



Real-time Communication Vulnerability Assessment Report

RTDiscover Evaluation Detailed Report

For

Acme Corp

August 2007

Prepared By: FaceTime Representative, Sales Representative

Tel: 650-631-6300, Email: FTRep@facetime.com

FaceTime Communications, Inc.
1301 Shoreway Drive, Belmont, CA 94002
(888) 349-FACE (3223) toll free, (650) 631-6300 phone, (650) 598-2820 fax
www.facetime.com

Executive Summary

Instant messaging (IM), Skype, Web conferencing and other real-time communication and collaboration tools are becoming required elements for strategic and competitive advantage in today's fast-moving enterprises. The productivity benefits reaped from the use of these tools have dramatically expanded the use of these applications in many organizations.

While frontline productivity is benefiting from the use of these channels, the back-end security risk is increasing, with the potential to more than cancel out the productivity boost. Because these 'greynet' applications operate below the radar of traditional information security measures, their existence and use is frequently invisible to IT departments. Taking advantage of this situation and the fact that enterprise email installations are generally well-protected, hackers and malware purveyors have shifted their channel of operation to the greynets. Consequently, the widespread and uncontrolled use of real-time communications tools has brought new risks for malware infection, loss of intellectual property, falling out of compliance with government regulations and more. They need to be monitored, controlled and managed to ensure the security of your business.

To assist Acme Corp in assessing the extent of and security risks posed by real-time communications usage by employees, FaceTime has deployed its Real-Time Discover (RTDiscover) application to detect all IM, P2P and spyware traffic traversing the company's networks. This report provides a detailed review of the results of this deployment, together with FaceTime's recommendations for Acme Corp to improve the security of its real-time communications.

Key findings of the discovery process are:

- 613 users were accessing public IM networks
- 117 users were using P2P applications
- 116 instances of spyware infections were detected



Table of Contents

- Executive Summary..... 2**
- Corporate IM and P2P Security Concerns..... 4**
- Real-Time Discover..... 5**
 - The Discovery Process 5**
 - RTDiscover Vulnerability Assessment Results Summary 5**
 - Real-time Communications Traffic 6**
- FaceTime Solutions Overview..... 11**
- Common Questions and Answers 13**
- Summary..... 14**
- About FaceTime 14**
- Appendices..... 15**
 - I: Spyware Danger Level Ratings..... 15**

Corporate IM and P2P Security Concerns

The ability to communicate in real-time is becoming a core requirement of 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.

Adoption of Enterprise Instant Messaging (EIM) is proceeding apace - Gartner estimates that 30% of enterprises have already deployed some form of EIM, with 100% adoption expected by 2010. 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; it is 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 number of EIM deployments, users are still accessing 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 public IM network connections 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.

Most enterprises today have taken steps to ensure that their email systems are secure and compliant with the relevant data protection and privacy legislative mandates. But a recent InformationWeek survey of 325 business technology professionals found that 87% erroneously believed real-time communications to be secure. Instant messaging is the first and still the major hole in this worrying scenario.

While email communications are routinely scanned for malware, IM is enabling malware to hop from public to enterprise networks. And not only are more attacks entering the network over IM 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 IM and other real-time communications channels. A recent survey conducted by a British security software company found that 30% of US workers have discussed business-related issues over social networks.

Compliance regulations - SOX, HIPAA, SEC, eDiscovery rules, and others - largely apply in the same way to IM and other digital 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 - public and enterprise.

Securing, managing, and controlling these communications channels is a corporate imperative. Instant messaging has 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.

Real-Time Discover

The Discovery Process

Understanding the extent of spyware activity and unauthorized IM and P2P use over your network is the first step in charting a course of action to implement controls and protect your enterprise. Until you know the scale of the greynet problem in your organization, you can't even begin to chart a plan to control it.

The RT Discover process that enabled this report is designed to give you that initial level of insight into the levels of spyware, IM and P2P activities across your networks:

- Gain complete visibility into spyware traffic on the network
- Obtain insight into bandwidth abuse, source and destination IP addresses, and port abuse
- Block the spread of spyware
- Identify spyware-infected PCs without desktop client software
- Prevent unauthorized IM and P2P connections
- Ensure safe and secure IM by blocking high-risk features
- Mitigate business and security risk

RTDiscover Vulnerability Assessment Results Summary

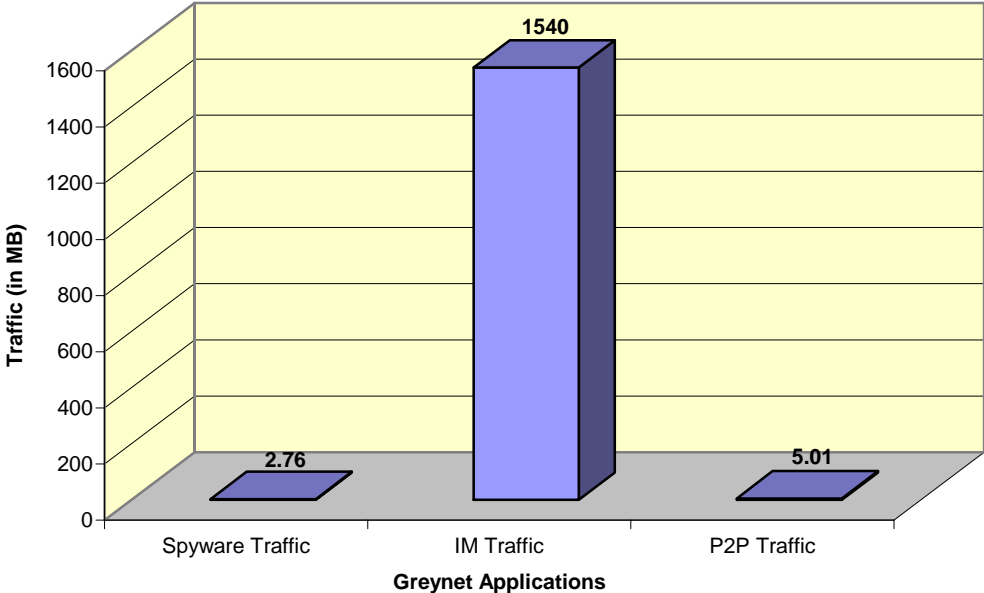
The RTDiscover process has revealed that Acme Corp has

- **613 users running public IM clients**
- **117 users running P2P applications**
- **120 individual computers infected with spyware**

This means that Acme Corp is vulnerable to a number of security problems, including compliance breaches through confidential information exposure, intellectual property issues, copyright infringement risks, computer/network slowdown, and system instability/crashes due to spyware infections.

Real-time Communications Traffic

Greynet Traffic Snapshot

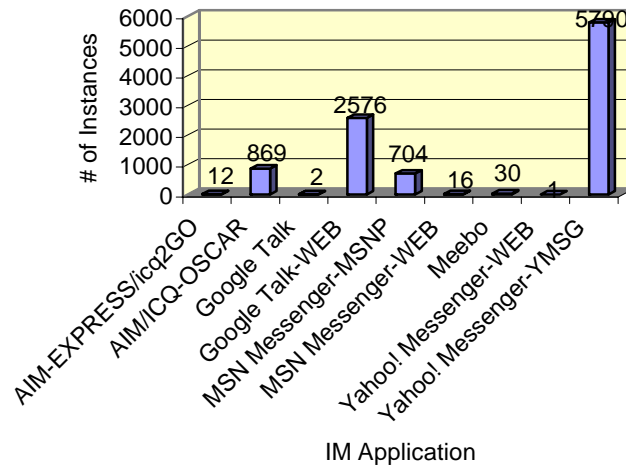


Traffic Type	MB Transferred
Spyware Traffic	2.76
IM Traffic	1540
P2P Traffic	5.01
HTTP Traffic	124060
Other TCP/IP Traffic	278540
UDP Traffic	5390

The chart above shows the different real-time communications applications running on Acme Corp network during the vulnerability assessment. None of these communications channels is visible to IT staff or information security personnel, because all are highly evasive, hopping around the network looking for open ports and not detected by your existing security infrastructure Risk Analysis:

IM Traffic Analysis

IM Traffic by Application



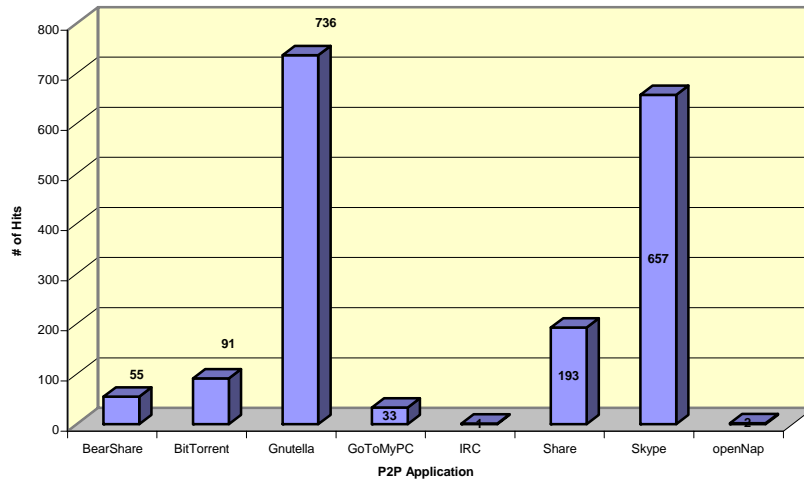
- 613 users are running public instant messaging clients such as MSN, Yahoo, or AOL, with the risk that company-confidential information may be leaving the network via file transfers or plain-text chat threads, and that malware-infected files may be entering the network via the same route.

Network	Number of Hosts
AIM-EXPRESS/icq2GO	5
AIM/ICQ-OSCAR	191
Google Talk	2
Google Talk-WEB	179
MSN Messenger-MSNP	114
MSN Messenger-WEB	3
Meebo	3
Yahoo! Messenger-WEB	1
Yahoo! Messenger-YMSG	307

Protocol Name	Number of Hosts
BearShare	1
BitTorrent	13
Gnutella	11
GoToMyPC	6
IRC	1
Share	45
Skype	50
openNap	1

P2P Traffic Analysis

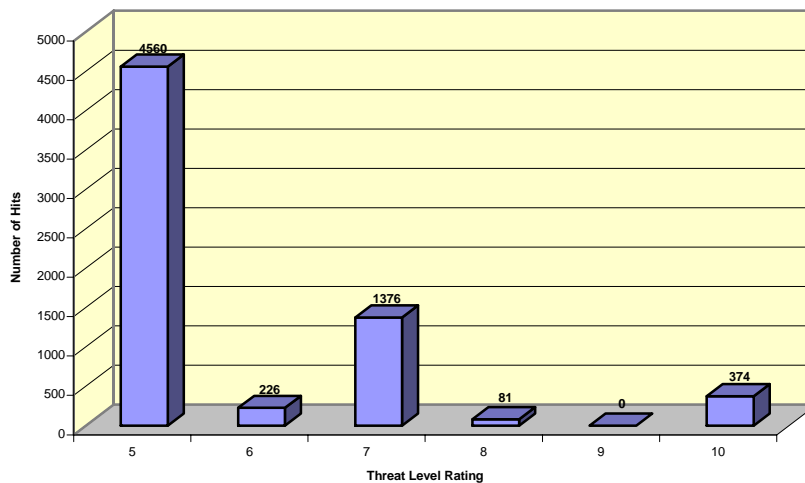
P2P Application Report



- 117 users are running P2P networks such as Skype and other VoIP programs and shared downloads, running the risk of copyright infringement in addition to the public IM channel threats outlined above.

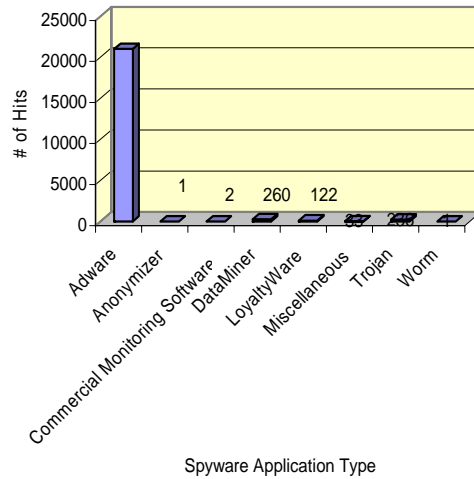
Spyware Traffic Analysis

Spyware Threat Level Index Analysis



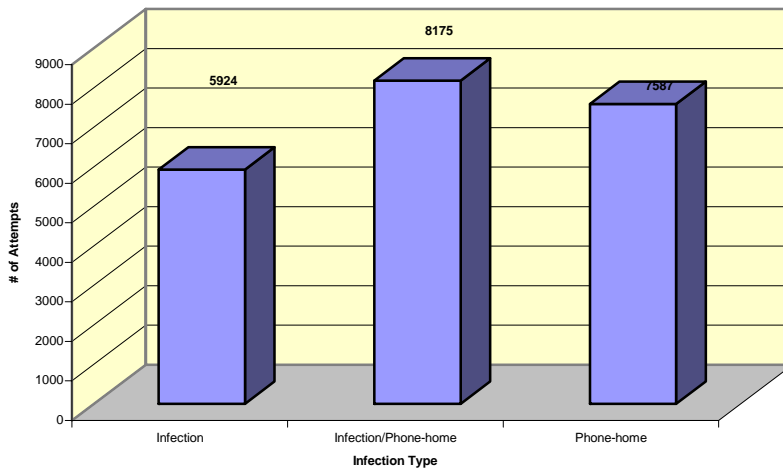
The chart above shows the spyware that was actively running on the Acme Corp network during the vulnerability assessment by threat level. While the lower numbers indicate a lesser threat, every spyware program running on the network is sapping productivity and opening the company to potential for compliance breach by not exercising due diligence in the protection of personally-identifiable information. A full explanation of the different threat levels may be found on FaceTime's SpywareGuide website at http://www.spywareguide.com/txt_dangerlevel.php, and further information on FaceTime's greynet research efforts and the FaceTime Security Labs is available at <http://www.facetime.com/securitylabs/securitylabs.aspx>.

21031
Spyware Hits by Application Type



- 21686 number of spyware attempts were made without the knowledge or permission of users or network personnel and which may be phoning home confidential corporate data to an external third party, putting the company in breach of compliance legislation as well as slowing network and system performance.

Spyware Hits by Infection Type



Product	Attempts	Category	Threat Level
Gator	75	Adware	0
SearchitBar	1	Adware	0
Viewpoint Media Toolbar	599	Adware	0
2020Search	4	Adware	1
Active Shopper	27	Adware	1
Alexa Toolbar	259	DataMiner	1
Aurora	64	Adware	1

Consumer Alert System	767	Adware	1
Coolbar	50	Adware	1
Coupon Bar	87	Adware	1
HotBar	6484	Adware	1
Kuaiso Toolbar	5	Adware	1
MSWsearch	5	Adware	1
Need2Find	14	Adware	1
OTXMedia	12	Adware	1
Search123	7	Adware	1
SpamBlockerUtility	425	Adware	1
The Cloak	1	Anonymizer	1
WhenU-DesktopBar	1817	Adware	1
Zango	11	Adware	1
CoolWebSearch	373	Adware	10
DownLoader-Adv	1	Trojan	10
Fake Delete	1	Adware	2
GameFiesta Toolbar	105	Adware	2
PopUpWithCast	40	Adware	2
Transponder.kz515	97	Adware	2
2nd-thought	5	Adware	3
Blowsearch	1	Adware	3
CINMUS	1	Adware	3
CmdService	97	Adware	3
Coolsavings	72	Adware	3
Covenanteyes	1	Commercial Monitoring Software	3
Deluxe Communications	1	Adware	3
Downloader-AB	17	Trojan	3
Drive Cleaner	7	Miscellaneous	3
E2Give	8	Adware	3
ILookup	3	Adware	3
IWon CoPilot	67	Adware	3
MakeMeSearch	4	Adware	3
MyFunCards	3	Adware	3
Netster	104	Adware	3
OpinionBar	12	LoyaltyWare	3
OverPro	12	Adware	3
PrecisionPop	5	Adware	3
Purityscan	51	Adware	3
QuickLinks	21	Adware	3
SearchMeUp	1	Adware	3
Sidesearch	235	Adware	3
TargetSavers	499	Adware	3
Top Moxie	94	LoyaltyWare	3
TrojanDownloader.Win32.Qoologic	83	Trojan	3
Webcrawler	1	Adware	3
WinFixer	22	Miscellaneous	3
Your Screen	85	Adware	3
Zeno Search Assistant	42	Adware	3
A Better Internet	106	Adware	4
BonziBuddy	794	Adware	4
CasinoRewards	1	LoyaltyWare	4
Commander Toolbar	13	Adware	4

Dogpile Search Toolbar	20	Adware	4
Ebates Moe Money Maker	15	LoyaltyWare	4
FlowGoBar	27	Adware	4
FreeScratchAndWin	11	Adware	4
Internet Optimizer	155	Adware	4
MarketScore	1	DataMiner	4
NaviSearch	3	Adware	4
PerfectNav	1	Adware	4
Powwabar	10	Adware	4
Starware Toolbar	1295	Adware	4
StealthWatcher 2000	1	Commercial Monitoring Software	4
Troj/Agent-CL	7	Trojan	4
WinAntiVirus	4	Miscellaneous	4
XPL	6	Trojan	4
YourSiteBar	76	Adware	4
BargainBuddy	6	Adware	5
CrackSpider	1	Adware	5
DollarRevenue	3771	Adware	5
Ezula	611	Adware	5
Popwin	50	Trojan	5
ShopNav	17	Adware	5
SpotOn	11	Adware	5
Windupdates	66	Adware	5
Winsync	27	Adware	5
DailyToolbar	10	Adware	6
Delfin Media Viewer	39	Adware	6
EliteBar	1	Adware	6
ISTbar	4	Adware	6
SurfSideKick	110	Adware	6
Tafbar	51	Adware	6
Trojan.rmass	2	Trojan	6
Zuvio	9	Adware	6
180 Search Assistant	349	Adware	7
Comet Cursor	905	Adware	7
New.Net	51	Adware	7
Troj.Activate_crack	70	Trojan	7
w32.Kmeth Worm	1	Worm	7
Websearch	81	Adware	8
NeededWare	12	Adware	Pending Rating

FaceTime Solutions Overview

Real-Time Guardian, the full-function appliance version of the RTDiscover software tool used to carry out this vulnerability assessment, is the most advanced perimeter security solution for blocking the spread of spyware in the enterprise and securing unauthorized IM and P2P usage. RTGuardian integrates with FaceTime's Greynet Enterprise Manager (GEM) and IMAuditor to form FaceTime Enterprise Edition, the leading solution for securing and managing all real-time communications channels.

With RTGuardian, organizations can:

- Prevent spyware from spreading across the network
- Block unauthorized IM and P2P connections

- Ensure safe and secure IM usage by blocking high-risk features
- Create a standardized profile of IM use within the enterprise
- Detect and manage Skype 2.0 in their network
- Ensure non-stop protection with the latest protocol updates
- Mitigate business and security risk
- Gain insight into bandwidth abuse, source and destination IP addresses, and port abuse

Add GEM to provide

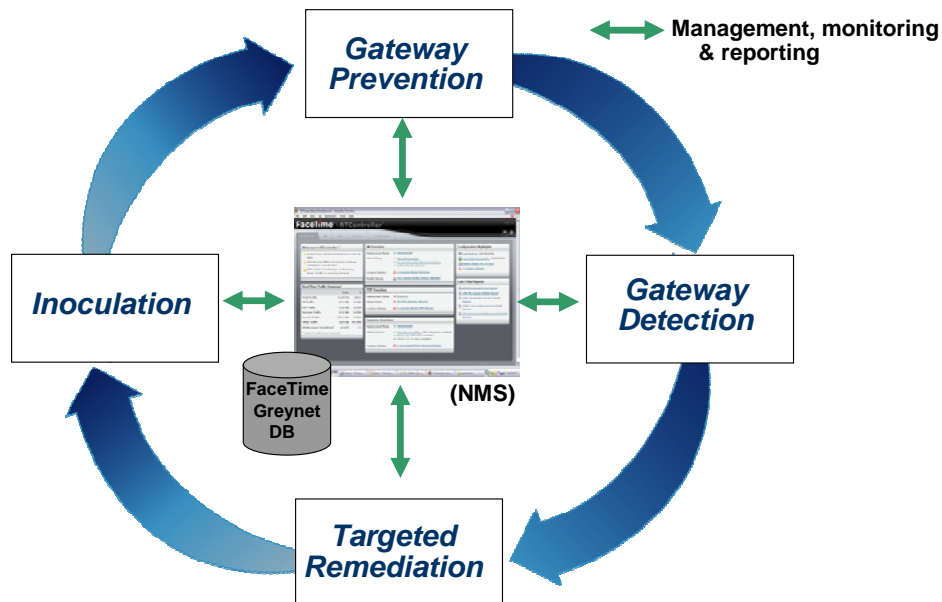
- Centralized management and reporting across distributed RTGuardian appliances
- Targeted remediation of spyware-infected endpoints

Together, these products deliver end-to-end security defenses for real-time communications networks:

- **Gateway Prevention**—Prevent infection by blocking user access to known spyware sites, stop installations of spyware across multiple channels
- **Gateway Detection**—Detect and block spyware on the wire, multi channel listening capability to prevent “phone home services”
- **Targeted Remediation and Inoculation** – Clientless remediation of infected machines and inoculation of endpoints to known spyware applications, freeze existing infections in place by cutting off OS resources

IMAuditor, a fully-featured IM proxy to secure and manage all IM use, can be integrated with RTGuardian and GEM to provide ongoing monitoring and audit trails to deliver the industry’s only guaranteed TrueCompliance™:

- Security across all major public, enterprise, and community IM networks
- Regulatory compliance workflow and archiving
- Integrates with existing security and storage infrastructure
- Flexible deployment solutions



The FaceTime Defense-in-Depth Model for Enterprise Spyware Prevention

Common Questions and Answers

What types of threats exist for unmanaged Instant Messaging?

Here are just a few examples of new threats uncovered by FaceTime security researchers:

- March 28, 2007: NetBrowserPro, a Web browser, promises secure porn browsing, but installs a rootkit and a Trojan. Hackers are increasingly creating fake browsers to deceive users and direct Internet traffic - with fake browsers and other adware, they can gain control of computers by tricking the user, instead of exploiting more complex software vulnerabilities. Users can also fall victim to data and identity theft or violations of privacy when using rogue browsers.
- May 22, 2006 - Unsafe "Safety Browser" affected Yahoo! Messenger clients. The first, and extremely inventive, instance of a self-propagating worm, named yhoo32.expl, installing a web browser to hijack the Internet Explorer homepage, leading users to a site that put spyware on their PCs.
- March 15, 2006: The "Carder" botnets collectively represented up to 150,000 compromised computers, which used a custom built PERL script to fraudulently scan desktop and back-end systems to obtain credit card numbers, bank accounts, and personal information including log-ins and passwords. The operators could potentially launch these scans from any computer on the botnet to mask their actual location. Relevant files and information on a large number of "at risk" credit card accounts were provided to federal authorities by FaceTime researchers.

There are new examples every day of IM threats that can cause significant disruption in your organization or steal your intellectual property or your personal information.

The only risk with P2P is the liability associated with unauthorized exchange of copyright-protected music... Right?

Not True. Where there is copyright breach, other security hazards frequently exist. For example, one FaceTime customer approached us because a user happened to stay late one Friday night to transfer some music. That user downloaded a virus-infected file and the entire network was down by Monday morning. How much would an incident like that cost your organization?

Spyware just bugs me with popups, right?

Unfortunately, no. Spyware can record keystrokes, monitor browsing habits, or transmit privileged information to external organizations without the user's knowledge. Spyware is also used as a distraction to prevent users from noticing that other malware, such as rootkits and Trojans, are being installed in the background.

Spyware is annoying but why should I spend money fixing the problem?

Spyware is sadly far more than a simple annoyance. Many spyware incidents are targeted at specific types of information theft (banking or health-related information) or specific types of organization (government, finance, manufacturing) and can cripple entire networks if allowed to proliferate. Systems can become so overburdened with spyware and associated unnecessary programs and processes that they crash. Organized crime has latched on to the possibilities of spyware, creating a new category of malware known as crimeware or ransomware. Many spyware programs are intelligent enough to thwart traditional anti-spyware tools, and the cost of removing these products can become extremely high – not only in reformatting hard drives and rebuilding systems from scratch to return them to productive use but the legal and public relations costs of surviving a compliance breach lawsuit resulting from spyware-driven information theft.

Summary

- 613 users running public IM clients
- 117 users running P2P networks
- 21686 number of spyware attempts

The RTDiscover test has revealed several significant risks to Acme Corp's network from unmanaged and unmonitored greynet usage.

FaceTime would be pleased to prepare a costed proposal to bring these unauthorized applications back under the control of the IT department and ensure that Acme Corp is no longer at risk of losing intellectual property, being infected by malware, or falling into breach of compliance legislation through the use of otherwise-productive real-time communications tools.

About FaceTime

Founded in 1998, FaceTime Communications is the leading provider of security solutions for the management and control of greynet applications including instant messaging, webmail, peer-to-peer file sharing, web conferencing and VoIP. FaceTime solutions are used by over two million people in over 800 organizations, among them nine of the ten largest US financial institutions.

FaceTime Enterprise Edition, the company's flagship solution, was awarded Best Buy in SC Magazine September 2005 issue and in February 2007 received the SC Magazine Reader Trust Award for Best IM Security for the third year in a row, as well as the NetworkWorld Best of the Tests 2007 Award for Best Anti-Malware. All FaceTime products are backed by FaceTime Security Labs, the industry's largest research team dedicated to the collection, analysis, understanding, and management of real-time communications threats.

Appendices

I: Spyware Danger Level Ratings

Level 1:  **Minor annoyance**

No immediate threat, may profile users, but has specific privacy policies in place. Not so dangerous, fairly easy to remove, using standard "Add/Remove Programs" function.

Level 2:  **Annoyance**

May profile users and no privacy policies in place. May make use of "drive-by installation". Removal is possible by end user.

Level 3:  **Minimal Threat**

May profile users or broadcast data back to a server with ("opt-out") permission. Removal is hard.

Level 4:  **Moderate Threat**

Nearly impossible to remove manually.

Level 5:  **Threat**

Level 6:  **Potentially Dangerous**

Logs keyboard activity, takes system snapshots.

Level 7:  **Moderately Dangerous**

Logs activity and removal is difficult.

Level 8:  **Highly Dangerous**

Logs activity uses stealth installation and removal is difficult.

Level 9:  **Highly Dangerous**

May open up communication ports, use polymorphic tactics, stealth installations, and/or anti-spy counter measures. May contain a security flaw.

Level 10:  **Extremely dangerous**

May open up communication ports, use polymorphic tactics, stealth installations and/or anti-spy counter measures. There exists a high possibility of potential system damage or security flaw. Attacked has complete control over your machine, can execute command in your place. May (attempt) to disable anti-virus or firewall programs.

For more information on how these levels are assigned, see www.spywareguide.com/txt_dangerlevel.php.