BlueCoat™

Spyware Prevention for the Enterprise

Whitepaper

EXECUTIVE SUMMARY

Spyware is a hot topic. Legislators, security professionals, business people, IT staff, executives, and consumers all know about spyware – and its negative impact on privacy, security, and productivity. The rampant growth of spyware is driven by strong spyware developer skills, and more importantly, investment from advertisers and organized crime. Unfortunately, few organizations can effectively and efficiently halt the influx of spyware into their networks. Existing enterprise defenses are not capable of defending organizations against the spyware threat. Unfortunately, many of the proposed new defenses against spyware are reactive (only effective against installed spyware), incomplete, and/or difficult to manage. An ideal enterprise solution will not only stop spyware before it installs, but it will be capable of detecting and removing spyware already in place at the desktop. Furthermore, this ideal solution needs to be deployed without introducing significant management challenges, nor can it impede the business process. Spyware, like other information security threats, will continue to evolve, and incorporate new and different installation and information gathering techniques. As such, any enterprise solution must embrace an in-depth spyware defense that is powerful and flexible enough to cope with the unpredictable evolution of spyware and other hybrid threats.

Blue Coat's new anti-spyware solution is preventative – and thus will stop spyware from entering the enterprise. Blue Coat's solution also copes with existing installations of spyware. This comprehensive approach to controlling spyware functions as a high-performance, flexible, gateway-installed solution to defend against current and future spyware, without impeding business processes.

Control.

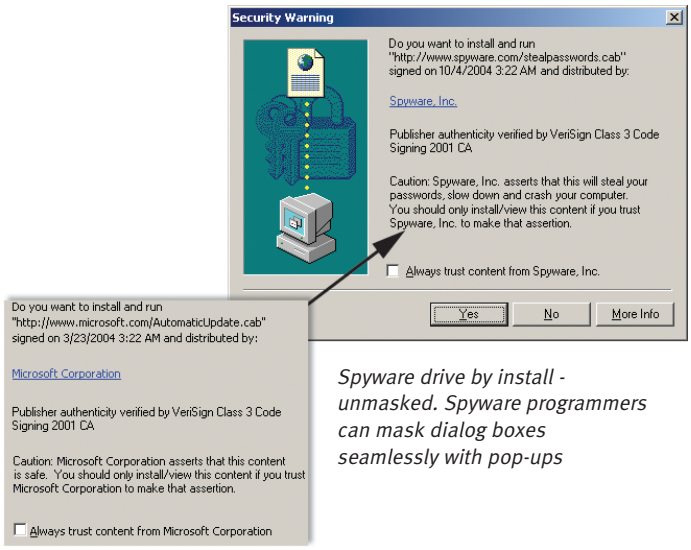
THE PROBLEM AND GROWTH OF SPYWARE

The IT, business, and consumer communities have seen a multitude of concerns, complaints, and legislation on "the spyware problem." Nearly all (92%) enterprises acknowledge a serious spyware problem (Web@Work, 2004). Estimated infection rates range from 30% of enterprise desktops (at any given time, despite cleansing efforts – Web@Work, 2004) to 90% of broadband connected desktops (US National Cyber Security Alliance). Further evidence of pain is obvious by looking at Mozilla, whose Firefox browser has enjoyed significantly increased adoption as a result of spyware (most spyware targets Microsoft's Internet Explorer browser). Most enterprises, however, won't switch browsers, and must deal with this rapidly evolving threat.

There has been some debate about what constitutes "spyware." Commercial advertising companies that develop "adware," state that they are not malicious, and as such, should not be categorized with viruses and worms. The enterprise view of "spyware," however, can include any software that collects information on user behavior (surfing patterns, keystrokes, preferences, etc.) from desktops and ships it offsite to an unknown third-party server. There are distinctions between commercial spyware (adware) and malicious spyware, but in the end, it's all spyware. Another defining characteristic of spyware is its installation methods – typically spyware installs in one of three ways:

- **Drive-by installs** – this is the most common – a drive-by install typically begins downloading software through the browser upon a visit to a Web page. Depending on the browser, its patch level, and the user's security settings, the user may be prompted with a "yes/no" dialogue box, or not. Sometimes, these boxes are masked using pop-ups. Please see Figure 1. In some cases, even if the user clicks "no," the installation may continue.
- **Browser exploit** – some spyware installs via a downloader Trojan, which takes advantage of vulnerabilities in Internet Explorer and acts as a sort of beachhead agent for spyware. This agent, once installed, can download multiple flavors of spyware.
- **Embedded install** – often spyware will be packaged with "free" programs (e.g., KaZaA) and the user agrees to accept the spyware in payment for using the program for free.

Spyware drive by install - what the user sees.



Spyware drive by install - unmasked. Spyware programmers can mask dialog boxes seamlessly with pop-ups

Figure 1

The risk and costs of spyware to enterprises are substantial. There are many risks associated with spyware including credential theft, intellectual property theft, liability (privacy lawsuits, regulatory censure), fraud, and corporate espionage. Often, managers and executives within the organization who are focused on risk management find these concerns to be of utmost importance. Many IT managers, however, note that the productivity impact – crashing browsers, sluggish desktops, slow networks, help desk calls, and idled users – is of far greater concern, and often more quantifiable. Regardless of perspective, spyware is having a significant negative impact on the enterprise.

WHY HASN'T SPYWARE BEEN STOPPED?

Legislation is only part of the answer

U.S. legislative efforts are attempting to tackle the problem of spyware, and the prosecution of authors and distributors of spyware has begun. While the effort may have some impact, the Internet is borderless and difficult to control through legislation. The common reaction for spyware purveyors will be to simply move their operations offshore. Commercial spyware vendors will most likely seek to comply with regulations by making license agreements more clear when asking end-users for permission to install spyware. Unfortunately, spyware licensing agreements never go beyond the end user, and the enterprise – who owns the infrastructure – is left out of the decision.

Spyware creates large financial incentives

There are large financial incentives to distribute spyware. Spyware producers make money on the information they collect, such as market research and personal information, as well as advertisements distributed. Web property owners are paid by spyware distributors to distribute spyware. Both producers and distributors change dissemination and installation methods frequently to avoid detection and to ensure high distribution success.

Spyware is technically challenging

Spyware is difficult to stop technically for a variety of reasons. First, spyware is a new and evolving technology that quickly adopts all of the latest techniques from viruses, worms, and Trojans. Perhaps more importantly, spyware attracts the best and brightest hackers – who are finally being compensated for their efforts by either commercial spyware companies or organized crime.

Second, spyware is an application-level threat, and most existing enterprise defenses focus on the infrastructure layer – i.e., they defend file systems, general network traffic (at the port and protocol level), and known threats on application services (e.g, email servers, database servers, and web servers). Unfortunately, many of the existing defenses, such as firewalls and intrusion detection/prevention systems, lack the application-level visibility and granularity necessary to block spyware without shutting down Web traffic associated with legitimate business functions.

Several vendors have introduced solutions for enterprise anti-spyware, including spyware specific desktop agents, desktop anti-virus, and URL filtering. Unfortunately, most of these solutions are reactive – they only address installed spyware, i.e., they enable organizations to do something about spyware only AFTER it is a problem.

Control.

HOW IS SPYWARE CONTROLLED NOW?

Spyware-specific Desktop Agents

Spyware-specific desktop agents have been introduced by a variety of start-up companies, and have, until recently, been targeted at consumers or individual users. While they detect and clean up spyware at the desktop, most lack centralized management capabilities and represent significant deployment challenges for the enterprise. Many organizations will resist deploying yet another desktop agent and the associated operational expense. Ultimately, the limiting factor beyond deployment and management is the reactive nature of these tools – many only detect spyware after it has been successfully deployed to the desktop.

Desktop Anti-virus

Desktop anti-virus (AV) tools already have desktop footprint, and are typically deployed with robust centralized management frameworks. To date, however, most AV vendors have been slow to focus on spyware. On average, most AV tools today detect a small subset of known spyware – hundreds of potentially tens of thousands and in general, deliver reactive solutions – they detect after installation. While AV vendors will most likely adopt spyware as their next challenge by aggressively developing signatures, they have traditionally focused on high-frequency threats – leaving enterprises vulnerable to more rare exploits.

URL Filtering

URL filtering has some advantages in addressing spyware. URL filtering is typically a gateway solution, so it doesn't have desktop deployment and management issues. URL filtering can stop spyware before installation by blocking spyware sources, but is also reactive in a sense, because it only blocks known spyware sources, which change frequently. URL filtering also blocks spyware destinations (i.e., outbound spyware communication), which is useful for detecting installed spyware.

URL filtering alone is an inadequate technique for two reasons. First, commercial spyware is distributed by a variety of websites (whose owners are compensated by spyware vendors) that have nothing to do with spyware. This renders categorical blocking of the sites themselves difficult. Second, malicious spyware is often distributed by unregistered (and therefore, uncategorized) websites, which can be categorically blocked. Blocking all uncategorized websites, however, may cause problems with legitimate business traffic on an enterprise network.

WHAT DOES THE COMPLETE ENTERPRISE SPYWARE PREVENTION SOLUTION LOOK LIKE?

The best defense for enterprises is to stop spyware before it is installed on the desktop. As such, organizations need a preventative solution that avoids an additional desktop agent and reduces management headaches. An ideal enterprise solution to control spyware must operate at the network gateway.

Naturally, enterprises have concerns around gateway solutions that may impede business processes through slower Web traffic or widespread blocking of Web content. A gateway solution must not introduce latency into business-critical Web communications. The solution must also determine, in a fine-grained fashion, what Web content will be allowed into the enterprise. The ability to determine what is and isn't acceptable content, beyond source and basic content type, and make network policy decisions about it, is a high-priority for the enterprise.

Keeping pace with spyware's rapid evolution requires an effective solution with multiple blocking and control methods at its disposal. Web threats of any nature (spyware, worms, viruses, trojans) evolve in unpredictable ways.

Regardless of how effective an anti-spyware gateway may be, some users will take their laptops home, where, due to unprotected connections, spyware infestation is virtually guaranteed. Therefore, an enterprise solution must be able to address these "out-of-band" infections once they return to the corporate network.

BLUE COAT GATEWAY ANTI-SPYWARE

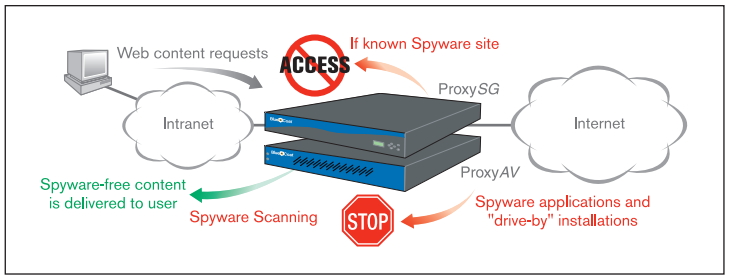


Figure 2: Spyware Prevention

Blue Coat Systems has introduced an anti-spyware solution that represents a new approach to this growing problem. The Blue Coat solution:

- Prevents spyware from reaching the desktop
- Detects spyware infections (out-of-band or existing)
- Doesn't impede the business process.

The Blue Coat anti-spyware solution is deployed at the enterprise gateway, eliminating the typical management and deployment issues. The Blue Coat Proxy*SG* is the preferred high-performance platform for customers who need secure content management (e.g., URL filtering, IM control, streaming control). The Proxy*SG*, coupled with its companion virus scanning appliance, the Proxy*AV*, has demonstrated one of the few enterprise-viable solutions for controlling and scanning Web traffic for viruses.

Blue Coat Prevents Spyware from Reaching the Desktop

The Blue Coat anti-spyware solution prevents spyware in three ways (see Figure 2):

1. Stop spyware installations
2. Block spyware sources
3. Scan Web traffic for spyware signatures.

Stop Spyware Installations

The Blue Coat gateway position as a Web proxy, coupled with rich content controls, enables customers to develop comprehensive policies that identify protocols, methods, and types of Web content that are permitted to enter the enterprise environment via the Web. These policy controls include permit/deny decisions on "drive-by installs," which are the prevailing method of spyware dissemination. Blue Coat also controls Web content access through deep content inspection. Coarsely blocking all drive-by installs will have undesirable effects (e.g., Windows Update will no longer function). Administrators have the option of implementing white list policies (only accept drive-by installations from specified sources) or black list policies (specifically deny drive-by installs from a list of sites/categories) for this control. Additionally, the Proxy*SG* policy can identify combinations of phishing and spyware threats that employ legitimate Web sites or pop-ups in their scams.

Block Spyware Sources

The Blue Coat anti-spyware solution includes high-performance, best-of-breed On-Proxy URL filtering, which enables organizations to block both spyware sources and the sites spyware report to. Blue Coat supports On-Proxy filtering from five vendors (Websense, Cerberian, SmartFilter, SurfControl, and ISS), and while URL filtering does not address all aspects of spyware control as outlined above, it is a critical component of an effective spyware solution.

Scan Web Traffic for Spyware Signatures

AV scanning is the third preventative element of Blue Coat's anti-spyware solution. Using best-of-breed AV scanning engines, Proxy*AV* scans HTTP traffic for spyware. If spyware is found in the HTTP stream, the connected Proxy*SG* can halt the threat at the gateway. With this proxy-based solution, Blue Coat has proven that Web AV can be performed on large enterprise networks without introducing significant latency. With new browser vulnerabilities and exploits being discovered regularly, many organizations are recognizing the need to scan HTTP traffic for threats – which increasingly include spyware. AV vendors have begun putting spyware signatures into their scan engines, recognizing that anti-spyware capabilities are crucial for the continued success of any AV engine.

Control.

Blue Coat Detects Spyware Infections

While Blue Coat's anti-spyware solution has comprehensive preventative coverage at the gateway, spyware is probably already installed on many user's desktops and laptops. Furthermore, users often use laptops outside the organization's controls and become infected via an insecure connection. Accordingly, Blue Coat has several techniques, based on the Proxy*SG*'s network position as the Web proxy, that address the detection aspect of spyware defense.

Because the Proxy*SG* sees all Web traffic, and can apply a variety of policies, customers can analyze and report on all spyware-suspected desktops based on surfing patterns and sites visited see Figure 3. Furthermore, when known spyware programs attempt to "phone home," On-Proxy URL filtering can block the communication. Simultaneously, the Proxy*SG* can inform IT management and send the user an internal message within a Webpage, informing them that they are infected with spyware, and provide them guidance on cleaning their desktop. To aid users in removing installed spyware, Blue Coat has partnered with a best-of-breed spyware cleansing vendor – InterMute See Figure 4.

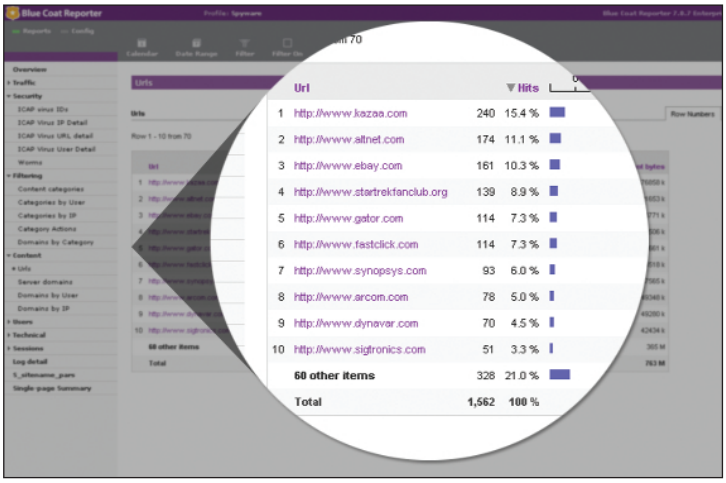


Figure 3: Reporting

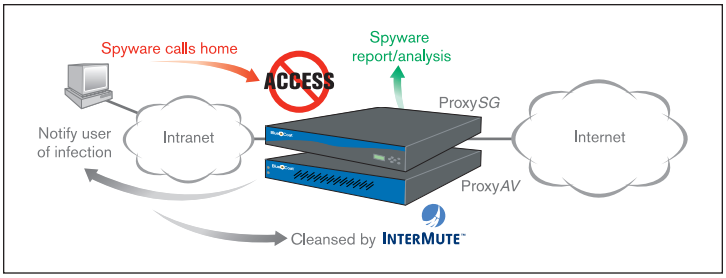


Figure 4: Spyware Detection

Blue Coat Doesn't Impede Business Process

The Blue Coat anti-spyware solution is deployed at the enterprise gateway – a position familiar to Blue Coat's proxy appliances. Blue Coat appliances have repeatedly shown that they can apply security policy and content controls without introducing noticeable latency. In fact, they accelerate Web performance – speeding and improving the business process. Moreover, the comprehensive, fine-grained policy controls found in the Proxy*SG* enable an enterprise to block inappropriate content (e.g., spyware drive-by installs, phishing pop-ups), while ensuring that legitimate Web requests for business needs (e.g., Windows Update drive-by installs, Outlook Web Access pop-ups) are met.

CONCLUSION

Spyware will continue to evolve – fueled by advertising revenues and hacker inventiveness. Effective spyware solutions must provide multiple techniques to address each new flavor of spyware and each ingenious method of penetrating the enterprise. Organizations should expect the worlds of spyware and viruses, worms, and trojans to merge in the near future – both from those who develop threats, and those who create technology to defend against these threats. AV vendors will incorporate spyware scanning and removal into their desktop scanners, but the reactive nature of these solutions will require organizations to continue a "defense-in-depth" strategy, involving preventative gateway solutions.

Finally, if nothing else, the development of viruses, worms, trojans, and spyware indicates that new and different threats will take advantage of business-critical Web communications. Organizations will need to have an infrastructure in place that is flexible, granular, high-performance, and powerful enough to stop current and future Web-borne threats, yet won't impede the business process. Only Blue Coat provides that integrated, high-performance infrastructure – delivering comprehensive Web content controls, URL filtering, and Web AV – enabling enterprises to prevent spyware and other Web-borne threats from impacting privacy, security, and productivity.

650 Almanor Ave.
Sunnyvale, CA 94085
www.bluecoat.com

1.866.30.BCOAT
408.220.2200 Direct
408.220.2250 Fax

Blue Coat Systems provides secure proxy appliances that control user communications over the Web. Blue Coat Proxy*SG* appliances integrate advanced proxy functionality with security services such as content filtering, instant messaging control and Web virus scanning – without impacting network performance. With more than 3,000 customers and over 14,000 appliances shipped worldwide, Blue Coat is trusted by many of the world's most influential organizations to ensure a safe and productive Web environment. Blue Coat is headquartered in Sunnyvale, California, and can be reached at 408.220.2200 or www.bluecoat.com.