Why plain and traditional Anti-virus software is not enough?

This white paper explains why anti-virus software alone is not enough to protect your organization against the current and future onslaught of computer viruses. Examining the different kinds of email attacks that threaten today's organizations, this paper describes the need for a solid server-based content-checking gateway to safeguard your business against email viruses and attacks.

Computer viruses will cost businesses around the globe more than $2.5 trillion in 2001, according to a PricewaterhouseCoopers study issued by Information Week Research in July 2001.

Email is the top distribution mechanism for the world's most dangerous electronic viruses, such as deadly email viruses transported through Word macros (e.g., Melissa), infected attachments (e.g., Love Bug) and commands embedded in HTML mail. Furthermore, email is now being used to launch email attacks, targeted specifically at your organization to obtain confidential information or gain control of your servers.

Hefty damage: both widespread and targeted

> *"The bill to 50,000 US firms this year for viruses and computer hacking will amount to $266 billion, or 2.5 percent of USA's GDP," reported Information Week Research in July 2001. By comparison, in 2000, computer viruses cost US business $12 billion, according to Computer Economics Inc.*

Organizations are threatened both by email viruses that are released in the wild and gain notoriety in the media and also by email attacks that are specifically targeted against them. Some of them are

- The VB-script worm Love Bug, which hit in 2000
- The Nimda virus, that proved its notoriety in 2001
- The macro virus Melissa and the Explore Worm in 1999.

Today, email has become a prime means for installing backdoors (Trojans) and other harmful programs to help potential intruders break into a corporate network. Described as "intrusive viruses" or "spy viruses" by computer security experts, these may become potent tools in industrial espionage.

In February 2000, for example, Japanese police arrested a young man suspected of emailing viruses to a company to obstruct its operations and cause its computer systems to shut down. Another case in point is the email attack on Microsoft's network in October 2000, which a Microsoft Corp. spokesman described as "clearly an act of industrial espionage ". According to reports, Microsoft's network was hacked by means of a backdoor Trojan virus (IWorm.Qaz) maliciously emailed to a network user.

Types of email attacks

To get to grips with the kind of email threats present today, it is best to take a quick look at the current main forms of email attack. These include:

Email Trojans

Trojans can be emailed to the victim and used to breach security (e.g., to steal information) or to cause damage (e.g., activate a distributed attack). As a Trojan attack usually requires the recipient to activate the program received, the sender often disguises the Trojan program as an attractive attachment, such as a joke, to convince the recipient to run the program.

Buffer overflows

Buffer overflows can be set up in such a way as to supply program instructions for the victim's computer to execute. By exploiting a bug in the program under attack, the attacker emails the recipient a program for execution by his/her computer. They can also be used as Denial-of-Service attacks, causing the program to crash. The most recent and glaring example is that of the Code-Red Worm, which hit thousands of Computer Servers running the Microsoft Software Program called IIS.

HTML viruses - that do not require user intervention

Also known as active content attacks or browser attacks, HTML attacks are aimed at those who use web browsers or HTML-enabled email clients to read their mail. Such attacks tend to use the scripting features of HTML or of the email client to illicitly execute code on the PC or to acquire private information from the recipient's computer. Sometimes, these are used to make the victim’s computer display some specific content or perform a Denial-of-Service (DOS) attack.

While devastating viruses, like the Melissa macro virus, require the victim to execute them by opening the infected email attachment, this frightening new breed of HTML virus does not require user intervention in order to be activated. Alarming as this is, it is actually extremely easy for virus writers to make a virus that is executed simply by opening one’s email client.

The shocking ease of creating a virus today...

Anyone with a little knowledge of Visual Basic (a Software tool manufactured by Microsoft) can unleash chaos by exploiting well-known vulnerabilities in various commonly used email clients and products. A visit to the SecurityFocus site, for instance, will reveal various exploits that are available for Outlook (once again a very popular email client made by Microsoft), currently the most popular email client. A malicious script kiddie with the intent of producing a virus can easily study these exploits, perform experiments or just modify the exploit code - which is publicly available! - to execute a new code of his/her own.

For example, an exploit for Internet Explorer and MS Access, which could be easily applied to Outlook and Outlook Express (when MS Access is available), is described on the web-site http://www.guninski.com. A virus writer could easily exploit this to run Visual Basic code as soon as the victim opens the infected email. This would infect all HTML files and send itself to all the contacts on the recipient’s email address book. A key feature of this virus, however, is that it would execute simply when the user opens the email containing malicious HTML.

Another intervention-free virus could make use of the GMT field buffer overflow vulnerability in Outlook and Outlook Express, as described on http://www.securityfocus.com. The victim would download the email sent by an infected user upon which the recipient’s Outlook client would crash and execute a malicious code. This in turn would send the offending email to all the contacts in the victim’s address book. Here, the virus would continue to replicate, repeatedly causing email clients to crash, and resulting in a total standstill in Internet traffic.

Does it sound like a clever script for a new science fiction movie? Unfortunately not: It is only a matter of time till we see a horrifying virus of this sort flooding global networks and mailboxes.

Why anti-virus software or a firewall is not enough

Some organizations lull themselves into a false sense of security upon installing a firewall. This is a wise step to protect their Intranet, but it is not enough: Firewalls can prevent access to your network by unauthorized users. But they do not check the content of mails being sent and received by those authorized to use the system. This means that email viruses can still pass through this level of security.

Nor does the normal breed of virus-scanning software protect against email viruses and attacks: The fact is that anti-virus vendors cannot update their signatures in time against the deadly viruses that are distributed worldwide via email in a matter of hours (such as the LoveLetter virus and its variants). This means that companies using a virus-scanning engine alone are not necessarily safeguarded when a new virus is released. This is because anti-virus tools work reactively, letting all emails in and then trying to disable a virus. At this point, it may already be too late: once a virus has entered the system, it takes one quick click for an unwitting user to activate it.

Anti-virus engines cannot protect against what they don't know. Therefore with regards to new, fast-spreading viruses or targeted email attacks, normal anti-virus software offers no protection at all! Besides, anti-virus software often does not even check the body of an email, which can actually contain the dangerous virus itself.

The above facts are proven by the alarming increase in the number of viruses that "bypass" or enter corporate networks, in spite of all the computers having AntiVirus software installed!

The solution: A proactive approach

So how does one protect against HTML mail viruses, future macro viruses, and email attacks?

A proactive approach is needed which involves the content checking of all inbound and outbound email at both the server level and the client level, before distribution to your users. This way, all potentially harmful content is removed from an infected or dubious email, and only then is it viewable by the user.

By installing a comprehensive email content checking and anti-virus gateway on their Mail Server, companies can protect themselves against the potential damage and lost work time that current and future viruses may cause. At the same time, AntiVirus utilities today do not check or scan TCP/IP traffic. They only check your files & folders present on your CD, floppies or hard disks, a traditional design not of much use in today's Internet driven world.

The kind of applications, such as **MailScan for Mail Servers**, **MailScan for SMTP Servers** and **eScan** by **MicroWorld**, are specifically designed to function like an email firewall. They also are the first software applications those feature TCP/IP Traffic scanning, in addition to the normal files scanning.

MailScan and eScan uses the revolutionary **MicroWorld Winsock Layer (MWL)** to scan and clean email traffic**.** MWL is a revolutionary concept in scanning Internet traffic on a *real-time* basis. This new concept is set to change the manner in which the content security threats are tackled in the knowledge and Internet-driven world. MWL gets data packets as they travel from your computer to the Internet & vice-versa. Hence, it has the ability to tackle a threat before it reaches the enterprises' applications. Other products, since they deal at file-system layer, deal with a threat after the applications have already processed it!

In that. it can block emails and attachments containing VB script, macros, Windows Scripting, Java scripts, executables and HTML scripts at email server level. This way, email attacks are blocked at server level before they can cause any harm, eliminating the fear of viruses that do not need user intervention to be activated. To add an additional layer of Security, eScan application, which is again developed using MWL, gives customized protection to users on their desktops.

MailScan also includes the option to clean remove scripts from all emails, so as to provide a 100% protection against viruses and email attacks. With such an approach, new viruses or variants that pose a huge threat and worry to traditional anti-virus engines become little cause for concern.

In addition to checking for email viruses or attacks, **MailScan and eScan** can also scan for offensive content, spam and information leaks. More information and a free evaluation version for download can be found at http://www.mspl.net.

MicroWorld.