# MyDoom.B Worm Analysis

Applied Watch Technologies, Inc.

Prepared by:

Eric S. Hines CEO, President

Applied Watch Technologies,

Inc.

4204 Commercial Way Glenview, IL 60025

Toll Free: (877) 262-7593

Date Prepared: January 30 2004 Last Updated: January 30, 2004 3:21am



### Table of Contents

INTRODUCTION	3
DOCUMENT SCOPE	3
ANALYSIS	5
THE MODIFIED HOSTS FILE	5
Explorer.exe	e
CTFMON.DLL	
REGISTRY KEYS	
NETWORK ANALYSIS	
CONTRIBUTIONS	18

#### **Document Scope**

The purpose of this document is to provide a detailed analysis of the MyDoom.B virus. The pragmatic analysis of malware and its impact on a system is an effective method for Security Event Analysts to understand newly surfaced threats posed against the Enterprise. This report is a documented analysis of malicious code designed to help other Security Analysts, System Custodians, and Management understand the impact it has on the Enterprise so appropriate remediation efforts and loss expectancies can be better understood

#### **Executive Summary**

The MyDoom.B variant surfaced two days after the release of its predecessor, MyDoom.A. The highly publicized MyDoom email virus is representative of characteristics of previous email-based viruses. However, the MyDoom virus is enjoying one of the most massive infection rates seen in quite some time.

Upon infection of a host caused by the user executing the virus from an infected email attachment, MyDoom.B quickly places explorer.exe into the c:\\$windows\system32\\ directory; careful to obviously not mistake it for the legitimate Windows file, c:\\$windows\explorer.exe. In addition, the worm also creates the c:\\$windows\system32\ctfmon.dll file. Because previous virus DAT files were looking for the MyDoom.A files, MyDoom.B was able to enjoy a relatively quick infection rate until networks were able to update their DAT files that protected them against MyDoom.A.

The significant changes to the MyDoom.B variant is the fact that the virus overwrites the C:\WINDOWS\system32\drivers\etc\hosts file, null routing domain URL's for Antivirus companies and several others to 0.0.0.0. In addition, the MyDoom.B variant also scans for MyDoom.A infected hosts and utilizes A's TCP port 3127 to upload itself to the machine, then executing it to infect it with the B variant.

Subsequent sections in this report provide more granular detail on the virus and includes screenshots and log entries caused from the MyDoom infection.

Below is a graph providing a current traffic rate for TCP port 3127, which is the backdoor port initially used by the A variant if its not in use. This graph is representative as of January 30, 2004 from the SANS Internet Storm Center<sup>1</sup>. Although several of these records are caused by individuals looking for MyDoom.A infected hosts, MyDoom.B causes significantly large amounts of traffic in its scanning attempts to find A infected machines. The spike in activity for port 3127 is attributed to this large increase in B port scans.

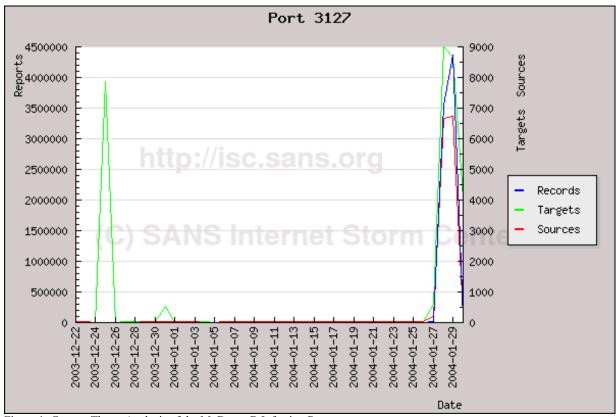


Figure 1: Current Threat Analysis of the MyDoom.B Infection Rate

#### All MyDoom.B Files

Name A	Size	Туре	Date Modified
BlackIce_Firewall_Enterprisea	29 KB	Application	2/3/2004 3:37 PM
	6 KB	Application Extension	1/30/2004 12:49 AM
🗐 data.txt.scr	29 KB	Screen Saver	2/3/2004 3:37 PM
explorer.exe	29 KB	Application	2/3/2004 3:37 PM
i hosts	2 KB	File	1/30/2004 12:49 AM

Figure 2: Complete listing of all files created by the MyDoom.B virus

<sup>&</sup>lt;sup>1</sup> ISC: Sans Internet Storm Center http://isc.sans.org

#### The Modified Hosts File

Upon infection of the victim host, the C:\\$windows\system32\drivers\etc\hosts file is overwritten. The hosts file is used by the local machine for DNS resolution. System administrators will often plug IP addresses for domain names into this file to allow for much quicker DNS resolution to be performed. The system will check this file first for the IP address of the domain prior to checking the primary nameserver.

First we see the file being created by the MyDoom.B virus:

12:24:08.315 AM data.txt.scr:944 IRP\_MJ\_CREATE C:\WINDOWS\system32\drivers\etc\hosts SUCCESS Options: OverwriteIf Access: All

#### The modified hosts file is provided below:

127.0.0.1	localhost localdomain local lo
0.0.0.0	0.0.0.0
0.0.0.0	engine.awaps.net awaps.net www.awaps.net ad.doubleclick.net
0.0.0.0	spd.atdmt.com atdmt.com click.atdmt.com clicks.atdmt.com
0.0.0.0	media.fastclick.net fastclick.net www.fastclick.net ad.fastclick.net
0.0.0.0	ads.fastclick.net banner.fastclick.net banners.fastclick.net
0.0.0.0	www.sophos.com sophos.com ftp.sophos.com f-secure.com www.f-secure.com
0.0.0.0	ftp.f-secure.com securityresponse.symantec.com
0.0.0.0	www.symantec.com symantec.com service1.symantec.com
0.0.0.0	liveupdate.symantec.com updates.symantec.com
0.0.0.0	support.microsoft.com downloads.microsoft.com
0.0.0.0	download.microsoft.com windowsupdate.microsoft.com
0.0.0.0	office.microsoft.com msdn.microsoft.com go.microsoft.com
0.0.0.0	nai.com www.nai.com vil.nai.com secure.nai.com www.networkassociates.com
0.0.0.0	networkassociates.com avp.ru www.avp.ru www.kaspersky.ru
0.0.0.0	www.viruslist.ru viruslist.ru avp.ch www.avp.ch www.avp.com
0.0.0.0	avp.com us.mcafee.com mcafee.com www.mcafee.com dispatch.mcafee.com
0.0.0.0	download.mcafee.com mast.mcafee.com www.trendmicro.com
0.0.0.0	www3.ca.com ca.com www.ca.com www.my-etrust.com
0.0.0.0	my-etrust.com ar.atwola.com phx.corporate-ir.net
0 0 0 0 ww	w.microsoft.com

Any subsequent attempts to go to <a href="www.microsoft.com">www.microsoft.com</a>, <a href="www.nai.com">www.symantec.com</a>, <a href="www.microsoft.com">www.symantec.com</a>, <a href="www.symantec.com">www.symantec.com</a>, <a hre

Explorer.exe is created by MyDoom.B in the c:\\$windows\system32 directory. Unlike the legitimate c:\\$windows\explorer.exe, this file is executed upon system startup, which then reinitializes and runs the virus.

12:24:08.285 AMdata.txt.scr:944 IRP\_MJ\_CREATE C:\WINDOWS\System32\explorer.exe SUCCESS Options: OverwriteIf Access: All

# file explorer.exe

explorer.exe: MS-DOS executable (EXE), OS/2 or Windows

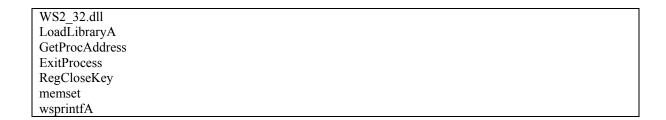
From this Unix utility above, the file command allows you to identify what type of file a particular file is.

From the file(exec) man page:

"file tests each argument in an attempt to classify it. There are three sets of tests, performed in this order: filesystem tests, magic number tests, and language tests. The first test that succeeds causes the file type to be printed."

Below is a list of words found in the explorer exe executable file found using the strings command. The strings command in Unix searches through a specified file for printable strings and prints them to STDOUT (the screen).

.text .data .rsrc .rdata (sync-1. 01; andy I'm just doing myk ob, noth personal system 32\driv \etc\ho ;mailBody Mess > smithMC &Fad joe?neo USERPROFILE 123456789+/{ **OUIT** KERNELDLL ModuleBaseN|pG FilEx SAPI\ Wi!owsDictory LibraFpy?d KERNEL32.DLL ADVAPI32.dll MSVCRT.dll USER32.dll



As we see here, using the diff command to find any differences between the Worm's explorer.exe file and the data.txt.scr virus attachment, there are no differences between the two. We can now determine that the explorer.exe file placed in \$system32\ is in fact the Worm itself. We can also derive this by using the md5sum command in Unix, which provides the checksum of the file being compared. This is an invaluable tool in incident response when you have the original md5 checksum of a known clean file. This md5 checksum can be used to compare it to a compromised system to identify if a particular binary has changed or been trojaned. Below we see identical md5 checksums of both files.

chicago-gw# diff data.txt.scr explorer.exe chicago-gw#

chicago-gw# md5 explorer.exe MD5 (explorer.exe) = cc6e6aa338385fbb0a005ba3d3e060f3 chicago-gw# md5 data.txt.scr MD5 (data.txt.scr) = cc6e6aa338385fbb0a005ba3d3e060f3

#### ctfmon.dll

The CTFMON.DLL file is created by the MyDoom.B worm into the c:\\$windows\system32 directory and is injected into the Windows Explorer.exe process. This causes the worm to remain resident in memory without being listed in the processes list in Windows.

# file ctfmon.dll ctfmon.dll: MS-DOS executable (EXE), OS/2 or Windows

#### Output from strings command

UPX0
UPX1
UPX2
1.24
UPX!
kernel32.dll
""%s"
abcdefghijk
WriteFileCrea

loseHand

irtualQueryGetModul8Nl

LoCLibra< rocAdd[ss TickCount Object RegS Y=Key

KERNEL32.DLL
ADVAPI32.dll
MSVCRT.dll
USER32.dll
WSOCK32.dll
LoadLibraryA
GetProcAddress
RegCloseKey
memcmp
wsprintfA

#### **Registry Keys**

The following Windows Registry keys are created by the worm upon execution.

SetValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache SUCCESS "C:\Documents and Settings\Eric Hines\Local Settings\Temporary Internet Files"

SetValue HKCR\CLSID\\E6FB5E20-DE35-11CF-9C87-00AA005127ED\\InprocServer32\(Default\)

SUCCESS "C:\WINDOWS\System32\ctfmon.dll"

SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Explorer

SUCCESS "C:\WINDOWS\System32\explorer.exe"

SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Internet

Settings\Cache\Paths\Directory

SUCCESS "C:\Documents and Settings\Eric Hines\Local Settings\Temporary Internet

Files\Content.IE5"

SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Paths

SUCCESS 0x4

SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Internet

Settings\Cache\Paths\Path1\CachePath

SUCCESS "C:\Documents and Settings\Eric Hines\Local Settings\Temporary Internet

Files\Content.IE5\Cache1"

SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Internet

Settings\Cache\Paths\Path2\CachePath

SUCCESS "C:\Documents and Settings\Eric Hines\Local Settings\Temporary Internet

Files\Content.IE5\Cache2"

SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Internet

Settings\Cache\Paths\Path3\CachePath

SUCCESS "C:\Documents and Settings\Eric Hines\Local Settings\Temporary Internet

Files\Content.IE5\Cache3"

SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Internet

Settings\Cache\Paths\Path4\CachePath

SUCCESS "C:\Documents and Settings\Eric Hines\Local Settings\Temporary Internet

Files\Content.IE5\Cache4"

SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Internet

Settings\Cache\Paths\Path1\CacheLimit SUCCESS 0x23233

SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Internet

Settings\Cache\Paths\Path2\CacheLimit

SUCCESS 0x23233

SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Internet

Settings\Cache\Paths\Path3\CacheLimit

SUCCESS 0x23233

SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Internet

Settings\Cache\Paths\Path4\CacheLimit

SUCCESS 0x23233

SetValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies

SUCCESS "C:\Documents and Settings\Eric Hines\Cookies"

SetValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\History

SUCCESS "C:\Documents and Settings\Eric Hines\Local Settings\History"

SetValue HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common

AppData

SUCCESS "C:\Documents and Settings\All Users\Application Data"

SetValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData

SUCCESS "C:\Documents and Settings\Eric Hines\Application Data"

SetValue HKCU\Software\Microsoft\windows\CurrentVersion\Internet Settings\MigrateProxy

SUCCESS 0x1

SetValue HKCU\Software\Microsoft\windows\CurrentVersion\Internet Settings\ProxyEnable

SUCCESS 0x0

SetValue HKCU\Software\Microsoft\windows\CurrentVersion\Internet Settings\ProxyServer

SUCCESS "http=hodc-cache:8088;https=hodc-cache:8088"

SetValue HKCC\Software\Microsoft\windows\CurrentVersion\Internet Settings\ProxyEnable

SUCCESS 0x0

SetValue HKCU\Software\Microsoft\windows\CurrentVersion\Internet

Settings\Connections\SavedLegacySettings SUCCESS 3C 00 00 00 5B 08 00 00 ...

SetValue HKCR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InprocServer32\(Default)

SUCCESS "C:\WINDOWS\System32\ctfmon.dll"

SetValue HKCR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InprocServer32\(Default)

SUCCESS "C:\WINDOWS\System32\ctfmon.dll"

Here we see the outgoing traffic causing outbound port 3127 scans for infected A hosts.

data.txt.scr:1724 TCP	0.0.0.0:1080	0.0.0.0:0	LISTENING
data.txt.scr:1724 TCP	0.0.0.0:3831	0.0.0.0:0	LISTENING
data.txt.scr:1724 TCP	192.168.0.7:3831	193.231.169.3:25	SYN SENT
data.txt.scr:1724 TCP	0.0.0.0:3833	0.0.0.0:0	LISTENING
data.txt.scr:1724 TCP	0.0.0.0:3834	0.0.0.0:0	LISTENING
data.txt.scr:1724TCP	192.168.0.7:3833	205.244.99.48:3127	SYN SENT
data.txt.scr:1724TCP	192.168.0.7:3834	45.86.117.48:3127	SYN SENT
data.txt.scr:1724 TCP	0.0.0.0:3835	0.0.0.0:0	LISTENING
data.txt.scr:1724 TCP	192.168.0.7:3835	193.231.169.3:25	SYN SENT
data.txt.scr:1724 UDP	0.0.0.0:3836	*:*	_
data.txt.scr:1724 TCP	0.0.0.0:3837	0.0.0.0:0	LISTENING
data.txt.scr:1724TCP	192.168.0.7:3837	192.168.0.52:3127	SYN_SENT

The highlighted line above is the worm listening on port 1080 for incoming connections. This is the remote control backdoor port for the worm, whereas version A used TCP port range 3127-3198. In addition, the lines **bolded** are outgoing scans for A infected hosts. The rest of the traffic is associated with the outgoing emails generated by the MyDoom virus.

Here we see the worm attempting to brute force the hostname of the mail server for an outgoing attempted email to the @COMPANY.com domain. The worm uses DNS to brute force the mail server names as shown below on UDP port 53.

```
01/30-00:24:10.059349 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x4A
192.168.0.7:3049 -> 209.242.0.2:53 UDP TTL:128 TOS:0x0 ID:7019 IpLen:20
DgmLen:60
Len: 32
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 .........[#....E.
0x0010: 00 3C 1B 6B 00 00 80 11 8C A2 C0 A8 00 07 D1 F2 .<.k.....
0x0020: 00 02 0B E9 00 35 00 28 5C D1 02 64 01 00 00 01 .....5.(\..d....
0x0030: 00 00 00 00 00 0A 66 6F 75 6E 64 73 74 6F 6E
                                             ....COMPANY.COM
0x0040: 65 03 63 6F 6D 00 00 0F 00 01
01/30-00:24:10.065481 0:2:E3:9:9F:92 -> 0:9:5B:23:EF:8D type:0x800
len:0x71
209.242.0.2:53 -> 192.168.0.7:3049 UDP TTL:60 TOS:0x0 ID:50043 IpLen:20
DgmLen:99
Len: 71
0x0010: 00 63 C3 7B 00 00 3C 11 28 6B D1 F2 00 02 C0 A8 .c.{..<.(k.....
0x0020: 00 07 00 35 0B E9 00 4F B7 B1 02 64 81 80 00 01 ...5...0...d....
0x0030: 00 02 00 00 00 00 0A 66 6F 75 6E 64 73 74 6F 6E .....COMPANY.COM
```

And then we see the worm make a successful guess of the COMPANY.com mailserver's hostname with a completed 3-way TCP handshake. Before a TCP session between two hosts can be established, machine A must establish a completed 3-way TCP handshake with the remote host. This consists of 3 packets, the first packet being a SYN, the response from Host B being a SYN+ACK, and the final packet from the initiator Host A, ACK.

```
01/30-00:24:10.099259 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x3E
192.168.0.7:3253 -> 66.000.000.000:25 TCP TTL:128 TOS:0x0 ID:7021 IpLen:20
DgmLen:48 DF
*****S* Seq: 0x108DDA9D Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 ........[#....E.
0x0010: 00 30 1B 6D 40 00 80 06 C8 FD C0 A8 00 07 42 A1 .0.m@......B.
0x0020: 13 0D 0C B5 00 19 10 8D DA 9D 00 00 00 70 02 .....p.
0x0030: 40 00 34 C9 00 00 02 04 05 B4 01 01 04 02
                                         0.4.......
01/30-00:24:10.159309 0:2:E3:9:9F:92 -> 0:9:5B:23:EF:8D type:0x800
len:0x3E
66.000.000.000:25 -> 192.168.0.7:3253 TCP TTL:40 TOS:0x0 ID:34246 IpLen:20
DamLen:48 DF
***A**S* Seq: 0x97893E97 Ack: 0x108DDA9E Win: 0x4410 TcpLen: 28
TCP Options (4) => MSS: 1452 NOP NOP SackOK
0x0010: 00 30 85 C6 40 00 28 06 B6 A4 42 A1 13 0D C0 A8 .0..@.(...B.....
0x0030: 44 10 5A 8F 00 00 02 04 05 AC 01 01 04 02
                                         D.Z.....
01/30-00:24:10.159384 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x36
192.168.0.7:3253 -> 66.000.000.000:25 TCP TTL:128 TOS:0x0 ID:7022 IpLen:20
DgmLen:40 DF
***A**** Seq: 0x108DDA9E Ack: 0x97893E98 Win: 0x4410 TcpLen: 20
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 ........[#....E.
0x0010: 00 28 1B 6E 40 00 80 06 C9 04 C0 A8 00 07 42 A1 .(.n@......B.
0x0030: 44 10 87 4B 00 00
                                         D..K..
01/30-00:24:10.220860 0:2:E3:9:9F:92 -> 0:9:5B:23:EF:8D type:0x800
len:0x50
66.000.000.000:25 -> 192.168.0.7:3253 TCP TTL:40 TOS:0x0 ID:37091 IpLen:20
DgmLen:66 DF
```

```
***AP*** Seq: 0x97893E98 Ack: 0x108DDA9E Win: 0x4410 TcpLen: 20
0x0000: 00 09 5B 23 EF 8D 00 02 E3 09 9F 92 08 00 45 00 ..[#.....................
0x0010: 00 42 90 E3 40 00 28 06 AB 75 42 A1 13 0D C0 A8 .B..@.(..uB.....
0x0030: 44 10 8E F3 00 00 32 32 30 20 66 6F 75 6E 64 73 D.....220 COMPAN
0x0040: 74 6F 6E 65 2E 63 6F 6D 20 45 53 4D 54 50 0D 0A Y.COM ESMTP...
01/30-00:24:10.221296 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x51
192.168.0.7:3253 -> 66.000.000.000:25 TCP TTL:128 TOS:0x0 ID:7023 IpLen:20
DgmLen:67 DF
***AP*** Seq: 0x108DDA9E Ack: 0x97893EB2 Win: 0x43F6 TcpLen: 20
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 .........[#....E.
0x0010: 00 43 1B 6F 40 00 80 06 C8 E8 C0 A8 00 07 42 A1 .C.o@......B.
0x0030: 43 F6 BF AA 00 00 45 48 4C 4F 20 63 76 73 2E 61 C....EHLO cvs.a
0x0040: 70 70 6C 69 65 64 77 61 74 63 68 2E 63 6F 6D 0D ppliedwatch.com.
0x0050: 0A
```

## Next, the worm then introduces itself to the COMPANY mailserver and sends the virus infected email to john.doe@company.com

```
01/30-00:24:10.241348 ARP who-has 192.168.0.2 tell 192.168.0.7
01/30-00:24:10.278145 0:2:E3:9:9F:92 -> 0:9:5B:23:EF:8D type:0x800
len:0x68
66.000.000.000:25 -> 192.168.0.7:3253 TCP TTL:40 TOS:0x0 ID:44272 IpLen:20
DgmLen:90 DF
***AP*** Seq: 0x97893EB2 Ack: 0x108DDAB9 Win: 0x4410 TcpLen: 20
0x0010: 00 5A AC F0 40 00 28 06 8F 50 42 A1 13 0D C0 A8 .Z..@.(..PB.....
0x0030: 44 10 D2 1F 00 00 32 35 30 2D 66 6F 75 6E 64 73 D.....250-COMPAN
0x0040: 74 6F 6E 65 2E 63 6F 6D 0D 0A 32 35 30 2D 50 49 Y.COM..250-PI
0x0050: 50 45 4C 49 4E 49 4E 47 0D 0A 32 35 30 20 38 42 PELINING..250 8B
0x0060: 49 54 4D 49 4D 45 0D 0A
                                         ITMIME..
01/30-00:24:10.278786 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x5E
192.168.0.7:3253 -> 66.000.000.000:25 TCP TTL:128 TOS:0x0 ID:7026 IpLen:20
DgmLen:80 DF
***AP*** Seq: 0x108DDAB9 Ack: 0x97893EE4 Win: 0x43C4 TcpLen: 20
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 ........[#....E.
0x0010: 00 50 1B 72 40 00 80 06 C8 D8 C0 A8 00 07 42 A1 .P.r@......B.
0x0030: 43 C4 D4 2E 00 00 4D 41 49 4C 20 46 52 4F 4D 3A C....MAIL FROM:
0x0040: 3C 73 61 6C 65 73 40 63 76 73 2E 61 70 70 6C 69 <sales@cvs.appli
0x0050: 65 64 77 61 74 63 68 2E 63 6F 6D 3E 0D 0A
                                        edwatch.com>..
```

```
01/30-00:24:10.336472 0:2:E3:9:9F:92 -> 0:9:5B:23:EF:8D type:0x800
len·Ox3E
66.000.000.000:25 -> 192.168.0.7:3253 TCP TTL:40 TOS:0x0 ID:41517 IpLen:20
DamLen:48 DF
***AP*** Seq: 0x97893EE4 Ack: 0x108DDAE1 Win: 0x4410 TcpLen: 20
0x0010: 00 30 A2 2D 40 00 28 06 9A 3D 42 A1 13 0D C0 A8 .0.-@.(..=B.....
0x0030: 44 10 A7 E1 00 00 32 35 30 20 6F 6B 0D 0A
                                       D.....250 ok..
01/30-00:24:10.336725 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x55
192.168.0.7:3253 -> 66.000.000.000:25 TCP TTL:128 TOS:0x0 ID:7027 IpLen:20
DgmLen:71 DF
***AP*** Seq: 0x108DDAE1 Ack: 0x97893EEC Win: 0x43BC TcpLen: 20
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 ........[#....E.
0x0010: 00 47 1B 73 40 00 80 06 C8 E0 C0 A8 00 07 42 A1 .G.s@......B.
0x0030: 43 BC 5A A8 00 00 52 43 50 54 20 54 4F 3A 3C 6C C.Z...RCPT TO:<1
0x0040: 61 62 73 40 66 6F 75 6E 64 73 74 6F 6E 65 2E 63 abs@COMPANY.c
0x0050: 6F 6D 3E 0D 0A
                                       om > ..
01/30-00:24:10.392618 0:2:E3:9:9F:92 -> 0:9:5B:23:EF:8D type:0x800
len:0x3E
66.000.000.000:25 -> 192.168.0.7:3253 TCP TTL:40 TOS:0x0 ID:48692 IpLen:20
DgmLen:48 DF
***AP*** Seq: 0x97893EEC Ack: 0x108DDB00 Win: 0x4410 TcpLen: 20
0x0010: 00 30 BE 34 40 00 28 06 7E 36 42 A1 13 0D C0 A8 .0.4@.(.~6B.....
0x0030: 44 10 A7 BA 00 00 32 35 30 20 6F 6B 0D 0A
                                       D.....250 ok..
01/30-00:24:10.392871 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x3C
192.168.0.7:3253 -> 66.000.000.000:25 TCP TTL:128 TOS:0x0 ID:7028 IpLen:20
DgmLen:46 DF
***AP*** Seq: 0x108DDB00 Ack: 0x97893EF4 Win: 0x43B4 TcpLen: 20
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 ........[#....E.
0x0010: 00 2E 1B 74 40 00 80 06 C8 F8 C0 A8 00 07 42 A1 ...t@......B.
0x0030: 43 B4 E1 4E 00 00 44 41 54 41 0D 0A
                                       C..N..DATA..
01/30-00:24:10.449902 0:2:E3:9:9F:92 -> 0:9:5B:23:EF:8D type:0x800
len:0x44
66.000.000.000:25 -> 192.168.0.7:3253 TCP TTL:40 TOS:0x0 ID:62066 IpLen:20
DgmLen:54 DF
***AP*** Seq: 0x97893EF4 Ack: 0x108DDB06 Win: 0x4410 TcpLen: 20
0x0010: 00 36 F2 72 40 00 28 06 49 F2 42 A1 13 0D C0 A8 .6.r@.(.I.B.....
0x0030: 44 10 C0 77 00 00 33 35 34 20 67 6F 20 61 68 65 D..w..354 go ahe
```

```
0x0040: 61 64 0D 0A
01/30-00:24:10.450218 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x58
192.168.0.7:3253 -> 66.000.000.000:25 TCP TTL:128 TOS:0x0 ID:7029 IpLen:20
DgmLen:74 DF
***AP*** Seq: 0x108DDB06 Ack: 0x97893F02 Win: 0x43A6 TcpLen: 20
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 ........[#....E.
0x0010: 00 4A 1B 75 40 00 80 06 C8 DB C0 A8 00 07 42 A1 .J.u@.......B.
0x0020: 13 0D 0C B5 00 19 10 8D DB 06 97 89 3F 02 50 18 ........................
0x0030: 43 A6 5D 9C 00 00 46 72 6F 6D 3A 20 73 61 6C 65 C.]...From: sale
0x0040: 73 40 63 76 73 2E 61 70 70 6C 69 65 64 77 61 74 s@cvs.appliedwat
0x0050: 63 68 2E 63 6F 6D 0D 0A
                                                       ch.com..
01/30-00:24:10.450917 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x5E2
192.168.0.7:3253 -> 66.000.000.000:25 TCP TTL:128 TOS:0x0 ID:7030 IpLen:20
DqmLen:1492 DF
***AP*** Seq: 0x108DDB28 Ack: 0x97893F02 Win: 0x43A6 TcpLen: 20
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 ........[#....E.
0x0010: 05 D4 1B 76 40 00 80 06 C3 50 C0 A8 00 07 42 A1 ...v@....P....B.
0x0020: 13 0D 0C B5 00 19 10 8D DB 28 97 89 3F 02 50 18 .........(..?.P.
0x0030: 43 A6 65 7E 00 00 54 6F 3A 20 6C 61 62 73 40 66 C.e~..To: victim
0x0040: 6F 75 6E 64 73 74 6F 6E 65 2E 63 6F 6D 0D 0A 53 @COMPANY.COM...S
0x0050: 75 62 6A 65 63 74 3A 20 55 6E 61 62 6C 65 20 74 ubject: Unable t
0x0060: 6F 20 64 65 6C 69 76 65 72 20 74 68 65 20 6D 65 o deliver the me
0x0070: 73 73 61 67 65 0D 0A 44 61 74 65 3A 20 46 72 69 ssage..Date: Fri
0x0080: 2C 20 33 30 20 4A 61 6E 20 32 30 30 34 20 30 30 , 30 Jan 2004 00
0x0090: 3A 32 34 3A 31 30 20 2D 30 36 30 30 0D 0A 4D 49 :24:10 -0600..MI
0x00A0: 4D 45 2D 56 65 72 73 69 6F 6E 3A 20 31 2E 30 0D ME-Version: 1.0.
0x00B0: 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 6D
                                                       .Content-Type: m
0x00C0: 75 6C 74 69 70 61 72 74 2F 6D 69 78 65 64 3B 0D ultipart/mixed;.
                                                       ..boundary="----
0x00D0: 0A 09 62 6F 75 6E 64 61 72 79 3D 22 2D 2D 2D 2D
0 \times 00 = 0: 3D 5F 4E 65 78 74 50 61 72 74 5F 30 30 30 5F 30 = NextPart 000 0
0x00F0: 30 31 30 5F 46 31 43 34 35 35 33 31 2E 32 37 31 010 F1C45531.271
0 \times 0100: 30 33 46 32 39 22 0D 0A 58 2D 50 72 69 6F 72 69 03\overline{F29}"..X-Priori
0x0110: 74 79 3A 20 33 0D 0A 58 2D 4D 53 4D 61 69 6C 2D ty: 3..X-MSMail-
0x0120: 50 72 69 6F 72 69 74 79 3A 20 4E 6F 72 6D 61 6C Priority: Normal
0x0130: 0D 0A 0D 0A 54 68 69 73 20 69 73 20 61 20 6D 75
                                                       ....This is a mu
0x0140: 6C 74 69 2D 70 61 72 74 20 6D 65 73 73 61 67 65 lti-part message
0x0150: 20 69 6E 20 4D 49 4D 45 20 66 6F 72 6D 61 74 2E in MIME format.
0x0160: 0D 0A 0D 0A 2D 2D 2D 2D 2D 2D 3D 5F 4E 65 78 74 ....---- Next
0x0170: 50 61 72 74 5F 30 30 30 5F 30 30 31 30 5F 46 31 Part 000 0010 F1
0 \times 0180: 43 34 35 35 33 31 2E 32 37 31 30 33 46 32 39 0D C455\overline{3}1.2\overline{7}103F\overline{2}9.
0x0190: 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74
                                                       .Content-Type: t
0x01A0: 65 78 74 2F 70 6C 61 69 6E 3B 0D 0A 09 63 68 61 ext/plain;...cha
0x01B0: 72 73 65 74 3D 22 57 69 6E 64 6F 77 73 2D 31 32 rset="Windows-12"
0x01CO: 35 32 22 0D 0A 43 6F 6E 74 65 6E 74 2D 54 72 61 52"..Content-Tra
0x01D0: 6E 73 66 65 72 2D 45 6E 63 6F 64 69 6E 67 3A 20 nsfer-Encoding:
0x01E0: 37 62 69 74 0D 0A 0D 0A 73 65 6E 64 6D 61 69 6C
                                                       7bit....sendmail
0x01F0: 20 64 61 65 6D 6F 6E 20 72 65 70 6F 72 74 65 64
                                                       daemon reported
0x0200: 3A 0D 0A 45 72 72 6F 72 20 23 38 30 34 20 6F 63 :..Error #804 oc
0x0210: 63 75 72 65 64 20 64 75 72 69 6E 67 20 53 4D 54 cured during SMT
0x0220: 50 20 73 65 73 73 69 6F 6E 2E 20 50 61 72 74 69 P session. Parti
0 \times 0230: 61 6C 20 6D 65 73 73 61 67 65 20 68 61 73 20 62 al message has b
0 \times 0240: 65 65 6E 20 72 65 63 65 69 76 65 64 2E 0D 0A 0D een received....
```

```
...- NextP
0x0250: 0A 0D 0A 2D 2D 2D 2D 2D 3D 5F 4E 65 78 74 50
0x0260: 61 72 74 5F 30 30 30 5F 30 30 31 30 5F 46 31 43
                                           art 000 0010 F1C
0x0270: 34 35 35 33 31 2E 32 37 31 30 33 46 32 39 0D 0A 45531.27103F29..
0x0280: 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 Content-Type: ap
0x0290: 70 6C 69 63 61 74 69 6F 6E 2F 6F 63 74 65 74 2D
                                           plication/octet-
0x02A0: 73 74 72 65 61 6D 3B 0D 0A 09 6E 61 6D 65 3D 22
                                           stream;...name="
0x02B0: 62 6F 64 79 2E 62 61 74 22 0D 0A 43 6F 6E 74 65
                                           body.bat"..Conte
0x02C0: 6E 74 2D 54 72 61 6E 73 66 65 72 2D 45 6E 63 6F
                                           nt-Transfer-Enco
0x02D0: 64 69 6E 67 3A 20 62 61 73 65 36 34 0D 0A 43 6F
                                           ding: base64..Co
0x02E0: 6E 74 65 6E 74 2D 44 69 73 70 6F 73 69 74 69 6F
                                           ntent-Dispositio
0 \times 02 = 0: 6E 3A 20 61 74 74 61 63 68 6D 65 6E 74 3B 0D 0A n: attachment;...
0x0300: 09 66 69 6C 65 6E 61 6D 65 3D 22 62 6F 64 79 2E
                                           .filename="body.
0x0310: 62 61 74 22 0D 0A 0D 0A 54 56 71 51 41 41 4D 41 bat"....TVqQAAMA
0x0320: 41 41 41 45 41 41 41 41 2F 2F 38 41 41 4C 67 41
                                           AAAEAAAA//8AALgA
0x0330: 41 41 41 41 41 41 41 41 51 41 41 41 41 41 41
                                           AAAAAAAAAAAAA
AAAAAAAAAAAAA
0x0360: 41 41 41 41 0D 0A 41 41 41 41 6D 41 41 41 41 41 AAAA..AAAAMAAAA
```

Below are some packets of the MyDoom.B variant attempting to find A variant infected hosts. Based on these timestamps, the level of network degradation caused by a single B variant infected host is relatively small. In the case of this lab machine, a single host sent roughly 9-10 packets a second, a substantially smaller amount of packets than previously devastating worms such as the MSSQL Slammer, which because UDP does not require a 3-way handshake to establish a session, can be used in a shotgun approach at a box in a trivial Denial of Service attack. However, because MyDoom must establish its session over TCP port 3127, the TCP session requires a 3way handshake, slowing the scans down substantially.

```
01/30-00:24:09.392061 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x3E
192.168.0.7:3248 -> 32.15.81.1:3127 TCP TTL:128 TOS:0x0 ID:7011 IpLen:20
DgmLen:48 DF
****** Seq: 0x10882ACC Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00
                                                .....[#....E.
0x0010: 00 30 1B 63 40 00 80 06 AD A5 C0 A8 00 07 20 0F
                                                .0.c@......
0x0020: 51 01 0C B0 0C 37 10 88 2A CC 00 00 00 70 02
                                                Q....7..*...p.
0x0030: 40 00 BD 24 00 00 02 04 05 B4 01 01 04 02
                                                @..$.....
01/30-00:24:09.392884 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x3E
192.168.0.7:3249 -> 158.221.11.1:3127 TCP TTL:128 TOS:0x0 ID:7012 IpLen:20
DgmLen:48 DF
****** Seq: 0x10890F6B Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00
                                                ......[#...E.
0x0010: 00 30 1B 64 40 00 80 06 74 D6 C0 A8 00 07 9E DD
                                                .0.d@...t.....
0x0020: 0B 01 0C B1 0C 37 10 89 0F 6B 00 00 00 00 70 02
                                                ....7...k...p.
```

```
0x0030: 40 00 9F B5 00 00 02 04 05 B4 01 01 04 02
01/30-00:24:09.393526 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x3E
192.168.0.7:3250 -> 131.47.177.1:3127 TCP TTL:128 TOS:0x0 ID:7013 IpLen:20
DgmLen:48 DF
*****S* Seq: 0x1089CCDB Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 .........[#....E.
0x0010: 00 30 1B 65 40 00 80 06 EA 82 CO A8 00 07 83 2F .0.e@...../
0x0030: 40 00 57 F1 00 00 02 04 05 B4 01 01 04 02
                                            @.W....W.D
01/30-00:24:09.393964 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x3E
192.168.0.7:3251 -> 34.27.84.1:3127 TCP TTL:128 TOS:0x0 ID:7014 IpLen:20
DgmLen:48 DF
*****S* Seq: 0x108A5F24 Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 ........[#....E.
0x0010: 00 30 1B 66 40 00 80 06 A8 96 C0 A8 00 07 22 1B .0.f@...................
0x0020: 54 01 0C B3 0C 37 10 8A 5F 24 00 00 00 70 02 T....7.. $....p.
0x0030: 40 00 83 BB 00 00 02 04 05 B4 01 01 04 02
                                            @ . . . . . . . . . . . . . . . . . .
01/30-00:24:09.722506 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x3E
192.168.0.7:3247 -> 192.168.0.1:3127 TCP TTL:128 TOS:0x0 ID:7017 IpLen:20
DgmLen:48 DF
****** Seq: 0x108714B3 Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 .....[#....E.
0x0010: 00 30 1B 69 40 00 80 06 5E 06 CO A8 00 07 CO A8 .0.i@...^.....
0x0020: 00 01 0C AF 0C 37 10 87 14 B3 00 00 00 70 02 .....7......p.
0x0030: 40 00 83 A6 00 00 02 04 05 B4 01 01 04 02
                                            @.....
01/30-00:24:09.724556 0:2:E3:9:9F:92 -> 0:9:5B:23:EF:8D type:0x800
len:0x3C
192.168.0.1:3127 -> 192.168.0.7:3247 TCP TTL:64 TOS:0x0 ID:54903 IpLen:20
DamLen: 40 DF
***A*R** Seq: 0x0 Ack: 0x108714B4 Win: 0x0 TcpLen: 20
0x0010: 00 28 D6 77 40 00 40 06 E2 FF C0 A8 00 01 C0 A8 .(.w@.@......
0x0030: 00 00 F0 56 00 00 FF FF FF FF FF FF
01/30-00:24:10.224076 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x3E
192.168.0.7:3247 -> 192.168.0.1:3127 TCP TTL:128 TOS:0x0 ID:7024 IpLen:20
DgmLen:48 DF
******S* Seq: 0x108714B3 Ack: 0x0 Win: 0x4000 TcpLen: 28
```

```
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 ........[#....E.
0x0010: 00 30 1B 70 40 00 80 06 5D FF CO A8 00 07 CO A8 .0.p@...].....
0x0020: 00 01 0C AF 0C 37 10 87 14 B3 00 00 00 70 02 .....7......p.
0x0030: 40 00 83 A6 00 00 02 04 05 B4 01 01 04 02
                                             @ . . . . . . . . . . . . . . . . . .
01/30-00:24:10.239630 0:2:E3:9:9F:92 -> 0:9:5B:23:EF:8D type:0x800
len:0x3C
192.168.0.1:3127 -> 192.168.0.7:3247 TCP TTL:64 TOS:0x0 ID:43301 IpLen:20
DgmLen:40 DF
***A*R** Seq: 0x0 Ack: 0x108714B4 Win: 0x0 TcpLen: 20
0x0010: 00 28 A9 25 40 00 40 06 10 52 C0 A8 00 01 C0 A8 .(.%@.@..R.....
0x0030: 00 00 F0 56 00 00 FF FF FF FF FF FF
                                              ...V.....
01/30-00:24:12.330842 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x3E
192.168.0.7:3248 -> 32.15.81.1:3127 TCP TTL:128 TOS:0x0 ID:7112 IpLen:20
DgmLen:48 DF
******S* Seq: 0x10882ACC Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 ........[#....E.
0x0010: 00 30 1B C8 40 00 80 06 AD 40 C0 A8 00 07 20 0F .0..@................
0x0020: 51 01 0C B0 0C 37 10 88 2A CC 00 00 00 70 02 Q....7..*....p.
0x0030: 40 00 BD 24 00 00 02 04 05 B4 01 01 04 02
                                             @..$....
01/30-00:24:12.331275 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x3E
192.168.0.7:3249 -> 158.221.11.1:3127 TCP TTL:128 TOS:0x0 ID:7113 IpLen:20
DgmLen:48 DF
****** Seq: 0x10890F6B Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 ........[#....E.
0x0010: 00 30 1B C9 40 00 80 06 74 71 C0 A8 00 07 9E DD .0..@...tq.....
0x0020: 0B 01 0C B1 0C 37 10 89 0F 6B 00 00 00 70 02 .....7...k....p.
0x0030: 40 00 9F B5 00 00 02 04 05 B4 01 01 04 02
                                             @....
01/30-00:24:12.331630 0:9:5B:23:EF:8D -> 0:2:E3:9:9F:92 type:0x800
len:0x3E
192.168.0.7:3250 -> 131.47.177.1:3127 TCP TTL:128 TOS:0x0 ID:7114 IpLen:20
DgmLen:48 DF
****** Seq: 0x1089CCDB Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 00 02 E3 09 9F 92 00 09 5B 23 EF 8D 08 00 45 00 ........[#....E.
0x0010: 00 30 1B CA 40 00 80 06 EA 1D CO A8 00 07 83 2F .0..@...../
0x0020: B1 01 0C B2 0C 37 10 89 CC DB 00 00 00 00 70 02 .....7......p.
0x0030: 40 00 57 F1 00 00 02 04 05 B4 01 01 04 02
                                             @.W....
```

#### **Contributions**

I just want to give a quick thank you to Johannes Ulrich @ SANS who helped me in this analysis by providing me the much anticipated B variant. Thanks Johannes, you made this possible.

**Contact Information** 

Applied Watch Technologies, Inc. 4204 Commercial Way Glenview, IL 60025 Toll Free; (877) 262-7593 <a href="http://www.appliedwatch.com">http://www.appliedwatch.com</a> "Enterprise Snort Management"