FaceTime™

WHITE PAPER

Spyware Prevention: Effective Network Protection Through Defense in Depth

Table of Contents

Executive Summary

Spyware has rapidly become one of the most insidious and dangerous forms of malware. It's not just script kiddies any more. Organized crime is busy harnessing the power of exploitative code to extort and launder money, redirect funds, hold intellectual property up for ransom, and more. There's a very good chance active spyware is on your PC right now because, quite simply, traditional approaches to malware protection don't work for spyware.

FaceTime Communications believes that only by understanding the true extent of the threat and applying a comprehensive, intelligent set of defense mechanisms at the desktop and the perimeter, backed with user-driven research, can spyware be effectively defeated.

This white paper takes a long, hard look at what's really happening in the spyware underworld, brings together expert opinions on the impact spyware can and does have on corporate networks, and shows how FaceTime's multi-layered Enterprise Spyware Prevention Suite delivers the only viable solution.

It's a jungle out there

Spyware is ubiquitous. It's getting onto corporate networks at an unprecedented rate, entering through multiple channels, in multiple guises, using multiple protocols. Unlike most worms and viruses, spyware cannot be classified simply by a static 'signature' or behavioral trait. Spyware may have several different signatures—the source, the package, the installer—and several different behaviors—how it installs, what it looks like on the user's system, how it interacts with what else is on the user's system. Every variable affects every other variable, producing an almost infinite number of attributes for each infection.[1]

Spyware is ubiquitous. It's getting onto corporate networks at an unprecedented rate, entering through multiple channels, in multiple guises, using multiple protocols.

For a problem that only emerged some four years ago, spyware has, by leveraging these multiple channels and multiple guises, made a remarkable impact on the world's PC users:

- 80% of all PCs have been infected by spyware
- 91% of PC users are aware of spyware
- The average PC has 93 spyware components on it
- 89% of infected users are unaware of the spyware found on their machines
- 95% of infected users did not give permission for the software identified as spyware to be installed on their machines

Source: The above statistics are from the AOL/NCSA Online Safety Survey October 2004

Additionally:

- 20% of calls to Dell's helpdesk are spyware related (source: Dell)
- Microsoft estimates that 50% of all PC crashes are a result of spyware
  (Source: InformationWeek April 26, 2004)

Spyware: the dark end of the greynet

To understand the potential impact of spyware on corporate networks, it's important to first understand the concept of greynets[2]. Greynets are network-enabled applications that are installed on an end user's system without the knowledge or permission of the IT department—or, frequently, without the knowledge or permission of the end users themselves. They are further categorized by the degree of 'evasiveness' they exhibit on the network—for example, how much use they make of techniques such as port agility and encryption to avoid detection by existing network security controls.

Challenges associated with information sharing occur throughout the enterprise, but greynet applications pose a unique set of challenges—logging and archiving, unauthorized use, circumvention, and network security risk—as if the IT department didn't have enough on its plate already.

[1] *For more information on the nature and behavior of spyware, visit* ***http://www.spywareguide.com/***

[2] *For more on greynets, see the FaceTime white paper The Rise of Greynets: Unsanctioned End User Applications and Their Impact on Enterprise Security*

The dilemma facing IT staff in managing the greynet is that these applications can be good or bad, and in some cases both. Public instant messaging (IM) such as MSN, AIM or Yahoo!, Voice over Internet Protocol (VoIP), anonymizers, peer-to-peer (P2P) file transfer, web conferencing, remote control utilities, adware, spyware—all exhibit traits typical of greynet applications, yet many such applications are an integral part of business productivity and collaboration today, whether officially sanctioned by the IT department or not.

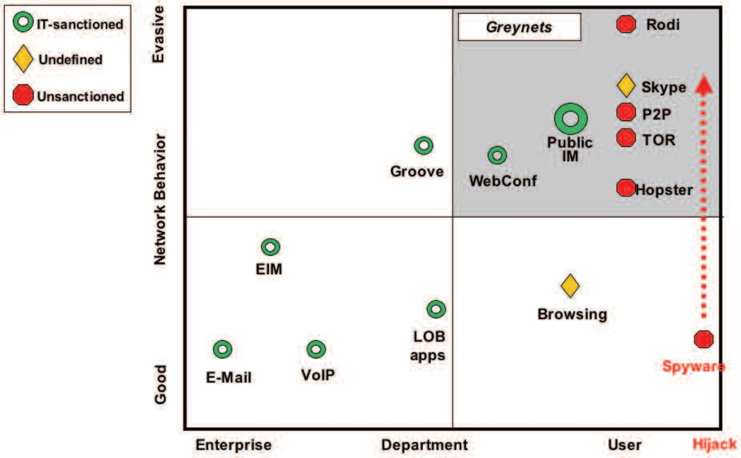


Figure 1
As can be seen here, spyware occupies the farthest reaches of the greynet.

As an example of the grey nature of the greynet, Skype, the popular VoIP/IM/P2P application, was developed by the same company that produced KaZaA, the P2P adware vector that regularly made bad-news headlines a couple of years ago. But with 20 million users, it's now one of the most widely-used greynet applications in the world, enabling even the smallest businesses to establish international communications. When 90% of businesses have public IM use approaching 50% penetration rate at the desktop level (Osterman Research), and 35% of business computer users regularly make use of electronic meeting facilities such as Webex and Placeware (Aberdeen Research), greynet applications are clearly here to stay.

While it's clear some greynet applications—like Skype, Webex, and Placeware—deliver significant business value, spyware and adware applications clearly do not. They can expose the network to external threats through unknown vulnerabilities. They may establish unmonitored outbound communication channels that could allow sensitive data to leak unchecked. And because they are 'flying below the radar' of the corporate security infrastructure, it's very likely they are also causing the organization to be in breach of compliance legislation:

- when credit card company databases are hacked, those companies are automatically in breach of Gramm-Leach-Bliley consumer protection legislation
- when a hospital's insurance records are compromised, that hospital is no longer HIPAA-compliant

“If the integrity of a user’s PC can’t be trusted”, comments Peter Christy, Principal at Internet Research Group, “compliance with any form of privacy or data protection legislation is out of the window. All the money spent to demonstrate compliance with Sarbanes-Oxley, HIPAA or Gramm-Leach-Bliley is neutralized. If you have a spyware-infected PC used as part of a material business process, you can’t possibly be compliant because you literally don’t know what that system is doing.”

Unfortunately, such incidents are reported far too frequently for anyone’s comfort level. Mandated measures for monitoring and protecting proprietary and confidential information were once industry best practice; now, laws require them across multiple industries. Adding to the complexity and urgency to meet these requirements, government agencies are cracking down and imposing harsh financial penalties on those that do not comply with regulations.

The spyware economy

The spyware economy exists to the tune of $2 billion annually. That money comes from ‘legitimate’ ad revenues and bundling deals, as well as less savory sources that may be linked to organized crime, such as intellectual property theft to order. To be effective, spyware applications must provide an end user experience that always works—the process is not monetized until an installation happens—and as we all know, money can be a great motivator to find ever more creative ways to sneak into the corporate network.

Spyware—and its close cousin, adware—are real businesses. They have business plans, sophisticated development groups, and venture capital. They generate revenue. And they sustain their growth and revenue streams by acquiring ever more desktops. Here are just a few examples of spyware/adware business methodologies:

CoolWebSearch	• 6 cents per install • $11,000 per week in commissions • 175,000 new installs per week
FlowBy botnet	• 32,000 unique IPs—installing adware • $584.99 per day
Recent trojan infection	• Arrived disguised as a business proposal • Was customized for each target, to evade scanners • Compromised machines were allegedly generating 17,000 British pounds per month • As many as 150 companies and government agencies in UK and Israel have been affected…so far

Clearly, spyware is a real issue, causing real problems, to real companies, right now. Knowledge is power, so in the next section, we’ll look deeper into the many different ways spyware can impact your organization, empowering you to formulate an appropriate strategy to protect your organization.

Spyware: the multidimensional threat

Spyware is a very much more complex form of malware than viruses or worms. It is stealthy and exploitative by nature, actively looking to deceive its host or target into acceptance. Among the many approaches spyware may take to get into a PC, and subsequently an entire network, are:

- Drive-by installations through automatic web-based downloads or scripts. Simply visiting a website that's been 'spiked' with hidden spyware applications can cause those applications to be downloaded to the user's machine without their knowledge or permission.
- Hidden installations inside an otherwise desirable application. Opening an email attachment—even one from a known individual—or downloading an apparently legitimate program can cause malware (most often a P2P file sharing program such as Grokster) to be installed on the local machine.
- Links embedded within public IM conversations can trigger the download of a spyware or adware payload that uses a variety of ports and protocols to install multiple malicious applications.
- Intentional malicious installation. Disgruntled employees and ex-employees also remain a significant vector for the introduction of malware designed to harm an organization by damaging electronic assets. Because these events frequently originate inside the organization, no firewall or other perimeter defense will ever see them.

Spyware applications will frequently use interdependency to subvert an application's original purpose—for example, a peer-to-peer application that under normal circumstances would be used to transfer large graphics files between a marketing department and an advertising agency may be harnessed to implant a keylogger.

IM, P2P, Web browsing, and other 'under-the radar' activities can also:

- Expose vulnerabilities that can be exploited through internal or external abuse
- Establish undetectable outbound communications that may facilitate data leaks
- Put organizations in breach of privacy legislation without their knowledge
- Sap employee productivity and increase helpdesk costs

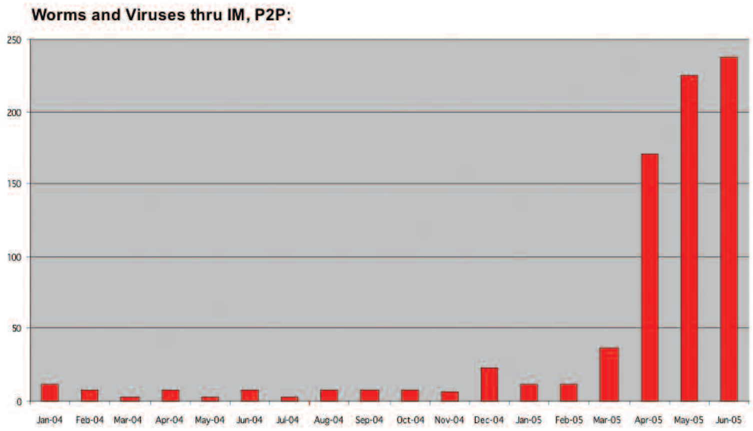


Figure 2
Number of IM, P2P and Related Threats Reported by FaceTime IMPact Center

See Appendix 1 for a detailed analysis of different types of spyware threats and their potential for damage to the organization.

"If a user gets three extra pop-ups a day and needs five seconds to close each ad, that's about 90 minutes spent in the course of a year."

Productivity impact

Pop-up ads are one of the most common manifestations of a spyware infection. They're irritating and intrusive, but most people don't consider them dangerous. However, according to spyware researcher Ben Edelman[3], the impact on productivity can be severe. "If a user gets three extra pop-ups a day and needs five seconds to close each ad, that's about 90 minutes spent in the course of a year", says Edelman. "Value users' time at a conservative $10/hour, and take 100 million PCs to be infected. Then these popups cost users about $1.5 billion of wasted time per year. Count users with worse infections (more popups) and more valuable time, and the problem only gets worse."

Pop-ups are unfortunately just the tip of the iceberg. Spyware-infected systems frequently become extremely sluggish. A bundled spyware or adware application that silently installs a number of other unauthorized programs can slow a brand-new machine to a snail's pace.

Privacy impact

Spyware also has a major impact on users'—and thus corporations'—privacy. A simple keylogger can capture every keystroke typed—credit card numbers, passwords, PINs, social security numbers, insurance claims, confidential medical data, industrial secrets—the list is endless. And because these applications are flying below the radar of the corporate security infrastructure, they are almost certainly causing companies to be unknowingly in breach of privacy legislation.

Social engineering

Virus and worm writers have long been aware of the alarming levels of trust users frequently place in those who communicate with them, regardless of whether there is any basis in fact for that trust. Spyware and adware vendors have taken this approach to new depths of deception by burying their true intentions deep in End User License Agreements (EULAs), knowing full well that almost everyone installing a downloaded application simply clicks the Agree button and moves on. Unfortunately, as those users will eventually discover, they have agreed to a lot more than just using the downloaded application responsibly.

Recent investigations of less-than-ethical EULAs have turned up the following (among many other) examples:

- 131 page down commands needed to read one EULA
- In addition, you further understand and agree, by installing the Software, that XXXXXXXXXX and/or the Software may, without any further prior notice to you, remove, disable or render inoperative other adware programs resident on your computer"
- To improve the features or functions of the XXXXXXXXX AdServer and/or third-party XXXXXXX-Supported Software, we may occasionally install and/or update software components."
- Any use of a packet sniffer or other device to intercept or access communications between XXXXX and the Licensed Materials is strictly prohibited"

Claria, one of the larger adware vendors, has been the subject of research by Ben Edelman:

[3] *Ben Edelman is a full-time spyware researcher who works closely with FaceTime and others. He maintains an extensive anti-spyware website at* ***http://www.benedelman.org****.*

"When KaZaA installs Claria, Claria's license agreement (**http://www.benedelman.org/spyware/claria-license/**) stretches to 5,936 words and 63 on-screen pages, and Claria makes a series of surprising demands (**http://www.benedelman.org/news/112904-1.html**). Claria restricts how users can remove its software—only in the way Claria provides, not by other methods users may prefer. And Claria limits how users may study or monitor Claria's transmissions over users' own Internet connection—according to Claria's license, they can't. Claria does generally mention advertising reasonably prominently, so most users probably understand that Claria will show them some ads. But Claria is far less forthcoming about facts of greater concern to typical users—that Claria will show ads in pop-ups, and that Claria tracks and stores users' online activities. So users press "Yes" and purportedly accept Claria's software, without prominent disclosures that reasonably explain what users are supposedly accepting."[4]

Spyware and the law

Many efforts are being made to draw up and deliver effective legislation to control and contain spyware, but the technology is so fluid and the perpetrators so nimble that there is almost nothing in the way of case law being established on the legality of spyware and adware companies' practices. Following are just a few examples of lawsuits involving spyware and adware vendors.[5]

Many efforts are being made to draw up and deliver effective legislation to control and contain spyware.

Claria

- In 2004, L.L. Bean sued Nordstrom's, JC Penney, Atkins, and Gevalia, each of which used Claria to display pop-up ads that cover L.L. Bean's site. Claria countersued L.L.Bean. Gevalia and Atkins settled with L.L. Bean.

WhenU

- WhenU has been sued by 1-800 Contacts, Overstock.com, Quicken Loans, U-Haul, Weight Watchers, and Wells Fargo Preliminary injunctions enjoined WhenU from delivering certain pop-up advertise ments. The company followed this by filing a lawsuit against the State of Utah to declare that state's anti-spyware law void.

180 Solutions

- Weight Watchers sued 180solutions and eDiets as to eDiets covering Weight Watchers' site using 180solutions software. 180solutions turned right around and sued two distributors of its software for installing its software without users' consent, which 180 claims was contrary to the distributors' contract with 180.

Direct Revenue

- In March 2005, a consumer class action was filed in Illinois on behalf of all Illinois residents who have had Direct Revenue sofware installed on their computers.
- In December 2004, Avenue Media sued Direct Revenue as to "systematic delet[ion]" of Avenue's software from users' hard disks.

Intermix

- In April 2005, the New York Attorney General sued Intermix for false advertising, deceptive business practices, and common law trespass. The case was settled in June 2005, with Intermix agreeing to pay $7.5 million and to permanently discontinue distribution of its advertising software.

[4] *See http://www.benedelman.org/news/112904-1.html for more on Claria's license agreements.*

[5] *A more complete list of spyware and adware related lawsuits may be found at* ***http://www.benedelman.org/spyware/#suits***

Comments Edelman: “Legislators are drafting new legislation that might grant consumers some relief from unwanted software, tricky installations, and endless advertising. But here too, industry lobbyists seem to be getting their own way. Last year, California passed a bill that multiple public-interest groups criticized as toothless. (**http://www.internetnews.com/security/article.php/3409281**) California’s approach started out reasonably tough, but somehow its major pro-consumer provisions disappeared before the bill was passed.”

The cost of spyware

In order to study the growth and impact of greynets, and specifically spyware, on corporate IT and end users, FaceTime commissioned NewDiligence, an independent market research company, to conduct a study of IT managers and end users in the summer of 2005[6]. The survey concluded that spyware can cost a corporation more than $130,000 per month, based on the following assumptions:

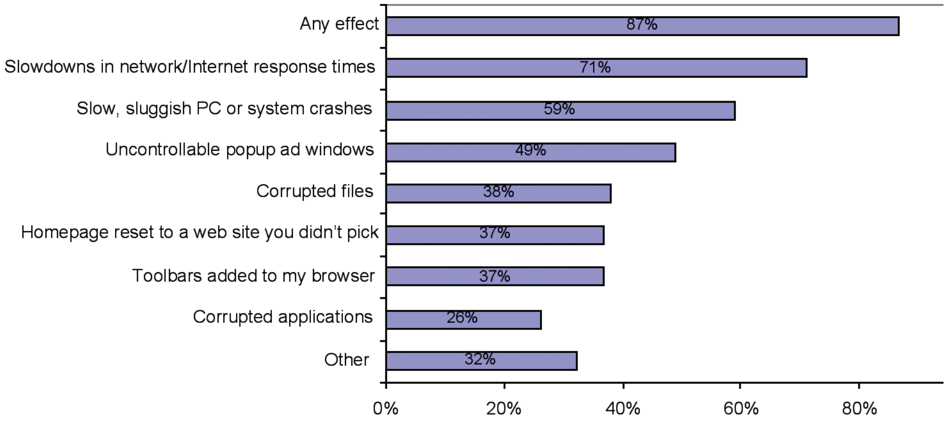
- 277 spyware incidents each month
- Average of 8 hours’ helpdesk time to remove one spyware instance
- Average $60/hour IT cost

On average IT managers at large organizations report 277 spyware or adware attempts or installations per month. The infection rate is correlated with company size—almost doubling at the largest organizations compared with all companies (152 average per month). Put another way, the more computers on the network, the more potential vectors for infection with spyware.

Worryingly for IT departments, end users generally believe they have the right to install greynet applications at the workplace. They also believe IT has any security issues associated with greynets under control. Yet 87% of those same end users reported a spyware or virus problem resulting in slow internet response times, pop up ads and corrupted files.

Figure 3

Spyware and virus attacks typically affect end users in a variety of ways.



[6] *A detailed report of the survey’s findings may be downloaded from the FaceTime website.*

The current state of the industry

Spyware is not a fix-and-forget threat. A worm or virus, once identified, can generally be halted by a single antidote. Spyware is fluid. It can be delivered by a plurality of vectors, so the signature of both the source and the package is different every time. Its behavior on installation may depend on the content of individual system registries. Such a threat cannot be defeated by a single string of code deployed to desktops or installed at the gateway; a multi-pronged approach is needed.

Data from the NewDiligence survey indicates that IT managers are fielding a variety of measures to combat spyware, with little success. For example, among IT managers who have rolled out perimeter security, consisting of gateway anti-virus, URL filtering and intrusion detection and/or prevention systems, 77% have had either a virus or spyware incident in the past 6 months. Underlining the increasing role of greynet applications in malware incidents, three in 10 IT managers who experienced a virus incident report that IM has been associated with such occurrences. A similar proportion report that IM has been associated with spyware.

Spyware infestations and virus attacks are most common. However, both types are so prevalent that they tend to occur at the same locations. Among those who have experienced a virus incident, 100% have also experienced a spyware attack. In spite of using a wide variety of network-based security measures, the incidence of attempts or successful installations of viruses, spyware and adware appears to be proceeding apace.

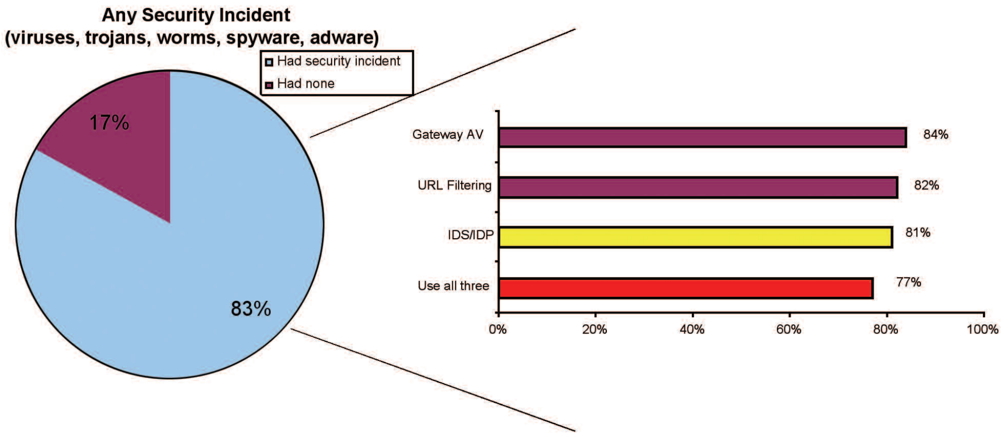


Figure 4

Three quarters of IT managers who use all three perimeter security methods report greynet-related spyware or virus security incidents.

In addition to the perimeter measures widely in use and outlined above, 91% of all IT managers surveyed have a desktop anti-spyware product installed, yet these are clearly not, even in conjunction with broad-based perimeter security, noticeably slowing the rate of spyware growth.

Recent product introductions for detecting spyware on corporate networks have tended to fall into two clear camps—those vendors who believe that a client-level solution is most effective and those who believe that any viable solution must be positioned at the gateway. Both represent a valid, and valiant, attempt to address the problem of spyware in corporations today.

Unfortunately, neither can offer a complete solution to the problem, and for one key reason—both are derived from ‘old’ concepts of anti-malware defense such as anti-virus (desktop) and URL filtering (perimeter). Spyware does not behave like a virus (although, as with viruses, fingerprinting may form one element of detection for a piece of spyware), and it does not behave like a ‘traditional’ hack attack, focusing on a single port; URL filtering is helpful in controlling what can enter the corporate network via the web channel, but is wholly ineffective when dealing with unauthorized internal or outbound behaviors. Attempting to retrofit conventional point products to deal with the rapidly evolving and all-encompassing threat of spyware will ultimately fail. Such products are not able to address the whole problem, so it’s unrealistic to expect either solution on its own to provide full protection.

Where existing protection falls short

A typical signature-based scanner would need an enormous database of signatures and take hours, if not days, to scan a user’s system—not to mention the time needed to deal with the inevitable volume of false alarms, false positives, and other time-wasters. While the desktop approach offers a familiar operational model for any IT staffer accustomed to managing anti-virus protection, the downsides of high false positives and general ineffectiveness of signature-based approaches, together with the resource-intensiveness associated with client-based solutions, far outweigh the convenience of familiarity.

Perimeter solutions don’t fare any better. A typical perimeter solution is only addressing the web (HTTP) channel, not IM, P2P, and other less visible—and less controlled—communication protocols. While offering operational simplicity through single-point control, perimeter solutions are for the same reason almost entirely ineffective against spyware’s ever-changing use of sites and applications as vectors for infection. Nor can they be an effective solution for a mobile workforce that is frequently connected to the Internet without the benefit of corporate network protection.

Dealing with spyware, adware, and other malware has become a daily challenge for IT staff. There’s no lack of potential solutions on the market, but finding an effective solution is a whole other challenge. Many products only react to spyware once an infection has occurred. The real answer to the spyware problem has to be proactive prevention—blocking spyware from entering the network and preventing pre-existing spyware installations from activating.

Defense in Depth

Rather than address the spyware problem with the traditional ‘point solution’ approach, FaceTime takes a broader view: spyware applications are addressed as part of the broader problems posed by greynets, which encompass both legitimate and unauthorized applications that, as we have seen, share common attributes—they are unsanctioned applications downloaded by end users and are capable of circumventing existing security infrastructure.

While spyware exists at the darkest end of the greynet spectrum, it still exhibits the same traits as legitimate greynet applications such as web conferencing or VoIP applications—evasive network behavior and end-user-level deployment. For this reason spyware, unlike viruses or worms, can be delivered by a plurality of vectors, and so poses a different prevention challenge—one that requires a multilayered approach.

Effective spyware prevention requires the intelligent harnessing and deployment of the most effective elements of both traditional approaches—gateway and desktop—integrated within a single management system and backed by targeted research.

Peter Christy of Internet Research Group again:

“We may think of a PC as just our window into the world, but under the covers that PC now has tens of millions of lines of operating system and application code. The PC gives us access to increasingly valuable business processes and assets. A great deal of investment has been to protect these valuable assets, but in the end the PC has to be equally secure if it not to be the weak link in the armor.

“Now consider one simple online task—an SSL session via the browser on a PC to create a ‘secure’ link to an application, for example. Investment has been made to require authentication of the user for the application and careful management of the certificates that provide the security underlying the SSL session, but if the user’s PC has been infected by spyware, all bets are off. SSL can’t be trusted, passwords can’t be trusted, nothing can be trusted. It’s really frightening because a virus planted on the machine could be happily sending the sensitive data back to Romania in real time.

“And of course, every infected PC means an under-productive user, additional helpdesk workload, and ever-widening holes in the corporate security armor. FaceTime’s ability to detect and act on “greynet” applications—the apparent high risk vector for system infection—is clearly a considerably more potent weapon against insidious spyware infections and complements the desktop or perimeter defenses in place today.”

The Solution: FaceTime’s Defense in Depth

Effective spyware prevention requires the intelligent harnessing and deployment of the most effective elements of both traditional approaches—gateway and desktop—integrated within a single management system and backed by targeted research. FaceTime Enterprise Spyware Prevention Suite[7] delivers on all fronts. By bringing together the best of both gateway- and client-based strategies, it delivers unparalleled efficacy and management of the spyware problem in the enterprise today.

[7] *For more on FaceTime Enterprise Spyware Prevention Suite, see* ***http://www.facetime.com/productservices/enterprisespywareprevention.aspx***

FaceTime Enterprise Spyware Prevention Suite consists of two key components:

- RTGuardian 3.0 (RTG 3.0) an anti-spyware gateway appliance at the perimeter, and
- FaceTime Enterprise Spyware Manager (ESM) - a centralized management, reporting and control server in the LAN.

Gateway Detection and Prevention

The RTG 3.0 appliance delivers advanced gateway-based spyware detection and prevention to protect organizations from spyware—before it infects the network.

- Monitors all possible channels—HTTP, IM, P2P, and more –for spyware activity.
- Blocks attempts by previously installed spyware to ‘phone home’ with unauthorized data, thus preserving the integrity of corporate information assets.
- Reports ‘phone home’ activity identifying both the infected PC and the specific spyware application. This allows for targeted remediation of the infected PCs, dramatically reducing the possibility of false positives.
- Blocks user access to known spyware sites, preventing accidental infections.
- Stops “drive-by” installations of known and unknown spyware applications distributed through Web, P2P and IM communications.
- Prevents unintentional downloads of spyware hidden within or co-opted by a seemingly helpful application using multiple behavioral factors.

Targeted Desktop Remediation and Inoculation

The Enterprise Spyware Manager provides centralized control and management of client scanning, remediation and inoculation and is completely transparent to the user avoiding any impact on productivity.

- Detections reported by RTG can be used to initiate a targeted scan of any managed PC or group of PCs based on custom policies set by the administrator.
- Patent-pending inoculation hardens PC operating systems to block new spyware installations and “freeze in place” existing installations, without the need to deploy any client software. This mitigates the need for continuous rescanning of PCs and helps to ensure that mobile users won’t get re-infected when outside the LAN.
- Optional, “headless” (no user interface) anti-spyware client can be pushed out ‘hands-free’ to PCs for removal and cleansing of targeted spyware applications and can be configured to stay resident or be removed from the PC. Enterprises can also choose to utilize their existing desktop software of choice.

Real-time Research from FaceTime Security Labs

FaceTime’s Greynet Research Database is the result of seven years’ working with customers to identify and address problems associated with greynet applications. Every instance reported by a customer is analyzed by security experts and incorporated as appropriate into our spyware database, enabling every customer to immediately take advantage of new detection and remediation through automated updates.

By combining analysis of all greynet applications from IM to P2P to spyware, FaceTime Security Labs is uniquely well-equipped to provide organizations with the information they need to make informed choices about application behavior that will and will not be tolerated on their networks.

Low-overhead Management
FaceTime's Defense in Depth spyware prevention is centrally managed through a single console. Every component is self-configuring using the intelligence generated by the solution itself. Systems administrators need only review reports on a regular basis to maintain a 360-degree view of the network's spyware protection status.

The combination of RTGuardian 3.0 and Enterprise Spyware Manager, backed by the FaceTime Security Labs real-time research effort, provides a comprehensive end-to-end solution to the spyware problem that cannot be matched by any other single anti-spyware solution on the market today.

Summary and Conclusion

FaceTime has been studying the parallel universe of the greynet for a number of years as the company's instant messaging and P2P security solutions have evolved, and it's become evident during this process that effective spyware protection can only be created with a full understanding of the fluid nature of greynets.

It's clear both from our own customers and from broader field data that existing measures—URL filtering, anti-virus scanning, intrusion detection/prevention, even desktop anti-spyware—are not delivering effective protection.

The future of spyware protection lies in the multi-layered approach of Defense in Depth, combining a broad understanding of greynet behaviors, targeted remediation of individual clients, and real-world research data to deliver 360 degrees of security.

About FaceTime

Founded in 1998, FaceTime Communications is the leading provider of security solutions for the management and control of greynet applications such as adware/spyware, instant messaging, webmail, P2P file sharing, web conferencing and instant voice. FaceTime delivers the industry's first IMPact Index, which assesses "point-in-time" risks posed by viruses, worms and other malware propagating through greynet applications. FaceTime's award-winning solutions are used by over 500 customers, among them seven of the eight largest U.S. financial institutions. FaceTime also supports or has strategic partnerships with all leading public and private IM network providers, including AOL, Microsoft, Yahoo!, Google, IBM, Bloomberg, Jabber and Reuters. For more information, visit **www.facetime.com**.

FaceTime is headquartered in Foster City, California. For more information visit **http://www.facetime.com** or call **888-349-FACE**.

Appendix 1: Examples of spyware and potentially unwanted technologies

The table below, developed by the Center for Democracy and Technology (**http://www.cdt.org**), describes technologies that have been used to cause annoyance or damage to electronic assets. As with all greynet applications, it's important to note that with the proper notice, consent, and control, some of these technologies can provide business benefits.

Common Terms for Unwanted Varieties	Underlying Technology	Description of Underlying Technology	Why the Underlying Technology May Be Unwanted	Why the Underlying Technology May Be Wanted
• Spyware (narrow)* • Snoopware • Keylogger • Screen Scraper	Tracking Software	Used to monitor user behavior or gather information about the user, sometimes including personally identifiable or other sensitive information.	• Done covertly, tracking is spying • May cause personal information to be shared widely or allow it to be stolen, resulting in fraud or ID theft. • Can slow machine down • May be associated with security risks	• May be used for legitimate monitoring: e.g. by parents or companies • May be a necessary component of adware that is linked to wanted software • May allow customization
• Nuisance or Harmful Adware	Advertising Display Software	Used to display advertising content (e.g. pop-ups)	• May be a nuisance and impair productivity • May display objectionable content • Can slow machine down or cause crashes and loss of data • May be associated with security risks	• May be linked to other software or content that is wanted, subsidizing its cost. • May provide advertising that is desired by the user.
• Backdoors • Botnets • Zombie • Droneware	Remote Control Software	Used to allow remote access or control of computer systems	• Can be used to turn a user's machine into a mass mailer or soldier for DDoS attack • Done covertly, it is stealing cycles and other resources • Can slow machines down.	• May allow remote technical support or troubleshooting • Can provide users remote access to own data or resources
• Unauthorized Dialers	Dialing Software	Used to make calls or access services through a modem or Internet connection	• May cause unexpected toll calls to be made and charged to the user.	• May allow access to desired services
• Hijackers • Rootkits	System Modifying Software	Used to modify system and change user experience: e.g. home page, search page, default media player, or lower level systemfunctions	• Without appropriate consent, system modification is hijacking • Can compromise system integrity and security	• May be used for desirable customization
• Hacker Tools	Security Analysis Software	Used by a computer user to analyze or circumvent security protections	• Are frequently used nefariously • Presence may violate corporate policies or family understandings	• Can be used for security research and other legitimate security purposes
• Tricklers	Automatic Download Software	Used to download and install software without user interaction	• May be used to install unauthorized applications including those in the	• May be used for automatice updates, or other automatic system maintenance categories above
• Tracking Cookies and other similar technologies (e.g. PIE)	Other Tracking Technologies	Used to gather limited information about user activities without installing any software on the user's computers	• May allow unwanted information to be collected about visited web sites	• May be used for desired customization e.g. "similar items you might like" • May allow advertisers to avoid showing the same ad too often to the same person.

FaceTime Communications, Inc.
1159 Triton Drive • Foster City, CA 94404

Toll Free	888.349-FACE (3223)
Phone	650.574.1600
Fax	650.574.2700
General Info	info@facetime.com
Sales	sales@facetime.com