303 Potrero Street | Santa Cruz, CA 95069-2790 | 831.471.1413 | http://www.indefense.com

Understanding the Email-Borne Threat

By Mary Landesman
INDEFENSE, INC.

December, 2001

Understanding the Email-Borne Threat

Overview

In the past few years, email has become the predominant purveyor of viruses. This rapid communications technology outpaces the signature-based scanner updates, allowing widespread infection to occur in a matter of mere hours. Attempts to address this problem have ranged from an assortment of active content and behavioral analysis tools, improved signature-based scanners, gateway content filtering applications, digital immune systems, and security patches. As with any product, each of these has its strengths and its weaknesses. The common denominator amongst all of them is that, even used together, they fail to provide a strong enough defense against email-borne threats.

Signature-Based Anti-Virus Scanners

Signature-based anti-virus scanners gained dominance in the market in the early to mid 1990's. These traditional anti-virus scanners relied on signature strings, hexadecimal equivalents of snippets of virus code. When new viruses were discovered, signature updates were provided, enabling the scanner to detect the virus should it encounter it. In those pre-Internet days, it was an effective means of virus prevention. Quite simply, viruses, relying on sneaker-net, did not travel very fast, there were not nearly as many of them, and the periodic signature updates were nothing more than a minor inconvenience.

When the Internet extended beyond the research and government domains, into homes across America and throughout the world, signature-based scanning still remained a viable means of protection. However, when email gained wide popularity and became the de facto standard of business and personal communications, it also became the de factor standard for viral spread. This first became apparent in 1995 when Word macro viruses were created. With Microsoft Office a dominant player in the field of office productivity suites, .DOC files were widely shared. Combining that with increased use of email not only meant that documents could be more quickly and efficiently exchanged, but their accompanying infection could just as efficiently travel.

Despite these early indicators, traditional signature-based anti-virus vendors did not change their methodology, instead focusing on more rapid means to distribute the same type of protection as before. In other words, it became a cat and mouse game, trying to get signature updates out as fast as a virus could be expected to travel. This continued to be moderately successful simply because viruses were still contained in documents or files that could not spread outside of a network unless manually forwarded (unknowingly, of course) by a user.

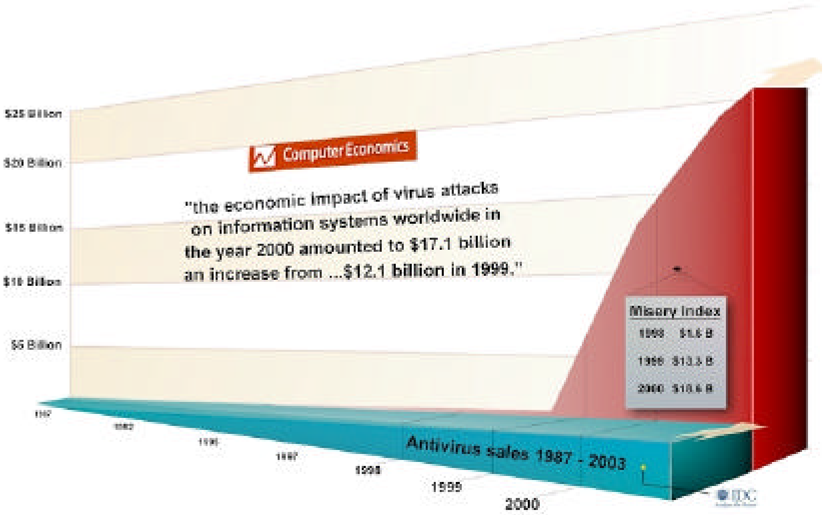
Melissa changed that in March 1999. The Melissa virus introduced a new breed of viruses that automatically forwarded themselves to others via email. For the first time, all that was required was one person to unwittingly open the file and the transmission outside of the network was accomplished. This new methodology also introduced the newest phenomenon of virus distribution – the socially engineered mass-mailing email worm.

On January 14th, 2000, Computer Economics[1] released grim figures denoting the high toll imposed by viruses: “the economic impact of virus attacks on information systems around the world amounted to $12.1 billion in 1999.” A signification portion of this was due to the release of the Melissa virus in late March 1999. Just months after the Computer Economics report, LoveLetter struck and suddenly the $12.1 billion damage estimate seemed conservative in comparison; Computer Economics’ estimate of damages for 2000 rose to $17 billion.

LoveLetter was an unprecedented success not because of sophisticated coding techniques, but purely because human nature responded to the promise of a “love letter” from someone they knew. Indeed, in spite of lessons learned with Melissa and LoveLetter, subsequent threats such as the AnnaKournikova worm and NakedWife have proved these social engineering techniques have continued to be successful. Most importantly, the combination of social engineering (guaranteeing a large number of willing “openers”) and mass-mailing coding (sending copies of the virus to addresses found in email address books) has completely out-paced the capabilities of the traditional anti-virus vendors. Indeed, viruses travel at the speed of technology, and can now integrate themselves into a network, across the Internet, and onto thousands of systems within only a couple of hours. Signature updates, on the other hand, travel far more slowly.

On May 11, 2000, Interhack Corporation published one of the first papers outlining the problem of rogue software and tackling the question of why the defensive strategies were not working. In their paper, “Why Anti-Virus Software Cannot Stop the Spread of Email Worms”, the authors noted that, “the picture is especially grim among end-users and non-expert information technology managers. The paper summarized, “As long as there are users who can be fooled, malware will continue to plague us.” They presented two possible solutions, “get rid of the user or help them to avoid getting fooled.”

Signature updates require that a virus sample be obtained. The virus must be analyzed, the unique string created, and the files must then be made available to users. Once in the hand of the users, these files must be deployed to all affected parties. In short, the virus is swift and signature updates are not. As a result, more persons are becoming infected and related clean-up costs are spiraling – clearly indicating that after-the-fact protection is simply not the viable means of protection it once was.



The Misery Index, depicted in Figure 1, and derived from Computer Economics and IDC forecasts[2], clearly demonstrates the dramatic rise in the economic impact of computer viruses – despite (or perhaps because of) the use of signature-based anti-virus scanners.

[1] **Malicious Virus Attacks Cost Organizations More Than $12 Billion in 1999**, Computer Economics press release, January 14, 2000

[2] Worldwide Anti-virus Software: It’s Not Just a Consumer Product Anymore, IDC Bulletin, Sept 2000.

Content-Filtering Software

Content filtering products are designed with control in mind. In fact, content filtering products existed first without anti-virus capabilities. The words content filtering imply lexical analysis to block email based on restricted keywords. Specifically, content filtering was devised to block confidential assets from being sent out of the organization, to protect against legal liability that might result from the email sharing of sexually explicit, racially discriminatory, or otherwise bias content. A third key feature is the ability to block spoofed email addresses and act as a spam filter. Naturally, anti-virus scanning is also a good fit and thus the product evolved into what we see on the market today.

The anti-virus toolkits used in all content filtering products are signature-based scanners. These bring the same limitations inherent in the conventional anti-virus products. Unknown viruses remain immune to these products, and it is the unknown virus that is directly responsible for the conservatively estimated $17 Billion in damage costs we confront today. (High end estimates range to $1.5 Trillion).

Thus, content filtering products are no more effective at deterring these damages than are conventional anti-virus methods. That is, without policy management.

What is Policy Management?
Policy management is the rule-set managed by the administrator to minimize threats to the enterprise. To affect effective policy management, the administrator must maintain constant vigilance over security matters. Generally, this means making virus awareness a full-time job, keeping abreast of new threats and creating on-the-fly policies to prevent their exploit. For example, during the LoveLetter epidemic policies were created to either block all .VBS files or block any emails containing the word LoveLetter.

While policy management is certainly effective, improperly implemented it can block unnecessarily. Most importantly it blocks only what is specified – in that respect blocking only what is known. This method of blocking known threats brings us full circle to the $17 billion problem.

Regardless of the effectiveness of policy management, there are serious concerns regarding the lexical analysis capabilities of content filtering products. While it may be useful to protect the company from legal liability (i.e. blocking pornographic materials to reduce the chance of lawsuits related to sexual discrimination), it also opens the door to complaints and lawsuits from employees concerning the intrusiveness of "reading" private email. Few companies are totally immune to the complaints of employees regarding this intrusiveness. Indeed, market research has indicated a strong interest in products that only block virus-prone executables and do not perform lexical analysis.

Certainly, simply because a feature exists it does not mean it has to be used. Thus, administrators could choose to forgo any policies regarding lexical analysis and focus solely on policies for virus detection. Combined with an anti-virus toolkit, this approach sounds sensible. However, as we've seen, both approaches focus on known threats only.

Lexical policy
Sexual – any emails containing the word sexual are blocked.
Problem: HR sends an email containing the new sexual harassment policy. It is blocked.
LoveLetter – any emails containing the word LoveLetter are blocked.
Problem: A legitimate warning from the anti-virus vendor is sent regarding a new variant of a virus similar to LoveLetter. It is blocked.

There are other problems with the content filtering approach. When anything in the email is deemed objectionable, the entire email is blocked. For example, a Word document containing infected macros that cannot be automatically cleaned will be quarantined and may never make its way to the user. An email containing any blocked keywords is quarantined and no part of it ever reaches the user – despite the fact that the email, and the use of the word(s), may be perfectly legitimate.

In short, a reliance on signature-based scanners, policy management requirements, privacy concerns, and undelivered email have made gateway content filtering applications less than ideal in the eyes of many users.

Firewall Protection

A good firewall, one that defends against both inbound and outbound connection attempts, plays a valuable role in malicious code prevention. Specifically, firewalls can be used to prevent Remote Access Trojans (RATs) from relaying sensitive information about you or your system and can prevent a Trojan from hijacking your system to attack others. Such were the tactics used to launch Distributed Denial of Service (DDoS) attacks against the likes of eBay and Yahoo in early 2000. These attacks were made possible by surreptitiously planting malicious programs on user's computers. These programs were under the remote control of unsavory crackers who then used the infected systems to send constant streams of data to these websites. More often, however, Trojans are used to steal passwords or account information from unsuspecting users. In fact, it was the desire to plant such a Trojan – to gain unlimited accounts for his dial-up use – that led to Onel de Guzman's release of the LoveLetter virus.

Firewalls are not actually charged with malicious code protection. Rather, they specialize in malicious person protection. The purpose of a good firewall is to ensure that only trusted users have access to, and from, the computer.

Perhaps one of the best known, and certainly a thoroughly capable, firewall is ZoneAlarm™ from ZoneLabs®. ZoneAlarm even takes a stab at email protection, providing renaming of extensions to prevent the accidental opening of certain types of executable files. Thus, in terms of using a firewall for malicious code protection, only specific types of Trojans and certain attachments are blocked. This leaves a vast number of malicious code threats to be concerned about.

Confronting the Email-Borne Threat

Given the complex prejudices of content filtering products and the inherent weakness of signature-based anti-virus scanners, how can we balance the needs of the user with the need for protection? Keeping in mind that we are all only as secure as our weakest link and the Internet connects all of us on one big global network – at least as far as email is concerned, we can see that security should be everyone's concern. Security must not only protect the user, however, it also must protect that user's information, i.e. personal email. Rather than get rid of the user to achieve high security, let's examine how we can prevent the user from being fooled.

At such a juncture, anti-virus vendors and security professionals often point to education as the key to success. Indeed, these fonts of wisdom recommend everything from disabling Windows Shell Scripting Host, to using Rich Text Format versus .DOC format and avoiding email attachments. Ironically, anti-virus vendor Trend Micro's Director of Public Education, Dave Perry, is so afraid of infected attachments that he stated during an interview, "I delete everything that has an attachment to it, even if it's from my own boss, unless I'm expecting it."[3] Clearly, if the anti-virus vendors are unwilling to open email attachments, despite their education in the field of virus prevention and their role as the number one provider of anti-virus protection, one has to wonder how the average user is expected to secure their system and exercise appropriate judgment.

The problem worsens when one examines the number of operating systems in use today, the types of mail clients employed, and the security vulnerabilities that exist in many of these. Microsoft®, by far the most popular developer of operating systems, is a favorite target for blame, though in reality they may simply have the disadvantage of being the most predominant and thus

[3] **Internet brings dangers new and old, and prevention is easier than repair, by** D. Ian Hopper, AP Technology Writer, August 2001

the biggest target for malicious code exploits. Though each successive operating system becomes a bit more secure than the last, vulnerabilities continue to be discovered leading Microsoft to release in excess of one hundred patches per year. The average user, no matter how dedicated to the cause of security, is undoubtedly going to experience some difficulty and some confusion when attempting to discern which patches need to be applied. To their credit, Microsoft has made this process much easier than in years past, but many users still are not aware of, or do not take seriously, the need to apply these critical updates.

The Nimda worm, discovered in September 2000, and the BadTrans.b worm which appeared a few months later, are just two of the high-profile threats that exploited Microsoft security vulnerabilities. In both cases, one of the exploits involved email attachments that would execute when the user simply read, or in some cases – previewed, the email.

The challenges, of course, are how to protect your system from threats that quickly outrun anti-virus updates, how to maintain privacy and control of your correspondence, and how to prevent vulnerabilities from being exploited? In short, how can email be made safe?

M@ilDefense™

MailDefense works by filtering harmful executables, scripts, and macros from email and attachments. By quarantining executable-type attachments, MailDefense protects the user from impulsive or unintended opening of these files from within the mail client. Additionally, by removing all scripts embedded within the email itself, users are automatically protected from email worms such as Kak, BubbleBoy, and Verona. Through the use of MailDefense, Microsoft® Office files can be exchanged without fear of macro viruses – the macros will be removed from the document before sending it on to the mail client and the original will be quarantined. Within the quarantine directory, files are registered to the MailDefense program and an alert is provided should the user attempt to open the file. By first moving the attachment into quarantine and then re-registering the file, the user is spared the possibility of impulsive or unintended opening of files.

MailDefense works with inbound and outbound email. Should a user become infected with a mass-mailing worm via the network, the infection would be stripped from the email automatically. This defense prevents viruses such as SirCam from spreading infection, compromising sensitive information, and embarrassing the corporation.

Additionally, files that are quarantined by MailDefense are protected with a registered MailDefense extension. Should the user attempt to open the file from within quarantine, an alert will be generated. This method prevents the spontaneous and inadvertent (or misunderstood) opening of harmful file attachments.

Despite the weaknesses presented by signature-based scanners, they do provide valuable protection against other types of threats, such as boot sector viruses and viruses spread by CD-Rom and floppy disk. Indeed, layered protection is the best approach in today's interconnected – and vulnerable – environment. Fortunately, MailDefense works cohesively with signature-based scanners, providing needed protection against fast-paced and often unknown email-borne threats. Indeed, one could argue that MailDefense allows signature-based scanners to do a better job, quarantining new threats until antivirus vendors are able to deploy the necessary detection and disinfection updates.

	MailDefense	Norton AntiVirus	McAfee VirusScan
Removes known harmful attachments	✓	✓	✓
Removes unknown harmful attachments	✓		
Removes known macro viruses	✓	✓	✓
Removes unknown macro viruses	✓		
Stops known email worms	✓	✓	✓
Stops unknown email worms	✓		
Removes known harmful attachments	✓	✓	✓
Removes unknown harmful attachments	✓		
Removes known malicious scripts	✓	✓	✓
Removes unknown malicious scripts	✓		
Removes known malicious ActiveX controls	✓	✓	✓
Removes unknown malicious ActiveX controls	✓		
Quarantines originals while sending cleaned files/email to users	✓		
Protects POP3 mail	✓	✓	
Protects IMAP mail	✓		
Never needs updating	✓		

Characteristic	M@ilDefense	Content Filtering
Blocks executable attachments and scripts by default	YES	No
Requires a database of identified viruses	NO	Yes
Requires signature updates to identify new macro viruses	NEVER	Constantly
Eliminates the opportunity for viruses to enter the system between updates	YES	No
Works at the desktop level	YES	No
Works at the server level	YES	Yes
Works at the SMTP gateway level	YES	Yes
Quarantine scan management	YES	No

Alternative Protection

Other methods of protection exist for email-borne threats. Microsoft's Outlook Security patch and ZoneAlarm's MailSafe protection both block undesirable file types. However, ZoneAlarm is confined to attachment protection only, leaving users to confront the risk of script and macro viruses alone. The Outlook Security patch is effective only for Microsoft Outlook users, leaving users of other mail clients vulnerable.

Feature Comparison – MailDefense and ZoneAlarm Pro

	MailDefense	ZoneAlarm Pro
Inbound executable filtering	Yes	Yes
Inbound script filtering	Yes	No
Inbound macro removal	Yes	No
Renaming/registering of extension	Yes	Yes
Ability to add extensions	Yes	Yes
Ability to exclude specific files	Yes	No
Ability to exclude specific extensions	No	Yes
Outbound executable filtering	Yes	No
Outbound script filtering	Yes	No
Outbound macro removal	Yes	No
Quarantine directory	Yes	No
Readily identifiable extensions	Yes	No

Compatibility testing indicates the two products work cohesively, with ZoneAlarm Pro renaming inbound files and MailDefense quarantining those renamed files with the appended .ndp extension. Additionally, MailDefense removes infected files ignored by ZoneAlarm, such as infected document files and scripted email worms.

The Microsoft Outlook Email Security Update provides three levels of protection for executable attachments other than Office documents. This protection is for Microsoft Outlook users only:

Level 1:
Incoming executables: The attachment remains with the email but cannot be directly accessed. Incoming files in this level cannot be opened, saved, or forwarded.

Outgoing executables: Receive warning that the file is "potentially unsafe".

Appendix 1 compares level one extension handling with MailDefense, ZoneAlarm, Norton AntiVirus, and McAfee VirusScan.

Level 2:
Incoming files specified by administrators can be saved to disk in order to open them.

Level 3:
All others. Nothing occurs.

Office Documents
Word – considered Level 3
Excel – considered Level 3
PowerPoint – considered Level 3
Access – considered Level 1

Scripts and ActiveX in email
Security permissions raised to prohibit unsigned ActiveX controls and some scripting disabled.

Critics opposed the Outlook security patch, objecting to attachment blocking that left the user with no options for retrieval and no ability to uninstall or configure the patch.

Summary

While many solutions exist for virus protection, only MailDefense addresses the underlying problem: email, while still keeping control where it belongs: the user. By removing the harmful active content embedded within email, users are protected from email viruses such as Kak and BleBla, and against header vulnerabilities that allow viruses such as Nimda and BadTrans.b to automatically execute on the system. Microsoft Office application files are left fully available to users who share them via email, with any potentially harmful macros removed. Finally, executable file attachments can no longer disguise themselves by taking advantage of Microsoft Windows default extension suppressing. Users will no longer be vulnerable to the Pandora's Box syndrome of opening any attachment received in email, and extension re-registering ensures true identification and alerting to the user. Because MailDefense requires no updating and no configuration, users are free to use their email without concern over email-borne viruses. Indeed, the hallmark of MailDefense is its ability to deliver virus-free, worry-free email, with no hassles, no configuration, and no updates required.