



## ***Spyware Overview***

Spyware is a class of computer programs that surreptitiously monitors user actions. While they may, or may not be sinister, like a remote control program used by a hacker, software companies use Spyware to gather data about customers. Often, these burdensome programs do more than monitor users' Web-surfing activities or inject unwanted advertisements. They also try to steal passwords, intercept information during Internet connectivity, and make changes to Internet browsers and network settings, to the point that they cause degraded performance, application inaccessibility, or potential system failure.

Spyware can share some qualities with Trojan horse programs, and that is where the traditional anti-virus vendors claim to provide protection. For the most part, however, these intruders are able to sneak their traffic through, bypassing firewalls and anti-virus programs, rendering traditional security practices useless against them. An added security concern is the countless number of ports and services these spyware instances open and initiate. Unnecessary open ports are open windows to systems. Ironically, there are also documented examples of poorly written spyware having been used as attack surfaces themselves.

### **Spyware – Key Concepts**

Spyware is...

- Software that sends information about a user or user's activity to its own or an external web or collection site.
- Software installed on a computer in combination with a download selected from a website.
- Software that is capable of transmitting information in the background as a user navigates the Internet.
- Software that states that the program performs anonymous profiling which means that the user's habits are being recorded.
- Software that is used to create marketing profiles; for example, people who go to Web site "A" often go to Web site "B" and so on.
- Software that can deliver competing products or information in real time, inclusive of third-party software definition.
- Some Spyware is categorized as a backdoor Trojan capable of providing illegal or unintentional data access.

Common Spyware Examples Include:

*Adware: ADvertisementWARE:* Software that automatically and periodically provides pop-up ads on a computer. It typically displays targeted ads based on words searched for on the Web or



derived from the user's surfing habits that have been periodically sent in the background to a Spyware web server.

*Key Logger:* A program or hardware device that captures every key depression on the computer. Also referred to as a keystroke logger.

*Browser/Session Hijacking:* Covert redirection to a different Web site, usually the default or selected "homepage" is changed to another website, or redirected through an intermediate server, without users' acceptance. Browser hijacking also refers to changing the home page as well as adding shortcuts to the Favorites menu or lowering security settings. Common changes are made through the use of JavaScript or ActiveX modules. The most common spyware installation is through Browser Helper Objects (BHO).

*Dialers:* A dialer is a very small program, often installed using the ActiveX technology. Once installed, a dialer offers to use your modem to call in to a service or 900 numbers, and can change system settings to use the unauthorized number by default.

### **Blink's Spyware Protection Strategy**

As mentioned above, Spyware is only effective when it is able to deliver its surreptitiously obtained information to a third party, be it for the purpose of serving up targeted advertisements, redirecting your web viewing sessions to a particular website or most importantly, security-wise, the offloading of customer, financial, personal data or intellectual property. Since its original release in 2004, Blink has always been able to defeat spyware attempts to open up unapproved ports to connect out to the Internet to deliver its payload of information. Additionally, via Blink's file integrity checking capabilities, browser helper objects or other similar spyware attempts to inject application changes in a browser would be detected and not allow to initiate.

To combat the growing performance concern surrounding spyware's impact on business continuity and system availability, Blink was enhanced to combat these malicious programs and address them *proactively*, before they can impact system resources and security. These enhancements come in two forms;

- **Real Time Malicious Code Protection** – Blink will actively block malware instances from being loaded into memory and give the option to quarantine or remove the suspected code. This is done by checking processes against a CRC (cyclical redundant check) database of spyware methods.
- **Disk Scanning and Removal** – As a 'last line of defense', Blink will also offer the capability to perform intelligent disk scanning and remove malware from disk, similar to traditional tools available today.

By adding this protection, Blink continues to innovate beyond single-agent technology vendors, combining host firewalls, local vulnerability assessment, intrusion prevention, policy management and now anti-spyware technology. By combining these critical security functions in a manner which they can be centrally deployed, administered and managed – the single agent – Blink delivers the most-value add for the enterprise.