

The Rise of Greynets: Unsanctioned End User Applications and Their Impact on Enterprise Security

Published by **FaceTime Security Labs**
FaceTime Communications, Inc.

Table of Contents

Introduction	3
The Growth of Greynets	6
Instant Messaging	6
Voice over IP (VoIP).....	7
Web Browsing	8
Peer-to-peer File Sharing in Business Networks.....	9
Security and Compliance with Greynets	11
How a Greynet Can Wreak Havoc.....	11
Challenges in Detecting and Managing Greynets	13
Greynets Are Becoming More Evasive.....	13
Greynet Management—Requires Defense in Depth	14
Managing PCs (Software Restriction Policies).....	14
Blocking at the Perimeter.....	14
Conclusion	16
About FaceTime Security Labs	17

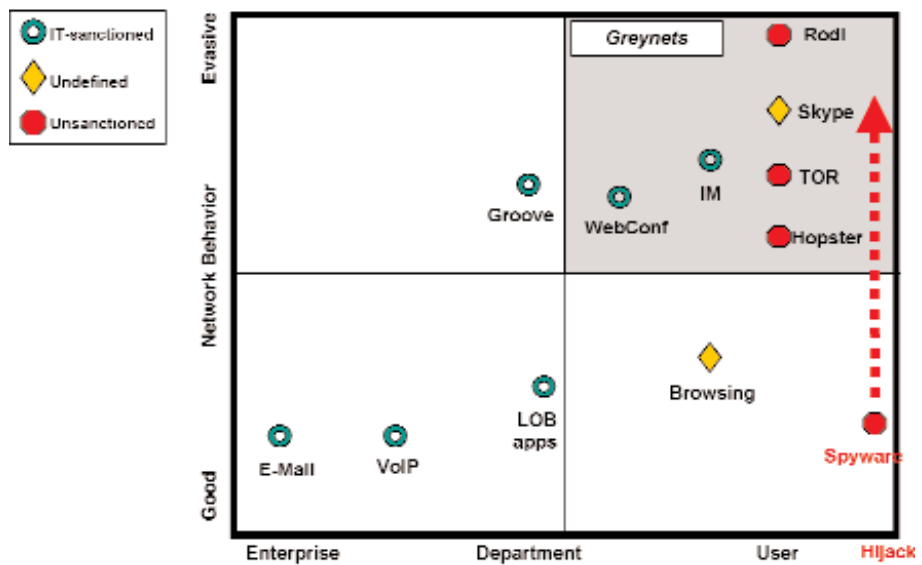
Introduction

A greynet is a network-enabled application that is downloaded and installed on an end user's system without the IT department's knowledge or authorization.

Enabling real-time communication has become a core requirement for IT infrastructures. Today's generation of workforce entrants expects instant messaging, Web conferencing, Voice over IP, and social networking to be "always on". The edge of the network is rapidly moving outwards to include the broader community of customers and trading partners, and end users are in the driving seat, bringing these applications into the enterprise without corporate IT consent. FaceTime Communications calls these applications "Greynets."

Greynet examples include public instant messaging (AIM, MSN, Yahoo!), P2P applications like Skype and file sharing clients, web conferencing, anonymizers, and remote control utilities (See Figure 1).

Figure 1
Greynet Landscape



Greynets are user-driven and highly evasive

A prime example of this real-time communications explosion is Skype. The peer-to-peer voice network that's taken the world of telecommunications by storm, signing up tens of millions of users in just three years, has become a key business communications tool. Not only is it extremely cost-efficient, potentially lowering phone bills to almost zero, but it blends the worlds of instant messaging and telecommunications in a way that is extremely attractive to individuals and businesses alike. There are over 190 million users on Skype of which over 30% are corporate users. There are nine million Skype users online concurrently every day. With leading computer manufacturer's adoption of Skype as a preinstalled option on their notebooks, the software has truly entered the mainstream of personal computing.

Real-time communications falls outside the scope of existing network and asset management tools; they are linked to the identity of an individual user rather than a device or application.

The need for time-sensitivity and speed in communications has always been critical to success in business. Business users are setting up virtual conferences, collaborating on projects and documents, augmenting phone conversations with chat threads, and exchanging documents across the Internet. Real-time communications build community and collaboration among different corporate locations, remote employees, telecommuters, supply chains, partners, and customers. They're delivering cost savings, lower telecommunications bills, greater accuracy in written transactions, and increased efficiency through rapid decision-making.

But whether security measures are keeping up with this communications revolution is a different story. Real-time communications falls outside the scope of existing network and asset management tools; they are linked to the identity of an individual user rather than a device or application. And it is a fundamental truth of the security business that users are the weakest link.

Despite the growing deployments of enterprise-strength collaborative environments such as IBM Lotus Sametime and Microsoft Live Communications Server, users are still accessing Skype as well as public instant messaging networks such as MSN, Yahoo, AIM, and GoogleTalk through the corporate firewall. They are using identities that cannot be verified, so authentication and content filtering policies cannot be applied to any information - conversation or files - traversing that channel. And these greynet networks port-hop for the next available connection, so firewalls are unable to see what connections are being made and anti-malware cannot check the traffic stream for malicious code. Skype even now has its own development platform, exponentially increasing the amount of mischief that can be wrought in that environment.

There are multiple reasons for this evasive behavior, many of which will be discussed in this paper, together with the growing security threats that accompany the adoption of greynet applications in the enterprise environment.

While email communications are routinely scanned for malware, channels like IM and P2P applications are enabling malware to hop from unprotected public networks into the enterprise. And not only are more attacks entering the network over real-time channels than email, but the attacks themselves are designed to bypass traditional security measures.

Most enterprises also have in place some form of content filtering or data leak prevention safety net to prevent confidential or privileged information from leaking out through email. But email content filtering systems aren't addressing real-time communications channels.

Compliance regulations - SOX, HIPAA, SEC, eDiscovery requirements, and others - largely apply in the same way to all real-time communications as they do to email. That means secure storage, easy retrieval of specific content, audit trails, tampering prevention, context preservation - all the processes that are in place for email must now also be applied to IM exchanges and Skype conversations (both chat and voice threads).

When greynets are installed ad hoc on the desktop by employees, the entire corporate network and beyond is at risk:

- Security** Greynets expose vulnerabilities and become vectors for malware distribution
- Privacy** Greynets establish undetectable outbound communication connections and allow holes through which sensitive corporate information may leak
- Compliance** Greynets establish invisible and unmanaged communication networks that corporate employees may use (or misuse) for business communications

Securing, managing, and controlling greynet applications is a corporate imperative. These tools have reached dial-tone status among the younger generation of workers, so blocking access is no longer a practical option. In fact, FaceTime's second annual Greynets Survey in October 2006 found that today's workers are remarkably resistant to imposed solutions - almost 40% believe they should be free to install the applications they need on their work computers, independent of IT oversight. A worrying concept indeed.

Specific areas of concern for the enterprise include:

Introduction of malware - Peer networking environments are increasingly targeted by malware, with blended threats (viruses, worms, spyware, and more) hopping from public to enterprise network.

Increasingly damaging malware - Not only are more attacks entering the network over greynets than email, but the attacks themselves are becoming more damaging. Crimeware, rootkits, exploits, and other malware are designed to bypass traditional security measures, and real-time communications channels only make that task easier.

Spam over IM (SpIM) - Just as malware is moving to the real-time communications platform to bypass existing security measures, spam is moving beyond the email inbox into the real-time stream, further increasing the risk of accidental malware introduction as well as increasing the traffic load.

Legislative compliance - Compliance regulations, including eDiscovery, largely apply to real-time communications conversations and chat threads just as they do to email records. Companies need to be able to "connect the dots" for all types of electronic communications, particularly when the installation spans multiple sites.

Leakage of intellectual property and other key proprietary information - In the same way that malware can hop across peer-to-peer connections unchallenged, proprietary information can be transferred, redirected, or hijacked both inside and outside the company networks using unmonitored real-time channels.

Insight and control - Communications that can't be seen can't be monitored. Unverified identities such as "buddy names" prevent appropriate corporate policies from being applied to greynet communications, and the port-hopping behavior exhibited by these applications renders simple blocking controls unusable.

The use of unmanaged greynets creates the possibility for each of the risks mentioned above to occur, regardless of whether or not end user systems are connected to the corporate network or the Internet.

The Growth of Greynets

Greynets are now virtually everywhere in the corporate business computing environment. More than 90% of enterprises have public instant messaging (IM) use at rates that are approaching 50% desktop penetration (source: Osterman Research). More than 70% of the enterprises surveyed by FaceTime have peer-to-peer (P2P) file sharing applications (including Skype) running on their networks.

Greynet applications are adopted directly by end-users who install them in a "download-and-run" manner and, once installed, they bypass corporate security and allow users to evade established rules and network use policies. Regardless of IT corporate edicts against unauthorized downloading of software onto PCs, either for business reasons or to prevent unintended "drive-by downloads" greynet applications are part of the landscape of modern enterprise networks, or IT needs to be able to control and secure their use.

It is important to consider the motivations behind greynet use to understand what drives this explosive growth:

Instant Messaging and VoIP	Private communications, collaboration and productivity
P2P Networks	Multimedia entertainment and efficient data transfer of large files (e.g., software images)
Web Conferencing	Sales meetings and collaboration
Blogging and Webmail	Private unmonitored online communications

Instant Messaging

Public instant messaging (IM) is one of the fastest growing greynets today. The rising adoption of IM is fueled by the community effect inherent in IM networks. What started as a way for consumers to stay in touch online has evolved into a business-critical application that links vendors and customers together in revenue generating relationships. Four networks (AOL, MSN, Google, Yahoo!) dominate the public IM scene but there are over 600 smaller IM networks and clients. Many of these variants aggregate connections to existing IM networks, giving users the ability to log in to multiple networks with a single client application (notable among these are Trillian and the open source application GAIM).

Voice Over IP (VoIP)

Another greynet application that has shown unprecedented growth is Skype, which is built on a proprietary peer-to-peer protocol and now delivering versions specifically tailored for the corporate user:

- Peer-to-peer communications service offering voice, video and IM
- Numerous features – encryption, audio/video conferencing, file sharing
- Growing library of third-party applications
- Able to traverse NAT
- Proprietary protocols
- PSTN connectivity via SkypeIn /SkypeOut
- No central server architecture
- Based on client nodes & super nodes
- Windows, Mac, Linux, PocketPC OS support

Skype is particularly seductive to the corporate user because it is:

- Flexible – you can access Skype anywhere there is Internet connectivity
- Presence – IM coupled with voice (are you there, can we talk?)
- High quality calling using wideband codec
- Free video capabilities

Not unsurprisingly, Skype is quickly becoming valued as a communications tool for businesses with remote offices, teleworkers, and distributed sales forces. Low cost telephone calls make Skype especially attractive in geographies where flat rate telephony plans are not the norm (e.g. AsiaPac and EMEA).

The Web has become the largest application to embody all the elements of the greynet concept.

While Skype is a very attractive collaboration application, it also presents new risks to IT departments. The Skype infrastructure cannot be integrated with IT control mechanisms. Corporate authentication and identity management are not supported. Bandwidth utilization cannot be managed for Skype users, and malware writers are making use of its open architecture. Even detecting which systems are Skype-enabled is difficult because the underlying network protocol is proprietary and evasive:

- With its P2P underpinnings, Skype connections are made to an infinite set of destination IP addresses (they appear to be “random” from the perspective of a network traffic analyzer).
- The Skype data payload for voice, instant messages, and file transfers is encrypted and therefore cannot be examined for policy violations.
- The Skype client does not conform to application policy management frameworks that are included in other enterprise class applications (e.g. Active Directory or other software usage and application policy managers).

Additional ‘red flags’ for IT in addressing the proliferation of Skype installations throughout their organization include:

- Skype was developed by the people who brought the world the Kazaa peer-to-peer adware network
- Skype encrypts all chat and voice traffic
- Skype keeps multiple connection channels open at all times, enabling it to port-hop at will
- Skype is **specifically designed** to bypass firewall and gateway controls

Web Browsing

The Web has become the largest application to embody all the elements of the greynet concept. It is the richest source of information ever assembled and at the same time it contains content depicting the darkest elements (images, viruses, etc) of the human experience. Web browsing in the corporation usually happens in a manageable context. In most cases, browsers connect to sites over well known ports (eg. port 80) and through approved network elements such as a firewall or proxy server.

Many corporations deploy URL filtering tools on these devices to monitor or restrict HTTP access to categories of content that may be deemed inappropriate—such as pornography. These same solutions are sometimes used by foreign governments to restrict and censor access of entire nations (nationalized ISPs). In both cases, the end user is confronted with restricted access. To counter this set of HTTP controls, many software applications have focused on providing tools that circumvent this monitoring (sometimes called “censorware”).

As an example: TOR is an application that was written explicitly for this circumvention purpose (<http://tor.eff.org/>). TOR is an “onion router”—a network layer software shim that encrypts and re-routes application traffic in order to disguise it and bypass restrictive policies and monitoring. This means that any web browser coupled with TOR (or any similar tool) becomes an evasive greynet application. It bypasses corporate security controls and exposes the organization to risk.

Peer-to-peer File Sharing in Business Networks

P2P is not just a consumer phenomenon. It is being installed by end users on business PCs and running over corporate networks. A recent survey by AssetMetrix & the RIAA found that 77% of all businesses in North America had P2P file sharing installed and running in their networks. On average they found almost one in ten desktops had P2P applications installed.

Because P2P networks are installed on local client machines and link directly to the Internet, those client machines are wide open to any Internet-borne security threat. The protocols used by these applications are stealthy, often tunneling undetected through open ports. Over and above the potential for productivity loss and bandwidth and storage resource abuse through employee usage of unauthorized software, P2P networks like Skype can:

- Open up back doors into the network, allowing hackers direct access to corporate assets and putting the organization in breach of privacy legislation
- Enable the exchange of copyrighted material under cover of encryption, rendering the corporation vulnerable to breach of copyright lawsuits
- Overload network bandwidth with unauthorized file sharing activities
- Allow bundled adware applications to be installed on the network without the user's or IT's knowledge

Given the seriousness of the risks and the potential damage to the organization that accompanies the uncontrolled use of P2P networks, IT departments need a powerful tool that will enable the productive use of P2P while protecting against their intentional or unintentional abuse.

At first glance, there does not seem to be any legitimate use case for P2P in corporate networks. However, P2P has advantages that apply to business applications as well. Because P2P file sharing is fully distributed, it does not require an expensive central infrastructure. The new economics of P2P networking mean that it is also used increasingly as an efficient digital distribution channel for legitimate purposes. These applications include:

- Distribution of OS software images (e.g. the DVD image of popular Linux distributions like Fedora Core are too big to transfer over traditional means such as email or disc)
- Broadcast feeds for RSS syndicated content (e.g. Podcasts)

**Legitimate vs. Malicious
Use of Greynet Applications**

Bittorrent, for example is a widely used P2P application, and it has already made a huge impact on the media industry, ISP networks, and software distribution models. Because of its unique properties, Bittorrent is an efficient way to distribute very large files.

Again, Skype is another P2P application that provides legitimate use scenarios for business users. While Skype does not conform to typical IT deployment and management norms, it is arguably the most cost effective voice and data collaboration tool in mass distribution today. As noted earlier, it is no longer realistic for businesses to block all forms of P2P and other real-time communications. At first, there will be a few exceptions for “power users” and special business cases. Then legitimate P2P will spread to a broader user base as application scenarios proliferate. P2P greynets offer a good example of how the line blurs between bad and good; black and white.

Application	Business Value	Corporate IT Threat
Public Instant Messaging (such as AOL or YAHOO)	Real time communications with business partners, customers and colleagues increases productivity, reach, and service levels.	Most rapidly adopted communication tool in history. Viruses and worm infections and other spIM threats to grow to 17.9 billion messages in 2008.
P2P File Sharing	Download large files quickly (e.g. OS updates).	P2P file sharing is predominantly used for illegal “swapping” of copyrighted materials. Viruses, spyware and other malware are distributed as trojans in many of these files.
Web Conferencing	Real time collaboration with business partners, virtual teams and customers. Increases productivity, reach and service levels.	Most web conferencing use occurs in an unmanaged state. The IT and compliance department do not have access to inspect content nor do they control how users identify themselves to external parties when they are using web conferencing.
Web Browsing	At-your-fingertip research and commerce for business efficiency.	Largest vector of spyware infections.

Security and Compliance with Greynets

Greynets are innovative and use an ever-evolving set of unanticipated actions to circumvent the security infrastructure.

Greynets have one common starting point: they all try to avoid detection. Greynets are innovative and use an ever-evolving set of unanticipated actions to circumvent the security infrastructure. Legitimate and responsible use of many of these applications is possible but it is important to note a few things that apply:

- Greynets are evolving in “Internet time” while security infrastructure is being adjusted in “fiscal time.”
- Greynet development is being funded by large, profitable, public companies.
- The technology base for greynets is expanding rapidly.
- Greynets were not designed for IT and greynet developers are not beholden to IT.
- Greynets are designed to connect by evading IT security.

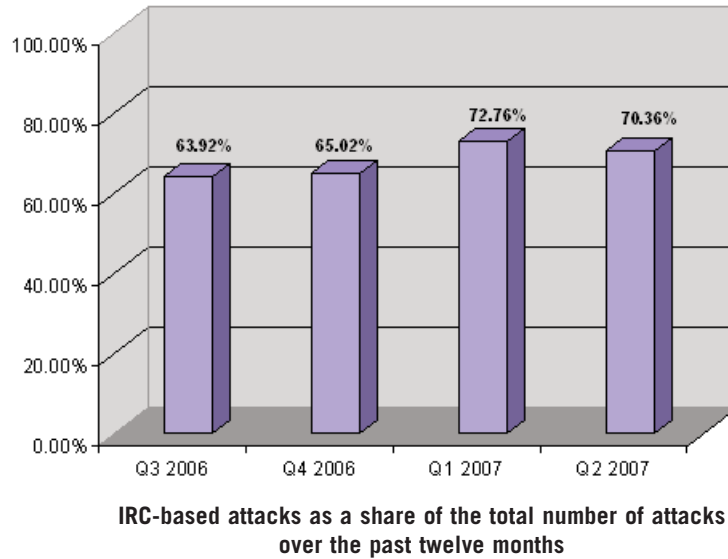
It is important to note that all applications have inherent risks. Perfect code is nearly impossible to find, so every new application in an environment should be handled with care. Greynets are complex interconnected applications. They introduce new variables into the IT security equation and this additional complexity is the enemy of good security. Greynets introduce new untested and uncontrolled code segments onto hosts and into the LAN environment. These applications are both interconnected internally and externally connected to other instances of the same code and/or to services running even more code. Frequent vulnerabilities have already surfaced in greynet host applications.

If these greynet host applications can be compromised, their network connectivity can create a spanning vector for the distribution of malicious code. This has been demonstrated with IM worms (e.g. Funner, Kelvir, Bropia). This external connectivity can also be used to leak proprietary information.

How a Greynet Can Wreak Havoc

The risks posed by unmonitored adoption of greynets do not depend on bad employees or malicious actions by those employees. Take for example the rise in the number of IRC-based attacks as a share of total attacks (See Figure 2). Suppose that all of the users in that setting are acting responsibly and according to corporate policies. Everything is going well until a new IM borne worm/virus breaks out. The worm attacks systems with up-to-date virus signatures, steals and corrupts local data, and transmits sensitive data to the attackers. If this worm were spreading on the corporate email system, it would be possible to isolate it quickly and shut down the vector of transmission. If this worm were spreading over IM networks, it would be nearly impossible to isolate it and shut down.

▶
Figure 2
IRC-based Attacks
Reported by FaceTime
Security Labs



This further illustrates that, despite all that is good about public IM services and new P2P applications from the perspectives of productivity, communication, and collaboration, there is a darker side. The same is true of other greynets. The only possible conclusion is that greynet adoption in the enterprise poses a number of security risks. To underline this, here are some statistics from FaceTime's most recent (Q2 2007) greynet security research survey:

- A total of 317 security incidents targeting IM/P2P channels were reported during Q2 2007, bringing the total since Jan. 1, 2007, to 618 incidents.
- Overall, the MSN network accounted for 50 percent of the attacks on the major networks, followed by Yahoo at 30 percent and AOL with 20 percent.
- Attacks spread via Internet Relay Chat (IRC) continue to account for a growing percentage of all attacks, rising in each of the last six quarters, from a 59 percent share in Q1 2006 to 72 percent in the current quarter.
- Similarly, multi-channel attacks—security incidents that propagate via multiple vectors, such as AOL, Yahoo or IRC—now account for over a quarter of all attacks.

Greynt communications in the enterprise environment also pose significant regulatory compliance and policy risks. This exposure spans numerous industry verticals and regulatory environments including SEC, NASD, HIPAA, FERC, SOX, and DoD regulated entities.

While innovative tools like Skype are providing real benefits to users and businesses, it is unfortunate for IT managers that Skype is a closed and proprietary grey network. This means that, once adopted by users, it cannot be controlled by IT. Users create their own identities and personas in the Skype network. All Skype traffic is encrypted and cannot be monitored or audited. File transfers over Skype cannot be scanned for viruses or checked against corporate policies (e.g. file size, type, extension.).

Challenges in Detecting and Managing Greynets

More than 90% of all enterprise environments tested by FaceTime are vulnerable to greynet security risks.

More than 90% of all enterprise environments tested by FaceTime are vulnerable to greynet security risks. These environments lack the tools to detect and apply consistent policies regarding application distribution and use. Even now these include some of the largest and most secure corporate and government network environments in North America.

Readers may wonder how these applications became so prevalent in private networks— or why they are so hard to control. The simple answer is that the tools and infrastructure in most enterprises have fallen behind the innovation curve of greynet developers.

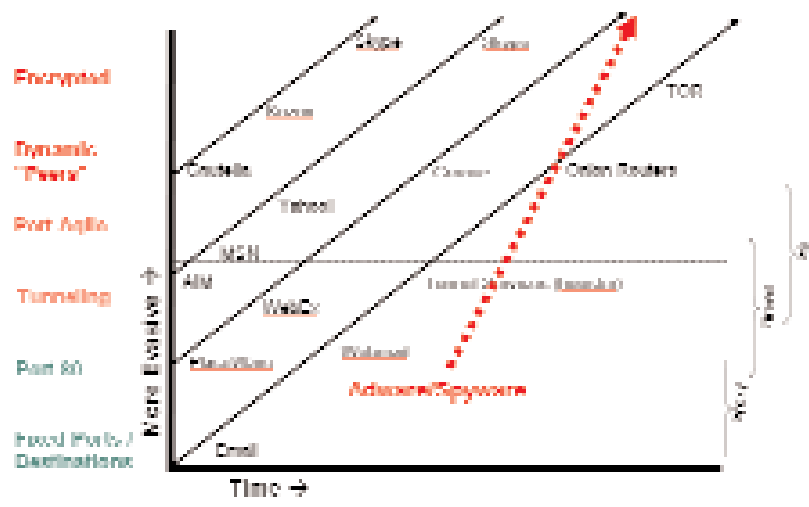
Greynets Are Becoming More Evasive

P2P application developers are leading innovators in the charge to create “private and invisible” network applications. P2P content distribution makes economic sense and represents the current state of the art in greynet development. The evasive nature of P2P is in the user’s interest because anonymity is especially appealing when a user does not want to be seen using the application in question (e.g. illegal file sharing). Experts note that P2P users actively migrate between applications based on the reputation for maintaining the privacy of their users:

- P2P overlays are here to stay: they will be used by more greynet applications because P2P offers huge cost advantages vs. traditional download distribution models. For example, podcasting combines independent audio programming with RSS to create Internet radio programs that users can subscribe to and listen to anywhere they choose. The podcaster’s RSS syndicated mp3 files are distributed over P2P using Bittorrent functionality.
- Greynet traffic is encrypted because encryption offers privacy and security to users (although not to the network on which it is traveling).
- All greynet applications adopt evasive network behavior because it allows the applications to work whenever and wherever users want them to, regardless of whether IT or ISP administrators are attempting to block or limit them.

The evasive trend in P2P networking has taken hold more generally across all greynet applications. As other greynets are targeted for control and management by corporate and ISP network administrators, they will adopt the evasion techniques of the P2P applications and become increasingly harder to detect at the network level (See Figure 3).

Figure 3
 Greynet Applications Are
 Becoming More Evasive



Malware infections increase with the proliferation of greynets

Greynet Management—Requires Defense in Depth

Effectively managing greynets requires a multi-layered investment in both technology and business practices. IT needs to start by implementing coherent policies and developing education programs for promoting awareness. Then there are the infrastructure investments necessary to provide end-to-end control and security.

Managing PCs (Software Restriction Policies)

Controlling host systems in large environments can be a daunting task. While many organizations have the means to push out and add software to the desktop, few are able to strictly limit what is installed and executed on end user machines. Even where strict policies are enforced, exceptions are made and holes exist. Most of the popular greynet applications do not require administrator access to the host to be downloaded and installed. Others use Java or browser-based access. Different techniques are required for managing software proliferation at the desktop.

Blocking at the Perimeter

Most enterprise environments have adopted a “best-of-breed” mix of security infrastructure. Firewalls, application proxies, and Intrusion Prevention Systems (IPS) may appear on the surface to be enough to filter out undesired greynet usage. Unfortunately, using these tools to detect and control greynets at the network perimeter is nearly impossible because greynets are specifically designed to exploit known structural gaps in that infrastructure.

▶
Structural Gaps in Existing Solutions

Network Elements	Intended Purpose	Security Risks
Firewalls	Manage flow by address, port and flow direction	<p>Greynets use any available open port</p> <p>Greynets do not have fixed address destinations</p> <p>Greynets initiate connections from the inside out; firewalls are generally more permissive/porous</p>
Proxies	Manage protocol adherence and enforce policies having to do with black-listed or white-listed destination addresses (e.g. no browsing www.playboy.com)	<p>Greynets mimic valid applications at the protocol level</p> <p>Greynets change their network address schemes faster than blacklists can be updated</p> <p>Greynets use P2P connection overlays that utilize an infinite set of destinations to conceal where they are going</p>
IPS	Scan packets looking for matches against static signatures (e.g. text strings in packet headers or data payloads)	<p>Greynets connect to an infinite, always changing and seemingly random set of destinations making the IP destination information in packet headers useless</p> <p>Greynets conceal their data payloads with proprietary encryption schemes</p>

Monitoring and managing greynets requires different tools and a different approach. FaceTime Communications has been leading the field in enabling businesses to secure and control greynet applications since 1999.

Our dedicated research team, FaceTime Security Labs, has led to significant breakthroughs in delivering a defense-in-depth solution to secure and enable greynets. Here are just a few recent discoveries by the dedicated team at FaceTime Security Labs:

March 28, 2007: NetBrowserPro, a Web browser, promises secure porn browsing, but installs a rootkit and a Trojan called MovieCommander. MovieCommander is disguised as a fake media codec. A rootkit is a set of tools intended to conceal running processes, files or system data from the operating system. When the user installs the NetBrowserPro from Browsezilla.org with the 121.exe file, they agree to allow the program to update and modify itself without notification and have third party applications interact with the browser. Many of the photo galleries linked from the browser will redirect the end-user to an unintended location, which is potentially a security threat.

March 13, 2007: A Trojan named Symfly may influence Alexa Web traffic rankings for several Chinese Web sites. The Symfly Trojan downloads and installs multiple files to an infected PC, primarily via HTTP. The daisy chain of installations includes the Trojan Adcheat and can install an Alexa Toolbar from Renwu.info without user consent.

October 3, 2006: A new threat targeting Yahoo! Messenger users known as the w32.KMeth worm. The new threat sends users to a Web site serving a barrage of Google AdSense advertisements related to mesothelioma, a rare cancer caused by exposure to asbestos. Because of its relation to toxic tort litigation, the cost-per-click for the keyword "mesothelioma" is one of the highest in the online advertising pay-per-click market, making it a prime target for financially-motivated malware writers. Systems are set up by these cyber-rogues to funnel traffic through illicit means, generating clicks on high-paying keywords to produce higher returns on established advertising commissions.

Conclusion

Today greynet applications are deeply embedded in the computing structure of corporate networks where they offer significant business benefits, but at the same time represent new vectors for threats. Because of their highly evasive nature, greynets have evolved into a parallel application network overlay that IT can't see, can't manage, and can't control. Existing security infrastructure provides little more than a comfort blanket. IT success in the era of greynets will be defined by those who understand how these new technologies operate, and deploy defenses that are designed to stop them.

FaceTime (www.facetime.com) is dedicated to researching and developing products that give IT the tools needed to effectively manage and control greynets.

About FaceTime Security Labs

FaceTime Security Labs is the industry's largest research team dedicated to the collection, analysis, understanding, and management of threats generated through the intentional or accidental use of greynet applications such as P2P file sharing networks, IRC, and instant messaging. With facilities in the United States (West Virginia and California), the United Kingdom, and India, FaceTime Security Labs employs dozens of dedicated researchers and supports a global community of concerned individuals who contribute their own experiences to the research effort. FaceTime Security Labs provides the foundation for complete instant messaging security and spyware prevention strategy, delivering detailed information about known threats that enable organizations to:

- Block P2P network use that could breach corporate security policy
- Prevent spyware from being accidentally or intentionally downloaded by users
- Secure instant messaging against worms, Trojans, malware and rootkits
- Remain in compliance with data privacy and information security legislation

The Labs also power the patent-pending inoculation and targeted remediation capabilities that keep clients spyware-free. FaceTime Security Labs underpins FaceTime's Defense-in-Depth spyware prevention strategy, delivering detailed information about known threats that enable the blocking of spyware distribution sites as well as powering the patent-pending inoculation and targeted remediation capabilities that keep clients spyware-free.

FaceTime Security Labs also maintains the popular **SpywareGuide.com** site, the leading public reference site for spyware research which provides details about spyware and adware applications, their known variants, and their behavior through an extensive and continually updated database. The site also offers a wealth of information to enable both IT professionals and home computer users to educate themselves on the problems and risks associated with spyware.



FaceTime Communications, Inc.

1301 Shoreway Rd, Suite 275 • Belmont, CA 94002

Toll Free	888.349-FACE (3223)
Phone	650.631.6300
Fax	650.598.2820
General Info	info@facetime.com
Sales	sales@facetime.com