



Zero-Hour Anti-Virus Defense

March 2005. Report #538

Ferris Research Product Brief

Ferris Research, Inc.
408 Columbus Ave., Suite 1
San Francisco, Calif. 94133, USA
Phone: +1 (415) 986-1414
Fax: +1 (415) 986-5994
www.ferris.com

Zero-Hour Anti-Virus Defense

Executive Summary

Companies have invested heavily in anti-virus defense on email boundary servers, email and other internal servers, and on client systems. This highly distributed approach is necessary because computer viruses can enter and propagate within an enterprise from a variety of sources.

Despite this large investment, organizations are still vulnerable to email-borne viruses that appear immediately after the so-called zero hour. That is, during the gap between their initial outbreak and the arrival of a matching anti-viral signature. This is typically a gap of some 10 hours.

Recently a number of approaches to eliminating this gap have entered the market, significantly reducing the chance of a rapidly propagating, email-borne virus entering an enterprise during this window of vulnerability.

Computer Viruses

In this report we employ the term “virus” to refer to all forms of malware, including viruses, worms, and Trojan horses.

Viruses often arrive as email attachments. When the attachment is executed, it does one of the following:

- Installs itself in a file and instructs the operating system to execute it on startup, at a scheduled time, or on the occurrence of some event.
- Overwrites an existing file that the operating system already executes, either on startup, at a scheduled time, or on the occurrence of some event.
- Inserts itself into an existing file that the operating system normally executes upon startup, at a scheduled time, or on the occurrence of some event.

A virus will also propagate itself to other computers. It does this by:

- Attaching itself to the boot sector of a writable floppy disk or other removable boot media.
- Including itself as the payload of email messages.
- Inserting itself directly into another system by exploiting a security vulnerability in some protocol. (Strictly-speaking, this is the behavior of a “worm,” not a “virus.”)

Traditional Anti-Virus Approaches

Traditional anti-virus techniques work by scanning files on hard disks or email attachments to determine whether any files include viral code. Basically, this consists of matching the contents of a file against a library of viral patterns, known as “viral signatures,” to determine whether the file contains a virus. Of course, this means that the detection of viral code is dependent upon the availability of an appropriate viral signature.

In order to run efficiently, anti-virus programs employ a variety of optimizations. For example, they will typically:

- Remember the identity of files that have already been scanned, and only rescan them if they have been modified (by verifying a checksum).
- Scan a file once for all possible viral signatures, rather than once for each viral signature.

Remaining Vulnerabilities

Following the arrival of a new computer virus, there is a window of vulnerability that occurs between an initial infection (the zero hour) and the publication of a matching viral signature.

The good news is that it has always been possible to construct a vaccine in the shape of a matching viral signature. Organizations often subscribe to several virus filter services, to increase the chance that a given virus will be caught.

The bad news is that it typically takes about 10 hours from initial release of a virus until a service distributes the corresponding signature. Lags of between four and 16 hours are typical.

During the window of vulnerability, email-borne viruses wreak considerable damage. As a panic response, users who rely on their computers are often told to stop work for several hours, or networks are disconnected, until a plan of action can be adopted by technical staff.

Recent Examples

During 2004, roughly 15 rapidly propagating email-borne viruses penetrated signature defenses in this way. The Dumaru, MyDoom/Novarg/Shimg, and Beagle/Bagle families of viruses are examples.

The initial outbreaks of each virus family are usually the most serious, from a zero-hour perspective. This is because “old” signatures often catch later versions in the same family. These are usually denoted by the letter ‘A’: e.g., *MyDoom.A*.

During the early spread of such infections, a typical mid-size organization in the US could have expected to receive around **25** separate copies of the virus by email, before signatures were available, assuming a five hour window of opportunity. However, that inbound rate is only the beginning of the organization's problem.

The inbound attacks would likely infect a proportion of the user PCs inside the organization. This would cause a cascade of additional email copies, each PC being capable of sending a conservative ten copies per second, many of which could infect other PCs in the organization. In total around 1,000,000 copies of the virus would typically be sent during the five hour window, peaking at an arrival rate of 100 per second.

This viral load would cripple many corporate email systems installed today. In addition to email, the organization's network performance would also be seriously damaged by malicious use of other viral vectors, such as network file shares.

Zero-Hour Countermeasures

This has led a number of new entrants to the anti-viral field to develop zero-hour, or near-zero-hour, approaches that target this window of vulnerability. Two such vendors are MailFrontier and Avinti.

Avinti is taking a novel approach, which is to invoke suspected email attachments—a category that includes in-line objects—inside a virtual machine “surrogate” for each recipient's computer. If an attachment is determined to have propagated itself, caused damage, or otherwise acted suspiciously, then it is deemed to carry a virus and is treated accordingly. If it hasn't, then it is deemed safe.

Note that Avinti's approach is used not only on obviously executable attachments such as .exe, .pif, and .com files, but also on apparently passive attachments such as .jpg files that may exploit a security hole to trigger their nefarious viral activity. Like conventional anti-virus filters, it also detects attachments encapsulated in .zip or other compressed-format files.

The good news about the Avinti approach is that it is a true zero-hour anti-virus defense.

The bad news is that there is a class of email-borne viruses that depend upon user input to trigger their behavior, and therefore will not be detected by Avinti virtual machine technology. The Bagel family is an example that has already been observed in the wild. This is probably more of a theoretical weakness. Viruses that require operator input to trigger their transfer to other systems are incapable of explosive propagation. So the fact that they escape detection by Avinti technology should not constitute a significant threat.

We describe MailFrontier's offering in the next section.

MailFrontier

MailFrontier sells an appliance and software that protect against unwanted email, including:

- Spam and viruses.
- Phishing attacks. An example of phishing is when an email pretends to be from a “trusted” source, so as to get someone to give away access to his or her personal finances, or to a corporation’s financial, employee, or intellectual property information.
- Directory harvest attacks. Here, someone determines valid email addresses at an organization by sending a very large number of emails to people with slightly different email addresses. The ones that aren’t bounced represent valid email addresses, and are often then used for sending spam, phish, or other unwanted malicious email.

There’s also a policy management capability, which allows the user to define what should happen when certain types of email are sent or received. For example, if an email is received from a competitor or is sent to a competitor, a copy can be sent to the HR department; or if an email contains profanity, it’s quarantined pending management approval.

The MailFrontier appliance or server software is located at an organization’s Internet boundary.

In the three years since MailFrontier was founded, the company has often been a technology innovator. It was early to apply multiple techniques to identifying, classifying, and filtering email as spam. It was also early in offering group and end-user mailbox-level filtering using LDAP definitions.

More recently, the company was one of the first vendors to filter phishing emails not as spam, but as phishing emails, and to then place them in a separate “fraud” quarantine.

How MailFrontier’s Time Zero Technology Works

MailFrontier’s virus control is innovative. It’s a layered approach, and works in conjunction with existing anti-virus defenses.

First, incoming email is scanned in a conventional way, using virus signatures from either Kaspersky Lab or McAfee, or both. The choice of Kaspersky is worth noting, because this lesser-known anti-virus firm has consistently detected and distributed signatures at the earlier end of the window of vulnerability.

Second, to cover the possibility that signatures have not yet been distributed, MailFrontier then applies what it terms “Time Zero” technologies. A series of tests (known as “heuristics”) takes place to check if the email looks suspicious. For example, the tests check whether the attachments are:

- .exe files, with misleading names that give the impression that they are .jpg files, as in *picture.jpg_____exe*.
- Written so as to exploit security holes in the MIME format.
- Files that internally look like .exe files, but which purport to be normal documents or text files.

These heuristic tests are updated dynamically by real-time sensing of email traffic patterns on the Internet. For example, MailFrontier monitors for sudden large-scale email distributions. If they contain potentially dangerous attachments with similar properties, then the heuristic filters are updated to place such emails in quarantine, pending validation or identification as a virus.

MailFrontier also monitors a series of test mailboxes for emails with potentially dangerous attachments. The heuristic filters are updated when a virus is recognized.

In addition, MailFrontier says it maintains a network of more than 825,000 human users. They can report a suspicious email on the fly, thus providing early warnings. These emails are analyzed to determine if there is in fact a new virus outbreak, in which case the heuristics filters are updated.

The final screening can, optionally, take place using Avinti's anti-virus technology. As discussed earlier, this conducts a virtual machine simulation to identify errant behavior.

MailFrontier (www.mailfrontier.com) offers a free 30-day trial of its products, including the anti-virus technology. For a trial of MailFrontier Gateway Appliance, see www.mailfrontier.com/forms/products_app_trial.jsp. For a trial of MailFrontier Gateway Server, Enterprise Edition, see www.mailfrontier.com/forms/register_asgtrial.jsp.

Authors: Nick Shelness, David Ferris, and Richi Jennings

Research Note Sponsored by MailFrontier

MailFrontier commissioned this document with full distribution rights. You may copy or freely reproduce this document, provided you disclose authorship and sponsorship and include this notice. Ferris Research independently conducted all research for this document, retaining full editorial control. The purpose of this document is to describe the sponsor's offering and put it in its industry context. All products and services have their weaknesses, and these are not discussed in this document.

Ferris Research

Ferris Research is a market research firm specializing in messaging and collaborative technologies. We provide business, market, and technical intelligence to vendors and corporate IT managers worldwide with analysts located in North America, Europe, and Asia/Pacific.

To help clients track the technology and spot important developments, Ferris publishes reports, white papers, bulletins, and a news wire; organizes conferences and surveys; and provides customized consulting. In business since 1991, we enjoy an international reputation as the leading firm in our field, and have by far the largest and most experienced research team covering messaging and collaboration.

Ferris Research is located at 408 Columbus Ave., Suite 1, San Francisco, Calif. 94133, USA. For more information, visit www.ferris.com or call +1 (415) 986-1414.

The Ferris Research User Panel

The User Panel consists of IT professionals who work with messaging and collaborative technologies, providing services to their organizations' users. People join to share experiences with other people like themselves, learn from each other, and keep current on news and trends.

If you provide technical support for an email system, and you are not a member of the User Panel, you can join and learn more about the User Panel at www.ferris.com/url/userpanel.html. There is no charge to join.

Recent Reports From Ferris Research

Bulletin: Microsoft IT Forum, Copenhagen, Denmark
Microsoft's Lookout Search Tool
Bulletin: Exchange Best Practices Analyzer Tool
Zero-Hour Defense Against Email-Borne Viruses
Implementing the Sender ID Framework in DNS
Syndication for Information Consumption and Publication
Sarbanes-Oxley and the Messaging Manager
An Assessment of Windows Sharepoint Services
Ironport's Virus Outbreak Filters
Voltage's Encrypted Email
Gwava and GroupWise Security
Email Records Management Survey: Guidelines, Technologies, and Trends
Spam: Corporate Practices and Priorities in 2004
New Trends in Spam
The Impact of CAN-SPAM on Legitimate Direct Marketers
Upgrading from Exchange 5.5 to 2003: A Financial Case Study
Bonded Sender: A Program for Legitimate Mailers
Exchange Server Reliability
Spim: Spam Over Instant Messaging
Gmail: Google's Entry Into the Webmail Market
Microsoft Tech-Ed 2004: A Messaging Perspective
The Cost of Migrating From Exchange 5.5 to Exchange 2003
Exchange Server Reliability
Electronic Privacy and Security Regulations
A Survey of Exchange Installations: Key Statistics
CIO Messaging Concerns and Priorities
Recent Innovations in Macintosh Collaboration
FrontBridge TrueProtect Email Boundary Security Service
Cloudmark's Spam "Immune System": Fighting Spam with Genetic Algorithms
The State of Email Denial-of-Service Attacks
Instant Messaging: Current Status, Key Trends
How Not To Be a Spammer – Updates
The Growing Threat of Questionable Patents
Bayesian Filters for Spam Control
Another Alternative to Exchange Servers at Branch Sites
Lotusphere 2004
TCP/IP Bandwidth Shaping as an Anti-Spam Measure