



WHITE PAPER

CISCO SECURITY AGENT—AN ENTERPRISE SOLUTION FOR PROTECTION AGAINST SPYWARE AND ADWARE

INTRODUCTION

Spyware—programs that install themselves on users’ computers without their knowledge—is a widespread and growing problem. According to a 2004 Harris Poll, 92 percent of IT managers report that spyware has infected their organizations, with an average of 29 percent of workstations affected; 40 percent indicated that such infections are on the increase.

Spyware can be used by hackers and identity thieves to record sensitive information, such as user names, passwords, and credit card numbers, or to steal sensitive company information. Information theft is one of the largest security challenges for businesses, and is the most financially damaging. However, most spyware is simply adware—programs typically bundled with freeware or shareware with the “spy” being a marketer collecting information, derived from cookies and URL history, about buying and surfing habits.

Spyware and adware share the ability to record keystrokes and possibly send data to Web servers, posing a serious security and privacy risk. Antispyware solutions on the market today are based on passive, reactive detection, and are not able to deal with this growing problem. Cisco® Security Agent offers a proactive approach to help protect against both spyware and adware infections, maintain system integrity, and provide defense-in-depth for endpoints. Cisco Security Agent combats infections in two ways: first, by preventing spyware programs from initially being installed; and if already installed, by preventing the spyware from executing and carrying out malicious behaviors, such as reading and relaying sensitive information.

SPYWARE OR ADWARE?

Understanding the differences between spyware and adware is important. The goal of spyware is to steal users’ information or money without their knowledge; adware intends to convince users to part with their money. Adware behaviors are generally much more noticeable—your computer suddenly starts sprouting pop-up ads or redirecting your search engine—while spyware is designed to go undetected, acting stealthily in the background. Both spyware and adware employ similar tactics to install and take control of your computer.

Spyware

Spyware originated in legitimate programs marketed to parents in the 1990s to monitor their children’s online activities and to employers wishing to monitor employee computer use. Many of these programs touted “remote installation” as a feature—the ability to install without having physical access to the monitored computer. Today, hackers and identity thieves are increasingly developing and exploiting spyware programs that enable them to record sensitive information, such as:

- User names
- Passwords
- Credit card numbers
- Social Security numbers
- Corporate secrets
- Home addresses
- Personal phone numbers
- Viewed URLs

- Screen shots
- Information relayed to “spy servers”

Spyware is designed to install remotely without a user’s knowledge. When true spyware is installed on a computer, the spy can see everything the user is doing—where the user surfs, what the user types, and the content of documents on the user’s screen. Some spyware includes a Trojan program that enables the spy to take complete control of the user’s computer.

Adware

Adware, more common than spyware, consists of marketing programs bundled with freeware that is designed to deliver pop-up ads to users’ computers, and that may redirect users to a search engine from which adware developers get a commission. Users may willingly and knowingly accept adware on to their computer, viewing it as a small price to pay in exchange for the benefits of using a certain program, such as receiving free stock quotes, weather updates, or traffic reports.

Some adware is designed to track surfing habits for market research purposes; however, most of today’s legitimate adware developers defend themselves by noting that they no longer monitor and record user activities, and therefore pose no security or privacy threat.

Certain adware has been labeled scumware because it incorporates disreputable practices, such as installation of dialer programs that make expensive international and toll calls via users’ computers, or it extorts users by charging them to remove the offending program.

While largely innocuous, the potential impact of adware on an organization should not be underrated. Dell recently reported that up to 12 percent of its technical support calls were related to spyware/adware issues. Repeated pop-up ads, hijacked browsers, and redirects to adware search engines frustrate business users. Poorly designed adware can tax CPU resources, introduce vulnerabilities, affect system performance, and cause error messages, system freezes, and crashes. Once installed, adware is difficult to remove. Sometimes removal is impossible, as the offending culprit often invites more adware to install itself.

The ideal solution allows administrators to prevent installation, or enables employees to continue safely using freeware and shareware while preventing the bundled adware to execute and wreak havoc on system stability and integrity.

Potential Spyware/Adware Behaviors

Other potential spyware/adware behaviors include:

- Monitoring keystrokes
- Scanning hard drive files
- Snooping on other applications, such as chat programs or word processors
- Installing other spyware programs
- Reading cookies
- Changing the default home page
- Launching upon startup and staying resident in memory
- Connecting to the Internet
- Dialing a phone number
- Transmitting URLs viewed
- Sniffing network traffic
- Installing remote administration tools
- Installing a Trojan to take over computer control
- Adding files, folders, cookies, dynamic link libraries (DLLs), and registry entries

HOW SPYWARE AND ADWARE ARE INSTALLED

Most adware is accidentally or deliberately downloaded along with freeware, such as screen savers, games, weather and stock tickers, or file-sharing software. Freeware is supported by revenue from the adware. While users can avoid adware by reading the fine print on any legal licensing agreement before consenting to download a program, many programs rely on “social engineering,” pestering users with repeated download screens until they finally click “yes” to accept the software.

Spyware is sometimes rigged to install even if the user clicks “no.” And adware vendors and hackers exploit “drive-by downloading” via active content code to secretly install intrusive programs when a Web page or e-mail message is viewed. Simply blocking suspect sites is ineffective—the freedom, anonymity, and growth of the Web lead to the proliferation of hundreds of new spyware sites.

In the Harris survey, only six percent of users reported surfing to sites suspected of containing spyware, and yet 92 percent of IT managers indicated their companies had been infected. Spyware is designed to be installed without the users’ knowledge or consent, and spyware programmers are becoming increasingly clever about their spyware delivery systems. Educating users on safe surfing practices and on carefully reading licensing agreements is critical, but these practices alone cannot solve the problem.

LIMITATIONS OF SPYWARE DETECTION AND REMOVAL TOOLS

Because most spyware is not delivered via e-mail, antivirus products are ineffective at detection. Spyware detection tools work essentially on the same principles as antivirus technology—they use signatures, pattern matching, and known file names to detect the presence of spyware on a computer. Spyware detection technologies share the same critical flaw as other traditional information security technologies—they are passive and reactive. Because these solutions are predicated on signature detection, even when they are efficiently installed and administered, new and mutating spyware attacks will still cause damage to network resources and files on individual machines.

No single detection tool seems to be able to detect all spyware. Product reviewers often advise that more than one detection tool be used, so that if one product misses a certain spyware program, the other might pick it up.

Just as in the antivirus world, antispymware developers find themselves with ongoing support issues:

- A constant signature update race to keep pace with spyware writers
- Keeping signatures current
- A high level of false positives
- Failure to catch new (day-zero) and evolving spyware programs

Spyware and adware eradication tools help determine what has infected the program, but cannot prevent infection in the first place. Prevention is vastly preferable—cleanup can be a long and involved process. Many spyware programs are persistent, designed to reinstall themselves once removed, to maintain multiple spyware programs simultaneously, and even to thwart detection by antispymware products. Spyware can be nearly impossible to remove. For example, some programs are designed to make thousands of entries to the Windows registry, requiring an almost never available amount of sophisticated IT support to check and repair registry information.

CISCO SECURITY AGENT—A DIFFERENT APPROACH

Cisco Security Agent takes a preventative approach, using behavior-based security to focus on preventing malicious activity on the host. Damaging activity is detected and blocked, independent of the type of spyware or adware. Cisco Security Agent is a crucial component of Cisco Theft of Information Prevention solutions.

Whereas other technologies provide single-point protection (and then only when a signature is known), Cisco Security Agent proactively defends against damage to a host throughout all stages of an intrusion, providing several layers of defense. And Cisco Security Agent is designed to protect against new attacks, where there is no known signature.

When an application attempts an operation, the agent checks the operation against the application's security policy, making a real-time "allow" or "deny" decision on the continuation of that operation, and determining whether logging of the operation request is appropriate. Security policies are collections of rules that IT or security administrators assign to protect servers and desktops, either individually or enterprisewide. These rules provide a safe environment for users to surf Websites. Cisco Security Agent provides defense-in-depth protection against spyware and adware by combining security policies that implement distributed firewall, operating system lockdown and integrity assurance, malicious mobile code protection, and audit event collection capabilities in default policies for servers and desktops.

Because protection is based on blocking malicious behavior, the default policies stop both known and unknown attacks without needing updates. Correlation is performed both on the agent and on the Management Center console. Agent-based correlation results in dramatically increased accuracy, identifying actual attacks or misuse without blocking legitimate activity.

Cisco Security Agent hardens the Windows operating system, preventing spyware from modifying critical operating system binary files or configuration settings. Because this capability does not require the use of cryptographic analysis of file system contents, it adds virtually no performance impact to the system.

Cisco Security Agent:

- Detects and prevents keyboard logging
- Prevents unauthorized writes to system executables, preserving the integrity of the operating system
- Prevents attacks from invoking arbitrary commands on a system via a shell
- Prevents possibly compromised applications from damaging existing applications or downloading new ones
- Monitors and enforces which applications can run on the desktop
- Detects and prevents Trojans
- Protects Web browsers from drive-by downloads using mobile code such as Java, JavaScript, and ActiveX
- Protects against "application hijacking" using a DLL control hook
- Prevents risky user behavior within applications, such as downloading files using an instant messaging application
- Protects against known and unknown buffer overflow attacks, which may be exploited to install spyware on a user's computer
- Allows central specification of which applications can run, allowing the administrator to prevent suspected spyware from executing
- Provides the ability to monitor or prevent which applications can read sensitive data files
- Monitors media devices, alerting the user when spyware turns on a Web phone or Webcam

What's Running on the Computer?

Cisco Security Agent can track which applications are installed on a single computer or workgroup, which are actually invoked, which use the network, whether the application is a network client or a network server, and the identity of all remote IP addresses with which it communicates. Cisco Security Agent also identifies the state of all applications on all remote systems, including user-specific installation information and whether undesired applications are attempting to run.

Cisco Security Agent allows the administrator to perform detailed forensics examination of any application on any computer. It observes the application's live behavior—all files accessed, whether for read or write; all network connections, whether inbound (server) or outbound (client), along with the address of the remote computer; all registry access, whether for read or for write; and all COM object loading. Cisco Security Agent collects information about the application's behavior, summarizes it in a report for the administrator, and generates a control policy based on the application's normal behavior.

Using the Cisco Security Agent framework, administrators can centrally:

- Identify unauthorized or unknown applications that are installed or run on remote computers
- Identify which behaviors unknown applications perform when they are run, separating unknown but malicious applications from unknown but benign ones
- Control which behaviors the applications are allowed to execute or which functions they can perform, based on behavior analysis

Cisco Security Agent enables administrators to build a list of suspected spyware applications running enterprisewide for analysis. From this analysis, administrators can develop policies regarding what the spyware is allowed to do. For example, the administrator may create a policy to automatically prohibit a program from installing on additional computers, strictly limit its behavior where it is already installed, or completely disable it from executing.

As a benefit, companies may allow users to have adware running safely. For example, a system administrator can set policy that states, “This application may serve ads to users, but cannot record users’ key strokes or open up a port to relay data back to the adware server.”

Figure 1. Cisco Security Agent Custom Report

Product	Number of hosts installed
Fun Web Products Easy Installer	1
Kazaa Media Desktop 2.5	1
My Web Search (Outlook, Outlook Express, and IncrediMail)	1
My Web Search (Smiley Central)	1
Search Assistant - My Web Search	1
Spin4Dough	1

Cisco Security Agent offers the capability to generate custom reports, such as this report showing all applications attempting to connect to outside IP addresses that are not on the approved corporate list.

To build a suspected spyware class, Cisco Security Agent enables administrators to generate reports to show, for example, all applications attempting to connect to outside IP addresses that are not on the approved corporate list (Figure 1). Depending on the environment and security policy, the administrator may exclude or include browsers, e-mail clients, or IM clients.

CISCO SECURITY AGENT IN ACTION

Cisco Security Agent effectively protects against spyware in two ways: by preventing installation, and by providing defense at every step of intrusion.

Preventing Installation

Adware, once installed, can be difficult to remove from a computer. Cisco Security Agent aids in preventing installation, even if the program uses drive-by downloading methods (Figures 2 and 3).

Figure 2. Some Adware Will Ignore a ‘Cancel’ Request and Download

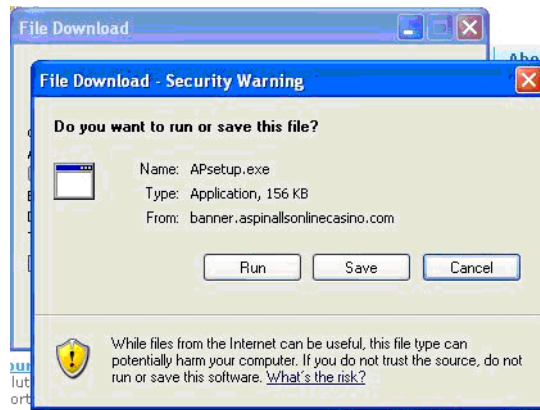


Figure 3. Cisco Security Agent Detects Adware and Offers Several Courses of Action

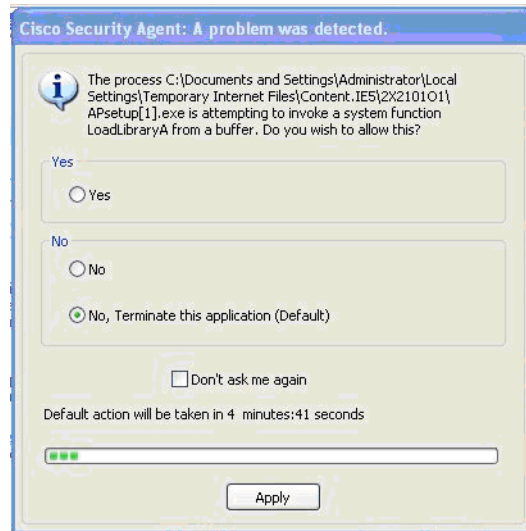


In response to stealthily downloaded adware trying to execute, Cisco Security Agent defaults to terminating the application unless the user clicks “Yes” (Figure 3). Administrators can configure the product to automatically stop the application from executing without user intervention. Note the “Don’t ask me again” option. If the spyware attempts to swamp the user with repeated requests to download—a form of social engineering intended to trick or frustrate the user into clicking “Yes”—the user need only click “Don’t ask me again” to stop the requests.

Preventing Malicious Behavior If Already Installed

Cisco Security Agent provides defense-in-depth at every stage of intrusion. Even if a user accepts download and installation despite repeated security warnings, Cisco Security Agent continues to protect against the spyware performing dangerous or disruptive actions (Figures 4–7).

Figure 4. Cisco Security Agent Continues to Track Suspicious Activity



If the user clicks “Yes” when Cisco Security Agent detects a problem and the program installs, Cisco Security Agent continues to monitor for suspicious activity and alerts the user (Figure 4). In this case, Cisco Security Agent prevents the spyware from an action that is typically seen when a program uses self-modifying code or has been subverted by a buffer overflow attack.

Figure 5. Querying the User About Keyboard Sniffing



In Figure 5, Cisco Security Agent detects a program called Silentlog, a “keystroke logger” program that silently captures all keyboard input and logs it to a file. Spyware often installs such keystroke loggers to capture passwords entered by users.

Figure 6.



Figure 6 shows Cisco Security Agent blocking key logging action from a popular commercial spyware program, WinSpy, that sells itself as being “immune to antispy software.” Note that Cisco Security Agent does not detect such key loggers by their file names, but by monitoring action that the application takes.

Figure 7. Cisco Security Agent Log Showing Blocked Spyware Activity

```
12/16/2004 2:53:02 PM: The process 'C:\WINNT\rvsvc32.exe' (as user W2KSP0-DESKTOP\win2k) attempted to call the function OpenProcess("<pid:66130>") from a buffer (the return address was 0x40f3cd). The code at this address is '008b5508 52536800 060000e8 c3a5ffff 8bf0fd7 3bf3740c 8b451050 56e89da6' This either happens when a process uses self-modifying code or when a process has been subverted by a buffer overflow attack. The user was queried and a 'Terminate' response was received. The response was the default taken after a timeout.

12/16/2004 2:53:14 PM: The process 'C:\WINNT\rvsvc32.exe' (as user W2KSP0-DESKTOP\win2k) attempted to call the function CreateProcessA("ipconfig") from a buffer (the return address was 0x404bcf). The code at this address is
```

Figure 7 shows the administrator log for a computer infected with WinSpy. The user was not given a security message because the actions occurred during boot-up. Cisco Security Agent automatically terminated the malicious activity without user intervention.

Responding to Specific Behavior Patterns

Table 1 lists various categories of potential spyware behavior and Cisco Security Agent rules that act to protect the endpoint.

Table 1. Cisco Security Agent Rules

Category	Behavior	Cisco Security Agent Rule
Cookie	Stores Website information, such as registration details, on the users' computer between visits.	Cisco Security Agent can protect access to cookie information from non-browser programs.
Adware	Delivers pop-up ads.	Cisco Security Agent does not provide browser-specific controls against pop-ups (JavaScript new window, for example). Adware programs running outside of the browser will trigger Cisco Security Agent installation policies (no silent installs).
Browser Helper Object	Hijacks browser upon launch, typically to redirect the user to an unknown search engine. May track, collect, and relay URLs.	Writing to Browser Help Objects is restricted to system processes only.
Browser Plug-in	Creates a new toolbar in the browser. May track, collect, and relay URLs.	Installation of a browser plug-in will trigger Cisco Security Agent installation policies (no silent installs). If allowed to install, these will be listed in deployment analysis reports.
Keylogger	"Sniffs" keyboard—records keystrokes and relays passwords, credit card numbers, and other sensitive information to a third party.	The System API rule detects and blocks keystroke loggers.
Network Management Tool	Remotely monitors network activity; can be exploited by attackers.	Installation of a network management tool will trigger Cisco Security Agent installation policies.
Remote Administration Tool	Gives user privilege on a remote computer, enabling the attacker to modify, forward, and delete files and to control the keyboard.	Installation of a remote administration tool will trigger Cisco Security Agent installation policies. Network-based applications cannot modify system files without specific permission.
Trojan	Malicious code embedded in a benign application; may damage operating systems, delete files, and destroy the hard drive.	Cisco Security Agent provides powerful protection against Trojans, worms, and viruses. For full details, please visit: www.cisco.com/go/csa
Worm	Self-replicating and self-propagating program that can crash the network; spyware may employ a worm to distribute itself.	
Virus	Self-replicating program delivered and replicated via e-mail; spyware may employ a virus to distribute itself.	

CONCLUSION

Cisco Security Agent provides robust and effective protection against both spyware and adware. Basing detection on behavior, Cisco Security Agent will block new and unknown spyware without needing signature updates. This “zero update” prevention reduces security management costs associated with deploying updates.

Robust enterprise management features enable administrators to efficiently deploy and manage hundreds of thousands of agents. Policy creation and alert reporting are centralized. Rules and policies can be applied based on the user, group, location, or Network Admission Control (NAC) status. The application inventory feature enables administrators to track unknown applications running in the organization, analyze their behavior, group them into suspected spyware or adware categories, and create rules to limit or prohibit their behavior.

Lastly, spyware protection is not an add-on; it is included at no additional cost. Cisco Security Agent also provides proactive protection against entire classes of attacks, including port scans, buffer overflows, Trojan horses, malformed packets, malicious HTML requests, and e-mail worms. By aggregating multiple security functions, Cisco Security Agent provides host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, application deployment investigation, and audit log consolidation—all within a single agent package.

For more information on Cisco Security Agent, visit: www.cisco.com/go/csa

For more information on Cisco integrated solutions for theft prevention, visit: www.cisco.com/go/theft



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International
BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratum, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)
204177_a_ETMG_MH_1.05