

# Outbreak Detection and Management

## Outbreak Detection and Management:

### Abstract

---

Throughout 1999 and 2000, virus and worm attacks have increased in intensity, and have gained more media attention and public awareness. This is principally because many of the more notorious viruses and worms took full advantage of the Internet to spread, beginning a long predicted assault. This, apparently random, flood of viruses impacted e-mail systems, web sites, newsgroups and other available channels, growing almost exponentially. They worked their way into network environments, spreading quickly and leaving a costly trail of disruption in their wake. The only requirement you needed to be repeatedly attacked was to be listed on another company's email system. When they were infected, you were the next target.

The ICSA Labs Computer Virus Prevalence Survey 2000 reports that Internet e-mail attachments were the source of 87% of the virus encounters in 2000. In 1999 this was 56%, and 32% in 1998. Hackers and virus writers have realised that the increased use of the Internet within businesses and homes has provided them with an enormous communications infrastructure to exploit. As virtually all Internet users use e-mail, it has become the preferred method of virus distribution. Internet e-mail provides writers with an easy means of replication with little effort on their part. They no longer have to devise schemes for virus replication or rely on file distribution; flexible e-mail systems offer scripted methods of generating mail.

Ultimately, this leads to fast and wide distribution. We have seen many different types of viruses making use of mail systems for distribution recently; Melissa, LoveBug, KAKworm to name but few.

The impact of a threat can be measured in many ways. The most telling sign of the worm impact on modern day folklore is how they are now familiar to the general public, having been publicised, criticised and reported upon in most corners of the world. Their effect, cause and suspected authors have been documented by everything from the computer press to the daily tabloid journals.

E-mail and Security Experts know the damage that these viruses and "Trojan Horses" can cause. In many cases, they result in the loss of service of a business critical system. This could disrupt an organisations day to day internal operation, or could prevent them from dealing with potential customers. This can be damaging to the business and reputation of the professionals involved in maintaining those systems.

*"The world changed [on March 26, 1999]—does anyone doubt that? The world is different. Melissa proved that ... and we are very fortunate ... the world could have gone very close to meltdown."*

*—Padgett Peterson, Chief Info Security Architect, Lockheed Martin Corporation, on the 1999 "Melissa" virus epidemic*

The biggest problem facing an administrator is the detection of new viruses and Trojans before their prevalence escalates into an outbreak. Their spread and proliferation is so great that it is difficult for even the most diligent administrator to detect the infiltration of a new virus. Most administrators have high workloads and are only human, which means they can't act as dedicated network monitors 24 hours a day, 7 days a week, 365 days a year. Whilst Microsoft Windows NT and other Operating Systems provide tools to profile and monitor the OS, and products like Microsoft Exchange offer performance counters, their use is limited because they are essentially passive. The administrator has to know about the problem and then use these tools to find the cause. It is this issue of outbreak detection that this white paper will address.

Who should read this paper?

CIO's, network administrators, security experts and anyone responsible for information security within an organisation should read this paper. The areas of responsibility might include the firewall, router, e-mail system or workflow system.

**BACKGROUND: The How, What and When of an Outbreak**

As already mentioned, e-mail systems have become the preferred distribution method of the virus writer/hacker. Why? Most e-mail systems will have at least one point of connectivity to the Internet, and scripting languages such as JavaScript and Visual Basic scripting have lowered the barriers to programmatically sending e-mail. The virus writer no longer needs to learn the intricacies of MAPI or Lotus C API, which are difficult to use and require high levels of skill and extensive knowledge of the e-mail system. The use of high level scripting languages can achieve in 5 lines of code what could take 20 to 40 lines using these API's.

Most e-mail systems will have at least one point of connectivity to the Internet designed for efficient throughput and heralded for its ability to deliver information quickly and easily to any part of the company – even to the extend of tracking this performance through an SLA.

The most recent new virus/Trojan attacks have specifically targeted the Microsoft Outlook and Exchange environments. Whilst Microsoft have made these systems easily configurable by the end user, this has also opened them up to the virus writer/hacker. Viruses like macros and worms cause havoc amongst the business community.

This is further proven by figures from McAfee AVERT labs. As of November 2000, AVERT were receiving over 400 new viruses for Microsoft platforms per month, as opposed to 1 or 2 viruses per month for non-Microsoft platforms. This equates to over 99% of new viruses being created to exploit Microsoft platforms.

### How?

E-mail-borne viruses typically (but not exclusively) enter organisations via the Internet as file attachments. How are they distributed? They simply require the user to open the attachment. By opening the attachment, the user is unwittingly running a Visual Basic script. This script will iterate through the address book on the Exchange Server (for example) sending a cloned message with the attachment to users in the address book creating an initially invisible (to the user) mail storm. Some viruses, like Melissa, e-mail the cloned message to the first 50 e-mail addresses in the address book. Unfortunately, in many organisations, the standard is to prefix department, site or global mailing lists with characters such as '#', '!' and '\$'. Due to the sorting of the address list these appear at the head of the directory, and the Trojan e-mails get sent to the widest possible audience.

### What?

The net result of one of these mass mailer viruses is not necessarily the permanent damage that some viruses cause, but the complete congestion of the mail system – or Denial of Service (DoS) as it is more commonly known.

The mass mailer will cause sufficient load on the mail servers within an organisation to cause them to become overloaded, slowing and eventually preventing mail delivery to users and customers alike. The administrator will almost inevitably have to isolate the e-mail server and other mail services in order to resolve this problem.

The management of the eradication of a mass mailer virus is difficult. Whilst the IT group need to provide uptime to its users, the eradication process usually requires substantial downtime. This downtime is required to perform on-demand scans across the e-mail system's database, to prevent the re-activation of any viruses that have already infiltrated the system.

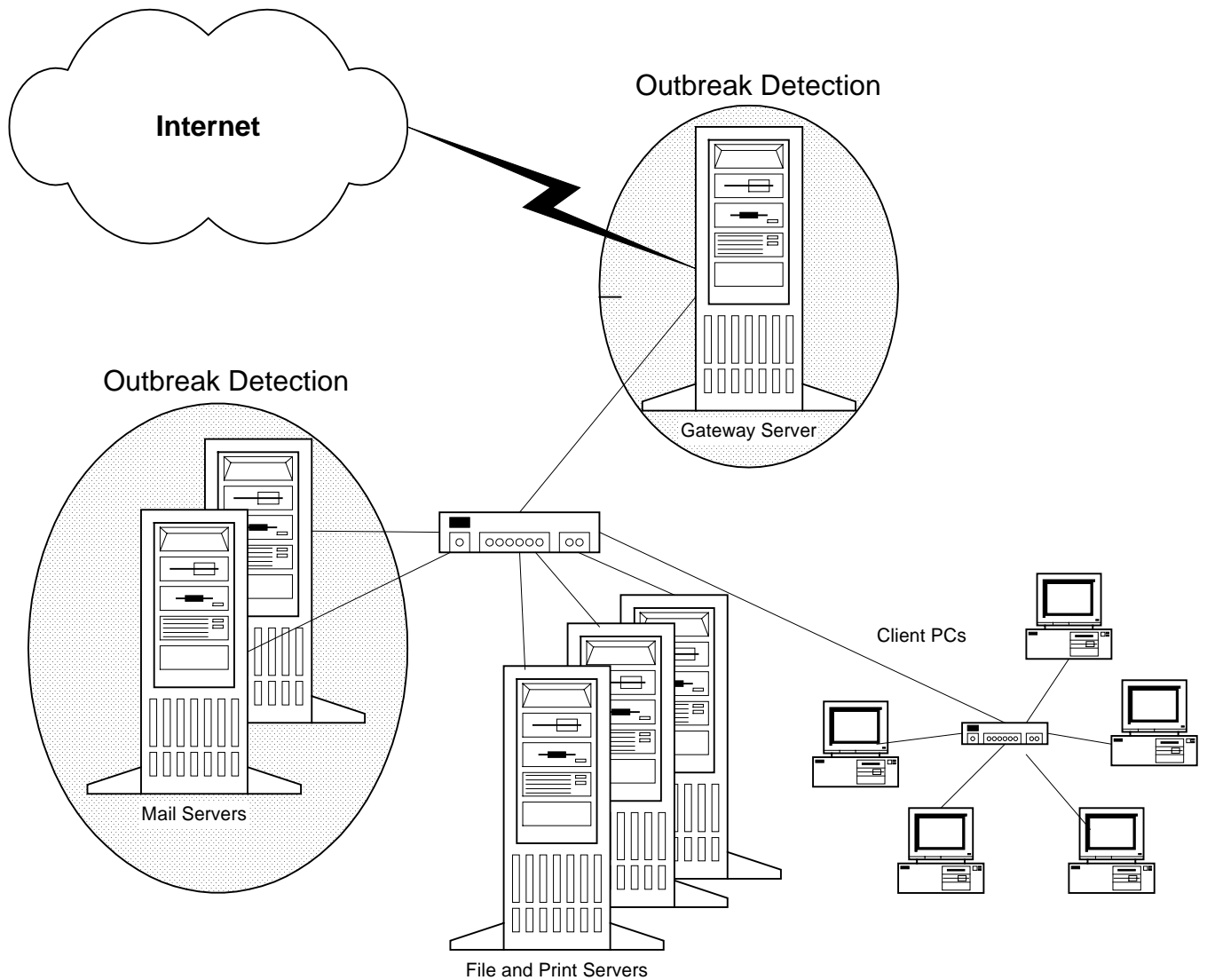
### When?

The 'when' of a virus outbreak is not when it starts, but when it's detected. Unfortunately, this is usually after the damage has been done. The time difference may only be 2 or 3 hours, but the difference in cost can be huge. For example, when Melissa was first detected on the 26<sup>th</sup> March 1999 it was early morning. By midday reports were being received from all around the world. This was an extremely fast spreading virus but by no means the fastest.

So how does an administrator detect the outbreak of a new virus like Melissa before it escalates? Some especially diligent administrators may detect increased activity on their mail servers, indicating that something is happening, but the cause of the problem will still need to be established. However, most administrators will not be watching the performance of their mail servers at the time of an outbreak, and will only become aware of the outbreak when alerted by users or helpdesk staff. By this time, of course, the damage has been done.

## Challenges and Requirements of an Outbreak Management Tool

Outbreak detection is a challenge. There are multiple points in the network where an outbreak can be detected and controlled. Given the nature of recent virus attacks, the focus should be on the Internet gateway and e-mail servers. In the diagram below, this would mean monitoring each mail server and a gateway server, 24 hours a day, 7 days a week.



If network administrators were able to achieve this, they would effectively be performing the following:

- Monitoring
- Detection
- Identification
- Action

What is needed is a mechanism to monitor for 'outbreak-like' behaviour at all times. A system that can detect patterns in e-mail traffic and act accordingly to prevent an outbreak from occurring, but that doesn't require dedicated administrator resource.

To do this, an Outbreak Management Tool is likely to need the following attributes.

#### Flexible Rules Based

The implementation of Outbreak Management will vary between organisations. Some may wish to enforce strict rules whilst others more lax. The events that a company may wish to monitor will also differ; some may wish to monitor attachments or attachment types, others may monitor actual known viruses caught.

In addition, the action carried out during a virus outbreak will differ from one company to another. In a large organisation the administrator will probably not choose to shut down their MS Exchange servers as their first line of defence, whilst in a small company this may be more acceptable.

The key is flexibility. No two companies are the same and all will react to a potential outbreak differently. Therefore, an effective Outbreak Management system must employ a rules-based approach.

#### Monitor

For an Outbreak Management system to be effective, every e-mail passing into a network and through the mail servers must be watched. It must record data and information about an e-mail as it passes with minimal or no impact on the system itself. This is a huge challenge. The type of information recorded can be used to uniquely identify each attachment, and the number of times the attachment has been received. This type of information will help determine if an outbreak, such as LoveBug is occurring, regardless of whether the virus is known.

#### Automatic Response

An automatic response to an outbreak is essential. The time taken for e-mail based viruses to spread within a large organisation and worse still be sent on out to the organisations peers and partners is minimal. Many attacks happen before an administrator can intervene, so the system must be able to take corrective action to solve the problem. It also needs to be empowered to react to the outcome of its actions, so if corrective action x fails, then, after crossing a predefined threshold, the Outbreak Management system should escalate the response and perform action y.

#### Manual Response

Alternatively, the administrator may wish to decide the outcome of the outbreak. In this case there should be some expert based system suggesting the actions required to quell the outbreak. Or, the Outbreak Management system can simply alert the administrator and they can decide what action to take, based on their previous experience.

### Enterprise Management

The Outbreak Management Tool needs to be managed across the enterprise. Administrators require the ability to deploy and role out rules across the enterprise from one desktop, so that in an outbreak situation new rules can be rolled out quickly and efficiently.

## **The Solution - McAfee Outbreak Manager**

McAfee are the first to provide a solution to the outbreak management challenge described in this document. It is a software solution, aptly named Outbreak Manager, and it is a component of McAfee's e-mail based anti-virus scanners; WebShield SMTP 4.5, GroupShield Exchange 4.5 and GroupShield Domino 5.

### **Product features**

#### Rules based management

Outbreak Manager allows administrators to create a rules based outbreak management system. Administrators would typically set up multiple rules specific to their individual environments.

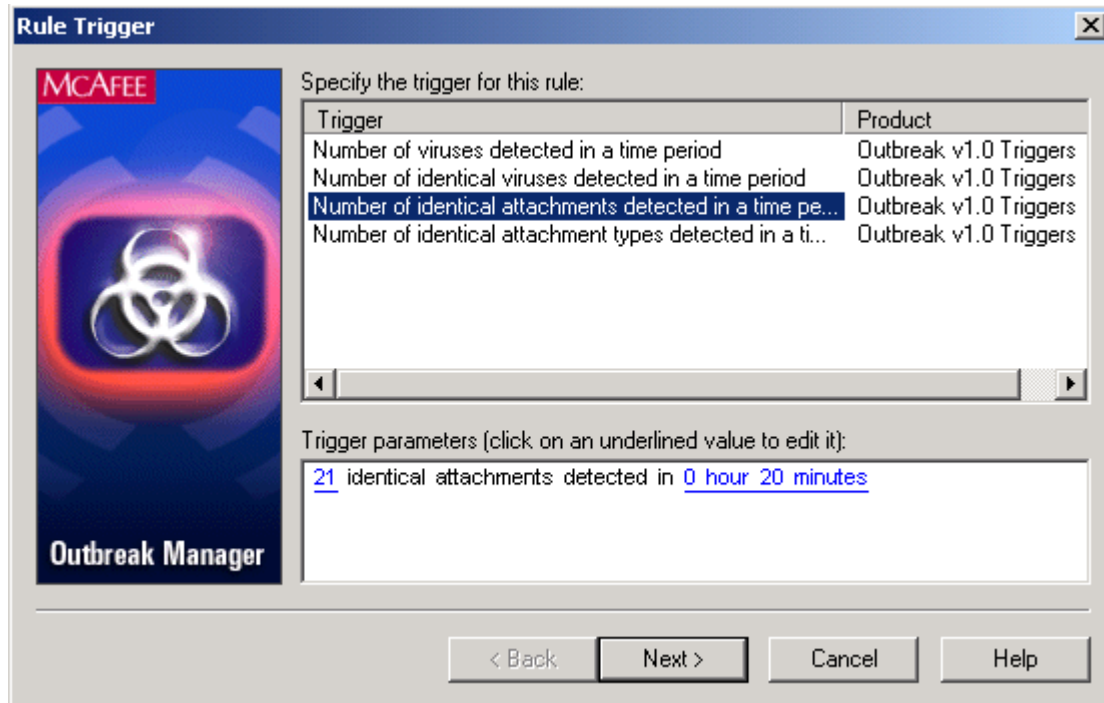
Each rule has four components; a trigger, threshold, a reaction and action or actions.

#### Triggers

There are four possible triggers

- Number of viruses detected in a time period
- Number of identical viruses detected in a time period
- Number of identical attachments detected in a time period
- Number of identical attachment types detected in a time period

In each case, the administrator can specify the number and the time period. For example, in the illustration below, the user has started to create a rule set to trigger when 21 identical attachments have been received within 20 minutes.



The trigger thresholds will of course vary from company to company. It may be inappropriate to use this trigger in a large organisation where a number of users receive financial report spreadsheets as attachments every Monday.

Multiple rules can be created using one trigger with different thresholds, to create an automatic escalation procedure.

### Response

Outbreak Manager has two primary response types, but can also apply a combination of the two. A response can be pre-configured to perform actions automatically or with manual intervention.

The automated response will carry out the first pre-configured action. If, after a period of time the trigger is still in an active state, then Outbreak Manager will escalate the response to the next configured action.

A manual response will prompt the administrator to carry out the pre-determined recommended action.

Outbreak Manager also offers a third response to an outbreak. By specifying the administrator's normal office hours, a rule can be configured to react automatically outside of office hours, but prompt for manual intervention during the day.

### Actions

Outbreak Manager offers action options appropriate to the platforms it is installed on.

The actions available for Outbreak Manager on a GroupShield Exchange server are

- Increase scan options by turning on file heuristics, macro heuristics, OLE scanning, compressed files, archived files and scan all files
- Reduce notifications
- Perform a DAT update
- Perform an on demand scan
- Block specific attachments
- Set actions to delete attachments
- Block all attachments
- Shutdown Exchange server and restart
- Shutdown Exchange server

The actions available for Outbreak Manager on a GroupShield Domino server are

- Increase scan options by turning on file heuristics, macro heuristics, OLE scanning, compressed files, archived files and scan all files
- Perform a DAT update
- Perform an on demand scan
- Shut down server
- Shut down mail router task

The actions available for Outbreak Manager on a WebShield server are

- Perform a DAT update
- Increase scan settings
- Reject inbound mail
- Block e-mail with attachments
- Stop the MailScan service

A rule can have multiple actions. For example, on GroupShield Exchange, using the trigger shown earlier, an administrator could choose to have a rule that performs a DAT update and carries out an on-demand scan.

## Example

Using Outbreak Manager on a WebShield SMTP server, a company could set up the following rules

### Rule1

Trigger – 20 e-mails with the same attachment received within 15 minutes

Response – Automatic, and notify the administrator via e-mail

Action - look for a new DAT update

Rule2 – 50 e-mail received with the same attachment in 25 minutes

Response – Alert administrator by pager for manual intervention if within office hours

Action – Block e-mail with attachments, look for a new DAT update

By applying these rules, a company would be able to prevent themselves from becoming flooded with virus produced e-mail, and equally importantly, prevent their mail servers from spreading the virus to other organisations.

Similar rules configured on the MS Exchange or Lotus Domino servers, using Outbreak Manager on GroupShield, would then alert the administrator, allowing them to intervene and quickly create a rule to delete the specified attachment or attachment types. In this way, the Outbreak could be controlled so successfully that the e-mail service would not even be disrupted.

Using Outbreak Manager in this way, companies like leading UK Internet Service Provider Drakken Ltd. can guard against being victims of new viruses that are distributed by e-mail.

**“Drakken relies on the Internet to drive our e-business initiatives with partners and customers, and we can ill afford to be offline if there is a virus outbreak like the Love Bug,” said Ian Hill, technical director of Drakken Ltd. “McAfee Outbreak Manager provides the extra layer of security against the potential damage caused by viruses allowing us to watch our Internet infrastructure 24x7 for unusual outbreak-like activity and address it immediately, before it can cause any damage.”**

## **References**

---

*GroupShield Exchange 4.5 Administrators Guide 25-April-2000-08-28*

## **About McAfee**

---

On December 1, 1997, McAfee Associates merged with Network General Corporation, Pretty Good Privacy, Inc., and Helix Software, Inc. to form Network Associates, Inc. The combined Company subsequently acquired Dr Solomon's Software, Trusted Information Systems, Magic Solutions, and CyberMedia, Inc.

A January 2000 company reorganization formed four independent business units, each concerned with a particular product line. These are:

- **Magic Solutions.** This division supplies the Total Service desk product line and related products
- **McAfee.** This division provides the Active Virus Defense product suite and related anti-virus software solutions to corporate and retail customers.
- **PGP Security.** This division provides award-winning encryption and security solutions, including the PGP data security and encryption product line, the Gauntlet firewall product line, the WebShield E-ppliance hardware line, and the CyberCop Scanner and Monitor product series.
- **Sniffer Technologies.** This division supplies the industry-leading Sniffer network monitoring, reporting, and analysis utility and related software.

Network Associates continues to market and support the product lines from each of the new independent business units. You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to the Network Associates Customer Service department at the following address:

Network Associates Customer Service  
4099 McEwan, Suite 500  
Dallas, Texas 75244  
U.S.A.