Add Value by Protecting Your Customers Against Spyware

Spyware is the single largest threat facing individual and corporate computer users today and is growing at twice the rate of viruses. This growing hazard also presents a unique opportunity for ISVs and appliance vendors seeking to protect their customers' computers and confidential data. Would you like to:

- Add world-class spyware blocking functionality to your products or services?
- Cultivate new business opportunities by incorporating powerful anti-spyware technology into your application(s)?
- Attain a significant competitive edge by integrating best-of-breed anti-spyware technology?
- Tailor and market your solution to your unique customer base of individuals and/or corporations with flexible private-labeling and co-branding options?
- Reduce your time to market by rapidly developing and deploying this value-added solution?
- Complement your existing security solutions and services?
- Capitalize on the lucrative anti-spyware opportunity while simultaneously limiting your risk, investment, and research?
- Improve your customer satisfaction and loyalty by proving your commitment to protect them from dangerous and destructive spyware?
- Help your customers boost their security and eliminate theft of confidential data?
- Reduce your customer service and technical support costs?
- Ensure customer bandwidth and memory consumption will not be drained due to spyware-related issues?
- Develop both consumer and corporate anti-spyware solutions from a single SDK?

If you answered "yes" to one or more of the above questions, then we invite you to keep reading to learn more about the spyware threat and how you can play an active role in eradicating this scourge.

Spyware: The #1 Internet Security Threat

Spyware is a multibillion-dollar industry that has replaced viruses as the greatest Internet security threat affecting corporations, IT professionals, and end-users worldwide. The National Cyber Security Alliance estimates that over 90% of Internet users unknowingly have spyware installed on their computers. While most viruses are created by individuals, most spyware originates in large corporations because of its massive

profitability. Teams of developers are aggressively creating ever-stealthier and more resilient spyware that sneaks onto computers to steal confidential information for advertising and, in some cases, criminal activity.

The term “spyware” refers to various types of undesirable software such as adware, malware, key loggers, Trojans, dialers, ActiveX applications, etc. Infected machines have an average of 25 spyware applications running at all times. Spyware impedes computer performance and compromises the privacy of the infected individual/corporation. Its effects range from benign (profiling user activity for targeting advertisements) to malicious (logging keystrokes to gather passwords, credit card information, and/or corporate espionage). Benign spyware is often used as a carrier for other, more malicious programs.

Trojan horse or system monitoring programs, two of the most malevolent and invasive types of spyware, were found on more than 30 percent of all systems scanned during a recent study. A recent EarthLink survey of three million computers found that 83 million instances of spyware had been installed over a nine-month period.

All of this means that your customers have a huge and costly problem on their hands.

Spyware Threatens Corporate Security and Productivity

Spyware attacks on corporate networks have numerous consequences, including:

- Compromised security of confidential data: Some forms of spyware allow unauthorized parties to monitor virtually every move made on corporate networks, which may allow attackers to gain access to your customers’ sensitive information. This threat is of particular concern for organizations that must comply with government information security regulations. For example, Barnes & Noble agreed to pay $60,000 in fines in April, 2004, after an Internet security breach exposed their customers’ personal information.

- Data loss due to malicious attacks: A spyware infection increases your customers’ vulnerability to data loss by giving attackers the ability to steal or destroy valuable files at will. In 2004, network security tool vendor PivX Solutions LLC reported that a hacker planted Trojans on corporate desktops using an adware program and collected confidential trade information for two months before the leak was detected.

- Increased technical support burden: Michael George, Vice President of Dell Computer’s United States consumer business, stated that more customers are calling Dell Technical Support seeking relief from spyware than for any other technical support issue. Corporations, including your customers, are expending valuable and costly IT resources in time-consuming efforts to identify and eradicate spyware and to repair the damage caused to individual computers.

- Reduced employee and workstation productivity: Sluggish system performance, downtime due to data loss, and distraction caused by increased pop-up advertisements are all byproducts of spyware infections. Corporations that manage their own technical support are dedicating increasing resources to

AUTHORED BY ANTHONY HERNANDEZ - (415)786-2081 - anthony94122@outlook.com

investigating, removing, and preventing spyware from infecting network computers. These activities reduce the amount of time employees can spend on strategic business-related projects.

- Bandwidth and memory consumption: The constant transmission of stolen information from corporate networks to unauthorized sources consumes bandwidth and diminishes network performance. Many spyware programs also store materials such as unwanted advertisements on the user's hard drive. Bandwidth intended for use by either individual subscribers (including dial-up accounts) or corporate customers, employees, and affiliates to grow their businesses is being hijacked to deliver potentially sensitive information to third parties vendors who, at minimum bombard desktop computers with spyware.

Spyware Threatens Individual Security and Productivity

Does your customer base include individual end users? The spyware threat is not limited to corporate computers and networks. Personal computers are also at risk from spyware. In fact, the threat to individuals can be even more severe than the threat to corporations because most people do not have access to dedicated IT resources and personnel. Self-employed individuals are at even greater risk because their computers store business-related information in addition to any personal data they may have. Spyware installed on a personal computer can perform any or all of the following:

- Harvest personal and private information including passwords, social security numbers, and other confidential data used to access bank, credit card, and other accounts.
- Track visited Web sites for use by marketers who bombard computers with irritating adware and relentless pop-ups.
- Record keystrokes for use by thieves to steal personal identities.
- Corrupt critical system files and trigger repeated crashes.
- Slow Internet browsing by draining bandwidth.
- Cause sluggish system performance because of bloated memory and system resources, which can even prevent uses from accessing programs, email, or the Internet.

How Spyware Infects Computers

Many seemingly innocuous activities can lead to spyware infections. The most common method of transmission involves bundling spyware with otherwise legitimate or desirable applications. This type of piggybacking most often occurs with freeware, whose developers allow the product to be installed free of charge in exchange for the right to harvest and sell user information. In most cases, the user is unaware that s/he has agreed to this arrangement because the request for such authorization is buried deep within the application's End User License Agreement (EULA) using confusing technical and legal language that few users read, let alone comprehend.

Software installation is only one vector of entry for spyware. Other methods of spyware delivery include “drive-by downloads”, where an HTML link serves as a gateway for the surreptitious installation of spyware applications. This type of clandestine download typically occurs when a user clicks a link in a spam message or other unsolicited advertisement. Spyware can also be attached to or embedded in email or instant messenger communications, included as part of an ActiveX installation, or may even be deliberately installed by someone with administrative access.

An Evolving Threat

Spyware is designed to be difficult to avoid and even more difficult to detect and remove. This threat is growing at twice the rate of viruses, with new threats emerging daily. Spyware authors frequently update their programs and configure them to distribute themselves across multiple operating system locations to foil detection and removal efforts. Some spyware programs even include self-repair features to correct any damage caused by removal attempts.

Polymorphic files are an emerging trend where spyware files mutate themselves (and therefore their MD5 signature) to avoid detection. An MD5 signature is a “fingerprint” used to verify data integrity. Each unique file has a unique MD5 signature. A polymorphic file mutates itself to remain functionally equivalent, but will have a new signature.

Anti-virus Protection Is Not Enough

Both spyware and viruses are dangerous and destructive; however, there are major differences between the two threats. Viruses are designed to wreak havoc on computers and networks and stealth is therefore not an issue. By contrast, spyware depends on stealth for its existence and is therefore designed not to interfere with the computer’s functioning.

Anti-virus vendors are arriving late to the spyware market and are struggling to adapt their technology to protect against spyware. Developers seeking to add anti-spyware functionality to their products or services should weigh the pros and cons of partnering with an anti-virus vendor who may be new to the anti-spyware field versus selecting a company whose focus is on developing time-tested and proven anti-spyware technology.

Reactive vs. Proactive Spyware Protection

Most anti-spyware solutions are designed to scan systems for existing spyware installations. This reactive approach means that spyware must already be present on the computer before protective measures can be taken. By then it may be too late, the damage already done. Traditional anti-spyware measures therefore offer too little protection too late.

For corporations, a proactive anti-spyware solution scans network traffic in real-time searching for suspect programs, files, and data transmissions. An immediate notification occurs when a problem is detected, meaning that spyware can be stopped in its tracks. In many cases, this proactive monitoring can prevent spyware from being installed in the first place- the best possible scenario. In cases where spyware enters a corporate

network behind its protective layer (such as employee connecting an infected laptop to the corporate network), the real-time scanning can intercept and neutralize malicious activity before it can complete its task. The anti-spyware program can then repair the infected computer.

Individuals also benefit from a proactive approach to spyware protection since most spyware can be stopped before ever infecting the user's computer. Reactive scanning can then take care of any spyware that may already be present on the computer. Combining both the proactive and reactive anti-spyware protection uses far less system resources than the actual spyware and prevents all of the problems associated with spyware infections.

What if you could leverage the benefits of a best-of-breed anti-spyware SDK to rapidly create robust applications that protect your customers' corporate networks and/or individual computers? Even better, what if the applications you create were backed up by dedicated anti-spyware resources that constantly scour the Internet to find and defeat emerging threats before they have a chance to infect your customers' systems? The Aluria Gateway and Client & Server Anti-Spyware SDKs let you do just that.

Enter the Aluria Anti-Spyware Solution

The fight against spyware has been an uphill battle, primarily because of the reactive nature of most anti-spyware solutions. Aluria Software provides best-of-breed proactive anti-spyware solutions that Fortune 500 companies, major ISPs, and millions of users around the world trust and rely on to protect against the worst spyware threats. We were among the first companies to define and categorize spyware and the criteria used to identify software as spyware. We then produced two software development kits (SDK) that enable you to create and deploy easy spyware detection and removal functionality across multiple platforms. Our multi-tiered, hierarchical approaches create a fully integrated anti-spyware solution that protects your customers' computers and networks against the hostile Internet environment:

- Real-Time Gateway Protection: Most corporate networks connect to the Internet using gateways. Providing protection at the gateway level is therefore of paramount importance. Aluria Software offers the Gateway Anti-Spyware SDK that allows developers to create a custom gateway-based security solution to prevent spyware from entering the network in real-time. Please refer to the Aluria Gateway Anti-Spyware SDK white paper for more information about this SDK version

- Host-Level Protection: Aluria Software's host-based Client & Server Anti-Spyware SDK offers a two-pronged approach for keeping spyware off individual computers and is suitable for creating both corporate and individual applications.

Introducing the Aluria Client & Server Anti-Spyware SDK

The Aluria Client & Server Anti-Spyware SDK enables easy spyware detection and removal on multiple platforms. This SDK targets all system functions to effectively scan for, detect, and remove spyware agents from a system and ensure its safe operation. It offers superior and proven scanning and blocking technology and a strategic range of features to software vendors looking to quickly integrate world-class anti-spyware

AUTHORED BY ANTHONY HERNANDEZ - (415)786-2081 - anthony94122@outlook.com

desktop, workstation, and server solutions into their existing security solution offerings. Developers can tailor the SDK engine to their specific needs. Our development team can work with you to customize the setup or develop an interface that provides the closest fit to your implementation requirements.

SDK adopters benefit from Aluria's widely trusted scan engine and kernel-level Active Defense Shield (ADS) technology, a robust and strategic feature set, flexible options, reduced development cycle, diverse OS compatibility, and the partnership and support that only an established industry leader can provide. We back all of our anti-spyware technology with an in-house team of spyware experts and engineers, automated spyware research technologies, and our massive database of verified spyware signatures and definitions. This reduces both your time to market and overall cost while enhancing the quality of your finished product.

The Client & Server SDK complements the Aluria Gateway SDK. It is designed for use against spyware that is trying to infect an individual Windows PC/host. The SDK includes two core strategies: a real-time Active Defense Shield and an On-Demand Scan & Removal Engine.

Aluria's exclusive Active Defense Shield (ADS) technology offers truly proactive real-time event-based protection that goes far beyond traditional reactive periodic/frequency-based monitoring. It guards PCs against all attempted spyware installations including but not limited to installers launched from the Web, an intranet, mapped network drive, CD-ROM, floppy drive, and USB drives. Configure the ADS once and forget about spyware forever. It's that simple. ADS catches spyware as soon as it writes, moves, or renames files and automatically performs a pre-configured Auto-Delete, Auto-Quarantine, or Ignore. It is compatible with popular antivirus products.

While most anti-spyware monitoring solutions require constant CPU cycles, ADS functions unobtrusively in the background to either automatically delete or quarantine any spyware attempting to write to the file-system. Even attempts by so-called "benign" files to generate a spyware executable are detected and blocked. ADS consists of a file-system driver that resides in Ring-0 or the kernel, which enables it to hook into the file system and listen for particular events such Open, Close, or Rename. When such an event occurs, ADS blocks the file from gaining any access for analysis and takes appropriate action if spyware is found. Safe files may then proceed with their normal actions.

The On-Demand Scan & Removal Engine is a backup scanning utility that is useful under certain circumstances, such as when ADS is turned off (which is never recommended). This engine can scan the entire file system including removable storage media, services, running processes/modules, cookies, and the system registry. Spyware can be tricky to remove; The SDK utilizes cutting-edge technology developed in our Spyware Research Center to remove every spyware component.

Key Features of the Aluria Client & Server Anti-Spyware SDK

The Aluria Client & Server Anti-Spyware SDK is a robust anti-spyware Application Programming Interface (API) that provides innovative and exceptional spyware scanning and removal services. It includes the following key features:

- Seamless integration: Seamlessly integrate this SDK to provide anti-spyware solutions for various platforms and multi-faceted services such as applications, gateways, firewalls, and corporate solutions.

- Comprehensive functionality: The SDK toolkit provides a strategic range of tools that target all system functions to effectively scan for, detect, and remove spyware agents infecting a system.

- Optimized: The SDK is optimized for fast performing scans and detection.

- Modular Architecture: The SDK is a modular solution, which gives developers the flexibility of incorporating anything from basic minimal scanning functions to real-time spyware protection.

- Multiple scan modes: Implement the SDK with any combination of the following modes:
    - Scan memory
    - Scan registry
    - Scan specific directories
    - Scan specific files
    - Scan current or logged-in user's cookie directory
    - Scan Alternate Data Streams (coming Q1, 2006)

- Multiple Removal Options: Available spyware removal options include:
    - Quarantining
    - Removing
    - Restoring (if the file has been quarantined)

- Customizable definitions: The SDK allows customizable definition files to best suit your company's objectives and your customers' needs.

- Versatility: The SDK is written in C++, allowing integration into popular languages such as VB, C++ (Console, MFC and Win32 applications) and C#, using various integrated development environments like VS 6.0, VS.NET, and Eclipse Framework.

- Unicode compliant: The SDK is Unicode compliant (coming soon).

- Various query methods: Various query methods allow the developer to retrieve basic information such as the number of spyware items found, names, and locations.

- Detailed reports: The SDK supports additional reporting details relating to spyware descriptions, threat levels, spyware variants and categories

- Windows DLL packaging: The SDK engine is packaged as a Windows DLL and is small enough for easy deployment using Web-based installers.

Key Developer Benefits

AUTHORED BY ANTHONY HERNANDEZ - (415)786-2081 - anthony94122@outlook.com

The features contained within the Aluria Client & Server Anti-Spyware SDK provide numerous benefits to you and your customers, including:

- Robust API for exceptional spyware scanning and removal.
- Comprehensive feature set
- Detection facilities locate surreptitious spyware hidden in Alternate Data Streams (coming 1Q 2006)
- Optimized scan & detection engine speeds performance.

These key benefits are built into an extremely flexible architecture that allows rapid development and deployment:

- Modular solution allows developers to incorporate basic to advanced real-time scanning functionality quickly and easily.
- Customizable definition files accommodate company preferences to help support security policies and eliminate false positives.
- C++ architecture offers flexibility for integration into VB, C++, C#, MFC, and Win32.
- SDK is highly configurable to allow finer, granular control of scans, detections, and trust.

The Aluria Client & Server Anti-Spyware SDK combines reliability and flexibility in an extremely powerful package:

- Powerful Smart Scan technology is fast, accurate, and provides detailed results.
- Kernel-level Active Defense Shield prevention technology proactively stops spyware before installation.
- Advanced trust mechanism automates removal or ignoring of detected spyware.
- Massive, verified spyware database prevents costly false positives.

Client & Server Anti-Spyware SDK Components

The Aluria Client & Server Anti-Spyware SDK includes the following components:

- Win 32 API DLL
- COM API DLL
- Active Defense Shield API DLL
- Active Defense Shield file system driver

- Active Defense Shield service
- Definition files
- Detailed technical manual
- Sample C++ and COM-VB applications
- Sample spyware for controlled testing. WARNING: Real spyware. May infect your PC.

How It Works

The Aluria Client & Server SDK contains all of the functionality required in a robust, flexible spyware detection and removal solution. The SDK is built around a central processing object referred to as the “ScanEngine” that requires up-to-date spyware definition (.dat) files to properly identify and remove spyware. Developers may locate .dat files wherever they with. Detection can begin once the ScanEngine initializes and loads the .dat files.

Developers can select various types of scans such as memory, registry, specific directories, specific files, and a user’s cookie directory. The SDK includes query methods that allow the developer to retrieve basic information such as the number of spyware items found, their names, and locations. It can also return spyware descriptions, threat levels, variants, and categories for even greater detail. Detected spyware can be processed by quarantining, restoring, or removal. The SDK includes methods for unloading the ScanEngine object and releasing used memory once scanning and removal are complete.

Programming Notes

The spyware detection and removal process begins with the creation of a “ScanEngine” object using the CreateScanEngine method. CreateScanEngine contains two parameters:

- Path to the directory containing the spyware definition (.dat) files
- Encryption key being used for .dat file decryption (typically left empty)

The “ScanEngine” session allocates memory and detects spyware. For efficiency, it can be set to perform partial scans at any one time. All created sessions must be disposed of before continuing using the DisposeScanEngine method.

The .dat files contain current spyware definitions and can be loaded and unloaded as desired. Each session can acquire .dat files from the server and can use the LoadDat and UnloadDat methods to control scanning options. Both LoadDat input parameters allow the developer to load selective definitions based on the type of scanning being performed. Each session can load and unload an unlimited number of .dat files.

AUTHORED BY ANTHONY HERNANDEZ - (415)786-2081 - anthony94122@outlook.com

Scanning can begin once a session is established and the .dat files are loaded. Scans can target different system areas such as memory, the registry, directories, files, and the user's cookie directory. Methods such as ScanMemory, ScanRegistry, ScanDirectory, ScanCookies, FileCheck, and FileCheckMem allow the developer to scan individual sections of the user's system. The ScanMemory method uses a single parameter to specify the level of scanning of the active processes. The ClearSpywareList method clears scan results at will.

Items detected during scanning are placed in a spyware list, and the GetSpywareDetected method can return the number of items contained therein. These items can be traversed using the GetSpywareFirst, and GetSpywareNext methods. The GetSpywareByID method can point to specific spyware items within the spyware list as referenced by the SpywareID parameter. The GetSpywareObject method returns detailed information regarding the spyware "object" that, based on the positioning within the spyware list, can return information such as SpywareID, DiscoveryType, spyware name, spyware path, and variant names of the specific spyware item. Passing a variant name to the GetSpywareData method can retrieve categories, threat levels, and descriptions for the specific spyware variant.

Detected spyware items can be either quarantined or removed through methods specific to the type of scan performed. Quarantined items can be restored or "rolled back" at a later time. Each quarantine method provides a parameter that specifies the location for quarantined items. Each restore method provides parameters for both the location of the quarantined item and the original location to restore the item to.

Scanning, quarantining/restoring, and removal are do not inhibit the system and do not degrade the user's experience.

About the Active Defense Shield (ADS)

The single most important thing to remember about the ADS is that it is not a scanning-based system; it reacts in real-time as spyware attempts to write to the hard drive. ADS protects any fixed drive in the computer. It consists of the following four components:

- Aluria Filter: Adsfilter.sys is an IFS driver service that runs early in the system boot stack. This is the backbone of ADS and runs at ring zero. The filter driver handles all file system interaction to the higher-level ring 3 components, including buffering data and file system event notifications. It also maintains a cache file so as not to impede the end user experience.

- ADS DLL: This file interacts with both the ring 3 Client/Server and the Aluria Filter. It communicates between the client and server through memory mapped files and talks to the Aluria filter through Device IOCTL statements. Ads.dll maintains the ADS state and processes all request.

- ADS Service: ADSService.exe is a tiny service that runs at system boot. This service runs at ring 3 and is responsible for instantiating ads.dll as a server.

- End-user application: The end-user application uses ads.dll as a client and can control and manipulate the ADS by passing commands to the ADS server.

ADS runs in automatic mode because the computer can be logged off or rebooted without signing on. ADS creates a default auto-action file the first time it starts, which effectively makes ADS run without external application control. An application sets an automatic action such as Quarantine, Delete, or Allow. The AutoStart option must be set to actually get ADS to start acting upon spyware. ADS performs this automatic action without intervention from a high-level application whenever it detects spyware. All actions are remembered and can be passed to a high-level application along with the results whenever requested.

The ADS system differs from current SDK behavior once the application sets up the auto-action because an application does not call the CreateScanEngine, LoadDats, UnloadDats, or DisposeScanEngine methods. ADS automatically performs these functions when the service either starts and stops or its auto-action AutoStart parameter is changed.

ADS is always active in the background and will delete, quarantine, or ignore intercepted spyware based on the chosen auto-action. If ADS detects spyware and the user shuts down the system before the application takes action on the spyware when the AutoSaveSpyware option is on, ADS will save the spyware list to the hard drive to ensure applications can access it the next time the computer is rebooted.

ADS is fully Unicode compliant, meaning that it will find spyware that attempts to hide in an existing or custom a Unicode name or path. All functions that deal with spyware file objects use Unicode paths; however, the ADS also provides ANSI routines for non-Unicode applications.

Higher-level application access ADS through a C++ DLL. The application must start ads.dll as a client. ADS uses functions similar to the SDK to allow higher-level applications to iterate through the list of spyware that ADS has taken auto-actions on. The Application decides when to clear the spyware list. Once cleared, all spyware history is removed from ADS.

The Aluria Spyware Research Center

Aluria’s Spyware Research Center is staffed with a team of spyware experts and engineers dedicated to researching, analyzing, and responding to spyware-related computer security threats. Our research analysts perform forensic analyses on spyware infestations and are experts in both hacker exploit tactics and malicious code defenses. The Spyware Research Center constantly scours the Internet for new threat specimens for analysis and examination in our state-of-the-art Spyware Research Lab.

The Spware Research Center includes an arsenal of proprietary tools and utilities such as bots, spyders, and honeypots that help automate research and analysis tasks in order to gather new specimens and collect data and intelligence. These tools greatly increase the speed and efficiency of our efforts and ensure that critical spyware updates become available in a timely manner.

Spyware Collection Network

Our mature spyware collection network consists of numerous spyware channels designed to find and report emerging suspect items in the wild. Suspect items receive careful scrutiny and analysis on a file-by-file basis against Aluria's exacting criteria to determine behavior, taxonomy, and threat level. Confirmed spyware threats are added to Aluria's massive database of proven threats. This attention to detail increases the reliability of spyware scans and prevents costly false positives.

Spyware Definitions, Updates, and Hot Fixes

Spyware changes by the day as developers release new variants to avoid detection. Aluria's dedicated Spyware Research Lab proactively monitors the Web and known/suspected spyware portals to detect and collect new spyware signatures, which are released in weekly updates. You can choose to completely replace your existing spyware definition file (full update) or add the latest definitions to your current definition file (incremental update). Incremental updates provide full protection while reducing download and installation times.

Spyware makers are constantly creating new methods and techniques to circumvent detection and removal by anti-spyware applications. New spyware variants appear daily utilizing new exploits and vulnerabilities in order to remain resident on infected PC's. While we normally provide updates on a weekly basis, we do have the ability to provide updated definitions within 4 hours under exigent circumstances. Should an emerging spyware variant require an immediate solution, Aluria's Spyware Research Center will publish a hot fix to eradicate the new threat while the SDK is updated. You can rest assured that you always have the absolute latest spyware protection.

Spyware Research Lab

Aluria's Spyware Research Lab is our online source for spyware-related information. It is dedicated to providing Internet users worldwide with the latest spyware information and research. Our searchable spyware database is an indispensable tool for educating users and corporations about the many specific forms and categories of spyware. The Spyware Research Lab includes the Spyware Forum, an online environment where industry experts, novice, and advanced users can exchange spyware-related information with our spyware detection experts.

Why Choose Aluria Anti-Spyware Technology

- Aluria is recognized leader in anti-spyware research, response, and solution development. We offer proven and superior anti-spyware detection, prevention, and removal technology.

- Fortune 500 companies, major ISPs, software developers and vendors, and over 35 million end-users worldwide rely and trust Aluria's anti-spyware solutions.

- Aluria has built an expansive and sophisticated spyware collection network with automated research technology, the largest user base in the industry, and a dedicated in-house Spyware Research, Analysis, and Response Team to collaboratively identify and eliminate spyware threats.

- Aluria's massive database of verified spyware contains a robust definition set with fewer false positives to prevent adverse end-user effects, accidental removal of legitimate software, and potential legal complications.

- Unlike our competitors, Aluria detects spyware at the kernel level, stopping it as it is written to the file system and before it has a chance to run, cause damage, morph, or self-replicate.

- Aluria provides comprehensive detection of various threat categories including spyware, adware, cookies, homepage hijackers, search page hijackers, rogue ActiveX, drive-by downloads, browser helper objects, emailers, key loggers, dialers, remote administration tools, retrospies, Trojans, malware, thiefware, dataminers, and/or surveillance software.

- Heuristics-based technologies are prone to false positives and unpredictable results. Aluria's results are more accurate and reliable because each and every file added to our spyware database is verified by a qualified team of spyware analysts and engineers.

- Aluria's SDK is a turnkey package that offers complete flexibility to allow incorporation into both, software applications, and hardware appliances.

- Aluria's SDK offers multithreading architecture for faster scanning and detection.

- Combining the Aluria Gateway Anti-Spyware SDK with the Aluria Client & Server Anti-Spyware SDK gives developers and their customers the benefit of a multi-tiered block-and-clean strategy that ensures total anti-spyware protection. Aluria's Gateway Anti-Spyware SDK leverages our renowned and proven spyware scanning/blocking engine to monitor file traffic, Web sites, and IP addresses for spyware signatures at the gateway level.

Minimum Technical Requirements for Evaluation or Integration

The following system requirements must be met in order to evaluate or integrate the Aluria Client & Server Anti-Spyware SDK:

- Windows® 95, 98, 2000, ME, and XP (ADS functions on Windows 2000 and XP only)

- Hardware actively supported for all Intel x86 architectures

- 15 MB free RAM.

- 7 MB hard disk space for evaluation, 2.5 MB for integration

- 400 MHz CPU

- Must have pre-installed Visual Studio for evaluating sample applications

- Uses Windows system files and Visual Studios libraries

AUTHORED BY ANTHONY HERNANDEZ - (415)786-2081 - anthony94122@outlook.com

About Aluria Software

Aluria Software is a respected leader in spyware research, response, and solution development for Fortune 500 companies, major ISPs, software developers and vendors, and millions of users worldwide. Please visit our Web site at www.aluriasoftware.com or contact us via either phone at 1.888.627.4650 x 112 or email at oemsales@aluriasoftware.com for more information on Aluria's SDKs and/or to discuss partnership opportunities. Aluria Software is an EarthLink® company.

Aluria Software
725 Primera Blvd Ste 220
Lake Mary, FL 32746