- **Centralized management with transparent deployment and operation.** Installing eTrust PestPatrol in an any-size company is quick and easy. The application can be executed at startup or any other desired time.
- **Efficient resource usage.** Because eTrust PestPatrol can operate through a central server, little code is installed on individual computers.
- **Customized protection for different levels of vulnerability.** Administrators can set eTrust PestPatrol to detect or ignore certain applications that may be considered pests based on circumstance. For example, network sniffers are acceptable when installed on IT department systems, but unjustified on computers used by non-technical staff.

eTrust PestPatrol coexists with and complements perimeter security solutions, such as antivirus software, firewalls and virtual private networks (VPNs).

Company-Wide Benefits of eTrust PestPatrol

Protecting more than half a million systems in more than 100 countries, eTrust PestPatrol offers a proven solution for eliminating the threats associated with spyware, adware, hacker tools and other malware applications.

Companies that deploy eTrust PestPatrol realize benefits that reduce legal liability and help to maintain a positive public image:

- **Improved regulatory compliance.** By reducing the chance of malicious tampering and helping to ensure that customer, financial, IP and employee data remain confidential, eTrust PestPatrol helps businesses comply with regulations regarding data privacy and security. Additionally, it minimizes the risk of associated penalties and lawsuits.
- **Enhanced protection of trade secrets.** Because eTrust PestPatrol guards against malware-enabled data access and transmission, companies benefit from increased protection of proprietary and competitive information.

- **Increased customer, shareholder and marketplace confidence.** By helping to ensure data confidentiality and privacy, eTrust PestPatrol minimizes the likelihood of embarrassing public disclosures about security breaches.

To reduce the total cost of ownership (TCO) and improve return on investment (ROI) for information security, eTrust PestPatrol enables companies to:

- **Improve employee productivity.** By reducing the amount of time that employees lose waiting for infected systems to boot, launch applications or access information, eTrust PestPatrol enables employees to work more productively.
- **Reduce administrative burden.** Because eTrust PestPatrol automatically identifies and eliminates spyware and other threats, administrators don’t need to individually troubleshoot and fix infected computers. Deploying and maintaining eTrust PestPatrol is simple, with all key functions managed through a central console. As a result, IT staff can focus on strategic projects without negatively impacting information security.
- **Effectively use computing resources.** By keeping unauthorized, bandwidth-consuming, resource-appropriating applications off the network, eTrust PestPatrol helps ensure that the IT infrastructure operates at optimal efficiency.

Free Test-Drive

If you’re not sure that spyware, adware and other malicious applications are presenting a problem for your organization, we invite you to conduct a free, no-obligation scan of your computer at <http://www3.ca.com/securityadvisor/pest/pestscan.aspx>. What you find on your computer may surprise you.

For a more extensive trial, you can download a free 25-user, 30-day, full-function evaluation version of eTrust PestPatrol by visiting <http://www3.ca.com/Solutions/Collateral.asp?CID=63383&ID=5222>

For More Information

For more information about how eTrust PestPatrol can combat the threats to your business posed by spyware, adware and other unwanted applications call **1-877-246-3674** or visit www.ca.com

References

Associated Press, "Softbank: Data Leak May Be Insider Job," March 18, 2004
eweek.com/article2/0,4149,1551111,00.asp

Morrison & Foerster, "EU Data Protection Requirements: An Overview for Employers (3/04)"
mofo.com/news/print.cfm?MCatID=&concentrationID=&ID=1184

Ferrell, Keith. Spyware Attracts Increased Scrutiny. TechWeb News. April 29, 2004
nwc.securitypipeline.com/howto/19205440

Huang, Joyce, "Ministry punishes bank for online security leaks." Taipei Times, November 26, 2003, p.10
taipeitimes.com/News/front/archives/2003/11/26/2003077341

Hulme, George V. and Claburn, Thomas, "Tiny Evil Things." InformationWeek. April 26, 2004
informationweek.com/showArticle.jhtml?articleID=19200218

Rosencrance, Linda. "Barnesandnoble.com hit with fine for online security breach." April 30, 2004 (ComputerWorld)
computerworld.com/industrytopics/retail/story/0,10801,92804,00.html

Silverman, Dwight. "Spyware: They came from cyberspace." April 15, 2004
chron.com/cs/CDA/ssistory.mpl/tech/2496487

TechWeb News, "Average PC Plagued With 28 Pieces of Spyware." April 17, 2004
securitypipeline.com/news/showArticle.jhtml?articleId=18901641

**For more information, call 1-877-246-3674
or visit ca.com**



Computer Associates®