Global Information Assurance Certification Paper

W32.Mydoom.M Worm

GIAC Certified
Incident Handler

Practical Assignment

Version 3.00

Date Submitted: 10/05/04

Michael Gunn
On-Line Course

Table of Contents

Introduction

A worm by definition is a program that propagates itself over a network, reproducing itself as it goes. [2]

Although the first so called worm program (the Creeper, 1971 by Bob Thomas) [1] was created as a non-malicious program, subsequent worms written by different individuals have become very malicious which in-turn has caused many businesses to loose billions of dollars and countless man hours.

The Mydoom worm variant - Mydoom.A, was released on January 26, 2004. It caused major damage to various networks (i.e. www.sco.com), and infected millions of computers on the Internet at a staggering rate never seen before.

Worms like this have prompted many large corporations to start putting bounties on the creators of these malicious programs. In January, Microsoft put up a $250,000 bounty for information leading to the arrest and conviction of MyDoom's creator. SCO has also put up a $250,000 bounty on head of the same, elusive individual. [17]

On July 26, 2004 a new variant of the Mydoom worm known as W32.Mydoom.M was released on the Internet. This worm caused major disruption for many of the big search engines companies like Google, Yahoo, Altavista, and Lycos. The disruptions ranged from slow access when processing search request to failed search request.

Statement of Purpose

In this paper, I will describe the Mydoom.M worm exploit and take the reader through an infection of the Mydoom.M worm that occurred at GZAC Inc. The reader will also learn the different phases of the Mydoom.M worm exploit. Lastly, this paper will summarize the six incident handling steps (Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned) that we followed to resolve the Mydoom.M worm outbreak in our organization.

The Exploit

Overtime the Mydoom worm writers have modified the code so the social engineering style has become more and more believable, thus gaining the trust of the recipient so that they will open the attached file and become infected.

Social Engineering is a term used in Information Security where by an individual (usually a would be attacker) will attempt to trick another unsuspecting individual into providing confidential information or executing files, thus allowing the attacker to compromise the target system or systems. With the Mydoom worm variants the social engineering goal is to trick unsuspecting users into opening the attachment so that the user will become infected, thus propagate the worm.

The W32.Mydoom.M worm is a mass-mailing worm, which spreads by emailing itself via its own SMTP engine. [8] Once a user becomes infected with the W32.Mydoom.M worm it plants a Trojan horse program on the infected system that will allow attackers to gain unauthorized access to the infected system via TCP port 1034. The Trojan horse that is planted on the infected system is called Backdoor.Zincite.A. [3] We will discuss this Trojan program in more detail in the "Description and Exploit Analysis" section.

In figure 1, we see an example of how the W32.Mydoom.M variant uses social engineering to try and trick the unsuspecting user into opening the infected attachment.

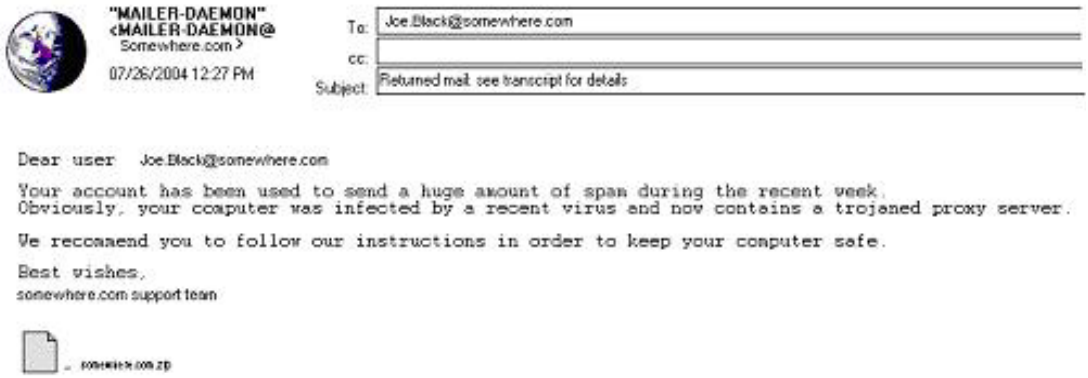


Figure 1 – Sample Mydoom.M email

Exploit Name

W32.Mydoom.M@mm [3]

Looking at the original worm name specified by Symantec – 32.Mydoom.M@mm [3], we can break down the name as follows:

- W32 – Win32, this signifies that the virus or worm is a 32-bit windows file infector
- Mydoom.m – Signifies the name of the virus or worm
- @mm – Signifies that the virus or worm is a mass mailing

Aliases Include:

- I-Worm.Mydoom.M [11]
- I-Worm.Mydoom.R [9]
- MyDoom.M [10]
- Mydoom.M@MM
- W32.Mydoom.M@mm [3]
- W32/Mydoom-O [12]
- W32/Mydoom.L [13]
- W32/Mydoom.N.worm [14]
- W32/Mydoom.o@MM [5]
- Win32.Mydoom.O [15]
- WORM_MYDOOM.M [16]

Discovery Date: July 26, 2004

US-CERT issued an alert SA04-208A that describes the Mydoom.O worm. [4] CERT mentioned the Mydoom.M worm in their current activities listing [39]

Operating System

The Mydoom.M worm and associated variant are targeted specifically at the Microsoft Operating Systems (OS). The Microsoft versions that are affected include: [3]

- Windows 95
- Windows 98
- Windows ME
- Windows NT
- Windows 2000

- Windows Server 2003
- Windows XP

The Mydoom.M worm will affect all Windows OS'es listed above despite the service pack level.

Protocols/Services/Applications

The W32.Mydoom.M worm uses it's own Simple Mail Transfer Protocol (SMTP) engine as a means to generate and send email messages to unsuspecting recipients. SMTP is a Transmission Control Protocol/Internet Protocol (TCP/IP) that resides on the Open System Interconnect (OSI) layer 4, which is used to send and receive email. The object of Simple Mail Transfer Protocol is to transfer mail reliably and efficiently. [23]

SMTP mail transfers are executed as follows:

The mail client initiates a connection to a mail server on TCP port 25 - SMTP port. The mail server begins communicating a string of text to the mail client (mail server id, state – ready to send or not?). A request is made from the mail client to send a message. The mail server will either accept the message or discard the message. Once the message is accepted, the message is sent to a SMTP mail spooler. In the SMTP mail spooler the message is queued for delivery. Once the message is in the queue, the mail server checks to see if any messages are waiting or queued to be delivered. The mail server then attempts to deliver the messages that are found in the queue. If for any reason the message is not deliverable, the mail server might attempt to deliver the message a second and third time (depending on the mail server setting). If at this point the message is not deliverable, the mail server will return the message to the original sender with an undeliverable error or it may discard the message all together. If the message is deliverable the mail server sends the message to its intended destination and the connection is disconnected. This is known as an end-to-end delivery system. See Appendix for SMTP email send sequence diagram.

The overall procedures for SMTP can be found in the Request For Comments (RFC) database under RFC 821 and RFC 822. The Internet Architecture Board (IAB) issues RFC's. IAB is responsible for the consideration of all Internet related architecture. RFC 821 basically defines SMTP and specifies the protocol that controls the exchange of mail between two machines, while RFC 822 defines the structure for the header and body of the message sent via SMTP. A basic message header will contain: TO, FROM, DATE, SUBJECT.

TO: Michael Gunn <mgunn@osme.jikn.com>
FROM: Synji <Synji@royyu.com>
DATE: Mon 24 Aug 2000 00:00:00
SUBJECT: Test message

If we were to connect to a SMTP mail server and try to relay mail to a recipient it would look like this:

```
>>> HELO someone.abmike.com
250 fun.com Hello someone.abmike.com., pleased to meet you

>>> MAIL From:<bishop@someone.abmike.com>
250 <bishop@someone.abmike.com>... Sender ok

>>> RCPT To:<bishop@abmike.com>
250 <bishop@abmike.com>... Recipient ok

>>> DATA
354 Enter mail, end with “.” on a line by itself

>>> .
250 Mail accepted

>>> QUIT
221 fun.com delivering mail

bishop@abmike.com... Sent
sent.
```

The actual commands used to transmit the message above are:

- HELO – Used to identify the sender to the receiver
- MAIL From – Used to initiate a mail transaction
- RCPT To – Used to identify the sender of the mail message
- DATA – Denotes mail data from the sender
- QUIT – Specifies end of transmission, receiver must send an OK and close the channel

TCP and IP were developed by a Department of Defense (DOD) research project to connect a number of different networks designed by different vendors into a network of networks (the "Internet") [18].

TCP/IP is a two-layer program. The higher layer, TCP, is a connection oriented protocol that manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, IP, handles the address part of each packet so that it gets to the right destination. [19]

When an originating or “source” computer tries to initiate a connection with the destination computer or vice versa using TCP, there is a distinct handshaking method that takes place called the three-way handshake, this is also known as a connection oriented session or end-to-end session. The TCP three-way handshake happens in this manner:

1. The originator (source) sends a “SYN” (Synchronize) packet to tell the destination that they are trying to establish a connection and synchronize the bytes of data that will be transmitted back and forth.
2. The destination sends a “SYN ACK” (Synchronize Acknowledge) packet back to the source to inform them that they have acknowledged the initial packet and Synchronized the byte count with the originator.
3. The source sends an “ACK” (Acknowledge) back to the destination to let them know that they received the packet that was just sent.

Once the three-way handshake is established, the connection between the source and destination are open and they can transmit data back and forth. See Figure 2.

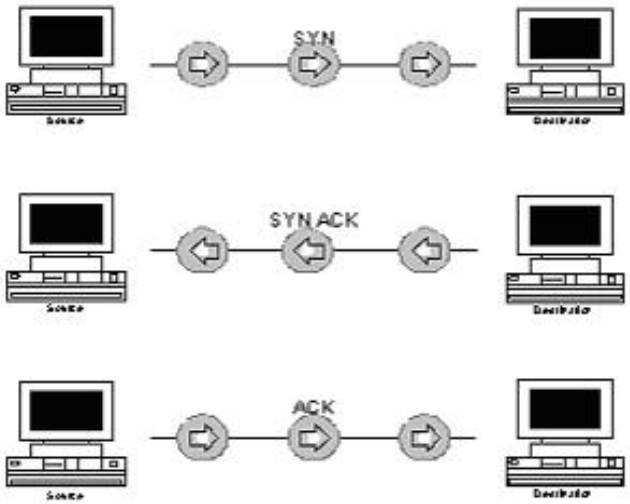


Figure 2 – Depiction of the TCP three-way handshake.

The Open System Interconnect (OSI) model, also known as the International Standards Organization (ISO) reference model, is a seven-layer reference model that is used to describe how network applications and devices communicate with each other. In the OSI reference model each level will communicate with the level above and below.

Layer 7 is placed at the top of the OSI model while Layer 1 is placed at the bottom of the OSI model. See figure 3.

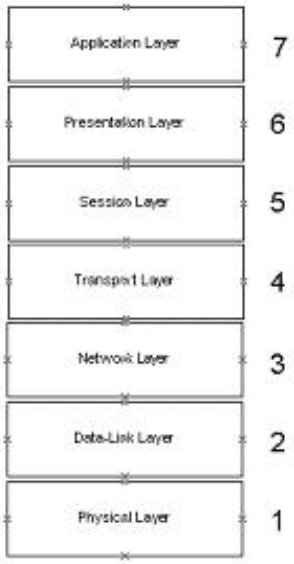


Figure 3 – Seven layers of the OSI Model

Each layer of the OSI reference model deals with a specific product or program as illustrated in diagram 1. [22]

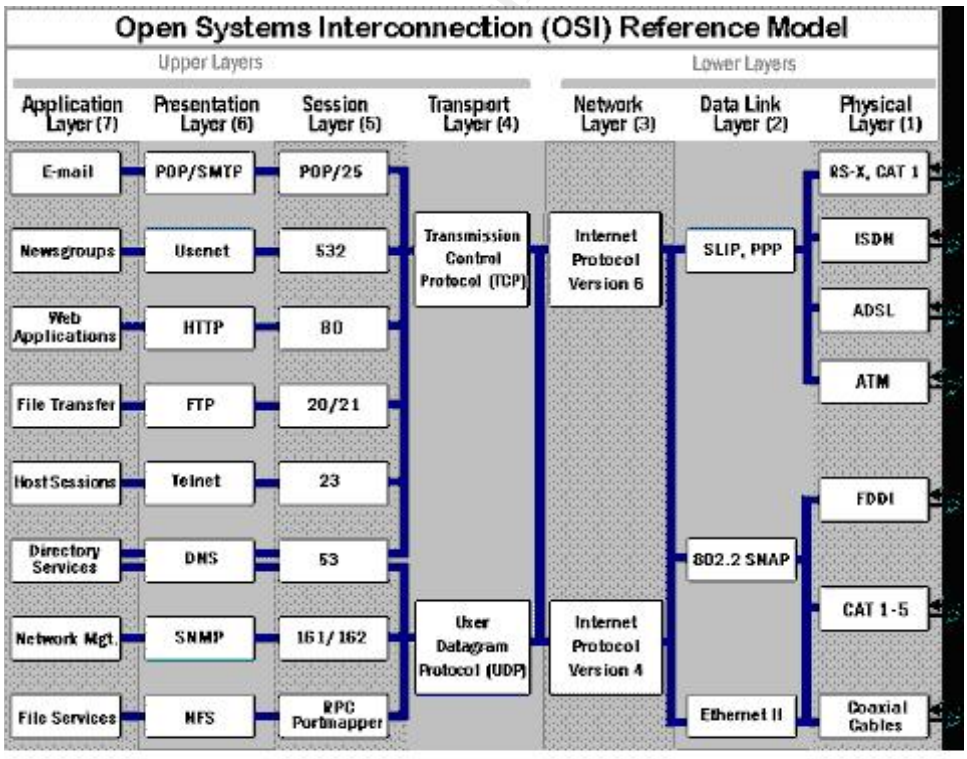


Diagram 1 – OSI Reference Model

The Mydoom.M worm queries the major search engines (Google, Yahoo, AltaVista, and Lycos) in an attempt to harvest more email addresses for

distribution. As we saw on July 26th this tactic caused a Distributed Denial of Service (DDoS) for some of the major search engines while slowing response times on others. As stated in theregister.com “Google goes gimpy from Mydoom infection”. [20]

Once an attacker compromises a system they sometimes install Trojan horse programs on the infected systems. These Trojan horse programs allow the attacker to remotely control the infected systems. In most cases infected systems are usually in the thousands. Most of these infected systems are used to mount an attack at certain targets. These attack that are mounted are called Distributed Denial of Service (DDoS). An example of this type of attack that caused major outages is the TRINOO and Tribe Flood Network attacks that were released in October 1999. [23]

It is unsure at this point in time whether or not the writers of the Mydoom.M worm coded the worm to have a DDoS affect on the major search engines such as Google, Yahoo, AltaVista, and Lycos, or if it was unintended and just a fluke. One thing’s for sure. Intended or not, it did impact the major search engines negatively.

Impact was also cause towards many mail severs, In our organization the mass amounts of emails that were queued to be delivered caused mail delivery to slow down. Where a regular email message with an attachment would take 1-2 seconds to reach its destination, the times were dramatically increased to roughly 20-30 seconds per email message. “A new variant of the MyDoom worm that hit the Internet hard on Monday is causing massive e-mail slowdowns across the Web.” [21]

Exploit Variants

To date there have been 13 Mydoom variants. A complete list below is compiled for easy viewing.

Variant	Description	Aliases	Discovered
W32.Mydoom.A@mm	• Mass mailing worm • Arrives as an attachment with the extension .bat, .cmd, .pif, .exe, .scr, .zip • Places a backdoor on the infected computer • Backdoor operates on ports 3127 to 3198 • Backdoor can be used to download and execute arbitrary files • Performs a DoS on www.sco.com • Size 22,538 Bytes	• W32.Novarg.A@mm, W32/Mydoom@MM [McAfee] • WORM_MIMAIL.R [Trend Micro] • Win32.Mydoom.A [Computer Associates] W32/Mydoom-A [Sophos] • I-Worm.Novarg [Kaspersky]	Jan 26, 2004
W32.Mydoom.B@mm.	• Mass mailing worm • Arrives as an attachment with the extension .bat, .cmd, .pif, .exe, .scr, .zip • Places a backdoor on the infected computer • Backdoor operates as a proxy that can allow attackers use the computer resources • Backdoor can download and execute arbitrary files • Performs a DoS starting Feb 3 against www.sco.com and against www.microsoft.com on Feb 1 • Contains a kill date to stop spreading on Mar 1 • Size 29,184 bytes varies in .zip format	• Mydoom.B [F-Secure] • W32/Mydoom.b@MM [McAfee] • WORM_MYDOOM.B [Trend] • Win32.Mydoom.B [Computer Associates] • I-Worm.Mydoom.b [Kaspersky] • W32/MyDoom-B [Sophos]	Jan 28, 2004
W32.Mydoom.dam	Damaged non working version of the W32.Mydoom.A worm	• W32/Mydoom.dam [McAfee] • I-Worm.Mydoom.a [Sophos] • W32.Mydoom.A@mm [Sophos] • WORM_MyDoom.DAM [Sophos]	Feb 19, 2004

W32.Mydoom.F@mm.	• Mass mailing worm • Arrives as an attachment with the extension .bat, .com, .cmd, .pif, .exe, .scr, .zip • Places a backdoor on the infected computer • Backdoor operates on port 1080 • Can allow attackers to download and execute arbitrary files • Backdoor operates as a proxy that can allow attackers use the computer resources • Performs a DoS between 17th and 22nd of any month targeted at www.microsoft and www.riaa.com • Size 34,568 Bytes exe format, varies in zip format	• W32/Mydoom.f@MM [McAfee], • WORM_MYDOOM.F [Trend Micro] • W32/MyDoom-F [Sophos] • I-Worm.Mydoom.f [Kaspersky] • Win32.Mydoom.F [Computer Associates]	Feb 20, 2004
W32.Mydoom.G@mm.	• Mass mailing worm • Arrives as an attachment with the extension .bat, .com, .cmd, .pif, .exe, .scr, .zip • Places a backdoor on the infected computer • Backdoor operates on ports 80 and 1080 • Can allow attackers to download and execute arbitrary files • Performs a DoS against www.symantec.com • May delete files with extensions .jpg, .bmp, .avi • Size 20KB	• W32/Mydoom.g@MM [McAfee], • WORM_MYDOOM.G [Trend Micro] • Win32.Mydoom.G [Computer Associates] • W32/MyDoom-G [Sophos]	Mar 2, 2004
W32.Mydoom.H@mm.	• Mass mailing worm • Arrives as an attachment with the extension .bat, .com, .cmd, .pif, .exe, .scr, .zip • Places a backdoor on the infected computer • Backdoor operates on ports 80 and 1080 • Can allow attackers to download and execute arbitrary files • Performs a DoS against www.symantec.com • May delete files with extensions .jpg, .bmp, .avi • Size 32,256 Bytes	• W32/Mydoom.h@MM [McAfee] • Win32.Mydoom.H [Computer Associates] • WORM_MYDOOM.H [Trend Micro]	Mar 3, 2004

W32.Mydoom.I@mm.	• Mass mailing worm • Arrives as an attachment with the extension .bat, .cmd, .pif, .exe, .scr, .zip • Uses it's own SMTP engine to send emails to individuals found on the infected system • Launches DDoS against www.domain1own.com by continuously requesting the main page of the url • Size 44,544 Bytes exe format, varies in zip format	• W32/Mydoom.i@MM [McAfee] • WORM_MYDOOM.I [Trend Micro] • I-Worm.Mydoom.h	Apr 15, 2004
W32.Mydoom.J@mm.	• Encrypted mass mailing worm • Arrives as an attachment with the extension .bat, .cmd, .pif, .exe, .scr, .zip • Contains key logging capabilities • Terminates some security programs • Size 50,688 Bytes exe format, varies in zip format	• WORM_MYDOOM.J [Trend Micro] • Win32.Mydoom.J [Computer Associates] • W32/Mydoom.j@MM [McAfee]	Apr 20, 2004
W32.Mydoom.K@mm.	• Variant of W32.Mydoom.A@mm • Mass mailing worm • Arrives as an attachment with the extension .bat, .cmd, .pif, .exe, .scr, .zip • Places a backdoor on the infected computer • Backdoor operates on ports 3127 • Backdoor can be used to download and execute arbitrary files • Worm also acts as a mail relay • Terminates some security programs • Performs a DoS on www.sco.com • Size 50,176 Bytes	• Win32:Mydoom [DLL] • Worm/Mydoom.C.1 • W32.Mydoom.B@mm • Win32:Mydoom-K [WRM] • Worm/Mydoom.C.2 • I-Worm.Mydoom.c • I-Worm/Mydoom.L • W32/Mydoom.k.dll	May 18, 2004

W32.Mydoom.L@mm.	• Mass mailing worm • Arrives as an attachment with the extension .bat, .com, .cmd, .pif, .exe, .scr, .zip • Uses it's own SMTP engine to send emails to individuals found on the infected system • Attachment name may contain a randomly selected domain, which was found on the senders system • Contains key logging capabilities • Acts as a backdoor on the infected system • 21,000 Bytes	• W32/Mydoom.n@MM [McAfee], • WORM_MYDOOM.L [Trend Micro] • W32/MyDoom-N [Sophos] • I-Worm.Mydoom.l [Kaspersky] • Win32.Mydoom.N [Computer Associates]	Jul 19, 2004
W32.Mydoom.M@mm	• Mass mailing worm • Arrives as an attachment with the extension .bat, .com, .cmd, .pif, .exe, .scr, .zip • Uses its own SMTP engine to send itself to email addresses it finds on the infected computer • Places a backdoor on the infected computer • Backdoor operates on port 1034 • Uses major search engines (Google, Lycos, Alta Vista, Yahoo) to lookup and verify email addresses • Size 28,800 Bytes	• W32/Mydoom.o@MM [McAfee], • W32/MyDoom-O [Sophos] WORM_MYDOOM.M [Trend Micro] • Win32.Mydoom.O [Computer Associates]	Jul 26, 2004
W32.Mydoom.N@mm.	• Mass mailing worm • Arrives as an attachment with the extension .bat, .com, .cmd, .pif, .exe, .scr, .zip • Uses its own SMTP engine to send itself to email addresses it finds on the infected computer • Places a backdoor on the infected computer • Backdoor operates on port 1034 • Uses major search engines (Google, Lycos, Alta Vista, Yahoo) to lookup and verify email addresses • Size 35,328 Bytes	• I-Worm.Mydoom-I [Sophos]	Jul 29, 2004

W32.Mydoom.P@mm.	• Encrypted mass mailing worm • Arrives as an attachment with the extension .bat, .cmd, .pif, .exe, .scr, .zip • Uses its own SMTP engine to send itself to email addresses it finds on the infected computer • • Size 17,408 Bytes	• WORM_MYDOOM.R [Trend Micro] • W32/Mydoom.r@MM [McAfee] • W32/MyDoom-R [Sophos]	Aug 9, 2004

Description and Exploit Analysis [3]

When W32.Mydoom.M@mm is executed, it performs the following actions:

1. Creates the following registry keys, which mark the computer as infected:
   - HKEY_LOCAL_MACHINE\Software\Microsoft\Daemon
   - HKEY_CURRENT_USER\Software\Microsoft\Daemon

2. Copies itself as %Windir%\java.exe.

   Note: %Windir% is a variable. The worm locates the Windows installation folder (by default, this is C:\Windows or C:\Winnt) and copies itself to that location.

3. Drops and executes %Windir%\services.exe, which is detected as Backdoor.Zincite.A. When executed, this file opens TCP port 1034 and listens for remote connections. The backdoor will also probe random IP addresses on port 1034 looking for other infected hosts.

4. Adds the values:

   "Services" = "%Windir%\services.exe"
   "JavaVM" = "%Windir%\java.exe"

   to the registry key:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

   so that the worm and backdoor load when Windows starts.

5. May create the following files for logging purposes:
   - %Temp%\zincite.log
   - %Temp%\<randomly named file>.log

6. Gathers email addresses from files with the following extensions:
   - .adb

- .asp
- .dbx
- .ht*
- .php
- .pl
- .sht
- .tbb
- .tx*
- .wab

7. Queries the following search engines to harvest additional email addresses for possible distribution:
   - search.lycos.com
   - search.yahoo.com
   - www.altavista.com
   - www.google.com

8. When the worm finds an open Outlook window, it will attempt to send itself to the email addresses that it found.

   The email has the following characteristics:

   From:
   The From address will be spoofed.

   Subject: (One of the following)
   - hello
   - error
   - status
   - test
   - report
   - delivery failed
   - Message could not be delivered
   - Mail System Error - Returned Mail
   - Delivery reports about your e-mail
   - Returned mail: see transcript for details
   - Returned mail: Data format error

   Body:
   The content contained in the body of the email will vary, based on a number of text options. One of each of the phrases or words in brackets, separated by a "|", will appear:
   - Dear user {<recipient's email address>|of <recipient's email domain>},{ {{M|m}ail {system|server} administrator|administration} of <recipient's email domain> would like to {inform you{ that{:|,}|}|let you know {that|the following}{.|:|,}}|||||}
     {We have {detected|found|received reports} that y|Y}our {e{-|}mail |}account {has been|was} used to send a {large|huge} amount of {{unsolicited{ commercial|}|junk} e{-|}mail|spam}{ messages|} during {this|the {last|recent}} week.

{We suspect that|Probably,|Most likely|Obviously,} your computer {had been|was} {compromised|infected{ by a recent v{iru}s|}} and now {run|contain}s a {trojan{ed|}|hidden} proxy server.
{Please|We recommend {that you|you to}} follow {our |the |} instruction{s|} {in the {attachment|attached {text |}file} |}in order to keep your computer safe.
{{Virtually|Sincerely} yours|Best {wishe|regard}s|Have a nice day},
{<recipient's email domain> {user |technical |}support team.|The <recipient's email domain> {support |}team.}

- {The|This|Your} message was {undeliverable| not delivered} due to the following reason{(s)|}:
  Your message {was not|could not be} delivered because the destination {computer|server} was
  {not |un}reachable within the allowed queue period. The amount of time a message is queued before it is returned depends on local configuration parameters.
  Most likely there is a network problem that prevented delivery, but it is also possible that the computer is turned off, or does not have a mail system running right now.

- Your message {was not|could not be} delivered within <random number> days:
  {{{Mail s|S}erver}|Host} <host used to send the email>} is not responding.
  The following recipients {did|could} not receive this message:
  <<recipient's email address>>
  Please reply to postmaster@{<sender's email domain>|<recipient's email domain>}
  if you feel this message to be in error.
  The original message was received at [current time]{
  | }from {<sender's email domain>]|{<host used to send the email>]|]}}
  ----- The following addresses had permanent fatal errors -----
  {<<recipient's email address>>|<recipient's email address>}
  {----- Transcript of {the ||}session follows -----
  ... while talking to {host |{mail |}server ||||}{<recipient's email domain>.|<host used to send the email>]}:
  {>>> MAIL F{rom|ROM}:[From address of mail]
  <<< 50$d {[From address of mail]... |}{Refused|{Access d|D}enied|{User|Domain|Address} {unknown|blacklisted}}|554 <<recipient's email address>>... {Mail quota exceeded|Message is too large}
  554 <<recipient's email address>>... Service unavailable|550 5.1.2 <<recipient's email address>>... Host unknown (Name server: host not found)|554 {5.0.0 |}Service unavailable;] blocked using {relays.osirusoft.com|bl.spamcop.net}{, reason: Blocked|}
  Session aborted{, reason: lost connection|}|>>> RCPT To:<<recipient's email address>>
  <<< 550 {MAILBOX NOT FOUND|5.1.1 <<recipient's email address>>... {User unknown|Invalid recipient|Not known here}}|>>> DATA
  {<<< 400-aturner; %MAIL-E-OPENOUT, error opening !AS as output
  |}{<<< 400-aturner; -RMS-E-CRE, ACP file create failed
  |}{<<< 400-aturner; -SYSTEM-F-EXDISKQUOTA, disk quota exceeded
  |}<<< 400}|}
  The original message was included as attachment

- {{The|Your} m|M}essage could not be delivered

Notes:

- <recipient's email address> is the email address of the person receiving the email.
- <recipient's email domain> is the domain of the receiver's email. For instance, if the email address is john_doe@example.com, the domain is "example.com."
- <sender's email domain> is the domain of the sender's email. For instance, if the email address is john_doe@example.com, the domain is "example.com."
- <host used to send the email> is name of the email server used by the infected computer. The worm gathers this information from the infected computer's registry.

Attachment:
The worm may generate a file name from a domain name of an email address gathered from the computer. For instance, if the worm finds an address john_doe@example.com on the infected computer, the attachment name could contain example.com.

The attachment name may also be one of the following:

readme	instruction	transcript	mail
letter	file	text	attachment
document	message		

with one of the following extensions:

.cmd	.bat	.com	.exe
.pif	.scr	.zip	

the attachment may have a second extension, which will be one of the following:

doc	txt	htm	html

Notes:

- Approximately 30% of the time, the attachment will be zipped. In these cases the attachment may be compressed several times over.

- There is a 15% chance the worm will attach a small junk file to the mail instead of a copy of itself.

The worm will not send itself to addresses that contain the following strings:

mailer-d	spam	abuse	master
sample	accou	privacycertific	bugs
listserv	submit	ntivi	support
admin	page	the.bat	gold-certs
feste	not	help	foo
soft	site	rating	you
your	someone	anyone	nothing
nobody	noone	info	winrar
winzip	rarsoft	sf.net	sourceforge
ripe.	arin.	google	gnu.
gmail	seclist	secur	bar.
foo.com	trend	update	uslis
domain	example	sophos	yahoo
spersk	panda	hotmail	msn.
msdn.	microsoft	sarc.	syma
avp			

Exploit/Attack Signatures

If we look at the variant table listed in the "Exploit Variant" section, you will notice that all of the Mydoom worm variants are pretty similar in nature. They are all mass mailing worms that arrive with some form of attachment using one of the various file extensions, pif, exe, zip, bat, cmd, or scr. The Mydoom worm variants rely on social engineering tactics for infection. If the recipient is not tricked into opening the email attachment, then the Mydoom worm variants cannot propagate.

Although Mydoom.M obviously has characteristics very similar to the previous variants of Mydoom, when a user is tricked into opening the infected attachment, we notice a few distinct characteristics that make this variant unique. We can classify these distinct characteristics as signatures.

With older version of the Windows Operating System (Windows 3.1 and Windows 3.11), autoexec.bat and config.sys files were used for system, applications, and device configurations. For Windows 9x, Windows NT, Windows ME, Windows 2000, and Windows XP, Microsoft introduced the windows registry. In these windows versions Microsoft utilized the windows registry for system, application, and device configurations.

The Windows registry is considered a hierarchical database that is used to store necessary information needed to configure the system for users, applications, and hardware devices.

Some of the signatures that occur once a system is infected with the Mydoom.M worm are:

- The registry keys will be created on the infected system:
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion \Run "JavaVM" = %WinDir%\JAVA.EXE [5]
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion \Run "Services" = %WinDir%\SERVICES.EXE [5]

All programs that are in the registry key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run\" will automatically be run when the system is booted. In this case the Mydoom.M worm is telling the OS to run the java.exe file, and services.exe file when the system is booted.

- Drops the following two files in the windows directory:
  %WINDIR%\java.exe
  %WINDIR%\services.exe

These two files are infected executable file that are placed in the windows directory. The java.exe, and services.exe files will be run via the registry keys HKLM\Software\Microsoft\Windows\CurrentVersion\Run "JavaVM" = %WinDir%\JAVA.EXE, and HKLM\Software\Microsoft\Windows\CurrentVersion\Run "Services" = %WinDir%\SERVICES.EXE, every time the system is booted. This is one of the hooks that Mydoom.M places on the infected system to ensure that the system is always infected, even if the processes are stopped and the system is rebooted.

Once the java.exe file is executed, it will trigger the SMTP engine to construct and propagate messages to recipients that are harvested from the victims system and from the major search engines (Google, Yahoo, Altavista, Lycos). See figure 9.

- Drops the Trojan horse program Backdoor.Zincite.A, which will listen for incoming connections on TCP port 1034.

The services.exe file is the actually Backdoor.Zincite.A Trojan program. Once the services.exe file is executed, it will open and listen on TCP port 1034 for incoming connections, which will allow unauthorized access to the infected system. See figure 4.

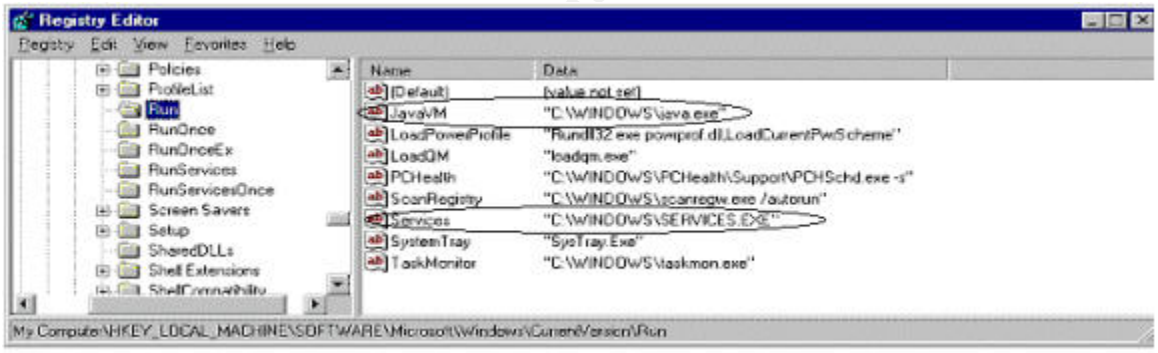


Figure 4 – Files dropped on system by Mydoom.M worm

Platforms/Environments

For the purpose of this paper we will use the following fictitious name for the company GZAC Inc.

The Mydoom.M infection took place on the 10.40.x.x segment of GZAC Inc's network.

Victim's Platform

The victim platforms were laptop and desktop systems located on the 10.40.x.x internal network.

As the Mydoom.M and associated variants, only affect windows systems, none of the Unix based systems were affected in GZAC's environment.

Employee laptops and desktops are configured as follows:

Laptop systems are primarily IBM ThinkPad A21M, Pentium III 800Mhz, configured with the following standard disk image:

- Windows 2000 Professional – SP4
- Lotus Notes R5
- Outlook 2000 – SP3
- Office 2000 – SR 1
- Internet Explorer 6.0.2800.1106
- SMS Client
- Mcafee VirusScan 7.1 – Latest DAT at the time was 4380, Scan engine 4320
- ePolicy Orchestator Agent 3.1.0.2221

Desktop systems are primarily Dell Dimension 2400, Pentium 4 2.8GHz, configured with the following standard disk image:

- Windows XP Professional – SP1
- Lotus Notes R5
- Outlook 2000 – SP3
- Office 200 – SR 1
- Internet Explorer 6.0.2800.1106
- SMS Client
- Mcafee VirusScan 7.1 – Latest DAT at the time was 4380, Scan engine 4320
- ePolicy Orchestator Agent 3.1.0.2221

All laptop and desktop systems receive Windows update via Software Update Services 1.0 (SUS) – SP1 [25], and Mcafee Anti Virus updates are distributed to laptops and desktops via the Mcafee ePolicy Orchestrator 3.0 (EPO) [26]. Both these servers are located on the 10.40.x.x network segment.

Systems OS has been hardened according to the National Institute of Standards and Technology (NIST) and respective SANS hardening guides. [40][29][30]

Source (Attacker)

The source of this incident stemmed from a laptop user that received the Mydoom.M virus while connected to their home email account.

The user had received the message, and because of the social engineering tactics that were used in constructing the message, the user was tricked into opening the attachment, thus infecting their system.

When the infected user connected to the corporate network to do some work the morning of July 26th, the Mydoom.M worm quickly began sending messages to internal users on the GZAC Inc. network. Again because of the social engineering style of the message many people were trusting and opened the attachment, thus becoming infected.

In figure 5 below, the infection rate per IP rose steadily from around 08:00 (when users stated the work day) till around 15:00. By that time roughly 90 users (comprised of laptop and desktop systems) were infected with the Mydoom.M worm.

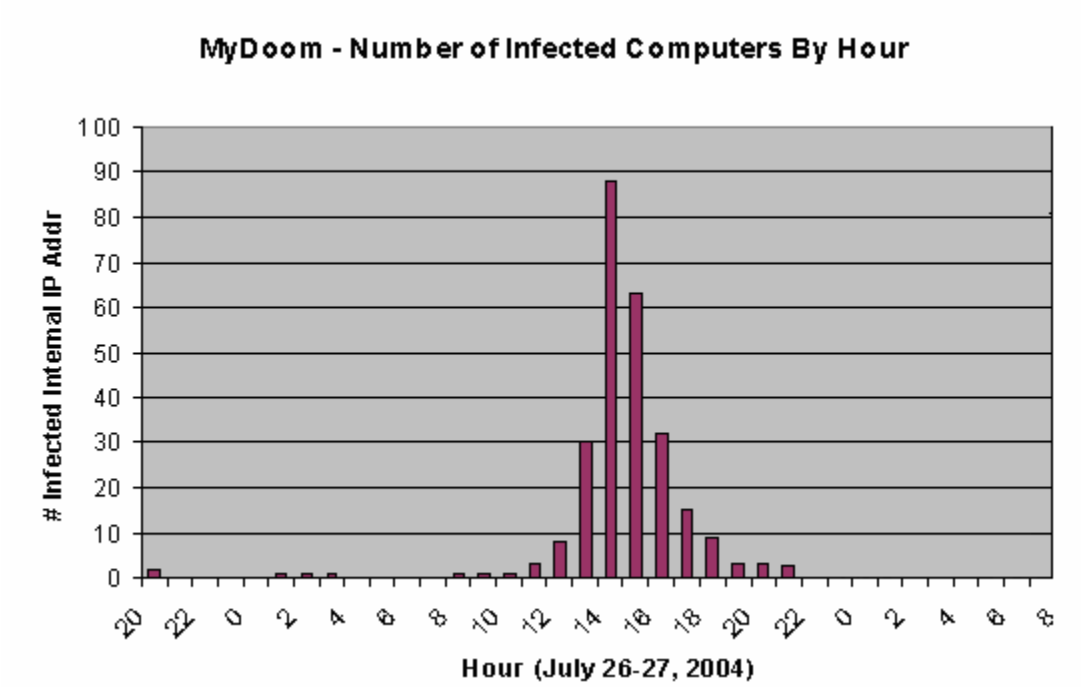


Figure 5 – Mydoom.M Infection rate

Target Network

Since this infection took place in an internal setting we can conclude that both the target network and source network are one in the same. Therefore, I will provide one network diagram for both the target and source network sections.

GZAC Inc. has a medium-sized enterprise network that is comprised of the following Table1 heterogeneous computers, networking hardware, and software:

Number of Devices	Device	Make/Software	Operating System	Hardware
1	Border Router	Nortel BCN Router	Site Manager 14	
2	Router	Cisco 7120	Cisco IOS 12	
2	Intrusion Detection System (IDS)	ISS Real Secure 7	Windows 2000 Server – SP4	Dell Power Edge 3250
2	Network Tap	Net Optics		
2	Firewall	Netscreen 208		
1	Proxy Server	Squid Proxy 2.5	Linux 2.2.26	Dell Power Edge 1750
1	Mail Server	Sendmail 8.13.0	Linux 2.2.26	Dell Power Edge 1750
1	DNS	BIND 8.2.3	Linux 2.2.26	Dell Power Edge 1750
1	Switch	Nortel BPS 2000		
1	Mail Server	MS Exchange 2000 - SP3	Windows 2000 Server – SP4	Dell Power Edge 1750
1	Mail Server	Domino 6.5	Windows 2000 Server – SP4	Dell Power Edge 1750
4	Database Servers	SAP R3	Solaris 9	Sunfire V480
1	ePO Server	EPO Console 3.0	Windows 2000 Server – SP4	Dell Power Edge 3250
1	SUS Server	SUS 1.0 – SP1	Windows 2000 Server – SP4	Dell Power Edge 3250
20	Laptop Systems	IBM	Windows 2000 Professional – SP4	IBM ThinkPad A21M
100	Desktops Systems	Dell	Windows XP Professional – SP1	Dell Dimension 2400

Table 1 – GZAC Inc heterogeneous hardware and software list

Components of the Target network perform the following functions:

Border Router:
ACL on the border router is configured with the following rule set:
access-list inbound deny tcp any any range 512 514 log
access-list inbound deny tcp any any eq 23 log
access-list inbound permit tcp any host <Mail Server> eq smtp
access-list inbound permit tcp any host <Web Server> eq http
access-list outbound deny ip 10.0.0.0 0.255.255.255 any log
access-list outbound deny ip 192.168.0.0 0.0.255.255 any log

Router:
All routers use OSPF and require authentication for routing updates.

***Real Secure IDS:**
ISS RealSecure network sensors provide network intrusion detection for all egress and ingress traffic. These IDS sensors will detect various events, which can be used to detect internal or external attacks.

The event that was used to detect and correlate the Mydoom.M infection within the GZAC environment was the “Email_Virus_Suspicious_Zip”.

The IDS event “Email_Virus_Suspicious_Zip” uses a specific signature that detects a suspicious zip attachment within an email message. The attachment is suspicious because it contains an uncompressed executable file. While executable files are often encapsulated by ZIP files, it is unusual for them to be uncompressed. This type of attachment is commonly used by worms and viruses, and is consistent with attachments seen with the MIMAIL and MyDoom worms. [27]

Netscreen Firewalls:
Both firewalls are configured to deny inbound access to all services and ports except for those needed for the purpose of the different lines of business within GZAC Inc.

The outbound firewall policy for "Netscreen FW1" is as follows:
- Allow outbound access - ports 80 TCP (http), 443 TCP (https), 21 TCP (ftp), 53 UDP (DNS), 25 TCP (SMTP).

The outbound firewall policy for “Netscreen FW2” is as follows:
- Allow outbound access - ports 80 TCP (http), 443 TCP (https), 21 TCP (ftp), 53 UDP (DNS), 25 TCP (SMTP).

The “Netscreen FW1” performs Network Address Translation (NAT) and Port Address Translation (PAT) function for internal IP's.

***Sendmail Server**
This is the SMTP server that manages all outgoing Internet email from the internal GZAC network

***DNS Server**
Provides domain name resolution for internal users.

***Exchange Server**
Provides mail services for laptop and desktop employees on the 10.40.x.x segment.

***Notes Server**
Provides mail services for laptop and desktop employees on the 10.40.x.x segment.

***Employee Laptops**
Perform various work related functions including but not limited to email, Internet, SAP, finance, customer service. Laptops are dominantly configured with Outlook 2000 mail client although some are configured with Lotus Notes R5 client.

***Suspect Laptop**
Laptop that was first infected with the Mydoom.M worm and introduced into the GZAC environment.

***Employee Desktops**
Perform various work related functions including but not limited to email, Internet, SAP, finance, customer service. Desktops are dominantly configured with the Lotus Notes R5 mail client although some are configured with the Outlook 2000 mail client.

***DB Servers**
Provide SAP database and related components to various employees within the GZAC environment.

***SUS Sever**
Provides Microsoft software updates to servers, laptops, and workstations located in the 10.40.x.x segment.

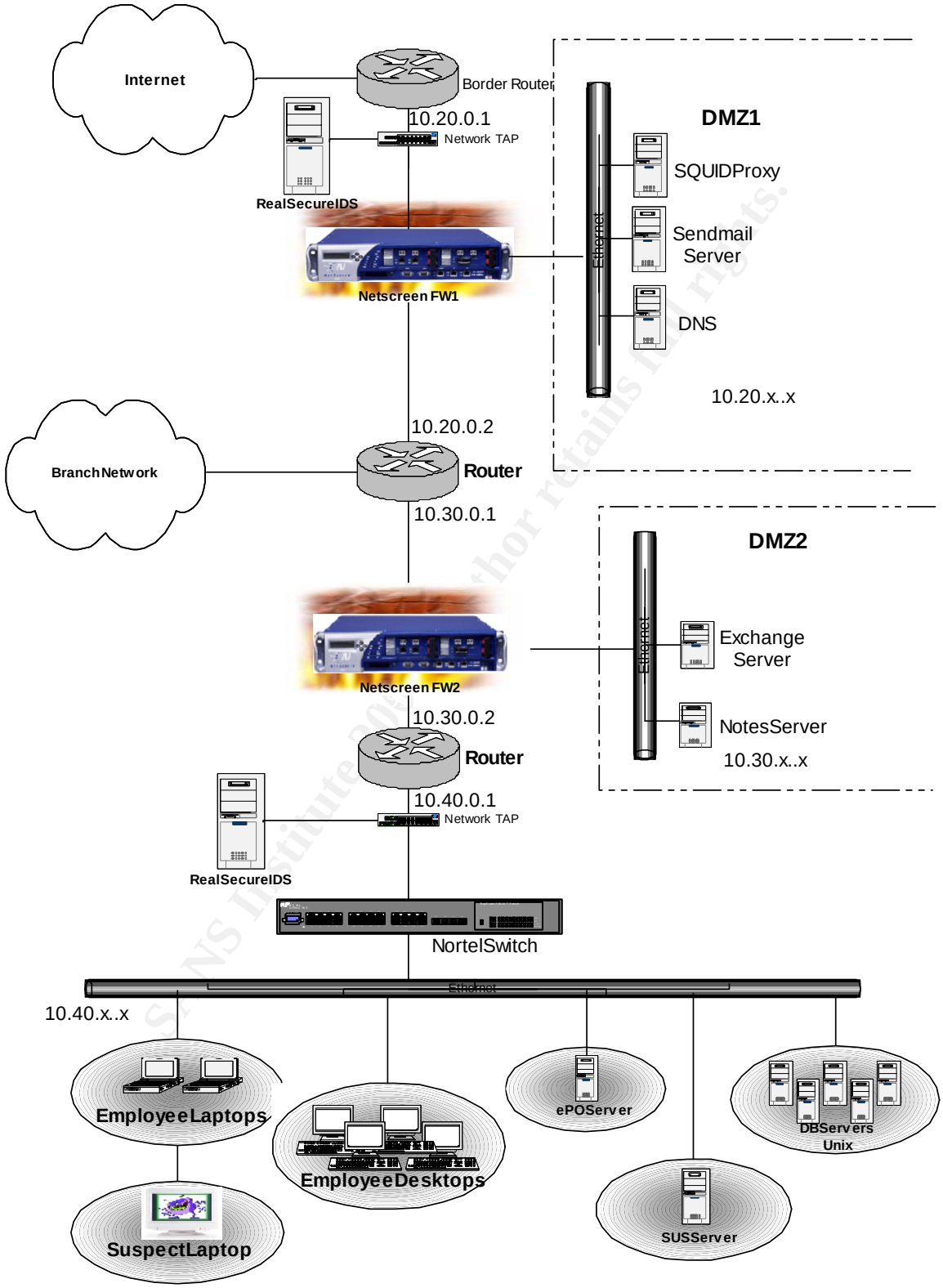
***ePO Server**
Provides Mcafee Anti-virus DAT file updates to servers, laptops, and workstations located in the 10.40.x.x segment.

**Note: All Windows, Solaris, and Linux systems were hardened according to the guidelines written in the respective NIST and SANS hardening guides. Server hardening measures are determined on a per server basis, as workstations*

images are hardened according to the requirements for each line of business. [28] [29] [30][40]

*Note: All the SUS updates and ePO updates are placed in their respective servers by the GZAC testing and development team.

Network Diagram



Stages of the Attack

This section of the paper will map the Mydoom.M worm using the five stages of the attack process as stated in the SANS GCIH course material. The five stages of the attack process are as follow: Reconnaissance, Scanning, Exploiting the System, Keeping Access, and Covering Tracks. [32]

Reconnaissance

The reconnaissance stage is when an attacker tries to use different methods to gain information about specific target(s) in order to launch a successful attack against the target system.

The Mydoom.M worm does not initially use any reconnaissance methods to attack a users system. But once the users is infected, the Mydoom.M worm will try the following reconnaissance type scans:

- Gather email addresses from files on the infected system with the following extensions, .adb, .asp, .dbx, .ht*, .php, .pl, .sht, .tbb, .tx*, .wab.

- Uses the big four search engines (Google, Altavista, Yahoo, Lycos) to try and harvest additional email addresses for distribution.

In the 10.40.x.x segment of the GZAC network we found a lot of evidence that the Mydoom.M worm was trying these propagation methods. Viewing the IDS event monitor we were able to see literally hundreds of event notifications pertaining to the Mydoom.M worm, as shown in figure 6 below.

Time	Tag Name	Source IP	Target IP	Target port	:ATTACHMENT	:FILENAME	:SIZE
2004-07-26 08:33:30 EDT	Email Virus Suspicious Zip	10.40.170.157	10.40.39.24	25	tammy.opal@qzac.com	tammy.opal@qzac.com	28832
2004-07-26 08:33:35 EDT	Email Virus Suspicious Zip	10.40.170.157	10.40.39.24	25	jimmy.fingers@qzac.com	jimmy.fingers@qzac.com.com	28984
2004-07-26 08:35:32 EDT	Email Virus Suspicious Zip	10.40.170.157	10.40.162.38	25	qzac.com	qzac.com	28832
2004-07-26 08:52:36 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	michael.ross@qzac.com	jimmy.ross@qzac.com.jpg.pif	28832
2004-07-26 08:54:15 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	bruce.smith@qzac.com	bruce.smith@qzac.com.jpg.pif	28832
2004-07-26 08:54:25 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	readme	readme.jpg.exe	28832
2004-07-26 08:55:15 EDT	Email Virus Suspicious Zip	10.40.164.36	10.40.162.38	25	tammy.opal@qzac.com	tammy.opal@qzac.com	28864
2004-07-26 08:56:04 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	qzac.com	qzac.com.jpg.pif	28832
2004-07-26 08:56:11 EDT	Email Virus Suspicious Zip	10.40.164.36	10.40.162.38	25	tammy.opal@qzac.com	tammy.opal@qzac.com	28832
2004-07-26 08:57:13 EDT	Email Virus Suspicious Zip	10.40.164.36	10.40.162.38	25	tammy.opal@qzac.com	tammy.opal@qzac.com	28832
2004-07-26 08:57:27 EDT	Email Virus Suspicious Zip	10.40.164.36	10.40.162.38	25	marie.jackson@qzac.com	marie.jackson@qzac.com.jpg.scr	28832
2004-07-26 09:02:19 EDT	Email Virus Suspicious Zip	10.40.164.36	10.40.162.38	25	rod.stelger@qzac.com	rod.stelger@qzac.com	28832
2004-07-26 09:02:25 EDT	Email Virus Suspicious Zip	10.40.164.36	10.40.162.38	25	jack.tripper@qzac.com	jack.tripper@qzac.com	28864
2004-07-26 09:02:33 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	mail	mail.scr	28832
2004-07-26 09:02:55 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	qzac.com	qzac.com	28832
2004-07-26 09:03:26 EDT	Email Virus Suspicious Zip	10.40.164.36	10.40.162.38	25	jack.tripper@qzac.com	jack.tripper@qzac.com	28864
2004-07-26 09:04:22 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	message	message.jpg.com	28832
2004-07-26 09:04:40 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	qzac.com	qzac.com.jpg.scr	28832
2004-07-26 09:05:41 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	qzac.com	qzac.com.jpg.scr	28832
2004-07-26 09:06:52 EDT	Email Virus Suspicious Zip	10.40.164.36	10.40.162.38	25	qzac.com	qzac.com	28800
2004-07-26 09:07:01 EDT	Email Virus Suspicious Zip	10.40.164.36	10.40.162.38	25	qzac.com	qzac.com	28832
2004-07-26 09:07:20 EDT	Email Virus Suspicious Zip	10.40.164.36	10.40.57.114	25	david.banner@qzac.com	david.banner@qzac.com.txt.exe	28864
2004-07-26 09:07:31 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	qzac.com	qzac.com.txt.scr	28832
2004-07-26 09:07:48 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	ross.clark@qzac.com	ross.clark@qzac.com.txt.pif	28832
2004-07-26 09:08:10 EDT	Email Virus Suspicious Zip	10.40.164.36	10.40.162.38	25	document	document.doc.pif	28864
2004-07-26 09:09:12 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	qzac.com	qzac.com.jpg.scr	28832
2004-07-26 09:09:24 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	lisa.lipps@qzac.com	lisa.lipps@qzac.com	28832
2004-07-26 09:09:43 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	ron.jeremy@qzac.com	ron.jeremy@qzac.com	28832
2004-07-26 09:10:18 EDT	Email Virus Suspicious Zip	10.40.164.36	10.40.162.38	25	qzac.com	qzac.com.jpg.scr	28864
2004-07-26 09:10:24 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	jim.fox@qzac.com	jim.fox@qzac.com	28832
2004-07-26 09:10:44 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	joe.brown@qzac.com	joe.brown@qzac.com.txt.exe	28832
2004-07-26 09:11:20 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.162.38	25	jim.fox@qzac.com	jim.fox@qzac.com	28832
2004-07-26 09:11:29 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	document	document.scr	28832
2004-07-26 09:12:30 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	document	document.scr	28832
2004-07-26 09:12:55 EDT	Email Virus Suspicious Zip	10.40.170.131	10.40.39.24	25	charles.biggs@qzac.com	charles.biggs@qzac.com	28832

:from	:to
"Post Office"	tammy.opal@qzac.com
"Mail Administrator"	jimmy.fingers@qzac.com
lawrence.welk@qzac.com	james.rawson@qzac.com
bruce.banner@qzac.com	jimmy.ross@qzac.com
bu.albano@qzac.com	bruce.smith@qzac.com
"Mail Delivery Subsystem"	rikell@qzac.com
"Returned mail"	tammy.opal@qzac.com
"Post Office"	mary.trooper@qzac.com
"Automatic Email Delivery	tammy.opal@qzac.com
"Automatic Email Delivery	tammy.opal@qzac.com
"Mail Delivery Subsystem"	marie.jackson@qzac.com
"Mail Delivery Subsystem"	rod.stelger@qzac.com
"MAILER-DAEMON"	jack.tripper@qzac.com
"Returned mail"	bu.albano@qzac.com
"Returned mail"	david.brown@qzac.com
"MAILER-DAEMON"	jack.tripper@qzac.com
"Post Office"	paul.jenkins@qzac.com
michael.jackson@qzac.com	justin.timberlake@qzac.com
michael.jackson@qzac.com	justin.timberlake@qzac.com
"Mail Delivery Subsystem"	michael.jackson@qzac.com
"Mail Delivery Subsystem"	robert.black@qzac.com
"MAILER-DAEMON"	david.banner@qzac.com
"Mail Administrator"	bob.dole@qzac.com
"Returned mail"	ross.clark@qzac.com
robert.black@qzac.com	olga.lacoste@qzac.com
"Mail Delivery Subsystem"	ruben.studdard@qzac.com
"Automatic Email Delivery	lisa.lipps@qzac.com
janice.kool@qzac.com	ron.jeremy@qzac.com
"Automatic Email Delivery	ben.johnson@qzac.com
"Post Office"	jim.fox@qzac.com
"MAILER-DAEMON"	joe.brown@qzac.com
"Post Office"	jim.fox@qzac.com
"Mail Administrator"	clayton.ellis@qzac.com
"Mail Administrator"	clayton.ellis@qzac.com
rob.georgeu@qzac.com	charles.biggs@qzac.com

Figure 6 – IDS Events triggered by Mydoom.M worm

The IDS event that was triggered was the “Email_Virus_Suspicious_Zip”. This event signature is used to specifically detect the Mydoom worm variants within the ISS Real Secure IDS product. The IDS signature detects a suspicious zip file attachment within a message, which contains an uncompressed .exe file.

In figure 6 above, you will notice the headings in each column. The column headings represent the following:

Column Name	Description	Details/Tips
Time	List the start time for each event	2004-07-26 08:33:30 EDT – This is the first event that we received on the 26th. This could be used to indicate that the original infection started at this system. The IDS will allow you to trace back to the IP address of the sender. This was useful in determining where the infection started.
Tag Name	List the event name that is generated for the specific IDS event	The tag name is useful because it enables us to quickly determine what type of attack is being executed. In this case the tag name Email_Virus_Suspicious_Zip alerted us that this was the Mydoom.M worm.
Source IP	List the source IP address or attacker in some cases	Source IP address allows us to easily track down infected suspect or infected system.
Target IP	List the target IP address or victim in some cases	Target IP allows us to easily track down system that may be compromised.
Target Port	List the target port that the attacker was accessing	Can be used to determine what protocol the attack is using. In this case port 25 (SMTP).
Attachment	List the attachment that is being sent to the recipient	The attachment lanny.opal@gzac.com.zip is useful to cross-reference the validity of viruses or worms that are detected. In this case we are able to cross reference the attachment extension with details from

		various Antivirus vendors to validate that this is the Mydoom.M worm
Filename	List the filename inside of the attachment	This can be used for the same purpose as the attachment.
Size	List the size of the attachment being sent	This can be used for the same purpose as the attachment. The file size 28K, which matches the Mydoom.M specs.
From	List who the sender is of the message	This is not very useful as the sender is usually spoofed. It is better to try and trace the IP address to find the real sender.
To	List the recipient of the sent message	Can be used to locate infected recipients.

On one of the infected desktop systems within the GZAC environment I ran the ethereal protocol analyzer tool. This allowed me to see and capture the request that were being made to the big four search engines from the infected system.

Ethereal is a protocol analyzer tool that will allow you to capture and/or view, in real-time, all the traffic that is sent or received on your system. Ethereal will run on Unix, Linux, and Windows platforms. [31]

Ethereal has the ability to add filters so that you can query and view only relevant data in the capture window. I have used the following filter to view a snippet of the Mydoom.M SMTP engine creating and sending a crafted email message in the GZAC network.

(ip.addr eq x.x.x.x and ip.addr eq x.x.x.x) and (tcp.port eq 1118 and tcp.port eq 25) – This filter will look for specific ip addresses equal to x.x.x.x and equal to tcp port 1118 and 25 (SMTP).

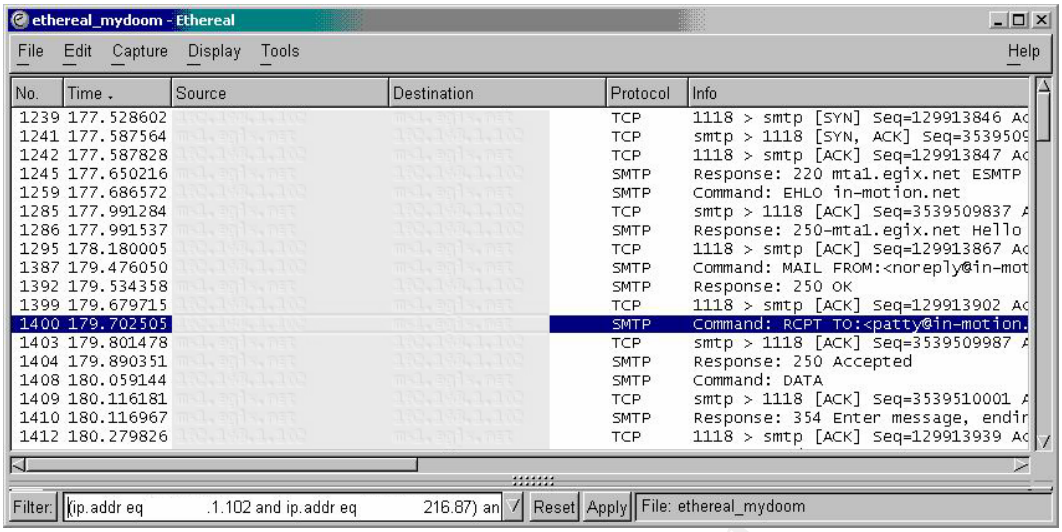


Figure 7 – Ethereal capture

Another great feature of ethereal is the ability to follow data streams. This will allow you to view the entire data stream in one window. Figure 8 below shows the data stream for the ethereal capture in figure 7.

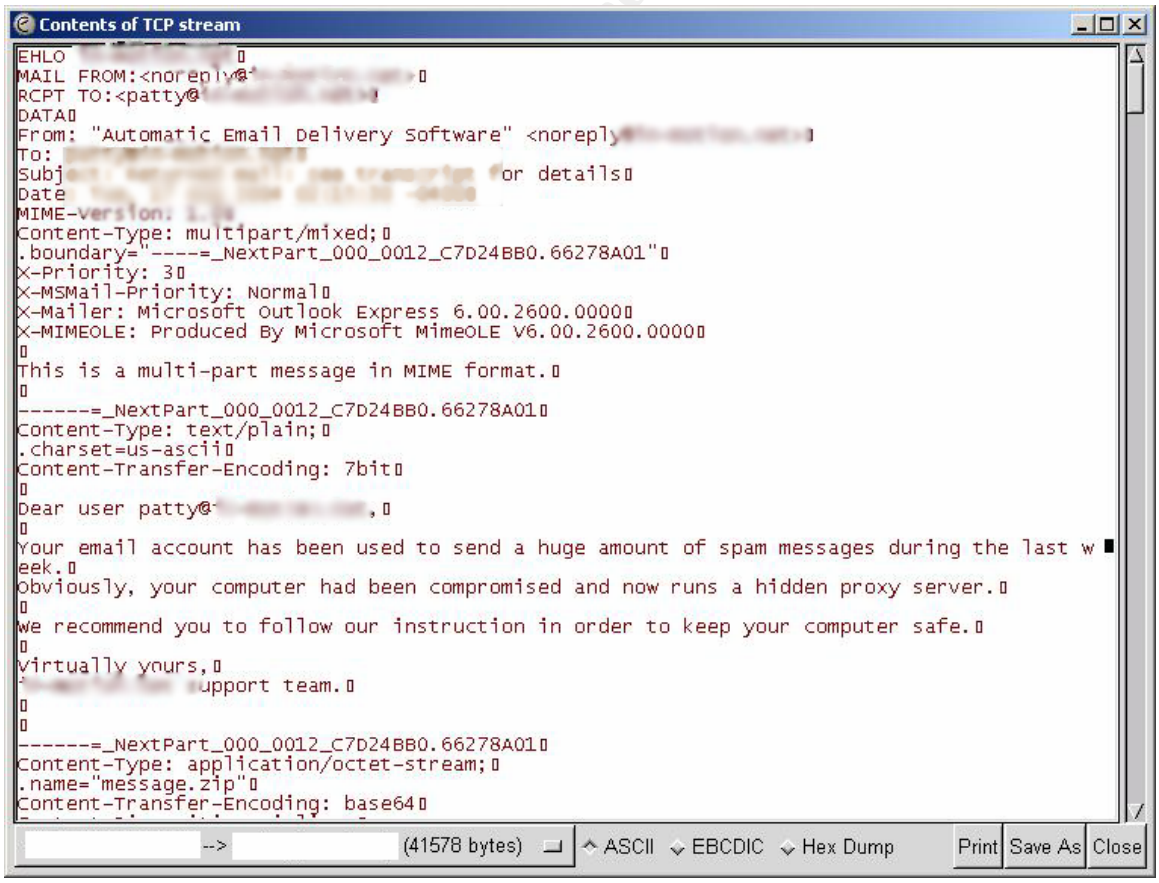


Figure 8 – Ethereal data stream

Scanning

The scanning stage of the attack process is when an attacker will try to search for vulnerabilities that may exist on the target system. Some methods or scanning are:

Scanning Method	Description	Tools used
Port scanning	Running a tool to scan a single or range of IP addresses for open ports.	Nmap, Retina, Languard, Foundstone.
War driving	Using a laptop with a wireless card and wireless sniffing software to locate open access points.	Air Magnet, Network Stumbler.
War dialing	Using special dialing software to dial a range of phone numbers in order to determine if carrier or tone signals exist for possible unauthorized network access or toll fraud.	PhoneSweep, Telesweep Secure, THC Scan, Toneloc

A hypothetical example of port scanning:

An internal attacker had an exploit for say Microsoft SQL server and they wanted to launch an attack against all Microsoft SQL servers in a particular network, they could use a scanning tool like nmap to scan the entire network for TCP port 1434 – SQL default port. Once they located all the systems on the network that have port 1434 open they would know which systems they could try the SQL exploit on.

Following the definition of scanning we can say that the Mydoom.M worm does not meet the criteria, therefore we can say that this worm does not perform this stage of the attack process.

Exploiting the System

We believe that the first user that was infected in the GZAC network was a laptop user that received an email, which was infected with the Mydoom.M worm. We will call this user Lanny Opel, and refer to their system as “Suspect Laptop”.

In this section, I will discuss how the Mydoom.M worm attacked and infected the Suspect laptop located on the GZAC network.

On July 26th 2004, Lanny connected to his home email account via pop3 (TCP port 110), and retrieved an email message, believed to contain the Mydoom.M worm. The email message was very convincing so Lanny decided to open the

email message and launch the attachment. Once he unzipped the attachment and executed the file, his system became infected with the Mydoom.M worm.

The Mydoom.M worm first copied the java.exe and services.exe files to the C:\Windows folder. Once that was complete, it added the following registry keys to the system:
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\JavaVM
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Service.
The auto run registry keys that were added to the Suspect laptop will execute the java.exe and services.exe files every time the system is booted.

When triggered, the java.exe the Mydoom.M worm will check for Internet connections, then it will connect to the local DNS server. Once connected it will query for its mail exchanger that matches the domain name of the target recipient's address. Once found, it uses this as the SMTP server. [34]

In figure 9 and 10 below, show what happens when the java.exe file is triggered.

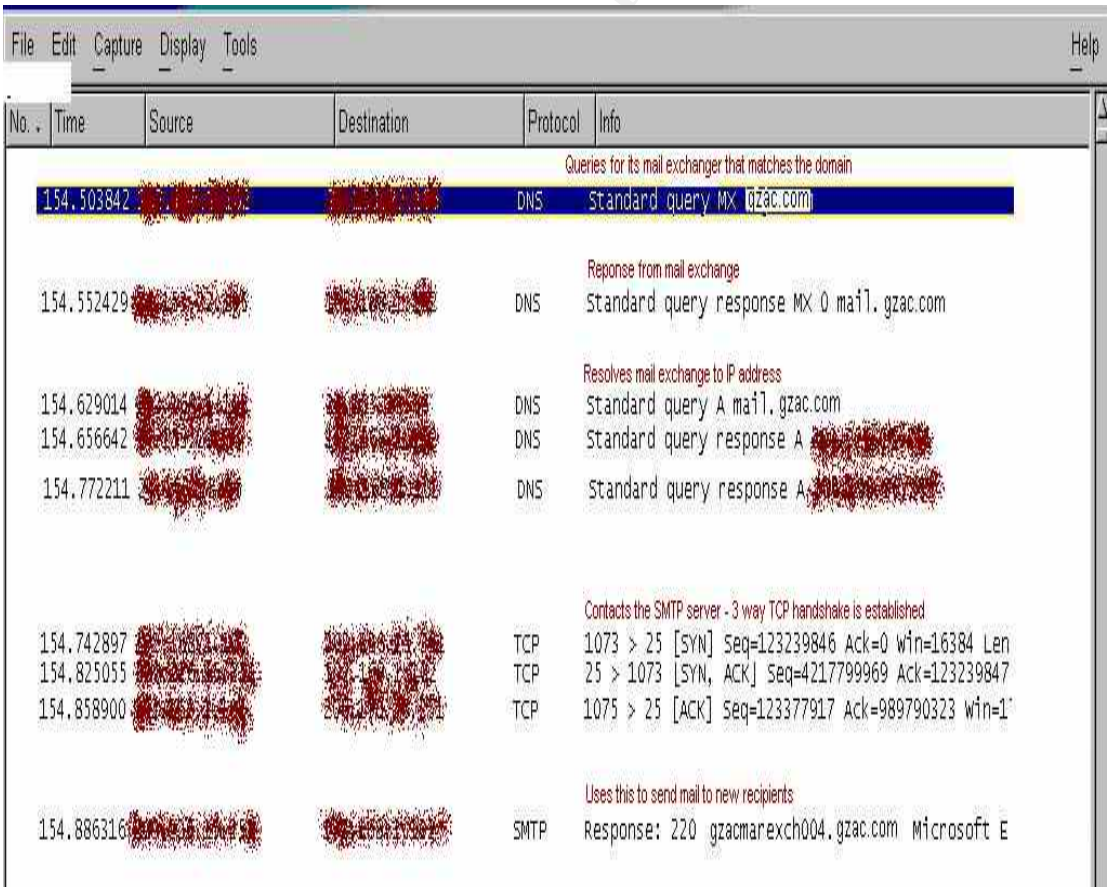


Figure 9 – Java.exe file executed triggers the Mydoom.M SMTP engine

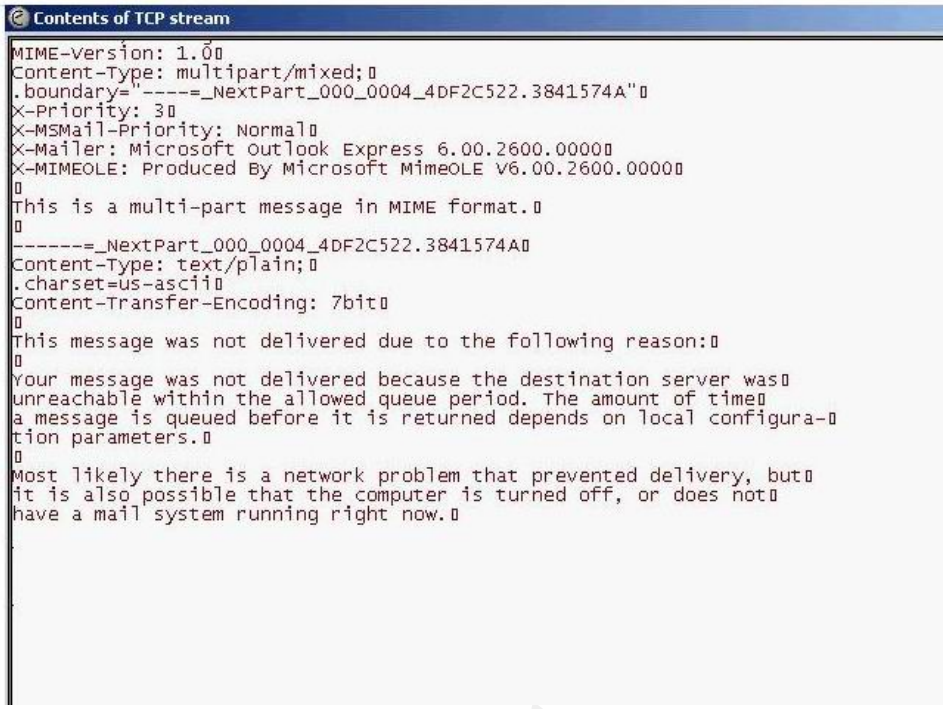


Figure 10 – Mydoom.M SMTP engine trying to send the crafted message

From the firewall logs we were able to detect the queries that were made to the big four search engines. See figure 11.

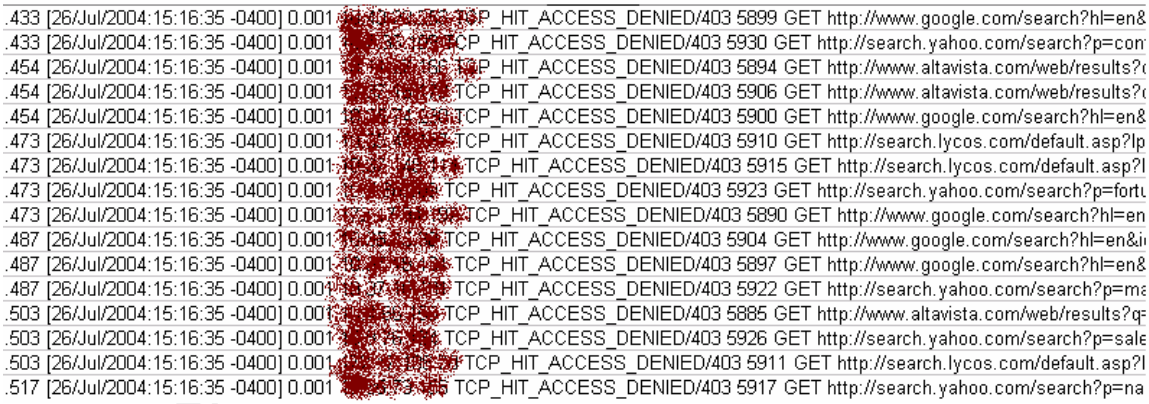


Figure 11 – Firewall logs - Mydoom.M worm trying to access big four search engines

The services.exe file that was dropped on the suspect laptop is the actual Trojan program, which is detected as Backdoor.Zincite.A from Symantec. This Trojan program opens a backdoor on port 1034. Which can later be used to gain unauthorized access to the infected system.

By using the netstat –an command, we are able to see the open Trojan port 1034 on the suspect laptop. See figure 12.

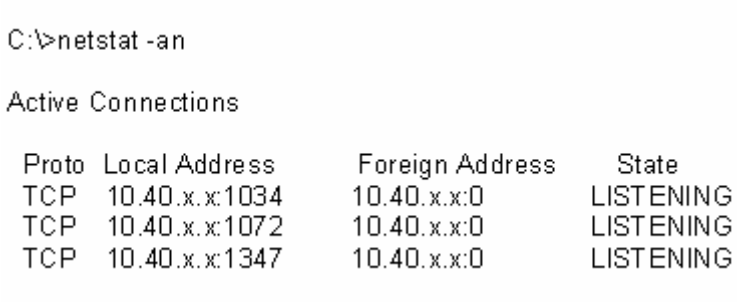


Figure 12 – netstat –an output shows TCP port 1034 open

The netstat command allows the user to check your network configuration and activity. The commands that can be uses with netstat are as follows:

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

-**a**	Displays all connections and listening ports.
-e	Displays Ethernet statistics. This may be combined with the –s option
-n	Displays addresses and port numbers in numerical form.
-p proto	Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, or IP.
-r	Displays the routing table.
-s	Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.
interval	Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

The installation of the java.exe and services.exe files would not be detected, as we did not deploy Host Based IDS (HIDS) on the laptops or desktops. The installation of HIDS would allow us to detect if files have changed on the system, it would also allow us to detect any changes to the registry.

Further into the attack when the Mydoom.M worm started to propagate we did detect this on our IDS sensors and by checking the firewall logs.

Keeping Access

In order to keep the system infected, the Mydoom.M worm does two things.

1) It creates two registry keys in the auto run registry section that call the main executable files used to infect the target system. These files are java.exe and services.exe. See figure 13.

2) It drops a back door on the infected system so that the attacker has unauthorized access to the system. The backdoor is initiated by the services.exe file, which opens port 1034 on the infected system. See figure 14.

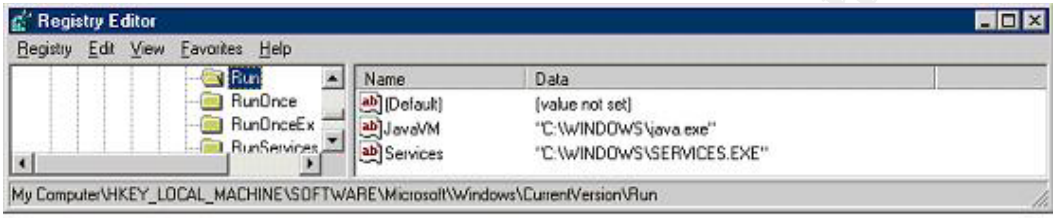


Figure13 – Registry keys created by Mydoom.M worm infection

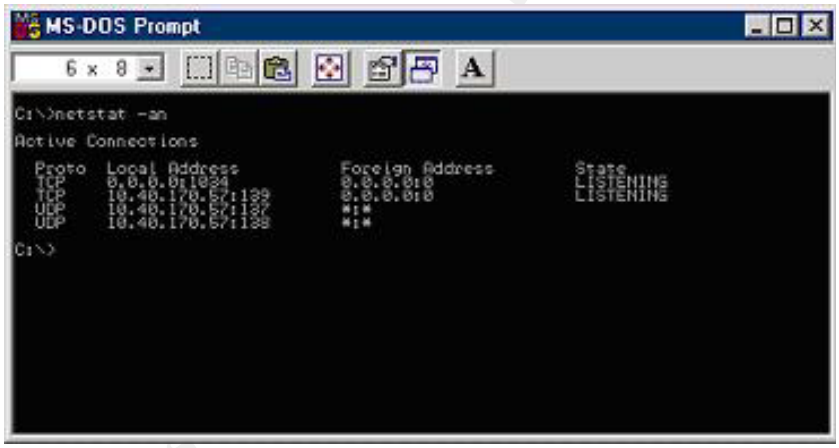


Figure 14 – Trojan listening on TCP port 1034

Covering Tracks.

The Mydoom.M worm tries to cover its tracks by disguising the critical attack files (java.exe and services.exe) on the system. These files do not have any inconspicuous names that would give them away. Instead the Mydoom.M worm writer makes these files blend in with the other files on the system by using common names. See figure 15 & 16.

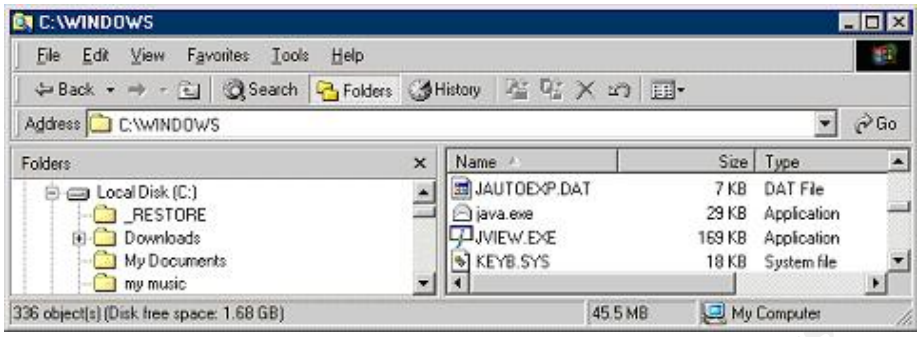


Figure 15 – Java.exe file is placed in the windows folder

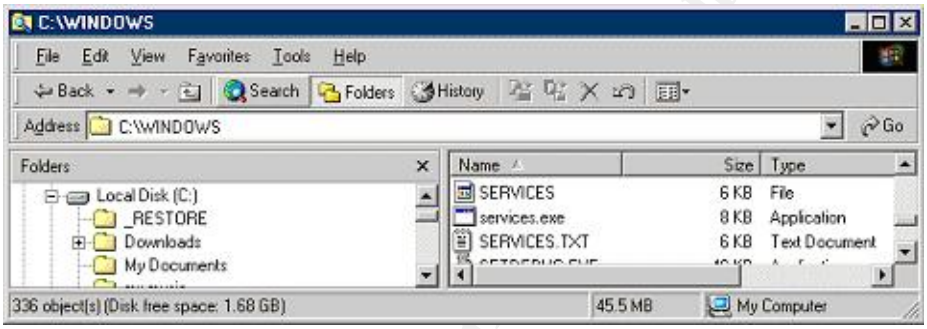


Figure 16 – Services.exe file is placed in the windows folder

The Incident Handling Process

In this section, I will take the reader through an outbreak of the Mydoom.M worm that occurred in the GZAC network environment, and explain the six phases (Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned) of the incident handling process as stated by SANS, that were used to resolve the Mydoom.M worm outbreak

Preparation Phase

Preparation is key to incident response. In my eyes this is stage 0, where a company will establish an organizational stance on how they will deal with an incident. It's not nice to be caught with your pants down when an incident hits, so it is key to be prepared.

Depending on the incident, you could loose a lot of time, money, and company face value if you are not prepared to respond promptly, and efficiently to an incident.

GZAC has an Information Security Team that also handles Incident response. The Information Security Team is comprised of a CISO, Senior Manager, and 15 top-notch security professionals. All of the individuals within the Incident response team have taken some form of SANS course and/or currently have their CISSP designations.[36] [35].

The CISO is highly respected by his peers and in the Information Security field, and has over 20 years experience in Information Security and has worked for various government agencies.

The Senior Manager of the Incident Security team has been in the Information Security field for 10 years and has worked in various technical and managerial positions throughout his career in Information Security.

Similarly, like the SANS 6 step Incident handling process, GZAC too has its own six-phase incident response process. The six phases that GZAC uses are as follows:

1) **Inform**

2) **Identify**

3) **Investigate**

4) **Contain**

5) **Eradicate**

6) Review

The Inform phase enables technical support or employees to contact us on a 24x7 basis in the event of any incidents that may arise. We also use this alerting feature with our IDS sensors. In the event of an attack or system outage the GZAC incident response team would be notified via pager.

At the Identify phase we would carry out a full investigation to determine the nature of the incident. Some of the things that we would consider are:

1) Is the threat real?
2) What is the geographical origin and destination of the attack?
3) What effect does the incident have on the destination or target system(s)?
4) Was the system compromised?
5) How many systems are being affected?
6) How critical are the devices or systems being attacked?

The Investigate phase allows us to assess the information gathered in the previous phase so that we can determine the course of action to take going forward. In this phase we would gather all the affected parties (directly and indirectly affected) within GZAC Inc. and assemble what we call a Security Problem Management Team (SPMT). Usually the SPMT is convened if the incident is wide spread and could impact multiple systems or groups.

Once the SPMT is convened they will assess the incident from the beginning and determine the necessary steps to resolve the issue(s). The SPMT along with Information Security will also handle the last three phases of our incident handling process.

In the Contain phase we would take the necessary steps to prevent the incident from spreading to other systems on the network. Other steps that we would take to contain the incident are: Establish a quarantine area to the affected systems so they cannot contaminate any other systems or data on the network. If need be we would also bring up the necessary backup systems.

Once we have contained the incident the next phase would be to Eradicate. This is the phase where we would use our Jump Kit. In this phase our first step would be to preserve a copy or copies of the infected systems as evidence or for forensic analysis. Once we have preserved a copy of the infected system(s), we would then determine if they should be re-imaged or restored. This would depend on the type of incident that occurred on the system.

Our final step is the Review phase. In this phase we would go over lessons learned from the incident and take the proper steps to ensure that the incident does not repeat itself.

GZAC also has a patch management process in place to ensure that all critical software and hardware vendor patches are updated on systems and appliances within one week of the release date. This includes testing and deployment.

Within the GZAC environment all networking duties have been separated. There is not a single network administrator for all components. Specific teams have been created to maintain and control the various network components.

The teams are as follows:

1) **Firewall Team** – Responsible for all Netscreen firewall rule changes, configuration issues, and maintenance. All firewall rule changes must go through a change review team for approval and follow due care process.
2) **Router Team** – Responsible for router configuration and related maintenance issues.
3) **Email Team** – Responsible for configuration and maintenance of all mail servers, and mail gateways.
4) **Proxy Team** – Responsible for Squid proxy server configuration and maintenance.
5) **Anti-virus Team** – Responsible for testing new DAT files, and deploying them to the laptop, desktops, and servers accordingly via Mcafee ePolicy Orchestrator (ePO).
6) **Field Services Team** – Responsible for software and hardware configuration of all laptop and desktop systems.

GZAC Inc has been through many different malware attacks and worm type outbreaks in the past, so they were well prepared for the Mydoom.M worm incident.

Policy

The Information Security Team within GZAC Inc. has developed an Information Security Guide (ISG). The ISG is meant to establish technology, process, and people requirements in support of GZAC information security policies and operating directives, also to document specific responsibilities of staff and management.

Sample Excerpts from the ISG

Incident Response Definition

A security incident is an adverse event or situation associated with an information resource that results in:

- An attempt to compromise GZAC information or networks.
- A failure to comply with security requirements or objectives as stated in the ISG.
- A vulnerability discovery.
- Unauthorized probing or potentially hostile probing of one or more computer systems or networks.

Operating Directives

- Establish an information security process framework to ensure consistent identification, measurement, and effective management of business risks that arise from information security threats and vulnerabilities.
- Establish clear Executive accountabilities for securing and protecting GZAC's information resources and managing related business risks
- Establish information security standards and a control framework to ensure consistent implementation of control measures.

Segregation of duties

- Segregation of duties, independent checks or other controls must be implemented as necessary to prevent individuals or groups from deliberately or inadvertently compromising the security of the GZAC's information resources.

Audit Logs

- Audit logs, that record access to and use of information resources, must be maintained.
- Logs should contain sufficient detail to ensure that individuals can be held accountable for their actions.

Identification Phase

The Identification phase of incident handling is where you would basically determine the following:
1) Is the threat real?
2) What is the geographical origin and destination of the attack?
3) What effect does the incident have on the destination or target system(s)?
4) Was the system compromised?
5) How many systems are being affected?
6) How critical are the devices or systems being attacked?

We believe the first user that was infected in the GZAC network was a laptop user that received an email via pop3, which was infected with the Mydoom.M worm. We will call this user Lanny.

On July 26th 2004 at approximately 07:00:00, Lanny connected to his home email account via pop3 (TCP port 110), and retrieved an email message believed to contain the Mydoom.M worm. The email message contained information implying that his system was infected with a virus, and offered instructions on how the virus could be cleaned from his system. Since the email was very convincing Lanny decided to open the email message and launch the attachment. Once he unzipped the attachment and executed the file, his system became infected with the Mydoom.M worm. This was the start of Mydoom.M infection in the GZAC network environment. See figure 17.

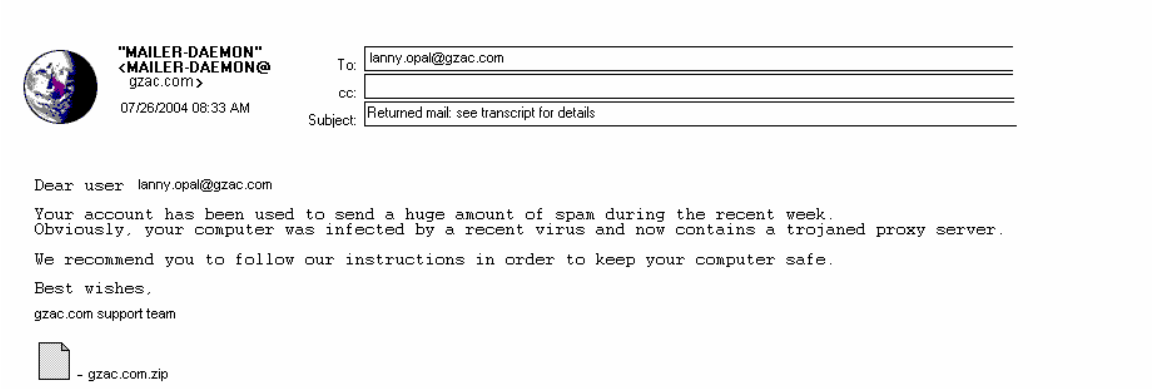


Figure 17 – Sample email generated by Mydoom.M infected system

The first signs of the Mydoom.M worm in the GZAC environment, was noticed by the on duty Information Security Analyst (Jason) on the morning of July 26 at approximately 08:00:00. Upon his review of the IDS event logs he noticed the unusually high number of events with the tag name “Email Virus Suspicious Zip”. [27] See figure 6 for a snippet of the IDS logs.

Jason promptly conveyed his findings from the IDS sensor to the Senior Security Analyst (Sylvain). Sylvain confirmed that the “Email Virus Suspicious Zip” findings on the IDS sensor were in fact suspicious. Further research of this issue through various AV vendors (Mcafee, Symantec, Kaspersky Labs), and other security related web sites lead to the conclusion that it was the Mydoom.M worm that was infecting the GZAC network.

Within the hour Enterprise Help Desk (EHD) contacted Information Security to inform them of the high volume of calls that they were receiving regarding the Mydoom.M worm.

At this point, Sylvain determined that the Mydoom.M worm posed a serious threat to the GZAC environment so he promptly contacted the Senior Manager of Information Security (Bob) and briefed him on the current situation. Sylvain also started to track the infection rate of the Mydoom.M worm in the GZAC environment.

Further research on the Mcafee web site allowed Sylvan to locate a tool that could be used to clean the MyDoom.M worm. The tool is called Mcafee Stinger. [38]

The DAT file (4381) needed to clean and protect systems from the Mydoom.M worm was not available on the Mcafee web site at this time, due to the timing and “LOW” risk assessment rating of the Mydoom.M worm.

Incident Timeline

Date	Time - EST	Event
July 26, 2004	**08:00:00**	The GZAC Information Security department was able to determine that a problem existed by reviewing the IDS sensor event logs.
	08:25:00	EHD contacted Information Security to inform them of the high volume of calls that they were receiving. All of the incoming calls that EHD received were similar in nature. Internal employees were complaining about: • Receiving unsolicited emails from colleagues regarding a virus on their system. Email that was received contained an attachment and instructions that they should open and run the attachment to clean the virus from their system. • Slow system response, or no response when using the Internet. Desktop and laptop users access to google.com and yahoo.com was slow or did not work at all.
	08:35:00	Sylvain contacted the Senior Manager of Information Security (Bob) and briefed him on the current situation. Sylvain also started to track the infection rate of the Mydoom.M worm in the GZAC environment.
	09:10:00	Bob contacted the CISO (Ross) and the various SPMT members and convened the SPMT meeting. The SPMT for the Mydoom.M incident consisted of the following members: • Information Security CISO • Information Security Senior Manager • Firewall Team Manager • Router Team Manager • Email Team Manager • Proxy Team Manager • Anti-virus Team Manager • Field Services Team Manager • Enterprise Help Desk Senior Team Lead

		Armed with the information that was gathered by the Information Security team members. Joe gave a brief history of the Mydoom.M worm and presented the findings to the SPMT members.
	09:55:00	SPMT members and Information Security reviewed the data and mapped out a course of action to handle the incident. The following course of action was determined for each team: Information Security • Continue to monitor the Mydoom.M worm via IDS and report the findings to the SPMT members on an hourly basis. • Gather more information pertaining to the Mydoom.M worm. • Notify Antivirus team when a new DAT file is posted on the Mcafee web site or ftp site to clean infected systems. • Update Internal Information Security web site with Mydoom.M worm information. Firewall Team • Monitor firewall utilization and report the findings to the SPMT members on an hourly basis. Router Team • On standby incase they are needed to assist. Email Team • Block attachments with the .zip extension on the mail gateway. This will not stop the Mydoom.M message from being sent but it will stop the .zip attachment from being sent. • Provide hourly updates on mail server utilization. • Update DAT file (4381) on mail gateways when available. Proxy Team • Implement filters on the proxy server to block outbound access to the big four

		search engines that the Mydoom.M worm targets (Google, Altavista, Yahoo, Lycos). • Provide hourly updates on proxy utilization. Antivirus Team • Deploy new DAT file (4381) to all desktops, laptops, and servers via ePO when it is available. • Check Mcafee web site or ftp site periodically for updated DAT file (4381) to clean and protect windows systems. Field Services Team • Assist in cleaning employee systems with the Mcafee Stinger tool. Enterprise Help Desk • Inform employees that call into the helpdesk about the Mydoom.M worm; tell them not to open the attachment. • Guide the employees on cleaning their systems with the Mcafee Stinger tool. • Provide SPMT with call statistics on an hourly basis.
	11:00:00	SPMT members distributed the information to their respective team leads for implementation.
	12:00:00	All teams provide status update to SPMT. Information Security • According to IDS event sensor data there is a 200% increase in infection rate since 09:00:00. • Notified AV team lead that the latest DAT file (4381) is available from the Mcafee web site. • Information Security web site has been updated to provide employees with information pertaining to the Mydoom.M worm. Proxy Team • Proxy utilization is 100% due to the fact that most employees are at work and connected to the network.

		• Proxy filter to block access to the big four search engines will be implemented within the hour. Antivirus Team • Latest DAT file (4381) has been downloaded from the Mcafee web site. • Antivirus team is currently testing the DAT file for production release. • DAT file will be ready for release within the next two hours. Email Team • Still receiving a high number of emails at the mail gateway. • Filter to block .zip attachments will be implemented within the hour. Field Services Team • Continue to assist clients with clean up of Mydoom.M infection. • 10 systems have been cleaned using the Mcafee Stinger tool. EHD • Call volume is still extremely higher then normal as a result of the Mydoom.M worm infection. • Support analysts have assisted 15 employees in cleaning their systems with the Mcafee Stinger tool. Router Team • No new updates.
	12:20:00	SPMT contacts Corporate Communications and they start drafting a notification to inform users of the Mydoom.M worm outbreak.
	13:00:00	All teams provide status update to SPMT. Information Security • According to IDS event sensor data there is a 300% increase in infection rate since 12:00:00.

	14:00:00	Proxy Team • Proxy utilization still 100% • Implemented the proxy filter, which is now blocking internal attempts to the big four search engines. Antivirus Team • DAT file is being tested and will be released within the hour. Email Team • Implemented the filter to block .zip attachments at the mail gateway. • Still receiving a high number of emails at the mail gateway. Field Services Team • Continue to assist clients with clean up of Mydoom.M infection. • Another 12 systems have been cleaned using the Mcafee Stinger tool. EHD • Call volume is still extremely higher then normal as a result of the Mydoom.M worm infection. • Continue to assist with worm clean up – 10 more systems have been cleaned. Router Team • No new updates. All teams provide status update to SPMT. Information Security • According to IDS event sensor data there is a 275% increase in infection rate since 13:00:00. • Internet security sites are reporting google.com service issues due to the Mydoom.M worm. Proxy Team • No new updates.

		Antivirus Team • DAT file is still being tested. Email Team • Still receiving a high number of emails at the mail gateway due to infection. • Waiting for DAT file from Antivirus Team. Field Services Team • Continue to assist clients with clean up of Mydoom.M infection. EHD • Call volume is still extremely higher then normal as a result of the Mydoom.M worm infection. • No new systems have been reportedly cleaned. Router Team • No new updates.
	14:35:00	Corporate Communications completes the draft message and sends it to all GZAC employees.
	15:00:00	All teams provide status update to SPMT. Information Security • IDS event sensor data shows that there is a 196% increase in infection rate since 14:00:00. Proxy Team • No new updates since last status update. Antivirus Team • DAT file has been tested and is ready for deployment. • Deploying new DAT file via epo. Email Team • Still receiving a high number of emails at the mail gateway due to infection. • Received new DAT file from Antivirus team, will update anti virus on the mail gateways.

		Field Services Team • No new updates, continue to assist clients with clean up of Mydoom.M infection. EHD • Call volume has decreased as a result of the email message sent by Corporate Communications. Router Team • No new updates.
	15:05:00	Email team has successfully deployed the new DAT file on the mail gateways.
	15:35:00	Antivirus team has successfully deployed the new DAT file to the organization. Configuration changes were made to auto scan systems once the new DAT file was received.
	16:00:00	All teams provide status update to SPMT. Information Security • IDS event sensor data shows that there is a 30% decrease in infection rate since 15:00:00. Proxy Team • Report a decrease in proxy utilization. Antivirus Team • New DAT file has been deployed to all systems at 15:35:00. • Employees that are not connected to the network will automatically receive the updated DAT file when they do connect to the network. Email Team • New DAT file has been successfully deployed on mail gateways. • Mydoom.M worm is now being blocked at the mail gateways.

		Field Services Team • No new updates EHD • Call volume has decreased even more as a result of the DAT file deployment. Router Team • No new updates.
	17:00:00	All teams provide status update to SPMT. Information Security • IDS event sensor data shows that there is a 50% decrease in infection rate since 16:00:00. Proxy Team • No new updates. Antivirus Team • No new updates. Email Team • No new updates. Field Services Team • No new updates. EHD • No new updates. Router Team No new updates.
	18:00:00	All teams provide status update to SPMT. Information Security • IDS event sensor data shows that there is a 53% decrease in infection rate since 17:00:00. Proxy Team • No new updates.

	19:00:00	Antivirus Team • ePO deployment query shows that the updated DAT file was successfully deployed to 98% of systems on the network. Email Team • No new updates. Field Services Team • No new updates. EHD • Call volume is back to normal levels. Router Team • No new updates. All teams provide status update to SPMT. Information Security • IDS event sensor data shows that there is a 27% decrease in infection rate since 18:00:00. Proxy Team • No new updates. Antivirus Team • ePO deployment query shows that the updated DAT file was successfully deployed to 100% of systems on the network.. Email Team • No new updates. Field Services Team • No new updates. EHD • No new updates. Router Team • No new updates.

	20:00:00	All teams provide status update to SPMT. Information Security • IDS event sensor data shows that there is a 73% decrease in infection rate since 19:00:00. Proxy Team • No new updates. Antivirus Team • No new updates. Email Team • No new updates. Field Services Team • No new updates. EHD • No new updates. Router Team • No new updates.
	21:00:00	All teams provide status update to SPMT. Information Security • IDS event sensor data shows that there is a 33% decrease in infection rate since 20:00:00. • A few systems are showing signs of infection on the network. Proxy Team • No new updates. Antivirus Team • No new updates. Email Team • No new updates.

		Field Services Team • No new updates. EHD • No new updates. Router Team • No new updates.
	21:10:00	• Since the Mydoom.M infection rate has almost been eliminated the SPMT decides that they will cease hourly reporting. • All teams are put on call. • Reports will be called into the SPMT hotline when and if new updates or issues arise.
	23:00:00	Information Security reports that the IDS event sensor data does not show any more signs of the Mydoom.M worm on the network.
July 27, 2004	**08:00:00**	SPMT contacts all teams for a status update
	08:15:00	Information Security • Performed a network scan for port 1034 to determine if any systems were still infected. • No more signs of the Mydoom.M worm on the network. Proxy Team • Removed the filter to block access to the big four search engines (Google, Yahoo, AltaVista, Lycos) at 06:10:00. • Proxy utilization is normal. Antivirus Team • No new updates. Email Team • Removed the .zip attachment block from the mail gateways. • Mcafee Groupshield does not show any signs of infection on the mail gateways.

		Field Services Team • No new updates. EHD • No calls regarding the Mydoom.M worm. • Call volume is normal. Router Team • No new updates.
July 28, 2004	**17:00:00**	SPMT disbands, as the Mydoom.M worm incident is resolved.

Chain of Custody

Chain of Custody is usually followed when legal action will be taken as a result of the incident. In order to establishing a chain of custody an identifiable person must always have physical custody of the evidence at all times. All involved persons that handle the evidence must be documented as well as documenting who, what, where, and when, each step was performed.
When handling evidence that will be used in a court of law it must be handled in a meticulously manner to avoid allegations of tampering or misconduct.

We did not follow chain of custody for the Mydoom.M outbreak within the GZAC network for the simple reason that we were not taking any legal action as a result of this incident. Our main goal with the Mydoom.M worm was to resolve the issue as quickly and efficiently as possible in order to minimize the business impact.

Containment Phase

As stated in the "Containment" section of the SANS GCIH course material, the goal of containment is to keep the problem from getting worse.

The steps taken to contain the Mydoom.M worm outbreak within the GZAC network were as follows:

1. Gathering information about the Mydoom.M worm.
2. Convening the SPMT meeting to address the issue.
3. Email team blocking .zip attachments at the mail gateways.
4. Proxy team implementing filters to block access to the big four search engines.

5. Corporate communications sending a notification to all employees informing them about the Mydoom.M worm.

Gathering information about the Mydoom.M worm was one of the key things to do in order to contain it. When fighting an unknown the best thing is to learn as much as you can about it. This way you will arm yourself with the correct knowledge to defeat it.

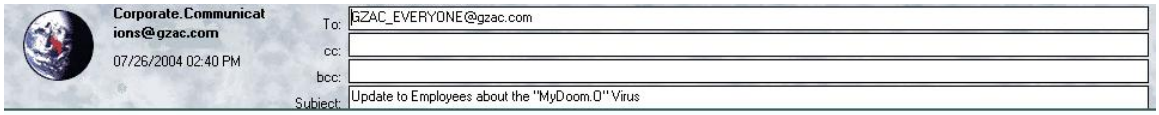
Once Sylvain verified that the threat was real he did further research by reading security updates on various AV sites (Mcafee, Symantec, Kaspersky Labs) to determine what it was that he was dealing with. In doing so, he was able to determine that the Mydoom.M worm was infecting the GZAC network. He also learned a great deal about the Mydoom.M worm (propagation pattern, affected operating systems, how to clean an infected system) that was use to inform the members of the SPMT.

Convening the SPMT meeting was another method used to contain the Mydoom.M outbreak. By convening the SPMT meeting, Information Security was able to arrange and inform the necessary groups that are needed to contain and resolve the incident in a timely manner.

The Email team was responsible for blocking the .zip attachments at the mail gateways. By blocking the .zip attachment at the mail gateway, this ensured that the .zip attachment used by the Mydoom.M worm would be stripped from all infected messages. Therefore, any systems that were infected with the Mydoom.M worm would not be able to infect other systems because the .zip attachment needed to infect a users system would not be attached to the message.

The Proxy team was responsible for filtering out any access to the big four search engines. This ensured that internally infected system could not access the big four search engines to harvest new email addressed.

Informing the GZAC employees about the Mydoom.M worm but sending out a corporate communications message was anther method that was used to contain the spread. Once the employees received the corporate communication they were prepared therefore they would not be caught off guard if they received the Mydoom.M crafted email. See figure 18.



Update to Employees about the "MyDoom.O" Virus

There is a new computer virus now circulating called "MyDoom.O". This virus
is spread when recipients open infected attachments in e-mail messages. GZAC Inc has already implemented controls to delete attachments with filename and extensions associated with this virus.

What you can do to help:
All employees should delete suspicious e-mail messages with attachments that have various extensions (predominantly ".zip") that in some cases may appear to be sent as "returned mail". The virus is contained in file attachments with various names, e-mail subject lines and messages.

What you should do if you received a suspicious e-mail
If you've received a suspicious e-mail (as described above), please delete it from your mailbox and do not open any attachments. However, if you inadvertently opened an attachment, which you suspect could contain the "MyDoom.O" virus, please contact the Enterprise Help Desk.

Special Note for Remote Access Users
GZAC owned Laptops/Desktops should be brought into the office or your "home" branch environment as early as possible so that they can be safely connected to the network to download automated updates. In the interim, delete all suspicious e-mails as described above.
Employees who use their personal PC to connect to the GZAC network should visit http://www.mcafee.com to download the appropriate file (DAT 4381) for their operating system and service pack level.

Figure 18 – Corporate Communication sent to all employees regarding Mydoom.M worm

Jump Kit Components

The Jump Kit is a collection of tools (hardware and software) that can be used to assist the incident handler in gathering necessary information from suspect systems.

With this particular incident, Information Security was not deployed to investigate or gather information from infected systems. The main concern was to resolve the outbreak as quickly and efficiently as possible. Therefore, Information Security did not utilize any components of the Jump Kit for this incident. Instead, through the SPMT meeting, Information Security was able to delegate the clean up effort to the necessary teams as per the incident handling process that GZAC Inc has in place.

The Information Security Jump Kit contains the following hardware and software items:

Hardware:

Number of Items	Item	Description
1	IBM Think-pad A21M. Dual boot configuration with Linux and Windows 2000	Laptop system with dual boot capability. System also had vmware which can be used as a sandbox for testing purposes
1	Solo 2 Forensic Unit	Stand-alone forensic hard disk copier that has MD5 hash capabilities. Copies bit-by-bit, sector-by-sector. Can also be used to erase disk to DOD standards.
4	Ethernet Cables	Ethernet cables used to connect systems.
1	Pen Flashlight	Pen Flashlight
1	Pen	Pen
1	Notepad	Notepad
1	Screwdriver with additional heads	Screwdriver with additional heads
2	256 MB USB memory sticks	USB memory stick used to transfer or capture data from systems. 256MB memory capacity.

1	3com 4port hub	4-port hub used to connect systems together.

Software:

Number of Items	Item	Description
1	Ghost boot disk with network support	Symantec Ghost boot disk with networking support. Used to clone suspect \evidence HD.
1	Bootable cd-rom	Bootable cd-rom with DOS.
2	Bootable floppy disk	Bootable floppy disk with DOS.
2	Antivirus Scan disk with latest DAT files	Floppy disk with Mcafee Antivirus Scanning software also includes the latest DAT files. Can be used to clean viruses on infected systems.
4	Blank floppy disks	Blank floppy disks used to gather information from suspect systems.

Eradication Phase

The eradication phase of the incident handling process is when the incident handler would take the correct measures to remove and or clean the infected systems that contain malicious code.

On the morning of July 26, 2004 when the new variant of Mydoom (Mydoom.M) was released on the Internet, none of the Anti virus vendors had released the updated DAT file necessary to clean infected systems. Given that the necessary DAT file (4381) was not available to eradicate the Mydoom.M worm from the infected systems within the GZAC network, the first cases of the Mydoom.M worm had to be cleaned using the Mcafee Stinger tool.

Mcafee Stinger is basically a mini virus-scan tool that has the necessary definition files needed to detect and remove the targeted worm or Trojan from the infected system. The Mcafee Stinger tool is a 798 KB executable file that can be downloaded for free from the NAI web site. [38]

The laptops and workstations that were infected within the GZAC network were all Windows based systems (Win 2000 or Win XP), with the latest Microsoft service packs available.

Symptoms of the infection were:

- Slow system access.
- Slow Internet access when opening the web browser or accessing web sites.
- Email messages take longer then usual to send.
- *Open tcp port 1034 on the infected systems.

**Note: Open tcp port was found by running netstat –an on the employee's system.*

In order to run the Mcafee Stinger tool on the infected systems, both Field Services and EHD teams had to copy the stinger.exe file to the infected systems. See figure 19

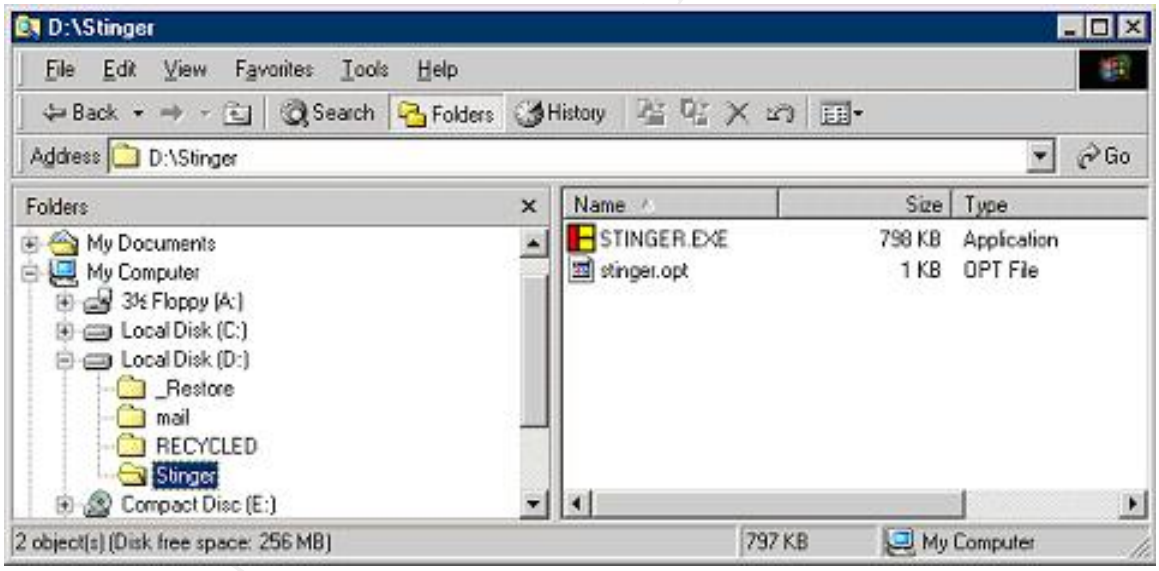


Figure 19 – Mcafee Stinger tool copied to an infected system

When the stinger.exe file was copied to the infected system they would run the file by clicking on stinger.exe. Once Stinger was launched, the next step was to click the "Scan Now" button to start the scan. See figure 20

Figure 20 – Starting the Stinger scan on the infected system

When Stinger finished scanning the system, the status box indicates that the system was infected with the Mydoom.M virus. It also listed the files and folders that were infected and current status of the files that were infected by the Mydoom.M worm. In this case we can see that all the infected files were deleted and the worm was cleaned from the system. See figure 21

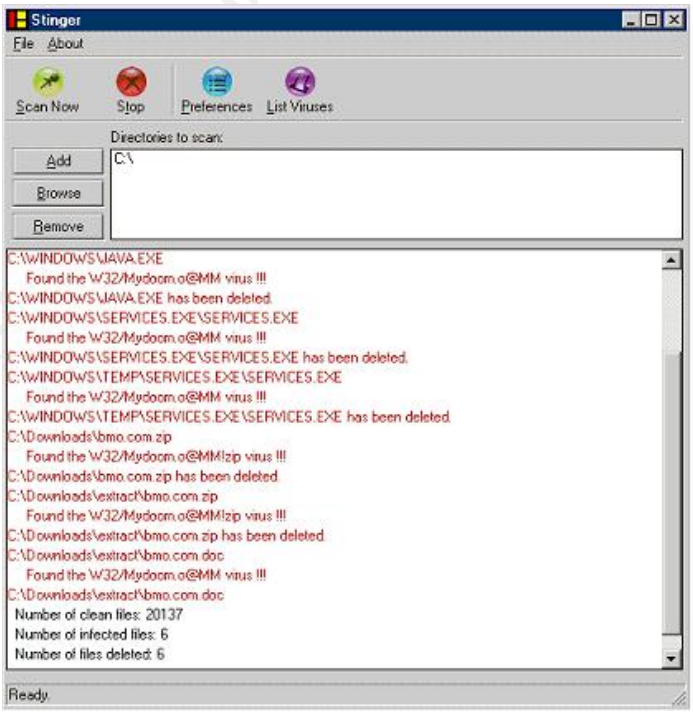


Figure 21 – Log file shows that Stinger cleaned the infected system

At around 12:00:00 when Mcafee released the DAT file (4381) that was necessary to clean the Mydoom.M worm infection, the Anti-virus team was able to push the DAT file to all clients on the network via ePO. This allowed all employee systems on the network to be updated with the latest DAT file - 4381. Once the systems received the latest updated DAT file, the ePO agent that resides on all employee systems would automatically trigger Mcafee Virus Scan to scan the entire contents of the system hard disk. This would ensure that the Mydoom.M worm and any other detectable malicious code were cleaned from the systems. See figure 22 and figure 23

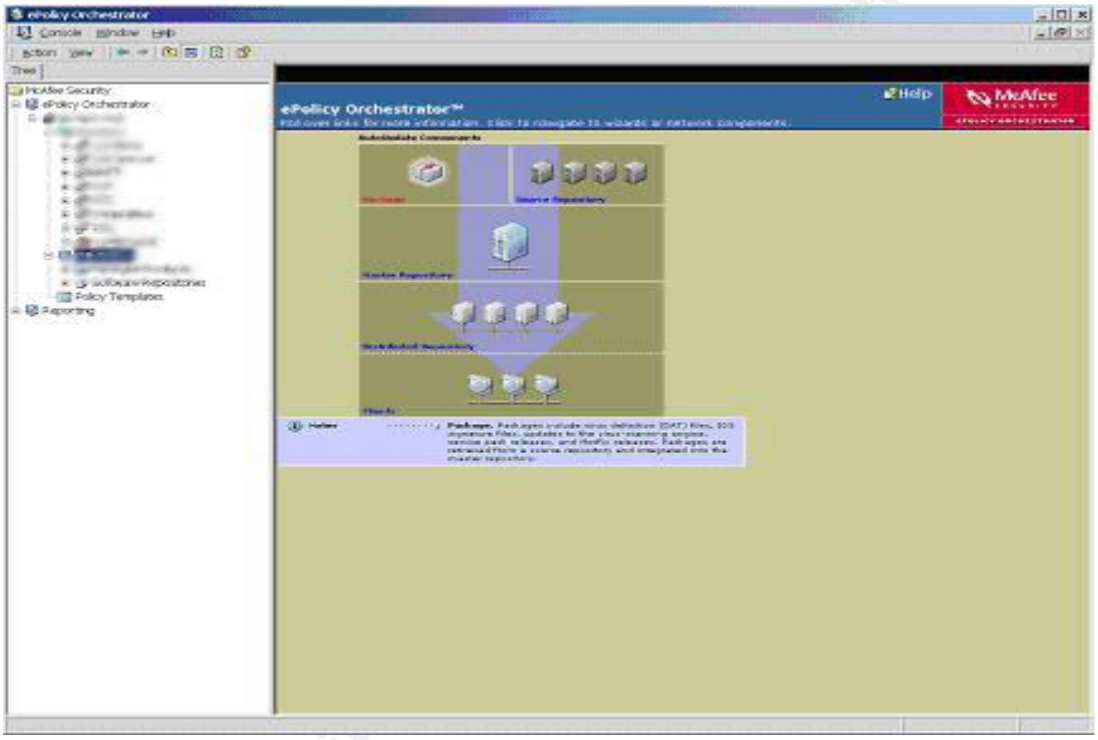


Figure 22 – ePO distributing latest DAT file to all systems on the network

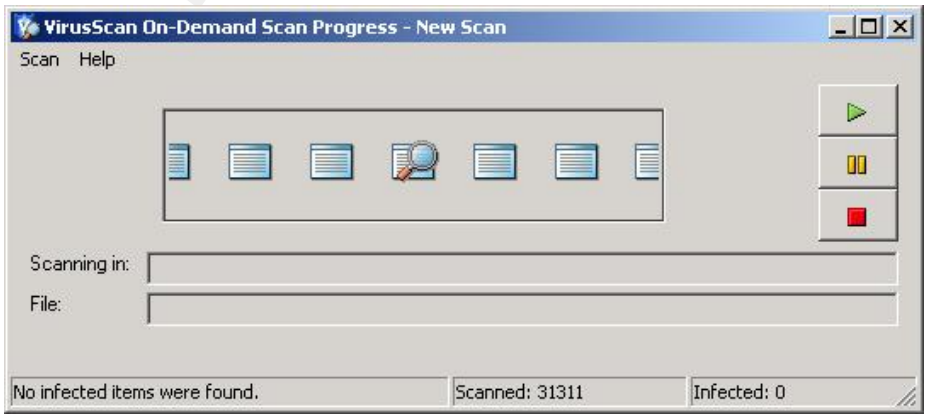


Figure 23 - Mcafee Virus Scan automatically scanned the system

Recovery Phase

Given that all employee systems were either cleaned manually with the Mcafee Stinger tool or automatically when they received the latest DAT file from the ePO server, it is safe to assume that all systems on the GZAC network were returned to a known good state. The IDS sensors that are monitored by Information Security also demonstrated further evidence of this, as no events pertaining to the Mydoom.M worm were generated after the latest DAT file was deployed.

Although all employee systems on the GZAC network have the latest AV software and are updated on a regular basis, we are at the mercy of the AV vendors when it comes to receiving the latest DAT files needed to clean new viruses that may crop up.

Lessons Learned Phase

A week after the Mydoom.M incident was over the SPMT team members gathered for a post mortem meeting. In the meeting they went over the incident chronology and other notes that had been gathered to determine how and what could be done better if a similar situation occurred again.

The meeting results turned up the following “could have done better” list.

- As the Mydoom.M worm relies on social engineering to propagate if employees were notified in a timelier manner the virus may not have spread so rapidly within our organization. Therefore, in the future corporate communication messages will be drafted and disseminated to employees within two hours of a SPMT meeting convening.

- The virus could have been eliminated much sooner if the new DAT file was distributed in a more timely manner. Therefore, in a crisis situation such as the outbreak of the Mydoom.M worm, DAT file testing does not need to be done before employee systems receive new DAT files. Due to the sensitive nature of servers within the GZAC network all new DAT files must still be tested before being placed on the servers.

In an attempt to protect against future outbreaks of this nature the SPMT members have also planned to concentrate more on promoting security awareness amongst the GZAC employees. This will be achieved by holding lunch and learn meetings to promote security awareness.

Extras

The following Incident summary was created by Information Security and sent to all executives within the GZAC network to inform them of the incident that took place.

Incident Summary

Summary

On July 26, a virus known as the Mydoom.M worm was released on the Internet causing latency issues with various search engines. The Mydoom.M worm was detected on the GZAC network, which caused an outbreak of the infection on employee laptop and desktop systems.

An SPMT team was convened to address the Mydoom.M incident. The necessary members of the affected areas addressed the infected systems. By July 27 at 08:00 we were able to clean all infected systems. On July 28 at 17:00, the SPMT team was disbanded.

Impact

Some employees reported incidents of slow Internet access, failed access attempt to some search engines, and slow mail delivery times.

Service has been restored to normal Since the Mydoom.M worm outbreak was resolved service has been restored to normal.

Recommendations

Recommendation	Owner	Progress
Plan and implement Host Based Intrusion detection on employee systems	Network Planning Team	Ongoing
Have users review the Information Security Guide on a regular basis	All	Ongoing

References

[1] http://www.snowplow.org/tom/worm/history.html

[2] http://computing-dictionary.thefreedictionary.com/Worm

[3] http://securityresponse.symantec.com/avcenter/venc/data/w32.mydoom.m@mm.html

[4] http://www.us-cert.gov/cas/alerts/SA04-208A.html

[5] http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=127033

[6] http://www.viruslist.com/eng/index.html?tnews=1001&id=1931854

[7] http://www.cert.org/advisories/CA-1999-02.html

[8] http://www.virusalert.info/?p=virus&id=624&name=W32.Mydoom.m@mm

[9] http://www.virusbuster.hu/en/viruslab/alerts/iworm_mydoom_r

[10] http://www.f-secure.com/v-descs/mydoom_m.shtml

[11] http://www.viruslibrary.com/virusinfo/I-Worm.Mydoom.m.htm

[12] http://www.sophos.com/virusinfo/analyses/w32mydoomo.html

[13] http://securityresponse.symantec.com/avcenter/venc/data/w32.mydoom.l@mm.html

[14] http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?IdVirus=50107&sind=0

[15] http://www.c-enter.hu/center/0227425.html

[16] http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYDOOM.M

[17] http://www.securityfocus.com/news/9265
[18] http://www.yale.edu/pclt/COMM/TCPIP.HTM

[19] http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214173,00.html

[20] http://www.theregister.co.uk/2004/07/26/google_mydoom_infection/

[21] http://www.eweek.com/article2/0,1759,1627771,00.asp?rsDis=MyDoom_Variant_Zaps_Search_Engines,_E_Mail-Page001-132183

[22] http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci523729,00.html

[23] http://staff.washington.edu/dittrich/misc/trinoo.analysis
http://staff.washington.edu/dittrich/misc/tfn.analysis

[24] http://www.faqs.org/rfcs/rfc821.html

[25] http://www.microsoft.com/windowsserversystem/sus/susdeployment.mspx

[26] http://www.networkassociates.com/us/products/mcafee/mgmt_solutions/epo.htm

[27] http://xforce.iss.net/xforce/xfdb/14960

[28] Hal Pomeranz, Deer Run Associates (ed), “Solaris Security Step-by-Step”, Version 1.0, SANS Institute, 1999.

[29] Lee E. Brotzman, Allied Technology Group, Inc. and David A. Ranch, Trinity Designs (ed), “Securing Linux Step-by-Step”, Version 1.0, SANS Institute, 1999, 2000.

[30] Jeff Shawgo (ed), “Securing Windows 2000 Step-by-Step”, Version 1.0c, SANS Institute, 2001.

[31] http://www.ethereal.com/introduction.html

[32] Ed Skoudis and SANS, Computer and Network Hacking Exploits, Track 4 Day 2, SANS, 2003

[33] http://www.datarescue.com/idabase/

[34] http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYDOOM.M&VSect=T

[35] https://www.isc2.org/cgi-bin/index.cgi

[36] http://www.sans.org/

[37] http://dshield.org/port_report.php?port=1034&recax=1&tarax=2&srcax=2&percent=N&days=40&Redraw=

[38] http://vil.mcafeesecurity.com/vil/averttools.asp

[39] http://www.cert.org/current/archive/2004/07/26/archive.html

[40] http://csrc.nist.gov/pcig/cig.html

[41] http://www.eventhelix.com/RealtimeMantra/Networking/SMTP_Sequence_Diagram.pdf

Appendix