White Paper February 2005

AVERT™

# Potentially Unwanted Programs

## Spyware and Adware

## What are Potentially Unwanted Programs (PUPs)?

Over the years, there have been a number of cases where a commercial entity of some kind produced a piece of code that was intentionally detected by AV software, including McAfee's. Usually these fell into categories like:

- Utility programs repackaged and distributed as part of a root kit or remote access Trojan, and scripted or altered in such a way to hide them or bypass all of the normal safeguards of the original application. Examples include IRC clients, FTP servers, sniffers, etc.
- Products which, by their very nature, are designed to ease administration by circumventing security measures or allowing remote administration. These sorts of programs, like password crackers, remote control programs, remote process creators and the like are natural backdoors for hackers or malware authors, and many users want to know if these programs are present on their systems.
- Applications that began as hacker tools or Trojans, but were good enough to find legitimate use as administrator software, e.g. Netbus.

Today a significant number of programs are using aggressive marketing techniques, akin to those long employed by spammers, to create more intrusive and, the developers would say, more effective products and services. The clear gap between malicious code written by anti-social teenagers and non-malicious code written by legitimate corporations is rapidly dwindling, where it exists at all. This aggressive marketing stance is even touted as "viral marketing", a term perhaps more appropriate than intended. Viral marketing can be defined as using a consumer's resources to generate more interest than could be achieved by direct marketing, with or without the consumer's knowledge and consent.

At a high level, Potentially Unwanted Programs (PUPs) are any piece of software which a reasonably security- or privacy-minded computer user may want to be informed of, and, in some cases, remove. Potentially Unwanted Programs are usually made by a legitimate corporate entity for some beneficial purpose (to whom they may be beneficial is debatable), but so alter the security state of the computer on which they are installed, or the privacy posture of the user using the computer, that most users will want to be aware of them.

2004 saw a marked shift in the motives for malware writing from political or mischievous purposes towards financial gain. Identity theft, phishing, extortion by threatening distributed denial-of service (DDoS) attacks, intellectual property theft, and selling compromised machine lists to spammers have become a common theme in malware. This trend began with the banking-specific autodialing in *Bugbear.b* and widespread utilization of *Sobig.f*-infected machines for spamming in 2003, and has become de rigueur in 2004, with widespread proliferation of keylogging, password-stealing, remote DDoS capabilities and backdoor installation amongst most major threats in 2004.

It is unclear whether the malware authors are adopting techniques used by aggressive marketing companies, or whether marketers are using ideas spawned by malware authors, but there is clearly a war going on for the use of YOUR computer system and its data and resources. Today we have:

- Adware removing other adware
- Viruses removing other viruses and backdoors
- Viruses distributing adware
- Bot armies being stolen or compromised and re-purposed
- Viruses and PUPs intentionally shutting down, disabling, or weakening security tools like IE security settings, firewall settings and AV products.

AVERT has for some time applied the technology developed for virus and Trojan detection to software products, that for whatever reason, our customers find objectionable. McAfee scan engines since version 4100 include an additional detection type (beyond virus or Trojan) called *app* or *program*.

So what exactly is this stuff, and what does it do?

## Behavior of Malicious Software

There are essentially six types of behavior seen by our researchers in traditional malware:

- Installation – getting onto a system and modifying that system so that the code runs frequently or every time the computer starts up
- Surveying – Finding new targets; seen only in viruses

- Replication – Getting onto those new targets; seen only in viruses
- Concealment – Hiding the presence of or preventing the removal of the software
- Injection – Getting inside the code or data of other innocuous processes on the system to gain additional privileges, achieve concealment, or deliver payload
- Payload – Doing something to the host computer, communicating data to third parties, or receiving commands from third parties

Surveying and Replication are only ever seen in viruses, but the other techniques used by both true malware and PUPs can be virtually identical. In fact, in AVERT's experience, there are few or no functional differences between many PUPs and many Trojan Horses except for the distribution of the former by a legitimate entity with an end-user license agreement (EULA).

Software that does one or more of the following is likely to be considered a PUP by AVERT:

- Bundling with other software, especially where the fact that the host software comes with additional components is not spelled out very clearly (Installation).
- Installing by taking advantage of an exploit (Installation).
- Failure to show taskbar or tray icons when running (Concealment).
- Hiding of processes, files, services, registry keys, or other evidence (Concealment).
- Filenames, resources attempt to mimic system files or other 3rd-party files (Concealment).
- Lacks of clear and obvious uninstall function (Concealment).
- Uninstall fails to work correctly, or installs or deletes files unrelated to the software (Concealment).
- Uninstall requires long surveys or other tricks to accomplish (Concealment).
- Firewalls, antivirus software, or other security measures disabled (Concealment).
- Application (e.g. Internet Explorer) or operating system (e.g. Window Firewall) security settings altered (Concealment).
- Injection into other running processes (Injection).
- Downloading and execution of arbitrary 3rd-party content (Payload).
- Interception, redirection, or retransmission of non-personal data (search keywords, URL history, etc.) to or by 3rd parties (Payload).
- Interception, redirection, or retransmission of personal data (names, addresses, passwords, account names, banking information, etc.) to or by 3rd parties (Payload).

## Types of PUPs

AVERT breaks PUPs down into 6 major categories and an OTHER category. Most PUPs are functionally similar, if not identical, to Trojan horses. In some cases, the software is innocuous by design, but can be easily misused in ways that have unintended security or privacy impacts.

### *Spyware*

Software whose function includes the transmission of personal information to a 3rd party without the user's knowledge and explicit consent.

### *Adware*

Software whose primary function is to make revenue through advertising targeted at the person using the computer on which it is installed. This revenue can be made by the vendor, or partners of the vendor. This does not imply that any personal information is captured or transmitted as part of the software's functioning, though that may be the case.

### *Password Crackers*

Software designed to allow a legitimate user or administrator to recover lost or forgotten passwords from accounts or data files. When in the hands of an attacker, these same tools allow access to confidential information and represent a security and privacy threat.

### *Remote Administration Tools*

Software designed to allow remote control of a system by a knowledgeable administrator. Remote administration tools, however, when controlled by a party other than the legitimate owner or administrator are a large security threat.

### *Dialers*
Software that redirects internet connections to a party other than the user's default ISP for the purpose of securing additional connection charges for a content provider, vendor or other third party.

### *Jokes*
Software that has no malicious payload or use, and does not impact security or privacy states, but that may alarm or annoy a user.

### *Other PUPs*
Many innocuous pieces of software, such as FTP servers, have been misused to assist the replication or payload behaviors of traditional malware.

### *Other definitions of "Spyware"*
Unlike the anti-virus industry, which has clear definitions and naming conventions, and cross-industry associations which develop and maintain some level of consistency, the press and the nascent anti-Spyware industry have much looser definitions that may overlap, agree or conflict with McAfee's definitions. This section is intended to help clarify the terminology, and explain how they are dealt with by AVERT and McAfee products.

**Common usage of the term "Spyware"**
In the press, and even in pending legislation, the term "spyware" is used as a catch-all phrase to mean any piece of software that has negative privacy or security implications. Many of the items called "spyware" by journalists or third parties are considered Trojans by the AV industry. And in some cases, unfortunately, hype and fear have labelled some innocuous software as spyware.

**Backdoors**
Backdoors are programs that allow a third-party attacker to access and to some degree control a machine remotely. Backdoors are largely Trojans and are dealt with correctly by most anti-virus products. Note that commercially-developed remote administration tools are called PUPs by AVERT and McAfee products.

**Keyloggers**
Keyloggers hook applications or the operating system such that the keylogger intercepts data between the user entering it, and it's reaching the intended recipient application. There are both Trojan and PUP keyloggers, which are to some degree, functionally identical. Both kinds of keyloggers are detected by McAfee due to the privacy implications.

**Browser Helper Objects**
Browser Helper Objects are a kind of DLL file that Internet Explorer allows to alter its behavior. This can include adding new toolbars and menu items, viewing incoming and outgoing traffic, and modifying HTML data before rendering. Though often used in Adware particularly, there is nothing inherently dangerous about the existence of Browser Helper Objects. McAfee does not detect all Browser Helper Objects, though many adware components that happen to be Browser Helper Objects are detected.

**Browser Hijackers**
Browser hijackers are programs that replace the browser home page, search page, search results, error message pages, or other browser content with unexpected or unwanted content. Browser hijackers may install cleanly and obviously, uninstall correctly, and make it very clear where the content comes from. Many do not. McAfee usually detects browser hijackers as Adware.

**Cookies**
Cookies are small text files used by many web sites to store state information about pages visited and other settings (temporary or persistent). For example, your favorite stock portfolio site probably uses a cookie to cache which stock ticker symbols you are interested in. While most cookies are innocuous, some may store personally-identifiable information about you. More commonly, they may store which pages you have visited or which ads you have clicked on to allow the advertiser to target your interests more closely. Some McAfee products will begin detecting certain cookies with privacy implications in 2005.

**Hacker Tools**
Hacker tools are often security utilities that happen to be equally adept at helping administrators secure their environment or attackers gain entry to it. Several types of hacker tools are discussed below:

- **Sniffers** are capable of monitoring network traffic and as such, are often utilized by attackers to locate new targets. While sniffers are important tools for the system administrator, the presence of a sniffer on an unexpected computer is a sign for alarm.
- Like sniffers, **Port Scanners** can be used to locate potentially vulnerable services running on target computers.
- **Vulnerability Scanners** may be used both by the administrator to locate machines that need patching, and by attackers to locate vulnerable, unpatched machines to compromise.
- **Password Stealers** are closely related to password crackers, though they are considered Trojans by AVERT, as stealing or remotely acquiring another's password has little to no legitimate use.

- The presence of **virus creation kits, source code, polymorphic engines, and other tools** for malware writers on a computer most likely indicates that the user (or a controlling attacker) of that system is developing or distributing malware from that machine.
- Like virus kits, the presence of **SpamTools** tools probably indicates objectionable or even illegal (depending on the jurisdiction) activity on the system.

**Proxies**
Tools that redirect information bound to an IP address or domain name (or ALL internet traffic) to a third party. The existence of a proxy on a system indicates that all traffic, including potentially personal information, is available to unknown parties.

**Peer-to-Peer (P2P Programs)**
P2P file-sharing programs are of concern for a number of reasons:

- They often act as the carrier for a wide variety of other adware and spyware.
- There may be legal liability for some users because of real or potential copyright violations.
- They are often a vector for viruses, which often copy themselves to shared P2P directories in the hopes of enticing another victim to install them.

However, P2P programs are also, in and of themselves, relatively harmless and obvious in function. McAfee does not at this time detect P2P programs.

**Layered Service Providers (LSPs) & Namespace Providers (NSPs)**
LSP's and NSP's are DLLs that utilize Winsock APIs to insert themselves into the TCP/IP stack. Once in the stack, layered service providers may intercept and even modify all inbound and outbound internet traffic. Namespace providers may redirect traffic from one site (say www.mcafee.com) to an intermediary (say adserver.com).

While used by personal firewalls and other security tools to block malicious traffic, they are often used by adware and other PUPs to redirect searches or other web page requests to advertising sites. Because they are in a position to see all internet traffic, there is also a possibility of more serious privacy or confidentiality breaches.

The following diagram may help understand the variety of behavior that different kinds of potentially dangerous behavior that commonly-encountered "spyware" or PUPs might engage in, and how McAfee treats them.

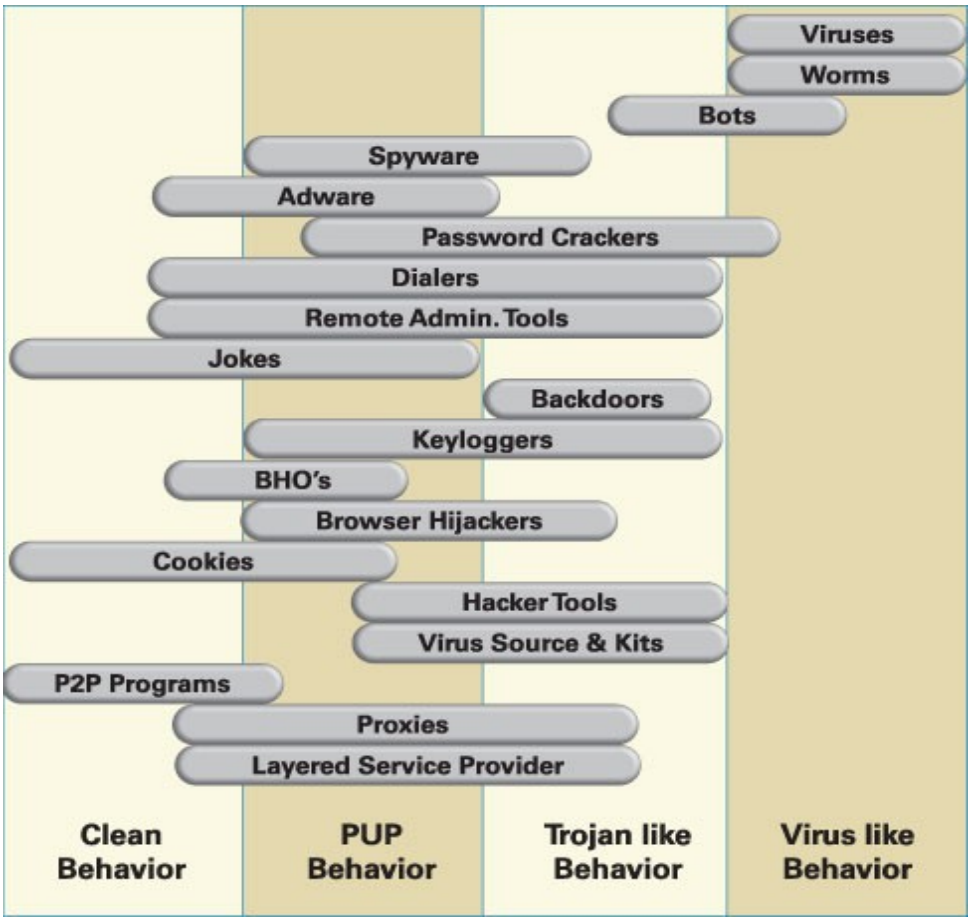


**Figure 1 - PUP Behavior**

## What are The Risks Associated With PUPs?

Not all PUPs carry the same risk. Possible consequences for having PUPs installed on a computer range from mere annoyance, to reduced performance or productivity, to serious security breaches or legal liability. Some possible outcomes are described below.

**Intellectual Property theft**
In 2003, Valve Software, makers of the popular computer game Half-Life had the source code for their much-anticipated sequel released to the internet by an anonymous attacker who installed keyloggers on a developer's computer[i]. It is unclear if this had actual revenue impacts on Valve, but the implications are obvious for anyone with sensitive information stored on a computer.

**Weakened security**
A recent trend in the gray area between Trojans and PUPs involves lowering Internet Explorer security settings to make it easier to get additional material onto a computer. Several PUPs and a fairly high proportion of malware shut down antivirus, firewall, and anti-spyware software to avoid detection and removal. Vulnerability scanners, and other hacking tools are as effective at helping attackers compromise machines as they are for the administrators trying to secure them. Knowing when and where tools like these are in use can help limit the exposure to other security or privacy problems.

**Legal consequences**
Numerous state and federal regulations have repercussions of some kind resulting from inadvertent disclosure of confidential information. Some examples include:

Gramm-Leach-Bliley (GLB) Financial Modernization Act[ii] – Comprehensive law requiring financial institutions to protect the security, integrity, and confidentiality of consumer information.

The Health Insurance Portability and Accountability Act (HIPAA)[iii] - HIPAA privacy rules require the protection of individually identified health information while ensuring the integrity, confidentiality and availability of electronically stored and transmitted healthcare information.

California State Regulation 1386 (CA 1386)[iv,v] - Entities or persons doing business in California will be required to notify California residents if their personal information--contained in databases under their control--may have been acquired by unauthorized people through a security breach.

Since PUPs may facilitate an intruder's access to confidential information, or steal the information outright, corporations need to be aware of the possible implications of PUPs in their environment.

In at least one child pornography case[vi], backdoor Trojan horses were blamed by the defense attorneys for allowing some third party to place the images on the defendant's computer, and the case was dropped. Regardless of whether this scenario is true, the fact that many PUPs allow a third-party unlimited access to victim machines means that the possibility for illicit material to be placed on the machine is real.

**Identity theft**
Identity theft is estimated to have cost businesses and consumers $50 billion in the US alone in 2002 though this includes a significant percentage of non-computer-related fraud as well[vii]. However, those of us who bank online, buy and sell securities online, or store information such as social security number, credit card numbers, maiden names, etc. on our computers are at risk if a thief or fraudster can acquire this information through keylogging, proxying, phishing, and other techniques.

Consequences include fraudulent charges, creating or closing accounts in your name, or even committing other crimes in your name. It can be difficult and expensive to prove that someone else had this information and misused it.

**Other privacy implications**
Many people are concerned about organizations being able to track their surfing habits, instant messaging conversations, email or other private information. Proxies, browser hijackers, tracking cookies, adware, and other PUPs enable companies to build detailed profiles of a computer user's tastes. Even though this may not be directly tied to the user's name or other personal information, the notion is disquieting at best.

**Resource consumption**
Spyware and adware all consume resources that could otherwise be used by the user for their own purposes. They take up disk space, clutter up favorites and menus with unwanted junk, eat up memory, throw up numerous popup windows and otherwise make the computer less responsive. Anecdotal evidence suggests that many home users and even system administrators periodically wipe out machines and reinstall from scratch, or even buy completely new computers to rid them of spyware, adware and other PUPs

**Productivity drain**
Several reports from Dell, AOL and other large corporations[viii,ix] suggest that spyware contributes to a large percentage of technical support calls. This drains IT staff and wastes users', administrators', service providers' and manufacturer' time and money.

## How Do You Get PUPs on Your System?

**Bundling**
The watchword of adware vendors seems to be "partnership". Relatively few vendors make adware compared to the number of applications that bundle said adware. It is not unusual to find a single program that downloads and installs 15-20 different files from 3-5 vendors when a single piece of ad-supported software is installed. While some application vendors (bundlers) disclose very clearly what is installed with their application, many do not, and some do so in the most confusing and obtuse way possible. And the same application vendor may change which adware they install on a weekly basis. In short, if software come with functionally-equivalent "free" and pay versions, the free version probably comes with adware and should be viewed with caution.

**EULA & Privacy Policy Tricks**
Closely related to bundling, many PUPs come with EULA's or privacy policies that may disclose exactly what they do, but are convoluted or obscured enough that the end-user is likely to miss important points. Common techniques for maximizing the likelihood that the user will give up and just accept it include:

- Having a very long text EULA displayed in a very small control that only allows the user to read one or two lines at a time,
- Exceedingly legalese language,
- EULAs that state that you will not use an anti-spyware tool to remove it,
- EULAs that state that by accepting it you also accept the EULA's for a variety of unnamed and anonymous other parties whose software may be installed,
- Software that installs even if the user declines the EULA,
- Installers that do not actually display the EULA without the user clicking on a link or taking extra action,
- EULAs or privacy policies hosted only on a web site, where they may change without notice,
- EULAs or privacy policies buried deep behind a series of links,
- Privacy policies that opt the user into other marketing activities, often buried deep in a lengthy document,
- Privacy policies that allow the vendor to sell the user's information to anyone they choose, often buried deep in a lengthy document

While no one enjoys reading EULAs, doing so routinely will not only keep one's machine safer and more functional, but be highly educational as well.

**Drive-by installation**
An increasingly alarming trend is for PUPs to be installed by using an HTML exploit that allows a mere visit to a web page to drop and execute the PUP installer. While the PUPs dropped in such a fashion may individually be well-behaved, the installation behavior is essentially the same as that used by viruses and Trojans.

**Distribution by other malware**
Another disturbing development is for actual viruses and Trojans to install adware as part of their payload. AVERT has noticed a number of SDBot variants doing this recently, but it is still unclear as to whether the PUP vendor is writing, encouraging or otherwise taking advantage of the malware author, or whether the malware author has found a way to make money via infected computers by bundling PUPs without the vendors' permission.

## How Big is The Problem?

### *Home user*

**Study results**
Market Analysis firm IDC estimated in November 2004 that 67% of computers (largely consumer) have spyware of some form on them[x].

An AOL/NCSA study[xi] showed that 80% of home users had some form of spyware on their system, with an average of 93 components per infested machine. Exactly whose definition of spyware was used is unclear.

Dell reports that 20% of all support calls are spyware-related, up from only 1-2% a year ago.

Whatever numbers you use, it is clear that spyware is a huge problem for consumers. It is also likely that home users are at higher risk than corporate users generally due to:

- The widespread use of file-sharing software (such as Kazaa, eMule, Limewire) which are often bundled with a variety of adware
- The lower frequency of antivirus and firewall deployment and policy compliance amongst home users
- Lower computer-security awareness, and the lack of dedicated staff to make up for this

**VirusScan Online figures and trends**
The AVERT Virus Map reporting service monitors the reported detections on 3-4 million consumer computers per month. In October and November 2004, approximately 45% of all detections reported resulted from potentially unwanted programs, and made up 48 of the top 100 most commonly reported detections. AVERT estimates that there is a world-wide average of 13 adware components per computer.

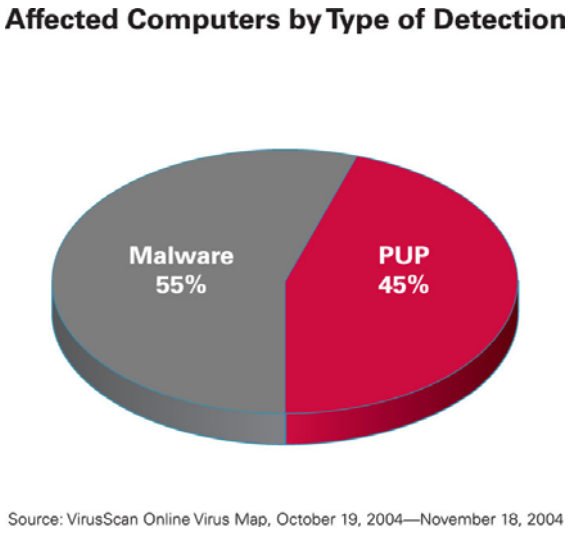


**Figure 2 - VSO Prevalence, Traditional Malware vs. PUPs**

PUPs now make up more than half of the most prevalent threats on a regular basis, and when combined with Corporate users

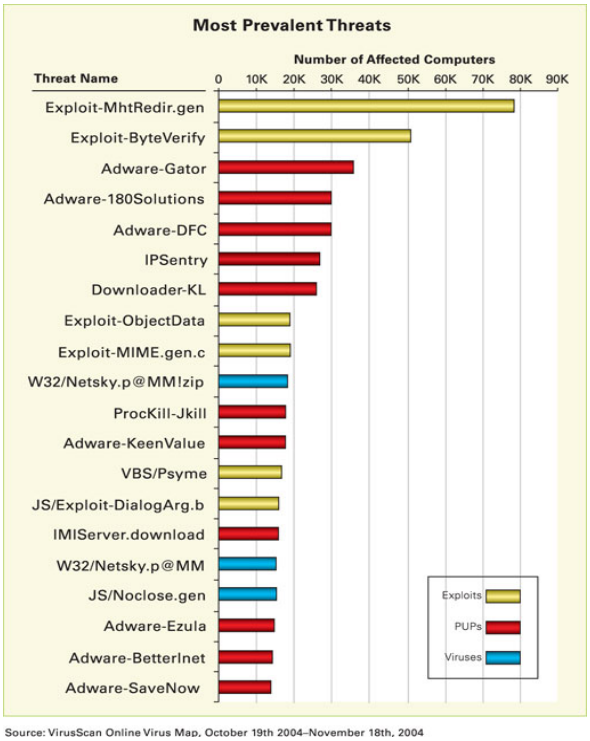


**Figure 3 - Most Prevalent Threats By Type**

A report published by Websense[xiii] states that 92% of corporate IT managers estimate that their organization has had spyware at some point.

**AutoImmune figures and trends**

In the month of December, 2004, 34% of all submissions to AVERT were PUPs. More than half of those were Adware. This data does not exclusively include corporate customers, and a more targeted survey is underway. Early results indicate that PUPs may be more of a problem in corporate environments than viruses or Trojans. While deployment and strong policy enforcement for anti-virus solutions exist in most large businesses, similarly mature anti-spyware products and policy are not as widespread yet.

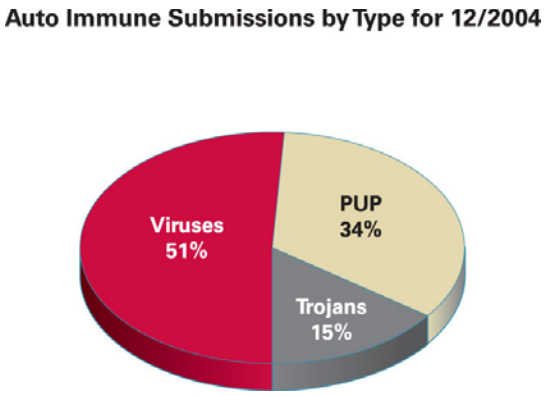


**Figure 4 – Number of Unique Senders to Avert by type of threat**

### *PUP Growth*

In 2004, PUPs surpassed viruses, both in terms of growth rate and absolute number of samples in AVERT's collection. In general, Trojan and PUP growth continues unabated, while virus growth is levelling off. We expect the explosive growth of Trojans and PUPs to continue for the foreseeable future.

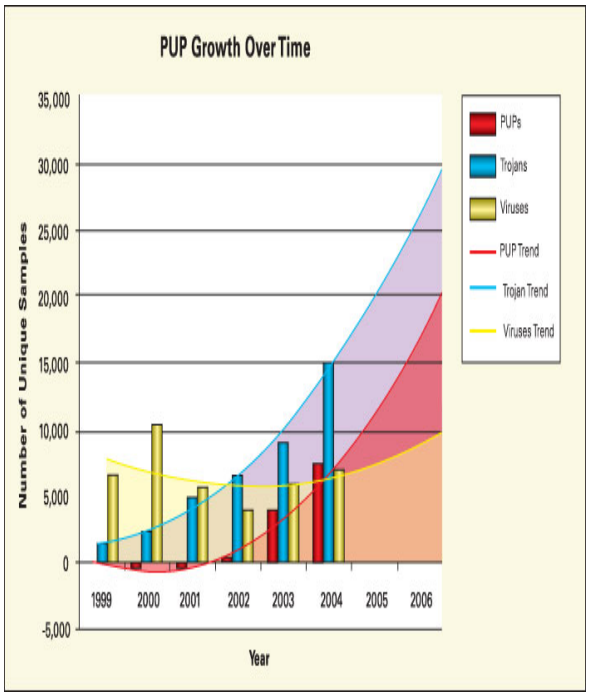


**Figure 5 – Growth Rate by Threat Type**

## What Can be Done About It?

### *Safe surfing habits*

The old saying, "an ounce of prevention is worth a pound of cure" applies to staying free from PUPs (and viruses and Trojans as well!). Your desktop anti-Spyware product should be the last line of defense against PUPs, if you are careful about how you use your computer.

**Read EULA's**

Like most viruses and Trojans, most PUPs are self-inflicted. While few would admit to finding license agreements interesting reading, many people click "OK", "Yes" or "Next" without even the most cursory glance at the contents of license agreements and privacy policies. The single most effective thing you can do to keep PUPs off of your system is to get in the habit of clicking "No" or "Cancel" to messages asking your permission to install unless you explicitly asked for software to be installed. Even when you are installing software, always carefully read the EULA and any privacy policy (whether part of the installer or web-based) for each product you install. Let the vendor know if you disapprove of their stipulations and why.

**Don't run as Administrator**

For users of Windows NT, 2000 or XP, set up and USE regular user accounts. Switch to the Administrator account only for installing software and patching. This will ensure that while you are browsing, PUPs that use drive-by installation techniques or other exploits to gain access to your system have as few privileges as possible. See http://www.microsoft.com/windowsxp/using/setup/learnmore/share/intro.mspx for more details.

**Safe Surfing**

Most web browsers come with a wide array of security settings, and the defaults may not be good enough. Use these techniques to make it more difficult for you to become an accidental victim:

- Keep it patched – the more frequently you close security holes in your web browser, the less time you will spend vulnerable to drive-by installations that take advantages of exploits to force PUPs onto your computer.
- Use Zones effectively – Increase the security for the Internet zone in IE to High, and move the few sites that you truly trust (your bank, ISP, etc.) to the Trusted Sites zone.
- Use Windows XP service pack 2 – Features such as the Pop-up Blocker and Active Content blocker in SP2 will further reduce your exposure to exploits.
- Use an alternative browser – Most exploits in the wild are targeted at Internet Explorer, given its large lead in popularity. Using Mozilla or Firefox may reduce the number of targeted attacks to which you are susceptible.

## Host-based IPS Products

### *Personal firewalls*

Personal firewalls are capable of monitoring or blocking any internet communication. Since anti-virus and anti-spyware products are largely signature-based, there will always be new threats that are not yet detected. Personal firewalls, if configured properly, are a great way to prevent new PUPs from being installed, or at least from communicating with the PUP vendors' sites. This may prevent release of confidential information or downloading of additional or updated components.

Recommended:

- Corporate: McAfee Desktop Firewall
- Consumer: McAfee Personal Firewall Plus

### *Host-based IPS*

Host-based Intrusion Prevention Systems (IPS) use behavioral techniques to block suspicious activities on a system, thereby avoiding the weaknesses of signature-based systems. They can often detect exploits of known and unknown vulnerabilities, and generically block or limit new threats. However, they are somewhat more likely to generate false positives and will require more tuning than signature-based products.

Recommended:

- Corporate: McAfee Entercept and VirusScan Enterprise 8.0*i*

### *AV products*

Many, or most, of the items detected by so-called anti-Spyware products are actually Trojan horses. Using an up-to-date antivirus product will protect against a large percentage of threats. However, many AV products do not detect a large number of PUPs created by legitimate vendors, so they are rarely enough in-and-of themselves to offer complete protection.

Recommended:

- Corporate: McAfee VirusScan Enterprise 8.0*i*
- Consumer: McAfee VirusScan 2005

### *Spyware products*

Dedicated anti-Spyware products often contain detection for PUPs not detected by antivirus products, though they often are less full-featured and/or use different technology to accomplish essentially the same task. However, like AV products, anti-spyware products are subject to limitation based on how quickly the database can be updated (and how often the user updates it!), and should be the last line of defense.

Recommended:

- Corporate: McAfee Anti-Spyware Enterprise (currently in beta)
- Consumer: McAfee Anti-Spyware

## Network IPS Products

### *Gateway scanners*

Gateway scanning offers a number of advantages to desktop-based anti-Spyware solutions. By blocking access to the sites that host PUPs, blocking the initial installation attempt, or blocking the traffic between the client (host) and server, PUPs can be curtailed or even eliminated prior to their reaching a vulnerable machine or user. Look for packages that combine signature-based antivirus and/or anti-spyware technology with content or URL-filtering techniques to prevent users from getting to suspicious sites in the first place.

Recommended:

- Corporate: McAfee Webshield 3000 Appliances

### *NIPS*

Network Intrusion Prevention combines the features of traditional AV with firewall, content inspection, statistical anomaly detection and other heuristic techniques.

Recommended:

- Corporate: McAfee IntruShield

## Management and Policy Enforcement

Installing desktop antivirus and anti-spyware software is relatively trivial. Managing AV and AS software to make sure it is up to date, running, and correctly configured is a more important long-term responsibility in most environments, since many kinds of malware and some PUPs will actively disable AV, redirect vendor web sites, and otherwise try to lower the host system's security.

The people trying to use and abuse your system are changing their tactics constantly. Security policy compliance rates and effectiveness should be reviewed regularly via reports and audits. Plan on adjusting and tuning your environment to balance business needs with security constraints on at least a quarterly basis.

## McAfee AVERT

McAfee AVERT Labs is one of the top-ranked anti-virus and vulnerability research organizations in the world, employing researchers in thirteen countries on five continents. McAfee AVERT combines world-class malicious code and anti-virus research with intrusion prevention and vulnerability research expertise from the McAfee® IntruShield® and McAfee® Entercept® organizations, two research arms that were acquired through IntruVert Networks and Entercept Security. McAfee AVERT protects customers by providing cures that are developed through the combined efforts of McAfee AVERT researchers and McAfee AVERT AutoImmune technology, which applies advanced heuristics, generic detection, and ActiveDAT technology to generate cures for previously undiscovered viruses.

## References

[i] http://www.halflife2.net/forums/showthread.php?s=&threadid=10692
[ii] http://www.ftc.gov/privacy/glbact/
[iii] http://www.hhs.gov/ocr/hipaa/
[iv] http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html
[v] http://www.onlinesecurity.com/Community_Forum/Community_Forum_detail102.php
[vi] http://news.bbc.co.uk/1/hi/england/devon/3114815.stm
[vii] http://www.ftc.gov/os/2003/09/synovatereport.pdf
[viii] http://www.crn.vnunet.com/news/1156261
[ix] http://www.msnbc.msn.com/id/6380633/
[x] http://www.idc.com/getdoc.jsp?containerId=pr2004_11_23_102854
[xi] http://www.staysafeonline.info/news/safety_study_v04.pdf
[xii] "Worldwide Spyware 2004-2008 Forecast and Analysis: Security and System Management Sharing Nightmares", IDC, Nov. 2004
[xiii] http://ww2.websense.com/docs/WhitePapers/Spywareyouprobablyhaveit.pdf

**McAfee, Inc.** 3965 Freedom Circle, Santa Clara, CA 95054, **www.mcafee.com**