



XOFTspy Portable Anti-Spyware

Security on the Go –
Facing the Threat of Spyware

Product White Paper
November, 2006

ParetoLogic – The Company

ParetoLogic is an international software development company headquartered in Victoria, British Columbia, Canada. We are a member of SIIA (Software Information Industry Association) and we specialize in providing advanced security applications and performance tools for business and personal computer users.

ParetoLogic creates solutions that combine sophisticated technology with a truly user-friendly interface. Our products empower people to secure and optimize their computers and are available in eight languages in 70 countries around the world. ParetoLogic has established partnerships on a global scale to make our products available to all computer users regardless of location, language, or computing experience.

We provide attention to your needs and we are committed to delivering exceptional software applications and resource-rich web sites. Our solutions will exceed your expectations.

© 2006 ParetoLogic Inc.

ParetoLogic XOFTspy Portable Anti-Spyware

XOFTspy Portable is the first application to offer spyware cleaning capabilities for multiple computers while simultaneously protecting your U3 smart drive.

XOFTspy Portable offers detection and removal of spyware, adware, Trojans, keyloggers, browser hijackers, and malware. It is the mobile solution to the threat of spyware cybercrime.

To download the product, check out: www.paretologic.com.

To view a video presentation of XOFTspy Portable see:

www.paretologic.com/media/videos/u3xoftspyportable.wmv

Addressed in this Product White Paper

This paper includes the following:

Mobile Vulnerability	4
- What and “Ware”	4
- Attack Vectors	6
What are the Clues	7
- Intelligent Cybercrime	8
- Up and Coming	9
The Latest Vulnerabilities	10
Solution	11
- The U3 Platform	11
- Common Online Uses	12
- The Advantages	13
- Safety	14
Security and Peace of Mind	14

This document provides information related to XOFTspy Portable Anti-Spyware. It is not meant for instructional purposes. We recommend using the help file that comes with the application for detailed steps and instructions.

Mobile Vulnerability

Technology has gone mobile. Our language accommodates this evolution with terms like: things that think, pervasive computing, and everyware. One such phrase, “ubiquitous computing”, is described by Wikipedia as the integration of computation into the environment. As devices are embedded in our everyday surroundings, proponents of this technology count on having consumers “...interact with information-processing devices more naturally and casually than they currently do, and in whatever location or circumstance they find themselves.”¹

The present concern and emerging threat to this kind of natural and casual interaction is vulnerability. Cybercrime has evolved from random virus attacks infecting computer desktops for unknown reasons bordering on mischief and belligerence, to a spyware epidemic fueled by profit. As computing technology advances so does the sophistication and, in some instances, the desperation of these malicious activities.

What and “Ware”

Spyware was once a term used to reference equipment used for espionage purposes such as tiny cameras and audio bug devices. Since early 2000 it has been used more widely to refer to software that installs itself on a computer without the consent of the owner and with the intent of taking over some level of computing control for the benefit of a third party. While surveillance and monitoring is the literal term and can occur with information tracking, there are other motives that can be malicious or criminal in nature and potentially more harmful.

The line of distinction between spyware and virus is fuzzy. Spyware is taking on much of the same attributes as viruses with perhaps only one real distinction: motive. Viruses are typically vandalistic or a hacker’s twisted way of feeling powerful by taking down a system by one notch. Spyware, on the other hand is an underground business. “Internet-related complaints made up nearly half of all fraud complaints received by the Federal Trade Commission in 2005, with people claiming losses of \$335 million.”²

Quite often, such strong motives turn to adaptation when faced with deterrents. According to reports, the increase in security protection and the infusion of hefty penalties have led to more organized and tenacious profiteers employing stealthier

¹ Wikipedia: “ubiquitous computing” (http://en.wikipedia.org/wiki/Ubiquitous_computing)

² Washington Post, Aug 8, 2006 “Viruses, Spyware Cost Users \$7.8 Billion”

and more targeted attacks.³ Spyware is installed using deception or by exploiting vulnerabilities in a system such as with “drive-by downloads” where a user picks up spyware by simply visiting a web site. Examples of deception include bundling the spyware with legitimate software or using a Trojan horse technique to smuggle the malicious item. Likely the most extreme example of deception involves “rogue anti-spyware”. These rogue applications offer security protection or promise to remove spyware threats when in fact they include adware, spyware, or other malicious code.

Many terms are currently used to describe these activities. While there is cross-over in the terminology we can categorize the terms as seen in the following table.

Type	Description
Spyware	A software program or code that downloads to a computer without your consent and engages in harmful activities related to monetary gain. Spyware can cause computer slowdown, application and system crashes, and even hard drive erasure. Spyware can also collect sensitive information like passwords, logins and banking/credit card details. Examples include Trojans, worms, keyloggers, flooders, hijackers, adware, and more.
Malware	A general term used to describe malicious software. This includes a variety of intrusive, annoying, or hostile items such as viruses, spyware, and adware. The term “badware” is also, more recently, used.
Adware	At one time Adware was considered a good thing – software that was given away. This term has in more recent times been used to describe programs that download to a computer without consent for the purpose of automatically displaying ads. The ability to remove the advertising mechanism is limited when using typical add and remove procedures.

Table 1: Definitions: Spyware, Malware, and Adware

³ IBM report Jan23, 2006 (<http://www-03.ibm.com/press/us/en/pressrelease/19141.wss>)

Many underestimate the significance of the spyware epidemic. In October of 2004 America Online and the National Cyber-Security Alliance released a study⁴ which included the following findings:

- Known spyware was detected on 80% of the computers;
- An average of 93 spyware components were detected on infected computers; and
- 89% of those surveyed were not aware the spyware programs were on their computer.

Attack Vectors

As technology becomes mobile, hackers seek out viable attack vectors – the entry point or means of gaining access to systems. Exploitation of these system vulnerabilities comes in many forms. One such example is theft of confidential information gained from tampering with public computer terminals. For more than a year, Internet terminals in Kinko's stores in New York were the vector point exploited by a hacker named Juju Jiang. Imagine sitting at your home computer some time after using a public terminal in a Kinko printing store. Suddenly your computer's mouse cursor begins to move on its own. The cursor is controlled from a remote access program and it begins opening files and applications. The intention of the remote intruder is to transfer your funds.

One victim saw just that and, upon reporting it, assisted in the arrest of Juju Jiang. Until his capture in 2003, Jiang had stolen more than 450 usernames and passwords by installing keyloggers on public terminals. Keyloggers are one form of spyware. They are designed to record keyboard input to a log file that is then transmitted to the criminal intruder. After pleading guilty to the crimes, Jiang admitted to using the confidential information to access financial accounts and to open up new on-line bank accounts. Along with attempts to steal funds he also sold the confidential information on the Internet. A new awareness is brought to the attention of a concerned public: malicious software can be placed on public terminals.

⁴ http://www.staysafeonline.info/pdf/safety_study_v04.pdf

What are the Clues

Like the classic game “Clue”, we can put on our detective caps and begin piecing together the bits of relevant information so as to uncover the elements of the crime. Here is a breakdown of the malware crime.

The Victim: according to research and reports, cybercrime has moved from global outbreaks to smaller and stealthier attacks. The primary target is the home user. They are less likely to be equipped to protect themselves from an attack. Financial service businesses and specific organizations are the next targeted level.

The Payload: fraud, theft of identification, or crimes financially motivated. At times this means tampering with your computing experience by bombarding you with advertisements designed to appeal to you based on your Internet browsing habits. In extreme instances extortion of funds is the payload.

The Method: exploiting attack vectors including e-mail attachments, web pages, links from pop-up windows, instant messages, and chat rooms. Malicious software is downloaded without consent from drive-by downloads. In extreme instances malware is utilized to hijack your computer, to provide remote access for a hacker, or to steal and compromise identity information.

The Weapon: there is an abundance of tools at the perpetrators disposal. The following table lists some of the malware items that can be downloaded on to a computer without consent.

Type	Description
Popup ads	Displays advertisements in an intrusive manner
Keyloggers	Records your personal data
Browser hijackers	Changes your web browser settings
Remote influence	Influences or control your computer remotely
Unsolicited files	Downloads and install files on your computer
Shutdown or disable	Disables programs or processes on your computer
Unauthorized phone calls	Makes calls via the phone modem

Internet connection floods	Interrupts or temporarily disable an Internet connection
Tracking	Tracks your Internet activity and sends this information remotely
Surveillance tools	Acquires sensitive information including passwords, logins, banking details, or credit card information

Table 2: Types of Spyware

Time of the Crime: this is perhaps the greatest unknown. The more advanced spyware used in cybercrime often goes unnoticed. They are designed to escape detection and to perpetuate their presence on the computer system they infect.

The Damage: aside from damages incurred from attacks based on theft (monetary, security, privacy and the like), there is also noticeable performance degradation to the computer system. This can include unexplained behaviours, sluggish processing due to unwanted CPU usage and network traffic, and system instability in the form of application and system crashes.

Computers can also be turned into botnets. According to an article⁵ by eWEEK, a botnet is a collection of computers that share broadband connections. These infected computers have been hijacked using malware and are seeded with malicious code so that they can connect back to servers controlled by remote attackers. During the first 6 months of 2006, over 4 million computers have been utilized for botnet purposes so as to deliver spam or to "...install malware or log keystrokes for identity theft."

If detected early the damage can be contained and the items removed. Rarely does the damage involve one piece of spyware. Typically there are several items that bring about a cumulative effect.

Intelligent Cybercrime

The technology that is employed in the creation of these crime tools is nothing short of intelligent. Recent malware development includes the ability to hide itself from being detected and to use morphing capabilities when it is being removed. The following is a breakdown of some of the malware techniques utilized.

⁵ "Is the Botnet Battle Already Lost" October 16, 2006 (<http://www.eweek.com/article2/0,1895,2029720,00.asp>)

Techniques	Description
Evasion	Malicious applications can use code designed to modify itself so that the presence of the malware goes undetected. Polymorphic algorithms can make it challenging for security software to locate the malicious code as it mutates itself while keeping the original algorithm intact. Randomization, decoy techniques, and other modifications are used to evade detection.
Propagation	While propagation is more common to viruses it can also be utilized with malware. For example, adware can seek out network shares in an attempt to distribute and propagate itself to other computers.
Self-repair	Some malware consists of several components with multiple starting points. When one component is terminated or uninstalled, the other works to re-spawn the missing piece. For example, some malware can add registry items that were removed. This is known as persistency.

Table 3: Types of malware coding techniques

Up and Coming

Some malware vendors attempt to legitimize malicious online activities to maintain a positive corporate image or to prevent the loss of clientele or business partnerships. This means flying just under the radar by minimizing any detectable trace of malware downloads and by being covert in their actions. For example, some vendors may have only one popup ad displayed in such a way that you would not know the source of the advertisement. Others will continue to investigate and employ sophisticated techniques of evasion to avoid detection and removal.

It is also evident that new software techniques will be construed. A recent buzz word in the cyber security arena is “fuzzers”. According to studies presented by InfoWorld⁶, for every 1000 lines of code there are approximately 5 to 10 bugs, some of which can be security holes. Legitimate fuzz testing is deployed as a testing technique for software. Hackers take this technique and use it to their

⁶ “The buzz about fuzzers” Sept 09, 2005 (http://www.infoworld.com/article/05/09/09/37OPsecadvise_1.html)

advantage. Fuzzers typically detect very simple coding faults but they frequently find severe security flaws that an attacker could easily exploit.

The Latest Vulnerabilities

The SANS Institute of Washington DC asked a panel of security experts several questions related to vulnerabilities.⁷ Some of the more salient warnings and cautions include the following:

- Attackers can create audio files that will take control of a victim machine after you download it and play it using iTunes.
- The number of machines turned into botnets is increasing and are being used to install spyware and adware.
- There has been a notable shift from attacks made on Windows operating systems to attacking programs running on Windows; targeted software includes backup applications, management programs, and licensing systems.
- There are notable vulnerabilities to media applications such as RealPlayer and iTunes.
- Although IE continues to be exploited for its security flaws, other web browsers such as Mozilla and Firefox are becoming more promising attack vectors. These browsers are gaining attention by attackers as many savvy home users are making the move away from IE and embracing alternate web browsers.

When asked about the biggest changes related to cybercrime and security, Ed Skoudis⁸ stated that attackers are changing their avenue of infiltration. “In particular, they are finding and exploiting flaws in client tools, because a victim user inadvertently pulls malicious code into the system via items like web browsers, mail readers, newsgroup readers, and media players.”

When asked about the significance of a 10% increase in the number of vulnerabilities, Skoudis responded:

⁷ http://www.sans.org/top20/2004/q2_update/experts.php

⁸ Author of Counter Hack and Malware; considered the top instructor in the US on hacker techniques.

“Quite simply, we are deploying flaws faster than we are deploying fixes. We think we're making progress, but we are barely scratching the surface of a mountain of underlying flaws, and a 10% increase, while not dramatic, is a sign that we are moving in the wrong direction.”

What are the solutions? Sound preventatives include updates and patching, as well as education and utilizing a good firewall policy. Like other colleagues in the panel, Skoudis advises that the deployment of “... anti-spyware tools, with continual (daily!) updates of signature bases is crucial.” By receiving recent updates to a spyware database, the most up-to-date malware threats can be detected and removed.

Solution

To recap and to simplify here is a condensed way of viewing the issue at hand and presenting a viable answer.

(Common and popular computing) + (Mobile technology) →

(Security threats and vulnerability due to malware) → →

(A secure mobile solution) = XOFTspy Portable Anti-Spyware

XOFTspy Portable Anti-Spyware runs on the U3 platform and provides spyware cleaning capabilities for multiple computers while simultaneously protecting your U3 smart drive.

The U3 Platform

Smart drive computing on the U3 platform offers an intuitive and effective mobile computing experience. Co-developed by hardware manufacturers SanDisk and M-Systems, the open-standard U3 platform provides the ability to take an entire selection of applications and launch them on any USB-equipped Windows computer system. In this way, software applications are no longer tied to a single machine; you do not have to install applications on the host computer.

The U3 device includes a Launchpad which emulates the start menu of the Windows platform and offers an easy point of entry to applications and U3 features. Considerable attention has been given to ensure that there is no trace of your data or application usage on the host computer after you remove the smart drive. The U3 platform provides privacy and security solutions for your

data and applications including encryption and password protection. Additionally, U3 powered smart drives offer portable file storage.

Common Online Uses

Online Internet activities have been targeted at all members of a household. Youngsters and adults turn to:

- Email, e-cards, e-greetings, and e-postcards;
- Blogs including vlogs for video, linklogs for links, and photoblogs;
- Chat rooms, online forums, instant messaging; and
- Media-enriched sites for video clips, Internet TV or online radio.

Taking part in these online activities involves downloading numerous files. Webaroo is a company that provides customers with web content they can access while offline. They started out by asking whether it was possible to put the entire web on a hard drive. Webaroo recently teamed up with the makers of U3 so that users can download and carry portions of the web on laptops and other mobile devices including U3-enabled flash drives. The hope is to, one day, have the flash drive capacity to download large content such as the entire Wikipedia encyclopedia.⁹ Mass meets mobility, but is it safe?

Many of us take advantage of mobile computing so as to remain “connected”. One significant example of this is bringing our work home. In an effort to protect privacy and security we ask the question: are we increasing our exposure to cybercrime? Online activities and mobile technology opens the door for hackers as the number of attack vectors grows exponentially. It is no wonder that malware components are so frequently downloaded to our computers.

Kate Purmal, CEO of U3, submitted a blog entry¹⁰ describing how she upheld her title as “Queen of IT” in her household. After getting the word that the kid’s computer was a bit “sluggish” she followed the advice of one review she had read and tried out XOFTspy. She blogged the following:

“Not only did this cool portable spyware program save me hours of anguish and headaches, I may have found my new favorite use for my U3 drive – portable IT assistant!”

⁹ PCAdvisor, Oct 16, 2006 (<http://www.pcadvisor.co.uk/news/index.cfm?NewsID=7348>)

¹⁰ August 11, 2006; <http://katesblog.u3.com/>

With the same XOFTspy enabled U3 smart card, she cleaned her laptop, the children's computer, and other PC's in her house.

Anyone that has some computer experience is familiar with the story outlined by Matthew Miller.¹¹ Being asked to assist with computer repair and troubleshooting is a regular occurrence for him. He has now included XOFTspy on a U3 device to his toolkit. With "a couple simple clicks" he can scan and clean the computers he works on. He advocates using it in the workplace for employees who carry their USB flash drive from work to home.

The Advantages

You can clean all the computers in your home or small business using one license of the XOFTspy Portable U3 solution. It detects and removes spyware on any Windows XP or Windows 2000 computer you plug in to. You can also detect and remove dangerous malware on your U3 device to avoid passing on infected items when you plug into other computers.

XOFTspy Portable only takes 7 MB of space on your U3 device and yet it performs quick and thorough scanning. Despite the small footprint, it utilizes one of the most powerful spyware and detection engines. This is because the application is set to automatically receive spyware definition updates that are frequently distributed by the ParetoLogic team of professionals. Recent malicious threats are dealt with using a team approach. A technical support crew is also at hand to back you in maintaining normal computer functioning.

Another unique aspect to the XOFTspy solution is being able to work on computers systems that suffer from performance degradation due to infection of malware. As Marc Spiwak reports:

Anti-spyware products are quite popular with most computer users and all solution providers. A big problem with most of these products is that computers are sometimes too infected to allow software to be installed or downloaded.¹²

XOFTspy runs directly from the U3 drive and can remove the malware despite the fact that the computer is bogged down or sluggish.

¹¹ <http://blogs.zdnet.com/mobile-gadgeteer/?p=76>

¹² Information Week, "Pocket Anti-Spyware", Aug 29, 2006

Safety

When you want to take advantage of mobile computing, the key advantage to using XOFTspy Portable is safety. It enables the safe use of computers belonging to friends or family, or public terminals in cyber cafes, libraries, or print shops. With a technology that leans to “sci-fi”, the XOFTspy Portable tool on a U3 device will be a common interfacing method. After we plug the device in to the host terminal, the application runs automatically and reports security issues or that the computing environment is secure to proceed.

Security and Peace of Mind

Relying on computer performance and security issues is crucial from a business, financial, and personal home-use perspective. Being exposed to spyware threats can result in hardships, frustration, loss of time, and can lead to being the victim of cybercrime. Having the necessary equipment to provide a safe and reliable computing experience is essential. ParetoLogic XOFTspy Portable Anti-Spyware is a dedicated software solution that provides security and protection and gives you peace of mind.

XOFTspy Portable is designed to be fast and it offers a friendly, easy-to-use interface with a step-by-step process that puts you in control. While there is no money to be made in viruses, malware creators are profiting and are advancing their technologies. With XOFTspy Portable you have innovation and dedication to security on your side and... in your pocket.

All information contained in this document is the proprietary information of ParetoLogic Inc. and is protected by international copyright treaties. This document contains information that is privileged and confidential. Any disclosure, distribution or copying of this document without the prior written consent of ParetoLogic is strictly prohibited under applicable law. ParetoLogic and XOFTspy Portable Anti-Spyware are registered trademarks or trademarks of ParetoLogic Inc. in Canada, the United States, and in other countries. All other trademarks are the property of their respective owners.

Copyright © 2006 ParetoLogic Inc. All rights reserved.