

White Paper



***New Threats Requiring
Gateway-level
Application Filtering***



Introduction

The vast majority of existing Internet security solutions fail to inspect certain types of Internet traffic and applications, allowing numerous security vulnerabilities to be easily exploited. Such threats are outlined below:

Threat 1: Gateway-level Malicious Code

Normal content security inspection inspects files which are transferred via standard protocols, namely HTTP, FTP, SMTP and POP3. Certain malicious codes propagate over the Internet but do not arrive as files. These exploit known security vulnerabilities and attack Web and SQL servers or use certain communication ports and protocols. Some examples are:

- **CodeRed, CodeBlue:** Use Microsoft IIS buffer overrun exploit by sending a malformed query with malicious code.
- **Nimda:** Exploits Unicode Web Traversal vulnerability on Microsoft IIS to execute malicious code.
- **SQL Slammer:** Exploits MS SQL Server vulnerability with buffer overrun by issuing a malformed SQL query with malicious code.
- **Blaster Worm:** Exploits RPC over port 135 vulnerability with buffer overrun that allows execution of malicious code on victim PC.

Threat 2: P2P File Sharing

P2P (Peer to Peer) applications such as Kazaa, iMesh, Gnutella, eDonkey and others pose the following threats to organizations:

- **Exposure to malicious code**
Shared files are located mostly on private PCs, many of which contain viruses and other malicious code. There are even viruses known to specifically infect and create new infected files in shared folders.
- **Exposure of confidential information**
Some users can configure the file-sharing application, deliberately or intentionally, to share the content of their entire hard disks or even their entire computer, including network drives. This is a tremendous security risk that can lead to serious consequences.
- **Distribution of copyright protected material**
Many of the files shared over P2P networks are copyrighted materials which are distributed without authorization, including pirated MP3 audio, movies and

InformationWeek

August, 2003

File-sharing applications such as KaZaa are found at 75% of all businesses and 9.3% of the total PCs in businesses.

<http://www.informationweek.com/story/showArticle.jhtml?articleID=12800731>

software. The distribution of such content is illegal and employers can be found liable for any copyright infringements.

- **Installation of unauthorized and pirated software**
Many P2P users will download and install pirated software. Such software is not only illegal and could lead to legal action by the BSA (Business Software Alliance), but can also cause IT problems where unauthorized software is not supported or when it conflicts with existing applications and hardware.
NOTE: Pirated software is also a prominent source of viruses.
- **Distribution of inappropriate and non-productive content**
Some content shared over P2P networks include pornography as well as drug-related or violent materials. As some of this content is even criminal in nature, depending on locale, employers can be found to have legal liability for the distribution and possession of such material.
In addition, much of the content found in P2P networks is obviously non-productive and non-work related, such as movies and music.
- **Bandwidth consumption**
Most of the content found in P2P networks consists of very large files. The average size of an illegally ripped movie is 700MB. The average MP3 album is 70MB. After downloading a few movies and songs, users are carried away and many start downloading constantly, creating bottlenecks and consuming tremendous amounts of your organization's bandwidth.

Threat 3: Instant Messengers

Instant messengers such as ICQ, MSN Messenger and Yahoo Messenger have become very popular in recent years and in many cases are also legitimate for business use. However, IMs can be a security threat or be used for non-productive or non-work related activity:

- Malicious code entry point: IMs can be used for file transfers. Transferred files are not inspected and may contain malicious code. An increasing number of Trojans and worms target IM applications, providing a very convenient propagation channel.
- Pirated and confidential content: IM applications can be used for file sharing or transfers and raise similar concerns to P2P applications mentioned above.
- Nonproductive activity: IM are often used for non-work related communications with people in or out of the organization.



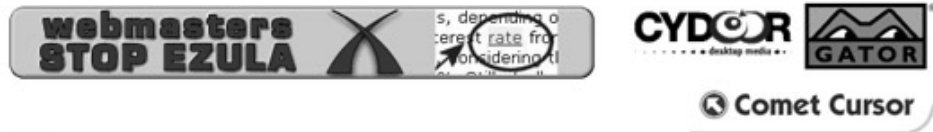
August 2003

Instant messaging has entered the corporate world and has brought with it another layer of security concerns.

Instant messaging applications **can provide attack points for hackers** seeking to gain entry into corporate systems **by presenting tunnels through firewalls.**

Threat 4: Adware / Spyware Applications

Spyware and Adware are common names to commercial software applications that are installed along with sponsored advertising or various information collection systems. The "extras" are installed either as part of the revenue collection business model of the vendor, or as part of an information collection system for anything from quality control to demographics and statistics collection. Collected information can be used to provide sponsors with targeted advertising or collect information to be used in other software or services.



There risks from such software are the collection of usually unsolicited information, unauthorized traffic, and potential conflicts with installed corporate software. Some known adware/spyware components found in many software packages include Gator, Cydoor, eZoola and many more.

More information about adware and spyware can be found at:

<http://www.tom-cat.com/links/links-i.html>

Current Situation of Fighting Adware/Spyware

Adware and spyware are usually legal, although some are notorious for very dubious behaviors. They are usually not regarded as viruses because they usually do not self-propagate. There are several reasons people install software with adware/spyware; neglect to fully read end-user license agreements (EULA) when installing new software, lack of awareness of the risks, and indifference to such risks, especially in corporate environments.

There are a few ways to fight adware/spyware:

- Refrain from installing such software. In many cases there are alternatives with no spyware/adware, some are free, some cost money. You can find out more information here: <http://www.tom-cat.com/spybase/index.html>. Many times this is not practical because users do not care or do not ask before installing new software.
- Use desktop-based adware/spyware blocking and removal tools. Some of these tools are free and some cost money and include auto-updates. The problem with these tools are that they require a medium to high degree of computer experience, can cause software conflicts or certain software from working and usually cannot be installed and controlled centrally in an organization.
- Use gateway-based signature inspection to block adware/spyware infected software, similar to conventional anti-virus. This method would require an extensive database that constantly updates with new adware/spyware versions and corresponding software they exist in. This is a complicated and reactive solution. It is also ineffective against users with laptops who install

adware/spyware infected software when outside the company, or if such software is otherwise brought into the organization, on CD-ROM for example.

- Centrally block adware/spyware communications with their corresponding servers. *This is a method unique to eSafe AppliFilter.*

Threat 5: Unauthorized Traffic Tunneling

Tunneling is a method used to circumvent firewall restrictions by disguising forbidden traffic such as P2P, remote computing and telnet - as ordinary Web surfing content. Tunneling could also be used by various software and even Trojan horses to transmit uninspected traffic to a remote server. Tunneling is possible because of the fact that organizations must allow HTTP, and usually also FTP and SMTP traffic to travel through the firewall in order to conduct normal business and allow their users to surf the web, download files and use email.

Tunneling examples:

A user could use a tunneling utility and set his home computer to tunnel POP3 traffic to his office computer on port 80, which is normally open. The traffic is encapsulated as normal HTTP traffic and will not be inspected.

A user could use a remote management tool such as GotoMyPC and use a browser with an ActiveX, or a special viewer to remote control or transfer files to and from his home PC. The traffic is again encapsulated as HTTP on port 80.

Actually, vendors promote such applications specifically to circumvent existing security policies.



A user could set up a tunneling utility to connect to an outside browser and actually establish an unauthorized and uninspected proxy.

Another threat within HTTP tunneling is remote control Trojans used to collect information on infected machines. The collected information is encapsulated as HTTP traffic and sent to an outside server on port 80.

Legitimate uses for tunneling:

Sometimes a tunnel has to be established in order to use remote secure telnet (SSH). In this case the whole tunnel is encrypted at the socket layer. In these situations, users (or IP) who are allowed this activity can be controlled by administrators at the firewall.

Aladdin's eSafe Solution

Aladdin's latest version of its eSafe content security solution now includes AppliFilter™ technology that addresses all of the above threats. AppliFilter™ is a new technology introduced in eSafe4 that:

- Allows real-time filtering of various malicious Internet content as it enters the organization
- Operates in a similar way to active IDS (Intrusion Detection Systems), extending the coverage of the content security solution while remaining
- Is easy to manage
- Allows the eSafe NitroInspection engine to examine all traffic at the gateway, analyzing the content of the passing packets and blocking traffic that is deemed malicious, inappropriate or otherwise restricted

What Can AppliFilter Block?

AppliFilter can protect from the following growing threats:

- Gateway-level (TCP/IP) malicious code attacks
- P2P (Peer to Peer) file-sharing such as KaZaa, iMesh, Gnutella, eDonkey
- Instant messengers such as ICQ, MSN, AOL, and Yahoo! Messengers
- Adware/Spyware components found in many "free" and commercial software
- Unauthorized HTTP-tunneling

Gateway-level Malicious Code: eSafe AppliFilter Solution

The eSafe NitroInspection engine can inspect all TCP/IP packet content. AppliFilter is looking for recognized signatures of malicious code or exploit attempts of known security vulnerabilities in the raw traffic before it is even constructed to files. By working similarly to active IDS, eSafe can detect malicious code and exploit attacks in transit and block them before they strike servers and desktops inside the organization.

eSafe is the only content security product that is capable of blocking non-file attacks (attacks that do not arrive in email or web-downloads). Other content security products are not inspecting traffic at the TCP/IP level but at a file/proxy level. Not only they cannot block such attacks, they are also limited to inspecting only email, HTTP files over port 80 or FTP files over port 21.

The AppliFilter code-attack signatures are part of the XploitStopper™ and are automatically updated as new attack vectors are discovered.

P2P File Sharing: eSafe AppliFilter Solution

eSafe Gateway with AppliFilter is the only content security solution that can identify and block P2P traffic at the gateway. The NitroInspection engine allows doing so regardless of the P2P port used. Other content security products cannot do that because they operate as proxies which can only block complete files and are bound to inspect only the standard HTTP port 80.

The administrator can assign which P2P applications are blocked and even an exclusion list for users who are allowed to use P2P applications.

Instant Messengers: eSafe AppliFilter Solution

eSafe Gateway with AppliFilter is the only content security solution that can identify and block Instant Messengers traffic at the gateway. The NitroInspection engine allows doing so regardless of the IM port used. Other content security products cannot do that because they operate as proxies which can only block files and are bound to inspect only the standard HTTP port 80. AppliFilter identifies the IM protocols used - while in transit, and block this type of communication. Desktop solutions are difficult to implement and manage.

To allow business productivity in organizations that do allow the usage of IMs, eSafe can be configured to allow IM traffic only for specific IPs and IP ranges.

Adware/Spyware: eSafe AppliFilter Solution

eSafe AppliFilter is the only existing product that uses a novel approach to protect against adware and spyware by taking advantage of the fact that virtually all adware/spyware has to communicate with central servers in order to exchange information. This information can include sending out collected information and receiving advertisement banners and/or links to those banners.

AppliFilter inspects all application-level traffic at the gateway and blocks all such communication with the central servers, rendering the adware/spyware components of the installed software useless, eliminating the risks. The implementation is very simple and centrally managed from eSafe's eConsole. The administrator can even decide to allow such communications to certain users.

HTTP Tunneling: eSafe AppliFilter Solution

eSafe Gateway with AppliFilter can identify and block HTTP-tunneling activities. AppliFilter monitors gateway traffic in real-time, making sure for example, that only standard HTTP packets are allowed on port 80.

Other content security products cannot do that because they operate as proxies which can only block files and cannot examine the packet structure in transit.

MS DCOM RPC Exploits: A set of vulnerabilities discovered in Microsoft operating systems. It allows attackers to initiate malicious code on vulnerable systems over port 135 or others, which are used by DCOM RPC components for some networking purposes and are usually closed on firewalls. Only eSafe - a gateway level content security product, which unlike proxy solutions examines all traffic, can detect and block such exploits.

However, if an infected PC, for example a laptop gets infected and is introduced into the network, only desktop solutions could block it. This is because the traffic does not pass through the gateway at all.

Non-file attacks: malicious code that usually exploits vulnerabilities to attack PCs and servers. Known examples are MS Blaster and CodeRed mentioned above.

Comparing eSafe to IDS/IPS systems: Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are designed to discover and block a wide range of attacks and intrusion attempts. They achieve this by examining the raw Internet traffic which is composed of TCP/IP, UDP, ICMP and other protocols usually across layers 4-7 but sometimes even on lower layers of the OSI model. Within this traffic, packets can be analyzed by looking for attacks pattern signatures, attack characteristics, etc. It is beyond the scope of this document to explain all the mechanics of IDS/IPS.

eSafe is a unique content security product; unlike proxy based solutions it can actually examine packets in transit in a similar way IDS does. By doing so, eSafe can block malicious code other content security products cannot, such as CodeRed, MS Blaster, etc. eSafe is different than IDS because it is not focused at this point to block Internet intrusion attacks and it only inspects TCP/IP traffic.

Full TCP/IP Traffic Inspection: Unlike proxy based products which examines files only that are being saved in a cache, eSafe NitroInspection examines files as they are in transit via the TCP/IP inter-network protocol. This allows inspection of various non-file attacks, blocking of certain traffic such as P2P, IM and tunneling, faster inspection, inspection of all ports and increased scalability.



For more contact information, visit: www.Aladdin.com/contact

North America	T: +1-800-562-2543, +1-847-818-3800	Italy	T: +39-333-9356711
UK	T: +44-1753-622-266	Israel	T: +972-3-978-1111
Germany	T: +49-89-89-4221-0	China	T: +86-138-18184444
France	T: +33-1-41-37-70-30	Brazil	T: +55-11-5539-5688
Benelux	T: +31-30-688-0800	Japan	T: +81-426-607-191
Spain	T: +34-91-375-99-00	All other inquiries	T: +972-3-978-1111

