

Greynets in the Enterprise

Third Annual Survey
of Greynet Trends, Attitudes
and Impact

FaceTime®

INTRODUCTION

Corporate networks are increasingly seeing traffic from a class of applications that FaceTime has identified as “greynets”. These applications have two key characteristics: first, they are installed by end users—who often do so while acting outside the purview of corporate Information Technology (IT), network or other computer-related departments.

Second, greynet applications use evasive techniques to traverse the network. Greynet applications may use proprietary protocols, encapsulate packets inside other protocols, and sniff for open ports on the network. Greynet applications include instant messaging (IM), peer-to-peer (P2P) file sharing, web conferencing and other more-or-less well-behaved collaborative applications.

IM	
ANONYMIZERS	
WEB CONFERENCING	
FILE SHARING	
VIDEO STREAMING	
VOIP	
WEB BROWSING	

The greynet application category also includes adware and spyware, which may install themselves without the explicit knowledge of end users. Other greynet applications—notably, IM and P2P file sharing--may serve as vectors for network infestation of viruses, Trojans and worms.

This research study, the third in a series commissioned by FaceTime, explores these greynet applications in order to understand their impact on corporate networks and corporate security.

METHODOLOGY

FaceTime commissioned NewDiligence, an independent market research company, to design and conduct a study of “greynet” applications—including both collaborative and well-behaved software as well as spyware, adware and other malware.

The survey was conducted among representative samples of corporate IT and IS managers and among computer end users. The samples were generated from purchased lists supplied by independent brokers as well as customer and contact lists supplied by FaceTime. List members were contacted by NewDiligence via email and invited to participate in an online survey.

Respondents were offered the chance to win one of five iPods, as an incentive to participate in the research.

FaceTime was not identified as the sponsor of the research, nor was its name or likeness used in any communication with respondents.

Field dates were between August 13 and September 17, 2007. Final respondent counts included 737 IT managers and end users. NewDiligence was independently responsible for all data collection, handling and analysis.

GREYNET USAGE

Pervasive and widespread use of greynets in the workplace is the norm. Currently, 86 percent of all end users report using one or more greynet applications on their work computer, up almost ten percent in the last two years. Moreover, end users are aggressively adopting greynet applications: based on stated adoption plans, application usage will soar. About 77 percent of end users, up from 68 percent in 2006, intend to try one or more of the 19 greynet applications measured in the study. As a result, the greynet usage rate will climb to 94 percent of end users in the next six months.

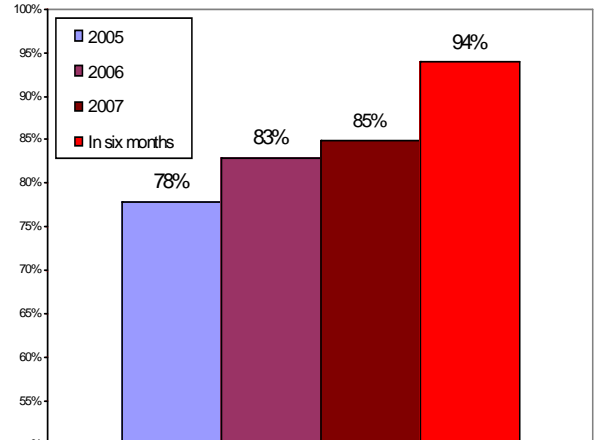
The most commonly used greynet application is for streaming media—either audio or video—reported by 80 percent of end users. Communications tools are also quite common: Web-based email, Web conferencing and public-network Instant Messaging (IM) each have upwards of a 70 percent share of desktops.

IT managers are aware of extensive greynet application usage at their work locations: 99 percent of them report one or more greynets found on user desktops.

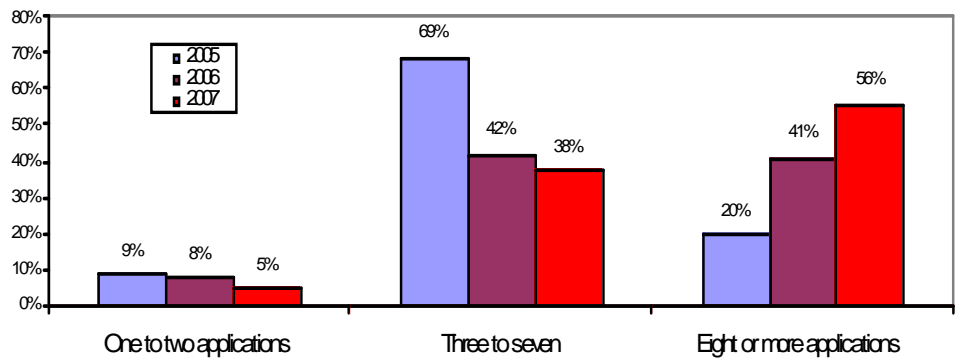
In the last three years the average number of greynets in use has climbed considerably.

The proportion of sites with only one or two greynets in use is in decline. At the other end of the spectrum, sites with multiple applications in use have almost tripled in three years.

End user Adoption of Greynets



Number of Greynet Applications In Use



Currently, sites with eight or more greynets installed, as reported by IS, account for 56 percent of all sites. In 2005, only 20 percent of sites reported such high greynet installation rates.

INFLUENTIAL FACTORS

What accounts for these high adoption rates? Among the main contributing causes is simple *popularity*, end user *attitudes about work and unsecured environments*.

Popularity

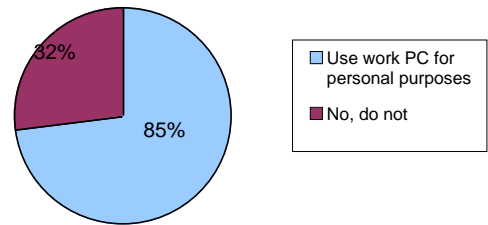
Greynets have a strong viral component and typically exhibit network effects. The more users of a given service, whether IM, file sharing or Digg, the more value the service produces for each individual participant.

For example, the “top tier” of greynet applications deployed is comprised of communications tools such as email, conferencing and IM. Each has network-effects and many implementations have viral qualities that promote the service to other end users.

The influence of sheer popularity may be seen in the second tier, which includes Google toolbars, social networking sites and services, as well as Web 2.0 media like Wikis or RSS.

The Google desktop toolbar, only a few years old, is now found on 56 percent of end user PCs. It is a testimony both to the positive brand halo that surrounds Google as well as the rapidity with which a greynet application can propagate through the end user community. Facebook, MySpace, Digg and other social networking greynets have similarly rapid growth patterns.

While these services may be innocuous for the most part, each also has the potential to expose the corporate network by acting as a conduit for malware infestations from the Internet. Each of these applications typically works its way around corporate networks, using a variety of protocols and any open port to send and receive bits from external sources.

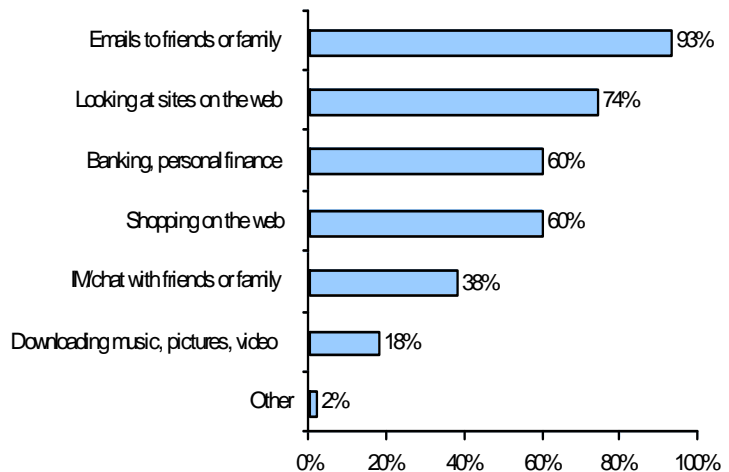


Attitudes About Work

For more than a decade now, personal and workspaces have blurred. For knowledge workers, it is as common to do work at home as it is to conduct personal tasks while at work. In fact, 85 percent of all end users use work PCs for personal purposes.

The personal use of work computers is independent of company size. Across the board, approximately eight in ten employees will surf, shop and chat over the company network, testimony to the continued blurring of personal and professional workspaces.

Not surprisingly, the most frequent activity is sending emails to friends and family. Corporate employees can also be commonly found “looking at interesting sites” on the Web, banking, shopping, chatting and downloading music, photos and video.



In FaceTime's previous two annual surveys, employees candidly proclaimed their belief that they have the right to download the applications they need onto their work PCs, regardless of whether or not those applications are sanctioned by IT. This trend continues, with 36 percent of employees proclaiming this right in this year's survey. In addition, 40 percent of employees said that they need more applications than are typically installed on their work PCs.

This trend underscores the need for IT management to work more closely with employees both to understand changing workplace needs, as well as to educate the workforce on security and compliance issues facing the organization.

Unsecured Environments

Securing the corporate network first requires policies that govern how PCs, the Internet and the Web are to be used by employees. However, fewer than half—45 percent of employees—are at work locations where personal IM messaging is monitored by the organization.

Even where such policies may exist, the IT staff is not brimming with confidence: while 41 percent agree that end users generally "comply with corporate Internet policies", the remaining 59 percent are somewhat less optimistic.

While some greynets such as Skype, IM and Web Conferencing have legitimate business uses, IT needs visibility and control over all network traffic to ensure safe and productive use. Other greynets, such as P2P file sharing, video streaming, and anonymizers, can pose further consequences to the organization. All real-time collaborative applications can be evasive on the network, often circumventing the traditional security infrastructure that was designed for email and standard Web traffic.

It is therefore not surprising to discover that 64 percent of IT managers agree that IM and P2P are "extremely risky" for their company networks. Further, only half (50 percent) believe their network security setup provides "effective methods" to block or filter IM and P2P traffic as needed.

Employees don't always see eye-to-eye with IT management regarding risky behavior on the network. For example, eight in ten IT managers find anonymizers – applications that disguise traffic to permit anonymous use of the Internet – risky to corporate networks. In contrast, just more than half of users (57 percent) find them to be risky, for a 19 percent differential in risk assessment.

The bottom line is that greynet usage makes IT nervous: 40 percent of IT managers report that public IM use at work poses "serious risk," while another 46 percent indicate that IM poses "some risk," for a total of 86 percent of managers who are wary of the public IM networks and their impact on the work environment.

IMPACT OF GREYNETS

In spite of the various security solutions that IT managers have deployed within their enterprise networks, and in spite of whatever corporate policies are in place, nine in ten IT managers have still experienced a greynet-related security incident in the last six months. In fact, only about three percent have avoided greynet-related security incidents during this period.

IT managers were asked whether, as a result of greynet usage at their work locations, the network had endured successful installations of any kind of malware: spyware, viruses, rootkits or bots (asked in 2007 only).

Each type of incident has increased in frequency from 2006 to 2007. Both the spyware and the virus incident category show seven percent increases in reports of one or more work location attacks, year-on-year.

The survey also shows that the average cost companies incur in recovering from greynet-related incidents on company PCs has doubled over last year. IT managers reported spending an average of about \$289,000 annually to repair or re-image company PCs after malware attacks. The cost reported in last year's study was nearly \$130,000 per year. On average, IT managers experience nearly 39 incidents per month that require some kind of repair or remediation to end user PCs and each repair requires, on average, nearly 10 hours of work.

