Global Information Assurance Certification Paper

Antivirus at SMTP Gateways Level

.

Overview

The distribution of viruses and the infection inside a company can come from different points of the network topology. The most common way to get an infection is the e-mail system that is now the most popular service on the web. To control the infection you could use an Antivirus in every computer but it is not enough to control viruses. Under this scenario we found a couple of Antivirus systems that work with the SMTP protocol as a relay server and detects and repairs viruses. The main objective of this article is to see if the protection at SMTP level is the securest way to protect my organization from viruses as complement of a desktop avntivirus solution. The second objective is to explain the function of this kind of antivirus and the technology associated with it.

History

At the beginning of the computer history the viruses spread at low speed in the network environment. The virus is an instruction that makes a code to copy itself from one host to another host.This code could be a software program or ADN or any type of code.
One of the factors involved in the success of antiviral programs is a study of the mindset of the user: a study of the psychology or sociology of the computer community. Since the spread of antiviral programs generally requires some action, sometimes unknown by the user, it is instructive to look at the security breaking aspects of other historical programs.
But with the public networks the problems become more complex. The virus maker takes care about the new technologies and designs viruses that can be spread at the speed of new communications.
The new environment creates multiple points of contact inside an organization's infrastructure, and each point of contact is a potential entryway. It is important that businesses realize that the main concern should not be the well- publicized e-mail viruses attacks – although this needs to be handled as efficiently as possible – because the threat comes from cyber terrorists.

The problem now is how to protect my organization from viruses. How can I maintain the integrity and privacy of the information inside the internal network (for example, from Trojan Horses)? Which is the securest way to protect my company from e-mail viruses attacks?

The Effects of Email Viruses

Computer viruses have enormous potential for damage: files crash, important data disappears, productivity is interrupted, entire networks go down. Anti-virus solutions protect multiple entry points to networks in organizations against known and unknown viruses.

Virus can impede the enterprise's ability to conduct business. Productivity and network performance are both negatively impacted as a result of a virus. While a business wants to devote its resources to do businesses, virus demands it respond to an unwanted solicitation. It distracts employees from their duties. Viruses can make you lose productivity, which means losing money. Remember that the ILOVEYOU virus worm began as unsolicited mail. Since virus comes in such huge volume, it also poses a considerable threat to introduce a variety of viruses to an enterprise system. Moreover, the organized flooding of a system with virus can effectively sabotage it.

What Is a Computer Virus?

A virus is generally defined as a program that infects documents or systems by inserting or attaching a copy of itself or by rewriting files entirely. A virus operates without the knowledge or consent of the user. Therefore, when an infected file is opened, the embedded virus is also executed – often in the background. A true virus is propagated by users themselves, almost always unintentionally. A virus does not deliberately spread itself from computer to computer. It may replicate itself within one computer, but in order to propagate to other machines, it must be passed on to other users through infected e-mail document attachments, programs on diskettes, or shared files. New malicious code strains have made self-replicating viruses more common.

World Famous Worms

Computer worms have been in existence for over fifteen years, since the creation of the Xerox worm, originally intended for benign network maintenance tasks. The first widespread malicious worm, the Morris worm, attacked networks in 1988, when the Internet was still revolutionary and not in common use. Since these early worms, the worm threat has evolved—and worm authors have produced some dubious firsts.

IRC Worms were the first consumer-oriented arbitrary protocol, self-launching worms. A popular IRC client, mIRC, uses a powerful scripting language that was exploited by the first IRC worm. The scripts were programmed to send themselves to new users as they logged onto IRC chat rooms. Once the user's system was infected, the mIRC would execute the worm logic and propagate the worm. These early worms were both benign and malicious. Users who spread the worm could send commands to infected systems to perform malicious actions. It was the first "remote control" worm, since it allowed the attacker to remotely control or damage infected systems.

Melissa, released in February 1999, was both a virus and a worm, or a hybrid. Melissa was the first mainstream corporate macro hybrid and caused millions of dollars of damage to corporations. When a user received and viewed the infected document, the Melissa macros ran in Word for Windows 97 and used the Outlook email client to send a copy of the infected document to the first fifty users in the Outlook address book. It also infected other Word for Windows documents.

As a deeper view in Melissa´s virus, here there is a table of the eometrical growth of the virus in just 6 steps.

g

E-Mail Messages Generated by Melissa	
Step	**Recipients**
1	50
2	2,500
3	125,000
4	6,250,000
5	312,500,000
6	15,625,000,000

ILOVEYOU was also a hybrid virus and worm. Once executed, the virus/worm mailed itself out to all contacts in the user's Outlook email address book. In addition, the worm/virus also located other scripts on the system and replaced them with copies of itself. Once the infected scripts were launched at a later time, the virus/worm was set off again.

Prettypark worm is an example of a remote control worm. It used the Internet connection of the infected machine to gain access to an IRC chat application to await commands from the attacker to perform malicious actions, such as stealing information or deleting files. Information stealing and remote control worms can export information such as passwords and files back to the worm author. They can also be programmed to enable the worm author to remotely access and control the infected machine. This new type of attack could be utilized in the future as tools of extortion, blackmail and proprietary information theft.

Antivirus at SMTP Gateways Level

The Antivirus at Gateways level scans email transactions for viruses before forwarding them to your SMTP or groupware server for delivery. MIME and UUENCODE attachments are decoded and ZIP files are decompressed for scanning.

Because the Antivirus for Gateways runs as a separate server to process email, there is no significant impact on network resources. The short processing time is, effectively, performed in

isolation; users on the network only become aware of antivirus for Gateways operation if a virus is detected.

Four components interact in Internet email protection:
_ Mail server: Your existing SMTP (for example, Sendmail) or groupware gateway (for example, Lotus cc:Mail, Lotus Notes, or Microsoft Exchange) server.
_ Scan server: The AntiVirus for Gateways server that performs the decoding, decompressing, scanning, and virus repairs.
_ User Interface server: Supplies the HTML interface that can be accessed by any workstation on the network with a suitable browser for remote management and configuration.
_ Domain Name Server (DNS) for your site: Resolves host names into their actual IP addresses.

The AntiVirus for Gateways processing is effected by modifying records at the Domain Name Server. There are two types of records that are involved with the delivery of mail: A records and MX records.
_ An A (Address) record is a mapping of host name to IP address. For example, the host name www.somewhere.com might map to the specific IP address 192.168.23.10.
_ An MX (Mail eXchange) record is a mapping of domains to mail exchange host names. In other words, any mail sent to a particular user at a domain (such as user@somewhere.com) is resolved by a DNS server MX record to a machine, such as mailer.somewhere.com, then the A record resolves the name mailer.somewhere.com to an IP address.

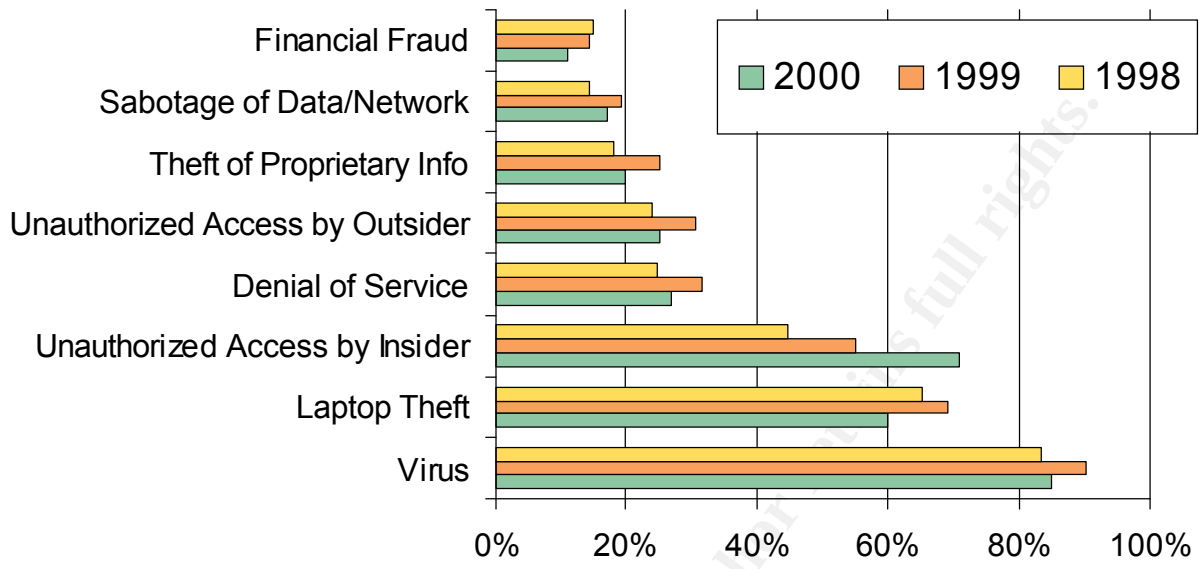
All email destined for the mail server arrives at the AntiVirus for Gateways first. After processing, the AntiVirus for Gateways then forwards the transaction to the mail server for delivery.

This structure gives the Antivirus for Gateways the right way to work at the Service Server level (sometimes you could find as DMZ).
The protection of the virus occurs outside the internal servers (as Lotus Notes Server or MS Exchange Server). The concept is to intercept the virus before the virus can spread around the internal Netwok.

Aditional Data

Why do I have to protect from viruses if I have a firewall? Because the Firewall des not protect you against viruses. As you can see in this chart the importance to protect your organization from viruses is really high.

Chart 1

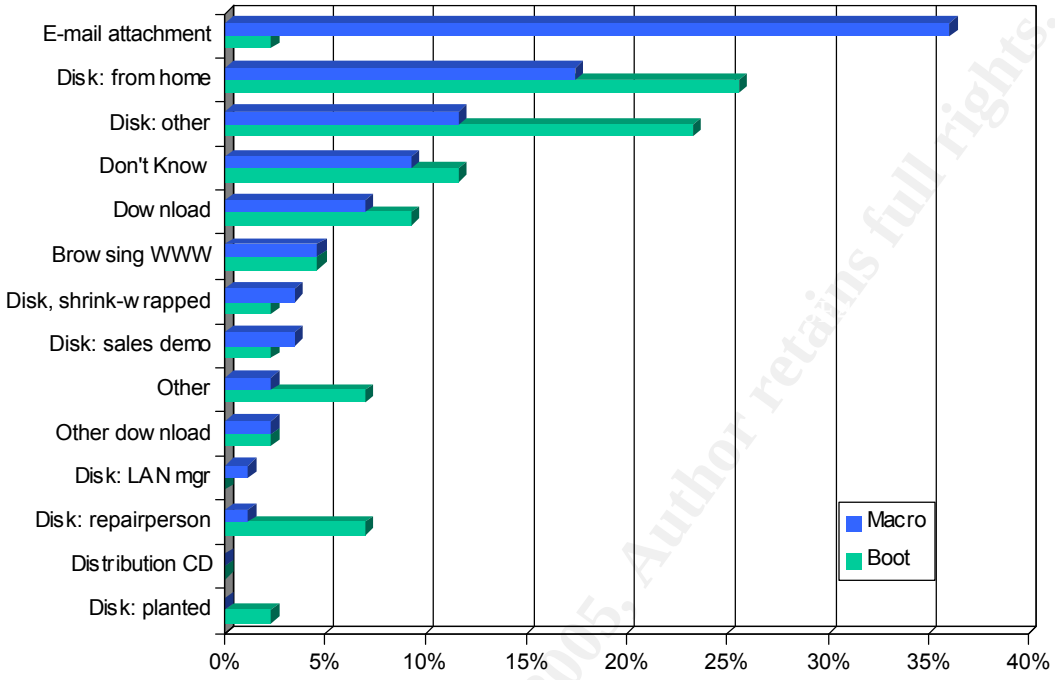


Source: FBI

The infection can come from different points. In this chart you can see the importance of the protection in the e-mail system. This chart is a little bit old (year 98) but the percentage des not change a lot, so you can trust in the information.
In this chart you can see that almost the 40% of the viruses infections come from e-mail system. The other interesting thing is that the viruses that are spread in the e-mail system are Macro viruses.

Chart 2

Source: NCSA Virus Study (Apr. 98)



Conclusions

As you can see in the additional data in chart 1, if you do not want to get the 80 percent of the

problem, it is important to get a good antivirus. In chart 2, you can see that the most popular way to get an infection is using the e-mail system.
To simple put an Antivirus in every machine in your organization could be a solution but not enough. You would try to cover every point of infection and stop the virus before getting into the network. Normally the area of service servers (known as DMZ) is a piece of the network that is not inside but is not outside the security perimeter and every company should have one. At this point the antivirus at the gateway level is the best point to control the virus because you can put the antivirus server in the DMZ area. And to troubleshoot any problem in the Antivirus server you just only have to redirect the e-mail traffic to another server.
Stop Trojan horses virus and other kind of malicious codes is a hard job but an Antivirus at Gateway Level could be the best way to the protect e-mail systems from viruses.If you stop at this point the e-mail-virus will never go into your internal network. This represents the 50 percent of the probability to get a virus.

Technology & Computer VirusesPage written & updated by Dave Phillips on Thursday, February 01, 2001http://antivirus.open.ac.uk/Tech&Viruses.html

History of Computer Viruses
by Robert M. Slade
1992
http://www.bocklabs.wisc.edu/~janda/sladehis.html

Edinburgh University Computer Virus Review 1999
http://mft.ucs.ed.ac.uk/pcvirus/reviews/vrev99.html
Computing Services, The University of Edinburgh
Tuesday, 29 August 2000

Gartner Report Malicius Code Viruses
Gatner Group
Symantec Internal Document
January 2000

Virus 99
Espasa Calpe Book Edition
Roque Moroa 11 september 1999