

2018-12-19 - MALSPAM PUSHING THE MYDOOM WORM IS STILL A THING

malware-traffic-analysis.net/2018/12/19/index.html

ASSOCIATED FILES:

Malspam examples: [2018-12-17-thru-2018-12-20-MyDoom-malspam-5-email-examples.zip](#) 108 kB (108,254 bytes)

- 2018-12-17-malspam-0334-UTC.eml (32,517 bytes)
- 2018-12-17-malspam-2019-UTC.eml (30,838 bytes)
- 2018-12-18-malspam-1922-UTC.eml (31,456 bytes)
- 2018-12-19-malspam-1454-UTC.eml (31,030 bytes)
- 2018-12-20-malspam-0405-UTC.eml (31,444 bytes)

Pcap of the infection traffic: [2018-12-19-MyDoom-infection-traffic.pcap.zip](#) 205 kB (204,725 bytes)

[2018-12-19-MyDoom-infection-traffic.pcap](#) (362,046 bytes)

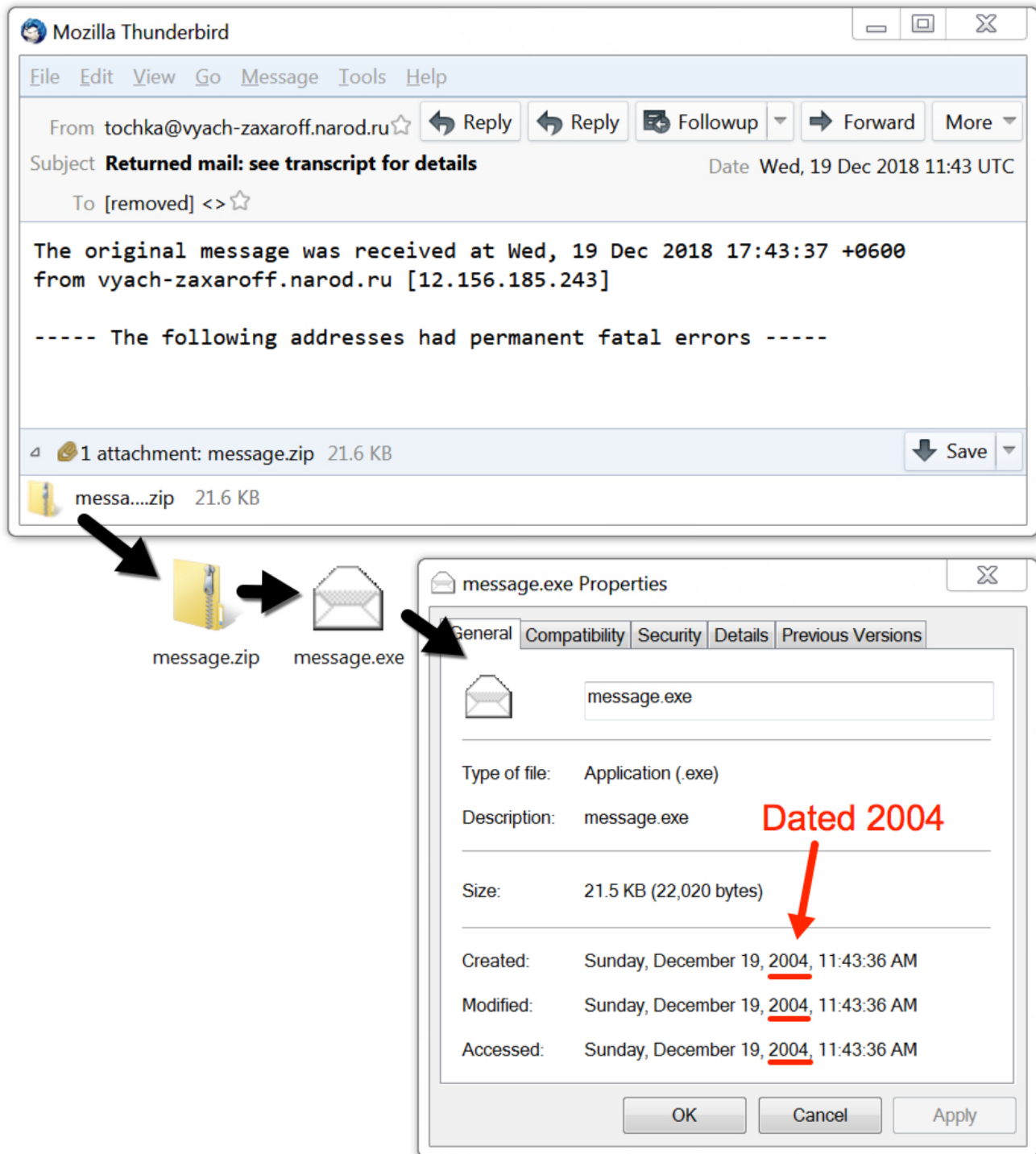
Associated malware: [2018-12-17-thru-2018-12-19-MyDoom-zip-attachments-and-extracted-EXE-files.zip](#) 213 kB (212,812 bytes)

- 17c7b0ccdf73b05a070443659715c9ae136aeda89f931e05cc80a8a05fbfea85.exe (22,020 bytes)
- 2ccf2b595b2c85fc17dafdf7ec3e0133b897ca2eb84da62189af023c2dc8a430.exe (22,020 bytes)
- 3335c2a089421bd1c19cff225d04f0c3d1f9192a41cd257ad93e608199b4d849.zip (22,140 bytes)
- 442c89956a623c10ea5e525dc85d8f8827c973569640ca266cab0a0f6aba0070.zip (23,060 bytes)
- 57b58feb49bd6de828371fc52c0e300a37cc7365720e1f961265f47fa5abeea8.zip (22,376 bytes)
- 78acb6f8d713e20f17f4bf6ca20e919845dfa1d8252487aa37958062b4fd146e.zip (21,966 bytes)
- 868289da1cf8aba7c2e9c38028accdfd989ef59cde9fc733543dff9fc4ce5826.exe (22,752 bytes)
- ab870f7f11ab105d92f2a29e8581992ae506bbc9e19e9c71e873b0c54639d8ad.exe (22,020 bytes)
- e3e809cd45c807ac832535a338003248739fa09ff9bcfa12a0acb7b1217e80f6.zip (22,140 bytes)
- ee004696baa06ae797449ac5dff683ddd3373d9fe38a2cf69c174fbd873673e8.exe (21,508 bytes)

NOTES:

- MyDoom worm was big in 2004, and it's been propagating around ever since. Some details can be found [here](#).
- I still occasionally see these, and other people like [@dvk01uk](#) have also [reported it's still active](#) over that past year or two.

EMAILS



Shown above: Screenshot from one of the MyDoom emails.

EMAILS:

Date range: 2018-12-17 03:34 UTC through 2018-12-20 04:05 UTC

- Received: from browsefox.com ([218.16.100.42])
- Received: from yhglobal.com ([113.91.55.46])
- Received: from adobee.com ([113.91.55.72])
- Received: from mozilla.org ([95.56.208.123])

- Received: from vanguardlogistics.com ([14.154.204.205])
- Subject: Returned mail: Data format error
- Subject: File Delivery failed
- Subject: File Returned mail: see transcript for details
- Subject: File RETURNED MAIL: SEE TRANSCRIPT FOR DETAILS

- From: File james@browsefox.com
- From: File john@yhglobal.com
- From: File flash@adobee.com
- From: tochka@vyach-zaxaroff.narod.ru
- From: dong.xiao@vanguardlogistics.com

- Attachment name: .zip
- Attachment name: message.zip
- Attachment name: document.zip

TRAFFIC

TRAFFIC FROM AN INFECTED WINDOWS HOST:

- Various IP addresses over TCP port 1042 - attempted connections (SYN packets only)
- Various mail servers over TCP port 25 - SMTP and attempted SMTP traffic

MALWARE

FROM 2017-12-17 03:34 EMAIL:

SHA256 hash:

442c89956a623c10ea5e525dc85d8f8827c973569640ca266cab0a0f6aba0070

File size: 23,060 bytes

File name: .zip

File description: File attachment (zip archive) from malspam on 2018-12-17 03:34 UTC

SHA256 hash:

868289da1cf8aba7c2e9c38028accd989ef59cde9fc733543dff9fc4ce5826

File size: 22,752 bytes

File name: .txt [97 spaces in middle of file name] .pif

File description: Windows executable file - MyDoom worm (Modified date: Dec 2004)

FROM 2017-12-17 20:19 EMAIL:

SHA256 hash:

3335c2a089421bd1c19cff225d04f0c3d1f9192a41cd257ad93e608199b4d849

File size: 22,140 bytes

File name: message.zip

File description: File attachment (zip archive) from malspam on 2018-12-17 20:19 UTC

SHA256 hash:

ab870f7f11ab105d92f2a29e8581992ae506bbc9e19e9c71e873b0c54639d8ad

File size: 22,020 bytes

File name: message.bat

File description: Windows executable file - MyDoom worm (Modified date: Dec 2004)

FROM 2017-12-18 19:22 EMAIL:

SHA256 hash:

57b58feb49bd6de828371fc52c0e300a37cc7365720e1f961265f47fa5abeea8

File size: 22,376 bytes

File name: .zip

File description: File attachment (zip archive) from malspam on 2018-12-18 19:22 UTC

SHA256 hash:

2ccf2b595b2c85fc17dafdf7ec3e0133b897ca2eb84da62189af023c2dc8a430

File size: 22,020 bytes

File name: .htm [*121 spaces in middle of file name*] .scr

File description: Windows executable file - MyDoom worm (Modified date: Dec 2004)

FROM 2017-12-19 14:54 EMAIL:

SHA256 hash:

e3e809cd45c807ac832535a338003248739fa09ff9bcfa12a0acb7b1217e80f6

File size: 22140 bytes

File name: message.zip

File description: File attachment (zip archive) from malspam on 2018-12-19 14:54 UTC

SHA256 hash:

17c7b0ccdf73b05a070443659715c9ae136aeda89f931e05cc80a8a05fbfea85

File size: 22,020 bytes

File name: message.exe

File description: Windows executable file - MyDoom worm (Modified date: Dec 2004)

FROM 2017-12-20 04:05 EMAIL:

SHA256 hash:

78acb6f8d713e20f17f4bf6ca20e919845dfa1d8252487aa37958062b4fd146e

File size: 21,966 bytes

File name: document.zip

File description: File attachment (zip archive) from malspam on 2018-12-20 04:05 UTC

SHA256 hash:

ee004696baa06ae797449ac5dff683ddd3373d9fe38a2cf69c174fbd873673e8

File size: 21,508 bytes

File name: document.htm [164 spaces in middle of file name] .exe

File description: Windows executable file - MyDoom worm (Modified date: Dec 2004)

IMAGES

The screenshot shows a Wireshark packet capture with a filter 'tcp.flags eq 0x0002 or dns'. The packet list pane displays the following data:

Time	Dst	port	Info
2018-12-19 16:15...	67.97.216.244	1042	49158 → 1042 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
2018-12-19 16:15...	67.97.216.244	1042	[TCP Spurious Retransmission] 49158 → 1042 [SYN] Seq=
2018-12-19 16:15...	67.97.216.244	1042	[TCP Spurious Retransmission] 49158 → 1042 [SYN] Seq=
2018-12-19 16:15...	16.101.73.169	1042	49159 → 1042 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
2018-12-19 16:15...	16.101.73.169	1042	[TCP Retransmission] 49159 → 1042 [SYN] Seq=0 Win=819
2018-12-19 16:15...	16.101.73.169	1042	[TCP Retransmission] 49159 → 1042 [SYN] Seq=0 Win=819
2018-12-19 16:15...	167.194.220.115	1042	49160 → 1042 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
2018-12-19 16:15...	167.194.220.115	1042	[TCP Retransmission] 49160 → 1042 [SYN] Seq=0 Win=819
2018-12-19 16:15...	167.194.220.115	1042	[TCP Retransmission] 49160 → 1042 [SYN] Seq=0 Win=819
2018-12-19 16:16...	68.7.245.229	1042	49161 → 1042 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
2018-12-19 16:16...	68.7.245.229	1042	[TCP Retransmission] 49161 → 1042 [SYN] Seq=0 Win=819
2018-12-19 16:16...	68.7.245.229	1042	[TCP Retransmission] 49161 → 1042 [SYN] Seq=0 Win=819
2018-12-19 16:16...	216.251.108.178	1042	49162 → 1042 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
2018-12-19 16:16...	216.251.108.178	1042	[TCP Retransmission] 49162 → 1042 [SYN] Seq=0 Win=819
2018-12-19 16:16...	216.251.108.178	1042	[TCP Retransmission] 49162 → 1042 [SYN] Seq=0 Win=819
2018-12-19 16:16...	16.102.140.125	1042	49163 → 1042 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
2018-12-19 16:16...	16.102.140.125	1042	[TCP Retransmission] 49163 → 1042 [SYN] Seq=0 Win=819
2018-12-19 16:16...	16.102.140.125	1042	[TCP Retransmission] 49163 → 1042 [SYN] Seq=0 Win=819
2018-12-19 16:17...	10.12.19.1	53	Standard query 0xd927 MX mozilla.org.xpi
2018-12-19 16:17...	10.12.19.101	65203	Standard query response 0xd927 No such name MX mozill
2018-12-19 16:17...	10.12.19.1	53	Standard query 0xb3a7 MX mozilla.org.xpi
2018-12-19 16:17...	10.12.19.1	53	Standard query 0xd2a7 MX mozilla.org.xpi
2018-12-19 16:17...	10.12.19.101	65204	Standard query response 0xb3a7 No such name MX mozill
2018-12-19 16:17...	10.12.19.101	65205	Standard query response 0xd2a7 No such name MX mozill
2018-12-19 16:17...	10.12.19.1	53	Standard query 0x6704 MX getpocket.com.xpi
2018-12-19 16:17...	10.12.19.101	62968	Standard query response 0x6704 No such name MX getpoc
2018-12-19 16:17...	10.12.19.1	53	Standard query 0x30a8 MX getpocket.com.xpi
2018-12-19 16:17...	10.12.19.1	53	Standard query 0x24a6 MX mozilla.com.xpi

Shown above: Traffic from an infection filtered in Wireshark first show attempted TCP connections to various IP addresses over port 1042.

Time	Dst	port	Info
2018-12-19 16:17...	216.97.88.9	25	C: MAIL FROM:<MAILER-DAEMON@unicode.org>
2018-12-19 16:19...	173.194.66.27	25	C: MAIL FROM:<postmaster@mozilla.org>
2018-12-19 16:19...	173.194.66.27	25	C: MAIL FROM:<noreply@mozilla.org>
2018-12-19 16:19...	173.194.66.27	25	C: MAIL FROM:<unicode-inc@unicode.org>
2018-12-19 16:19...	31.7.4.183	25	C: MAIL FROM:<todd.miller@courtesan.com>
2018-12-19 16:19...	74.125.138.27	25	C: MAIL FROM:<postmaster@mozilla.org>
2018-12-19 16:19...	65.102.237.118	25	C: MAIL FROM:<postmaster@courtesan.com>
2018-12-19 16:20...	173.194.66.27	25	C: MAIL FROM:<noreply@mozilla.org>
2018-12-19 16:20...	64.233.180.27	25	C: MAIL FROM:<noreply@mozilla.org>
2018-12-19 16:20...	82.103.137.214	25	C: MAIL FROM:<MAILER-DAEMON@information.com>
2018-12-19 16:21...	63.245.210.103	25	C: MAIL FROM:<noreply@mozilla.org>
2018-12-19 16:21...	65.102.237.118	25	C: MAIL FROM:<postmaster@courtesan.com>
2018-12-19 16:21...	65.102.237.118	25	C: MAIL FROM:<postmaster@courtesan.com>
2018-12-19 16:21...	65.102.237.118	25	C: MAIL FROM:<postmaster@courtesan.com>
2018-12-19 16:22...	149.56.25.211	25	C: MAIL FROM:<MAILER-DAEMON@fscked.org>

Shown above: Filtering on **smtp and ip contains "MAIL FROM:"** shows some of the spoofed sending addresses sent from my infected Windows host.

Time	Dst	port	Info
2018-12-19 16:19...	173.194.66.27	25	C: DATA fragment, 1460 bytes
2018-12-19 16:19...	173.194.66.27	25	C: DATA fragment, 1460 bytes
2018-12-19 16:19...	173.194.66.27	25	C: DATA fragment, 1460 bytes
2018-12-19 16:19...	74.125.138.27	25	C: DATA fragment, 1460 bytes
2018-12-19 16:20...	173.194.66.27	25	C: DATA fragment, 1460 bytes
2018-12-19 16:20...	64.233.180.27	25	C: DATA fragment, 1460 bytes
2018-12-19 16:20...	82.103.137.214	25	C: DATA fragment, 1460 bytes

Shown above: Filtering on **smtp and ip contains "Subject:"** will results that you can follow a TCP stream and see a full malspam message sent from my infected Windows host.

```

Wireshark · Follow TCP Stream (tcp.stream eq 61) · 2018-12-19-MyDoom-infection-traffic
220 mail2.information.com - Welcome to the InformAction SMTP Server ESMTP
EHLO information.com
250-mail2.information.com - Welcome to the InformAction SMTP Server
250-STARTTLS
250-PIPELINING
250-8BITMIME
250-SIZE 200200200
250 AUTH LOGIN PLAIN CRAM-MD5
MAIL FROM:<MAILER-DAEMON@information.com>
250 ok
RCPT TO:<g.maone@information.com>
250 ok
DATA
354 go ahead
From: "Mail Delivery Subsystem" <MAILER-DAEMON@information.com>
To: g.maone@information.com
Subject: Message could not be delivered
Date: Wed, 19 Dec 2018 16:19:41 +0000
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="-----_NextPart_000_0014_8ECE14CB.ACAD80D1"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MIMEOLE: Produced By Microsoft MimeOLE V6.00.2600.0000

This is a multi-part message in MIME format.

-----_NextPart_000_0014_8ECE14CB.ACAD80D1
Content-Type: text/plain;
        charset=us-ascii
Content-Transfer-Encoding: 7bit

The original message was received at Wed, 19 Dec 2018 16:19:41 +0000
from information.com [49.3.61.188]

----- The following addresses had permanent fatal errors -----
<g.maone@information.com>

----- Transcript of session follows -----
        while talking to information.com.:
>>> MAIL From:"Mail Delivery Subsystem" <MAILER-DAEMON@information.com>
<<< 501 "Mail Delivery Subsystem" <MAILER-DAEMON@information.com>... Refused

-----_NextPart_000_0014_8ECE14CB.ACAD80D1
Content-Type: application/octet-stream;
        name=".zip"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
        filename=".zip"

UESDBAoAAAAAHSCkzELpEc3BFYAAARWAAAYAAAAZy5tYW9uZUBpbmZvcmlhY3Rpb24uY29tTVqQ
AAMAAAAEAAAA/8AALgAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
6AAAAA4fug4AtAnNIbgBTM0hVghpcyBwcm9ncmFtI
52 client nbs, 8 server nbs, 15 bytes

```

Shown above: Following one of the TCP streams to view malspam sent from the infected Windows host.

FINAL NOTES

Once again, here are the associated files:

- Malspam examples: [2018-12-17-thru-2018-12-20-MyDoom-malspam-5-email-examples.zip](#) 108 kB (108,254 bytes)
- Pcap of the infection traffic: [2018-12-19-MyDoom-infection-traffic.pcap.zip](#) 205 kB (204,725 bytes)
- Associated malware: [2018-12-17-thru-2018-12-19-MyDoom-zip-attachments-and-extracted-EXE-files.zip](#) 213 kB (212,812 bytes)

Zip archives are password-protected with the standard password. If you don't know it, look at the "about" page of this website.

[Click here](#) to return to the main page.