



# Malware Reverse Engineering

Report Issued: 07.30.2022 Prepared by: Jeff Malavasi Rochester Institute of Technology, Computing Security

# **TABLE OF CONTENTS**

OVERVIEW	3
ANALYSIS	4
Static Analysis	4
General	4
Basic	4
Strings	4
Findings	4
Floss	6
Findinas	6
UPX	7
Findings	8
PE View	8
Findings	8
PEiD	9
Findings	9
Resource Hacker	9
Findings	9
Virus Total	10
Findings	10
Advanced	13
Ida Pro	13
Finding 1: DNS Query Algorithm	13
Finding 2: Mass Mailer Algorithm	15
Dynamic Analysis	16
Basic	16
RegShot	16
Findings	16
Process Monitor	17
Findings	17
ApateDNS	20
Findings	20
netstat	22
Findings	22
Advanced	23
x32Debug	23
Finding 1: DNS Query Algorithm	23
Finding 2: Mass Mailer Algorithm	24
CONCLUSION	25
Potential Danger	25
Malware Removal	25
APPENDIX A - TOOLS	26
APPENDIX B – REFERENCES	27

# **OVERVIEW**

The MyDoom worm was first detected in January 2004. Although its origins are still unknown, artifacts within the binary most likely link it's development back to Russia. The virus was spread through a self-replicating email campaign that tricked users into opening a malicious attachment. The attachment, which appeared benign, was actually the malicious payload. Upon opening the file, it would silently scan the computer and the internet for any email addresses it could find to continue replicating. Additionally, the virus creates a backdoor on the machine which was used for multiple botnet attacks against large organizations such as Google and Microsoft. In fact, the virus successfully took down Google for nearly a day through a distributed denial of service attack.

When MyDoom was originally released, analysts reported that the virus accounted for one in ten emails sent worldwide. MyDoom crippled internet page load times by 50% globally and caused an estimated of \$65 billion dollars. Although today it only accounts for about 1% of all email and is detected by most antivirus software, successful campaigns have been reported as recently as a few years ago.

# ANALYSIS

# Static Analysis

# General

File Information				
Operating System	Windows 10 1709			
Description	A Windows Worm that was first sighted in 2004. It is infamously known as the fastest spreading email worm to date and is still heavily used today.			
Size (bytes)	26050			
Hash (SHA256)	6F064D4987B4202EBE2FAAAB28F3582DD784F24FA1A13F305051A6D7E85A78ED			
Source	https://samples.vx-underground.org/samples/Families/MyDoom/			

# **Basic**

# Strings

Strings is a static command line utility that is used to quickly pull readable text snippets out of a binary. This can be used to get a cursory idea of the function of the binary.

# Findings

In this binary, there are a small number of strings (548). This indicates that the file may be obfuscated through packing. Further analysis shows the strings "UPX0" and "UPX1" (Figure 1), which is a specific type of packing technology. Finally, we see the presence of the LoadLibraryA and GetProcAddress API calls (Figure 2), but not many others. This is another strong indicator of packing.

# Analysis

MyDoc	m > Analysis >		
1			
.2	Strings v2.51		C
3	Copyright (C) 1999-2013 Mark Russinovich		
- 4	Sysinternals - www.sysinternals.com		
5			
6	This program cannot be run in DOS mode.		
7	UPX8		
В	UPX1		
9	.rsrc		
10	1.24		
11	UPX!		
12	kernel32.d		
13	115root\IEFrame		
14	H_Noterctrl_renwnd		
25	ep^ug		
16	aSa'		
17	%s, %u		
18			
19	=Into		
20	zHSta		
21	(dnsapiUiphlp		
22	DQnr9A5		
23	workPals		
24	mail		
25	buse		
26	vl+ tifi		
27	.gKli/		
PROBLI	MS OUTPUT DEBUG CONSOLE TERMINAL	•	⊾ powershell + ~ 🗓 🔒 ^ ×
PS C: PS C: 548 PS C: PS C: PS C:	\Users\Calli\PMalTools> fstrings = .\Strings\strings.exe -n 4 \$%\users\Calli\PMalTools> fstrings.count Users\Calli\PMalTools> fstrings.count Users\Calli\PMalTools> fstrings   out-file \$%\users\Calli\PMalTools> []		

Figure 1 Strings UPX

MyDoom		
1	Strings v2.51	
a.	Copyright (C) 1999-2013 Mark Russinovich	
4	Sysinternals - www.sysinternals.com	
	This program cannot be run in DOS mode	
7	UPX0	
3.63	UPX1	
- 9	.rsrc	
10	1,24 1921	
12	kernel32.d	
- 13	115root\IEFrame	
14	H_Noterctri_remand	
10	asa'	
17		
18	.201 Juda	
20	zista	
21	(dnsapiUiphlp	
22	DQnr9A5	
2.5	workpals mail	
25	buse	
26	vl+[tifi	
27	.gxl1/ markited	
PROBLEM	S OUTPUT DEBUGICONSOLE TERMINAL	🗈 provershell + ~ 🖽 💼 ^ ×
Commission and		
PS C:\l	Jsers\Calli\JMalTools> \$strings = .\Strings\strings.exe -n 4 \$MyDoon/Binaries/MyDoon Jsers\Calli\JMalTools> \$strings.count	
548		
PS C:\U PS C:\U	sers\Calli\JMalTools> <u>sstrings   out-file</u> \$MyDoom/Analysis/strings.tzt Isers\Calli\JMalTools> []	
	){4'@	
	www.www	
	KERNEL32.DLL	
	ADVAPI32.dll	
	MSVCRT.dll	
	USER32.dll	
	WS2_32.dl1	
	LoadLibraryA	
	GetProcAddress	
	EXITPROCESS	
	RegCloseKey	
	memset	
	el tag	
	-ykaurg	
	14  cki Ni%	
	NK67E	
	Aiv)	
	ejt) Na//P	
	ng/(0	
	b)+B	
	7wGI	
	011/	
	a~75>	
	65ul,	
	MS OUTPUT DEBUG CONSOLE TERMINAL	
PS C:	\Users\Calli\JMalTools> \$strings = .\Strings\strings.exe -n 4 \$MyDoom/Binaries/MyDoom	
PS C:	\Users\Calli\JMalTools> \$strings.count	
548	Automatically autolication of the file of the and file for the state of the state o	
PS C:	\Users\call\\MalTools> \$strings   out-tile \$MyUoom/Analysis/strings.tzt	

Figure 2 API Calls

## Floss

Floss is another CLI tool that was created by the FireEye FLARE team. It builds upon the capabilities of strings by being able to decrypt encoded strings automatically.

## **Findings**

In this binary, FLOSS was able to decode a few different interesting strings. The first appears to be some sort of email template used to help replicate the virus across other hosts (Figure 3). The template appears to be able to send a few different message bodies to make it more difficult to detect. Since there are many variants of MyDoom, the email template can be used to help hone in on the specific version of the malware. This template is a strong indicator of MyDoom.m, which aimed to get people to open an email that mimicked an NDR from their system administrator.

The second string of interest appears to be used to help send the message (Figure 4). It is a series of message headers that will likely be passed to the built in SMTP server.

Finally, we see a series of strings that helps to understand how the worm gathers email recipients (Figure 5). On top of searching the local host for temporary internet files and contacts, the malware also queries search engines for publicly available addresses. This is likely how it became the fastest spreading email virus of all time.

# Analysis measure for the first of the first

Apericant 2 version of the second sec
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
Content-Type: multipart/mixed;
boundary="%s"
MIME-Version: 1.0
Date:
Subject: %s
To: %s
From: %s
=_%s_%.3u_%.4u_%.8X.%.8X
NextPart
-%s
%s
Content-Type: application/octet-stream;
name="%s"
Content-Transfer-Encoding: base64
Content-Disposition: %s;
filename="%s"
inline
%s
Content-Type: text/plain;
charset=us-ascii
Content-Transfer-Encoding: 7bit
This is a multi-part message in MIME format.
Figure 4 Freedulte days

urlmon.dll URLDownloadToCacheFileA http://search.lycos.com/default.asp?lpv=1&loc=searchhp&tab=web&query=%s &nbq=%d http://www.altavista.com/web/results?q=%s&kgs=0&kls=0 &n=%d http://search.yahoo.com/search?p=%s&ei=UTF-8&fr=fp-tab-web-t&cop=mss&tab= &num=%d http://www.google.com/search?hl=en&ie=UTF-8&oe=UTF-8&q=%s %c+%c

Figure 5 Email Recipient Worming

UPX

UPX is a command line utility that can be used to pack and unpack files. Malware developers often pack files to obfuscate the contents from a malware reverse engineer.

# Findings

In both the strings and PEiD analysis, we see that this file is packed with UPX. I was successfully able to unpack the file, which appeared to be compressed by about 70% (Figure 6).

Analysis

PS C:\Users\cal	li\JMalTo U	ols> .\up> ltimate Pa Copyrigh	-3.95-win64\u icker for eXec it (C) 1996 - 3	p <mark>x.exe</mark> -d \$MyDo utables 2018	oom/Binaries/MyDoo	om -o \$MyDoom,	/Binaries/MyDo	om.exe
UPX 3.95w Markus Oberhumer, Laszlo Molnar & John Reiser Aug 26th 2018								
File si	ze	Ratio	Format	Name				
41664 <-	28864	69.28%	win32/pe	MyDoom.exe				
Unpacked 1 file	÷	_						
Figure 6 Unpacked Binary								

# PE View

PE View is a graphical tool that can be used to quickly find embedded files, learn about when the binary was created, as well as quickly see the imported and exported API calls.

Findings

In this binary we can see references to a packed UPX file (Figure 7).

Analysis



# PEiD

PEiD is another graphical tool that can be used to detect which packing technology was used to obfuscate a particular binary.

# Findings

PEiD was able to detect that the binary was packed with UPX v0.89.6 (Figure 8).

Analysis

🌃 PEiD v0.	95		_		×	
File: C:\Users\calli\Samples\MyDoom\Binaries\MyDoom						
Entrypoint:	0000ED00	EP Section:	UPX1	L	>	
File Offset:	00006100	First Bytes:	60,B	E,00,90	>	
Linker Info:	7.0	Subsystem	: Win3	2 GUI	>	
UPX 0.89.6 - 1.02 / 1.05 - 2.90 -> Markus & Laszlo [Overlay]         Multi Scan       Task Viewer       Options       About       Exit         ✓       Stay on top       >>>						
Figure 8 Evidence of Packing						

# Resource Hacker

Resource Hacker is used to find hidden embedded binaries and other file artifacts. It can also be used to export different subfiles for isolated analysis.

# Findings

Although there weren't any hidden files in this binary, the embedded icon changed with each variant of MyDoom. This icon further validates our prediction that this sample is variant M (Figure 9).

# Analysis

RH Resource Hacker - MyDoom -		×
File Edit View Action Help	lcon : 1 :	1033
Dialog <pdialog< p=""> <pdialog< p=""> <pdialog< p=""> <pdialog< p=""> <pdialog< p=""> <pdial< td=""><td></td><td></td></pdial<></pdialog<></pdialog<></pdialog<></pdialog<></pdialog<>		
<ul> <li>✓ - ↓ Icon</li> <li>→ ☆ 1 : 1033</li> <li>→ ☆ 2 : 1033</li> <li>✓ - ↓ Icon Group</li> <li>→ ☆ 0 : 1033</li> </ul>	2	
Editor View Binary View		
2E8 / 64D8 32 × 32		
Figure 9 MyDoom.m Icon		

# Virus Total

Virus Total is an online tool that maintains a database of malicious files. It can be used to determine if a binary has already been deemed malicious as well as provide a basic report on what it may do.

# Findings

From the Virus Total report, we can see that this binary has been deemed malicious by 66 different anti-virus vendors. Additionally, Virus total can detect when the file was first seen in the wild (6/4/2022) as well as the packing technology (Figure 10). From the behaviors tab, we can see what the file is expected to do once run. From our analysis, we can see that the file makes many DNS requests, as well as creates a startup task that automatically starts the binary on boot (Figure 11). Finally, we get a better look at the various search queries the binary makes to find more victims.

# Analysis

66	66 security vendors and 1 sandbox flagged this file as malicious		C <sup>B</sup>
771 ? X Community V	CI064d4987b4202ebe2faaab28f3582dd784f24fa1a13305051a6d7e85a78ed MyDoom Checks-network-adapters direct-cpu-clock-access long-sleeps nxdomain overlay peex	28.19 KB Size persistence runtime-modules susp	2022-07-25 02-16-57 UTC a moment ago coust-ons up:
DETECTION DE	ETAILS RELATIONS BEHAVIOR COMMUNITY		
Security Vendors' Analy	ysis 🕕		
Ad-Aware	() Worm Generic 24461	AhnLab-V3	() Win32/Mydoom.worm.49344.B
Alibaba	Malware:Win32/Dorpal.ali1000029	ALYac	() Worm.Mydoom
Antiy-AVL	() Trojan/Generic ASMalwS.118	Arcabit	() Worm.Generic.D5F8D
Avast	() Win32:Banker-FNW [Trj]	AVG	() Win32:Banker-FNW [Tr]
Avira (no cloud)	() WORM/Mydoom.O.1	Baidu	Win32.Worm-Email.Mydoom.a
BitDefender	() Worm.Generic.24461	BitDefenderTheta	Al:Packer.6236D6581F
Bkav Pro	() W32.MyDoom.M.Worm	ClamAV	Win.Worm.Mydoom-90
Comodo	() Worm.Win32.Mydoom.R@348I	CrowdStrike Falcon	() Win/malicious_confidence_100% (W)
Cybereason	① Malicious 28f59b	Cylance	() Unsafe

#### Basic Properties ①

MD5	13c05f728f59b645759ccff2469dd2b2
SHA-1	a2879876885d68be54bc0d9307a8ea0b4182560b
SHA-256	6f064d4987b4202ebe2faaab28f3582dd784f24fa1a13f305051a6d7e85a78ed
Vhash	02403e0f7d1019z301lz15z17z
Authentihash	8275243725139b9e8403115b265b8c532e6590f2c5a37f272350c7b64de96452
Imphash	98cd465c2ab2841f9fd90d5e847563f4
SSDEEP	384:1vxBbK26lj5ld8SpHx9jLhsznnVxA1WmP5w7GGCJlqqwMyNTbs4:Dv8lRRdsxq1DjJcqfo7
TLSH	T150D2C085B050FAA2C01682331D86C471FD119C611AAAD2CBBA24BF7FFDB17850B0CD2B
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	UPX compressed Win32 Executable (34.7%)
TrID	Win32 EXE Yoda's Crypter (34.1%)
TrID	Win32 Dynamic Link Library (generic) (8.4%)
TrID	Win16 NE executable (generic) (6.4%)
TrID	Win32 Executable (generic) (5.7%)
File size	28.19 KB (28864 bytes)
PEiD packer	UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser
Cyren packer	UPX

### History ()

First Seen In The Wild	2022-06-04 15:39:32 UTC	
First Submission	2021-07-26 10:48:24 UTC	
Last Submission	2022-07-25 02:20:07 UTC	
Last Analysis	2022-07-25 02:16:57 UTC	

#### Names 🕕

MyDoom

mydoom.exe

instruction.html .com

Figure 10 VT Basic

#### HTTP Requests

- + http://search.yahoo.com/search?p=mail+shazow.net&ei=UTF-8&fr=fp-tab-web-t&cop=mss&tab
- + http://search.yahoo.com/search?p=acm.org+mailto&ei=UTF-8&fr=fp-tab-web-t&cop=mss&tab=
- + http://search.yahoo.com/search?p=mailto+cynosure.com.au&ei=UTF-8&fr=fp-tab-web-t&cop=n
- + http://search.lycos.com/default.asp?lpv=1&loc=searchhp&tab=web&query=contact+mail+shaze
- + http://search.lycos.com/default.asp?lpv=1&loc=searchhp&tab=web&query=mailto+acm.org
- + http://search.yahoo.com/search?p=email+cynosure.com.au&ei=UTF-8&fr=fp-tab-web-t&cop=m
- + http://search.yahoo.com/search?p=python.org+mail&ei=UTF-8&fr=fp-tab-web-t&cop=mss&tab=
- + http://www.altavista.com/web/results?q=mailto+shazow.net&kgs=0&kls=0&nbq=50
- + http://search.yahoo.com/search?p=jaraco.com+mailto&ei=UTF-8&fr=fp-tab-web-t&cop=mss&tz
- + http://www.altavista.com/web/results?q=mailto+skippinet.com.au&kgs=0&kls=0&nbq=20
- ~

#### SMTP Communications

- + iquest.net
- + opentaal.org
- + openoffice.org
- + python.org
- + openoffice.org
- + openoffice.org
- + web.de
- + cryptsoft.com
- + pobox.com
- + nibsoft.com

#### **DNS Resolutions**

- + zko.dec.com
- + yassou.net
- + hpl.hp.com
- + openoffice.org
- + burtleburtle.net
- + aladdin.com
- + opentaal.org
- + mail.ru
- + qnx.com
- + gzip.org

#### File System Actions

#### Files Dropped

+ %TEMP%\services.exe

#### Registry Actions

#### Registry Keys Set

- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\drivers\ndis.sys[MofResourceName]
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\System32\Drivers\portcls.SYS[PortclsMof]
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\drivers\en-US\ACPI.sys.mui[ACPIMOFResource]
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\DRIVERS\HDAudBus.sys[HDAudioMofName]
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\System32\Drivers\en-US\portcls.SYS.mui[PortclsMof]
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\advapi32.dll[MofResourceName]
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\en-US\advapi32.dll.mui[MofResourceName]
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\drivers\en-US\mssmbios.sys.mui[MofResource]
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\DRIVERS\en-US\HDAudBus.sys.mui(HDAudioMofName
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\drivers\en-US\ndis.sys.mui[MofResourceName]

#### Registry Keys Deleted

HKLM/SYSTEM/ControlSet001/Services/WmiApRpI/Performance/First Counter HKLM/SYSTEM/ControlSet001/Services/WmiApRpI/Performance/Last Counter HKLM/SYSTEM/ControlSet001/Services/WmiApRpI/Performance/First Help HKLM/SYSTEM/ControlSet001/Services/WmiApRpI/Performance/Last Help HKLM/SYSTEM/ControlSet001/Services/WmiApRpI/Performance/Object List

Process And Service Actions 0

#### **Processes Terminated**

wmiadap.exe /F /T /R

#### Processes Tree

- → 7840 wmiadap.exe /F /T /R
- 8012 %windir%\system32\wbem\wmiprvse.exe
- $\mapsto$  2816 %windir%\services.exe
- 2988 %windir%\system32\DIIHost.exe /Processid:{3EB3C877-1F16-487C-9050-104
- $\rightarrow$  2832 %windir%\java.exe
- → 2844 "%TEMP%\services.exe"
- $\mapsto$  2596 %SAMPLEPATH%
- $\mapsto$  2664 "%windir%\services.exe"

Figure 11 VT Behaviors

# Advanced

# Ida Pro

Ida Pro is a commonly used disassembler, that can be used get a detailed picture of all the functions within a binary.

# Finding 1: DNS Query Algorithm

The first algorithm that was investigated was the DNS query algorithm. This function is used to find potential victims on the internet to aid in replication of the worm. I first started by looking at any imports related to networking (Figure 12). Next, I examined any cross reference to GetHostByName until I found the function of interest (Figure 13). The address of this function was later used for dynamic analysis.

## Analysis

			-
Address	Ordinal	Name	Library
00000000.		SetThreadPriority	KERNEL32
00000000.		Sleep	KERNEL32
00000000.		UnmapViewOfFile	KERNEL32
00000000.	115	WSAStartup	WS2_32
00000000.		WideCharToMultiByte	KERNEL32
00000000.		WriteFile	KERNEL32
00000000.	3	closesocket	WS2_32
1 00000000.	4	connect	WS2_32
00000000.	52	gethostbyname	WS2_32
00000000.	57	gethostname	WS2_32
00000000.	9	htons	WS2_32
00000000.	11	inet_addr	WS2_32
00000000.		isalnum	MSVCRT
00000000.		isdigit	MSVCRT
00000000.		isspace	MSVCRT
00000000.		IstrcatA	KERNEL32
00000000.		IstrcmpA	KERNEL32
00000000.		IstrcmpiA	KERNEL32
00000000.		IstrcpyA	KERNEL32
00000000.		IstrcpynA	KERNEL32
00000000.		IstrienA	KERNEL32
00000000.		malloc	MSVCRT
00000000.	••	memcpy	MSVCRT
00000000.		memset	MSVCRT
00000000.	15	ntohs	WS2_32
00000000.	16	recv	WS2_32
00000000.	18	select	WS2_32
00000000.	19	send	WS2_32
00000000.	20	sendto	WS2_32
00000000.	23	socket	WS2_32
00000000.		strchr	MSVCRT
00000000.		strstr	MSVCRT
00000000.		tolower	MSVCRT
00000000.		wsprintfA	USER32
00000000.		wvsprintfA	USER32
Line 62 of 89		wvsprinuA	USEK32

Figure 12 GetHostByName





Figure 13 DNS Algorithm

# Finding 2: Mass Mailer Algorithm

The second finding is the function that is used to construct the phony email message. To find this function, I looked for the cross references to PostMessageA, which is used to queue messages (Figure 13). Next, I looked for any calls to this function, which would be used to initiate the email phishing campaign (Figure 14).

Analysis

00000000000503110					
0000000000503110					
000000000050311C	; Attri	ibutes: no	preturn		
000000000050311C					
000000000050311C	; DWORD	)stdcal	ll StartA	dress(LPVOID 1	pThreadParameter)
000000000050311C	StartAd	idress pro	oc near		
00000000000503110	InThree	dDopomoto	- duand	ata 4	
000000000000000000000000000000000000000	ipinrea	aparamete	er= awora	ptr 4	
000000000000000000000000000000000000000	nush	esi			
00000000000000000000000000000000000000	mov	esi. ds:	FindWind	Awa	
0000000000503123	push	0		1pWindowName	
0000000000503125	push	offset C	lassName	; "rctrl_renwn	d32"
000000000050312A	call	esi ; Fi	indWindow	N	
000000000050312C	push	eax .		hlind	
000000000000000000000000000000000000000	call	mass_mai	ller		
000000000000000000000000000000000000000	pop	0		InkindowName	
00000000000503135	push	offset a	AthNote	"ATH Note"	
000000000050313A	call	esi ; Fi	indWindow		
000000000050313C	push	eax		hillind	
000000000050313D	call	mass_mai	iler		
0000000000503142	рор	ecx			
0000000000503143	push	0		1pWindowName	
000000000000503145	push	offset a	itetrame	IFFLawe.	
00000000000000000000000000000000000000	nush	esi; Fi eax	THOM THOOM	bWnd	
0000000000050314C	call	mass mai	iler		
0000000000503152	pop	ecx	-		
0000000000503153	push	0		dwExitCode	
0000000000503155	call	ds:ExitT	Thread		
0000000000503155	StartAd	idress end	ip		
000000000000003155					
	2.120				
00000000503	0F0				
00000000503	0F0				
00000000503	ØFØ				
000000000000000000000000000000000000000	AEA	int	edae1	mace mail	on/ULIND LU-
000000000000303	010;	THE -	_cuec1	mass_mal.	rei (HWND HW
00000000503	0F0 m	lass_ma	iler p	roc near	
00000000503	0F0				
00000000503	OFO h	Wnd= d	word n	tr 4	
	050				
00000000503	ини				
00000000503	010 -	uch	abu		
00000000503 00000000503	0F0 p	ush	ebx		
00000000503 00000000503 00000000503	0F0 p 0F1 p	ush ush	<mark>ebx</mark> edi		
00000000503 00000000503 00000000503 00000000	0F0 p 0F1 p 0F2 m	oush oush ov	<mark>ebx</mark> edi edi,	[esp+8+hWr	nd]
00000000503 00000000503 00000000503 00000000	0F0 p 0F1 p 0F2 m 0F6 x	oush oush ov cor	ebx edi edi, ebx.	[esp+8+hWr ebx	nd]
00000000503 00000000503 00000000503 00000000	0F0 p 0F1 p 0F2 m 0F6 x	oush ov or	ebx edi edi, ebx,	[esp+8+hWr ebx	nd]
00000000503 00000000503 00000000503 00000000	0F0 p 0F1 p 0F2 m 0F6 x 0F8 c	oush ov or mp	edi edi, ebx, edi,	[esp+8+hWr ebx ebx	nd]
0000000503 00000000503 00000000503 00000000	0F0 p 0F1 p 0F2 m 0F6 x 0F8 c 0FA j	oush ov or mp z	edi edi, ebx, edi, short	[esp+8+hWr ebx loc_50311	nd]
00000000503 00000000503 00000000503 00000000	0F0 p 0F1 p 0F2 m 0F6 x 0F8 c 0FA j	oush ov cor mp z	edi edi, ebx, edi, short	[esp+8+hWr ebx loc_50311	nd] 19
	0F0 0F1 p 0F1 p 0F2 m 0F6 x 0F8 c 0F8 j	oush ov cor mp z	ebx edi edi, ebx, edi, short	[esp+8+hWr ebx ebx loc_50311	nd] 19
	0F0 p 0F1 p 0F2 m 0F6 x 0F8 c 0FA j	oush ov cor mp z	ebx edi edi, ebx, edi, short	[esp+8+hWr ebx ebx loc_50311	nd] 19
	0F0 p 0F1 p 0F2 m 0F6 x 0F8 c 0FA j 030FC	push pov cor mp z push	ebx edi edi, ebx, edi, short esi	[esp+8+hWr ebx loc_50311	nd] 19
	0F0 p 0F1 p 0F2 m 0F6 x 0F8 c 0FA j 0FA j 030FC 030FD	push pov cor mp z push mov	ebx edi edi, ebx, edi, short esi esi	[esp+8+hWr ebx ebx loc_50311	l9 essageA
0000000503 00000000503 00000000503 00000000	0F0 0F0 0F1 0F2 0F8 0F8 0F8 0FA j 030FC 030FD 03103	push nov cor mp z push mov push	ebx edi edi, ebx, edi, short esi esi esi	[esp+8+hWr ebx ebx loc_50311	l9 essageA ; 1Param
00000000503 00000000503 00000000503 00000000	0F0 0F0 0F1 0F2 0F6 0F8 0F8 0F8 0F8 0F8 00F8 00F8 00F8	push push push mov push push	ebx edi edi, ebx, edi, short edi, short	[esp+8+hWr ebx loc_50311 , ds:PostM	19 essageA ; 1Param ; wParam
00000000503 00000000503 00000000503 00000000	00F0 00F0 00F1 00F2 00F6 00F8 00F8 00F8 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA 00FA	push pov push mov push push push	ebx edi edi, ebx, edi, short esi esi ebx	[esp+8+hWr ebx ebx loc_50311	lg essageA ; 1Param ; WParam
0000000503 0000000503 0000000503 00000000	00F0 p 00F1 p 00F2 m 00F6 x 00F8 c 00FA j 00FA j 00	push mov push push push push	ebx edi edi, ebx, edi, short esi esi esi ebx ebx 12h	[esp+8+hWr ebx bx loc_5031: , ds:PostM	essageA ; 1Param ; WParam ; Msg
00000000503 00000000503 00000000503 00000000	0F0 0F0 0F1 0F2 0F2 0F6 0F8 0F8 0F8 0F8 0F8 0F8 0F8 0F8	push mov push push push push push	ebx edi edi, ebx, edi, short edi, esi esi esi ebx ebx 12h edi	[esp+8+hWr ebx ebx loc_50311	d] essageA ; lParam ; wParam ; MParam ; Myaram
0000000503 0000000503 0000000503 00000000	00F0 p 00F1 p 00F2 m 00F6 x 00F8 c 00FA j 00FA j 00FA j 000FA j 00FA j 000FA j	push pov z push push push push push call	ebx edi edi, ebx, edi, short edi, short esi esi ebx ebx 12h edi esi	[esp+8+hWr ebx : loc_50311 , ds:PostMes	19 essageA ; 1Param ; wParam ; Msg ; hWnd sageA
	00F0 p 00F1 p 00F2 m 00F6 x 00F8 c 00FA j 00FA j 00FA j 00FA j 00F0 2 00FA j 00F0 2 00FA j 00F0 2 00F0 2 00F0 2 00F0 2 00F1 p 00F1 p 00F1 p 00F2 m 00F2 m 00F6 x 00F6 x	push nov cor mp z push mov push push push call	ebx edi edi, ebx, edi, short esi esi esi ebx ebx 12h edi esi	[esp+8+hWr ebx ebx loc_5031: , ds:PostMes	essageA ; 1Param ; wParam ; Msg ; hWnd sageA
000000000503 00000000503 00000000503 00000000	00F0 p 00F1 p 00F1 p 00F2 m 00F6 x 00F8 c 00FA j 030FC 030FC 030FD 03103 03104 03105 03107 03108 0310A	push nov cor mp z push push push call push	ebx edi edi, ebx, edi, short edi, short edi esi ebx 12h edi esi ebx	[esp+8+hWr ebx loc_50311 , ds:PostM ; PostMes	nd] essageA ; 1Param ; wParam ; Msg ; hWnd sageA ; 1Param
00000000503 00000000503 00000000503 00000000	00F0 p 00F0 p 00F1 p 00F2 m 00F6 x 00F6 x 00F8 c 00FA j 00F8 c 00FA j 00F8 c 00FA j 00F0 p 00F0 p 00F0 p 00F0 p 00F0 p 00F0 p 00F0 p 00F0 p 00F0 p 00F1 p 00F0 p 00F1 p 00F0 p 00F0 p 00F1 p 00F0 p	push mov arp z push mov push push push push push push push	ebx edi edi, ebx, edi, short ebx esi ebx ebx ebx ebx ebx ebx	[esp+8+hWr ebx ebx loc_50311 , ds:PostMes ; PostMes	essageA ; lParam ; wParam ; Msg ; hWnd sageA ; lParam ; wParam
00000000503 00000000503 00000000503 00000000	00F0 p 00F0 p 00F1 p 00F2 m 00F6 x 00FA j 00FA j 00F0 p 00F0 p 00F1 p 00F0 p 00F1 p 00F0 p 00F1 p	push pov por push mov push push push push push push push push	ebx edi edi, ebx, edi, short edi esi esi esi ebx 12h edi esi ebx 12h edi si 12h	[esp+8+hWr ebx loc_50311 , ds:PostM ; PostMes	nd] essageA ; lParam ; wParam ; Msg ; hWnd sageA ; lParam ; wParam ; Msg
	00F0 p 00F0 p 00F1 p 00F2 m 00F8 c 00F8 c 00F8 c 00F8 c 00F8 c 00F8 c 00F8 c 00F8 c 00F8 c 00F0 p 00F0 p 00F0 p 00F0 p 00F0 p 00F0 p 00F0 p 00F0 p 00F1 p 00F0 p 00F1 p 00F0 p 00F1 p 00F0 p 00F1 p 00F0 p 00F0 p 00F1 p 00F0 c 00F0 p 00F0 p 00F0 c 00F0 c	push mov z push mov push push push call push push push push push	ebx edi, ebx, edi, short ebx, short ebx ebx ebx ebx ebx ebx ebx ebx ebx edi edi	[esp+8+hWr ebx : loc_50311 , ds:PostM	essageA ; lParam ; wParam ; Msg ; hWnd sageA ; lParam ; wParam ; wParam ; Msg ; hWnd
	00F0 p 00F1 p 00F1 p 00F2 m 00F6 x 00F8 c 00F8 c 00F8 c 00F8 c 00F8 c 00F8 c 00F8 c 00F0 p 00F0 p 00F0 p 00F1 p 00F0 p 00F1 p	push mov push push push push push push push push	ebx edi, ebx, edi, short esi esi esi ebx 12h edi esi ebx 12h edi esi	[esp+8+hWr ebx ebx loc_50311 , ds:PostMes	d] essageA ; lParam ; wParam ; Mgg ; hWnd sageA ; lParam ; wSg ; hWnd
	0000 0000 0000 0000 0000 0000 0000 0000 0000	push mov por mp z push mov push push push call push push push call push call	ebx edi, ebz, edi, short esi esi ebx ebx 12h edi esi ebx 12h edi esi ebx	[esp+8+hWr ebx loc_50311 , ds:PostM ; PostMes ; PostMes	d] essageA ; 1Param ; wParam ; Msg ; hWnd sageA ; 1Param ; wParam ; wParam ; Msg ; hWnd sageA
	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 00000 0000 0000 0000 0000 0000 0000 0000 00000	push mov push push push push push push push push	ebx edi, ebx, edi, short esi esi ebx ebx 12h edi esi ebx 12h edi esi ebx 12h edi ebx 12h edi	[esp+8+hWr ebx ebx loc_5031: , ds:PostM ; PostMes ; PostMes	essageA ; lParam ; wParam ; Msg ; hWnd sageA ; lParam ; Msg ; hWnd sageA ; lParam
	0000 000000000000000000000000000000000	push mov push mov push push push push call push push push call push push call push	ebx edi, edi, ebx, edi, short ebx ebx ebx ebx ebx ebx ebx ebx ebx ebx	<pre>[esp+8+hWr ebx ebx loc_50311 , ds:PostMes ; PostMes</pre>	nd] essageA ; 1Param ; wParam ; Msg ; hWnd sageA ; 1Param ; Msg ; hWnd sageA ; 1Param
	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 00000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	push push push push push push push push	ebx, edi, edi, edi, edi, short esi esi esi ebx ebx 12h edi esi esi esi esi esi esi esi esi esi es	<pre>[esp+8+hWr ebx ebx loc_50311 , ds:PostM ; PostMes ; PostMes</pre>	essageA ; lParam ; wParam ; Msg ; hWnd sageA ; lParam ; Wsg ; hWnd sageA ; lParam ; JParam ; WParam ; WParam
	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 00000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	push mov push mov push push push push push push push push	ebx, edi, edi, edi, edi, esi esi esi ebx ebx l2h edi esi ebx l2h edi esi ebx ebx 2 l2h edi esi esi edi esi esi edi esi esi esi esi esi edi esi esi esi esi esi esi esi esi edi esi esi esi esi esi esi esi esi esi es	<pre>[esp+8+hWr ebx ebx loc_50311 , ds:PostMes ; PostMes ; PostMes</pre>	d] essageA ; lParam ; wParam ; Msg ; hWnd sageA ; lParam ; wParam ; Msg ; hWnd sageA ; lParam
	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 00000 0000 0000 0000 0000 0000 0000 0000 0000 0000 00000	push mov push mov push push push call push push push push push push push push	ebx edi edi, edi, edi, short esi esi esi esi ebx ebx l2h edi esi esi esi esi esi esi esi esi 2 ebx edi 2 edi, short	<pre>[esp+8+hWr ebx ebx loc_50311 , ds:PostMes ; PostMes</pre>	d] essageA ; 1Param ; wParam ; Msg ; hWnd sageA ; 1Param ; wParam ; Msg ; hWnd sageA ; 1Param ; Msg ; hWnd
	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 00000 0000 0000 0000 0000 0000 0000 0000 0000 0000 00000	push mov pr z push mov push push push push push push push push	ebx, edi, edi, edi, edi, esi esi ebx ebx l2h edi esi ebx l2h edi esi ebx 2 ebx 2 edi esi	<pre>[esp+8+hWr ebx ebx loc_5031: , ds:PostM ; PostMes ; PostMes ; PostMes</pre>	d] essageA ; lParam ; WParam ; Msg ; hWnd sageA ; lParam ; wParam ; Msg ; hWnd sageA ; lParam ; wParam ; wParam ; hWnd sageA

Figure 14 Mass Mailer Algorithm

# **Dynamic Analysis**

# **Basic**

## RegShot

RegShot is a graphical dynamic tool that will create a report of all the modified files and registry keys during a specific time window.

## **Findings**

The binary was run for a period of five minutes on a virtual air gapped network. In this period a total of 14 registry keys and 6 files were added. Additionally, 17 files and keys were modified (Figure 15). Some of the files are in the system directory, which is often a technique used to hide malicious files. Some variants of MyDoom will replace the taskmon.exe with a malicious version. Additionally, the registry keys indicate the creation of a startup task which runs the binary each time the host boots.

Analysis
🧧 ~res-x64.txt - Notepad
File Edit Format View Help
Computer: DESKTOP-OXIGERQ , DESKTOP-OXIGERQ Username: calli , calli
Keyn added: 8
MUX-5-1-5-21-2023441954-680927518-1200971125-10811SoftbarrelVEcrosoft/Ukindows/LurrentVersion/Saarch/MacentApps/(CBF8C52-7C84-622-8E85-57A165E7708)           MUX-5-1-5-21-2023441954-680927518-1200971125-10811SoftbarrelVEcrosoft/Ukindows/LurrentVersion/Saarch/MacentApps/(CBF8C52-7C84-622-8E85-57A165E7708)           MUX-5-1-5-21-2023441954-680927518-1200971125-10811SoftbarrelVEcrosoft/Ukindows/LurrentVersion/Saarch/MacentApps/(CBF8C52-7C84-622-8E85-57A165E7708)           MUX-5-1-5-21-2023441954-680927518-1200971125-10811SoftbarrelVEclosoft/SoftbarrelVEclosoft/Benomy/KM645E1006VEcrosoft           MUX-5-1-5-21-2023441954-680927518-1200971125-1082           MUX-5-1-5-21-2023441954-680927518-1200971125-1082           MUX-5-1-5-21-2023441954-680927518-1200971125-1082           MUX-5-1-5-21-2023441954-680927518-1200971125-1082           MUX-5-1-5-21-2023441954-680927518-1200971125-1082           MUX-5-1-5-21-2023441954-680927518-1200971125-1082           MUX-5-1-5-21-2023441954-680927518-120097125-1082           MUX-5-1-5-21-2023441954-680927518-120097125-1082           MUX-5-1-5-21-2023441954-680927518-120097125-1082           MUX-5-1-5-21-2023441954-680927518-120097125-1082           MUX-5-1-5-21-2023441954-680927518-120097125-1082           MUX-5-1-5-21-2023441954-680927518-120097125-1082           MUX-5-1-5-21-2023441954-680927518-120097125-1082           MUX-5-1-5-21-2023441954-680927518-120097125-1082           MUX-5-1-5-21-2023441954-680927518-120097125-1082           MUX-5-1-5-21-2023441954-680927518-120
Values added: 6
MUS-1-5-1-202141954-68072738-1208071125-1081/SoftwareVRIcrosoftValindows/LurrentWersion/LogLover/UserAssist/(CEBFSCD-ACE2-64F-0178-9026412084A)/Count/V:VHTerfpopyvVrzcyrFJZ[dzt_/hrr: 00 00 00 00 00 00 00 00 00 00 00 00 00
Values modified: 5
Files addet: 6
C:\Users\callUqpDtrailucal\Temp\Ligity.log C:\Users\callUqpDtrailucal\Temp\Jimp\Jons.exe C:\Users\callUqpDtrailucal\Temp\Jimp\Jons.exe C:\Users\callUqpDtrailucal\Temp\Jimp\Jons.exe C:\Users\callUqpDtrailucal\Temp\Jimp\Jons.pf C:\Users\varbay\Prefetch\SERICES.LDE-2FIFGO6.pf
Files [sttributes]] molified: 12
C: Wardhoad Streiferio Stefficiens of t Windows UlserClass.det.L001 C: Wardhoad Streiferio Stefficiens of t Windows UlserClass.det.L001 C: Wardhoad Streiferio Stefficiens of t Windows Stefficient of the Stefficient of th
Total changes: 37
Figure 15 File Modifications

# **Process Monitor**

Process Monitor is used to closely examine a particular running process. This is achieved by stacking filters that target process names, IDs, categories, and more.

# Findings

After launching the binary, I started with a basic filter on the entire process (Figure 16). A summary was run on operation names, which revealed many registry operations. Due to this, another summary was run against the registry paths modified. This revealed changes in both the user and local machine hive. Next, I wanted to look at the network operations, as the previous analysis had revealed many indicators of worming/mass mailer activity. A TCP filter was added, which revealed thousands of reconnect requests to various MX addresses (Figure 17). Finally, to further analyze where file artifacts where placed, the TCP filter was replaced with a CreateFile filter (Figure 18). This revealed artifacts in SysWow64 and the user's AppData folder.

# Analysis

Count Values	Occurrences		
Column: Opera	ation ~		
Value	Count		
RegQueryValue	16577		
RegQueryKey	9692		
RegOpenKey	8656		
QueryDirectory	4428		
CreateFile	3916		
RegCloseKey	3496		
RegSetInfoKey	3117		
CloseFile	3114		
RegCreateKey	656		
RegEnumValue	426		
Thread Create	417		
UDP Receive	416		
UDP Send	416		
TCP Reconnec	t 329		
Unex Basic lofo	294 m 273		
CreateFileMapp	ing 128		
QueryStandard	Inf 118		
QuerySecurityFi	ie 99		
Load Image	90		
QueryAttribute T	a 86		
QueryAttributein	m 62		
QueryNameInfo	r 57		
SetDispositionIr	nf 55		
SetBasicInforma	ati 32		
QueryEaInforma	ati 31		
QueryStreamInt SetEndOfEloled	or 31		
RegEnumKey	26		
RegSetValue	23		
QuerySizeInform	na 2		
Process Exit	1		
Process Start	1		
Count Values Occurrences			
Value			Count
HKLM HKLM System/CurrentControlSet/Services/Topip/Parameters/Interfaces/(d2/9c HKLM/System/CurrentControlSet/Services/Topin/Parameters/Interfaces/(d2/9c	5ef-d666-11ec-8c42-806e6f6e6963} 183e-6ed6-4bc0-85ef-8x52x72995603		10046 2904 2376
HKLM/System/CurrentControlSet/Services/DnsCache/Parameters HKLM/System/CurrentControlSet/Services/Topip/Parameters			1644 1644
HKLM\SYSTEM\CurrentControlSet\Services\Topip6\Parameters\Interfaces\2A HKLM\SYSTEM\CurrentControlSet\Services\Topip6\Parameters\Interfaces\[D	kE9083E-6ED6-48C0-85EF-8A52A7299560) 2F9C5EF-D666-11EC-8C42-806E6F6E6963)	De	1584 1320
HKLM/System/CurrentControlSet/Services/Topip/Parameters/Interfaces HKLM/Software/Microsoft/identityStore/Providers/(B16898C6-A148-4967-9171-	64D755DA8520]\LoadParameters		1320 861 799
HKCU HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Hostname			765 546
C:\Users\call\Samples\MyDoom\Binarles\MyDoom.exe HKLM\System\CurrentControlSet\Services\Topip\Parameters\Domain			539 536
HKLM System CurrentControlSet Services Unscache Interface Specific Parameter HKLM/SYSTEM/CurrentControlSet/Services/NetBT/Parameters C/sDirectory	era		528 528 476
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Intern HKLM\System\Setup	net Settings\5.0\User Agent\Post Platform		442 426
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\DnsClient HKLM\Software\WOW6432Node\Policies\Microsoft\Windows NT\DnsClient			411 411
C:\Users\call\AppData\Local\Temp\zincte log HKCU\Software\Microsoft\Windows\CurrentVersion\UAD\Package	www.worureaer.eao.za/200503/Doman		33% 343 287
HKLM\SOFTWARE\Microsoft\IdentityStore\Providers\(B16898C6-A148-4967-9 HKLM\SOFTWARE\Policies\Microsoft\System\DNSClient	171-64D755DA8520[\LoadParameters\LoginUs		287 268
HKLM\Software\WOW6432Node\Policies\Microsoft\System\DNSClient HKLM\System\CurrentControlSet\Services\DNS	2001 C. IC S. A SEL S. C. THERE		268 268
HKLM\System\CurrentControlSet\Services\Topip\Parameters\Interfaces\[2ae90 HKLM\System\CurrentControlSet\Services\Topip\Parameters\Interfaces\[2ae90 HKLM\System\CurrentControlSet\Services\Topip\Parameters\Interfaces\[2ae90	183e-6ed6-4bc0-85ef-8a52a7299560)\DhcpDomain 183e-6ed6-4bc0-85ef-8a52a7299560)\DhcpDomain 183e-6ed6-4bc0-85ef-8a52a7299560)\Name Server		264 264
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{2ae90 HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{2ae90	083e-6ed6-4bc0-85ef-8a52a7299560)\RegisterAdapterNam 083e-6ed6-4bc0-85ef-8a52a7299560)\RegistrationEnabled	e.	264 264
HKLM\System\CurrentControlSet\Services\Topip\Parameters\Interfaces\(d29c HKLM\System)CurrentControlSet\Services\Topip\Parameters\Interfaces\(d29c HKLM\System)CurrentControlSet\Services\Topip\Parameters\Interfaces\(d29c	5ef d656-11ec &c42 806e8f6e6963) \DhcpDomain 5ef d666-11ec &c42 806e8f6e6963) \DhcpName Server 5ef d666-11ec &c42 806e8f6e6963) \DhcpName Server		264 264 264
HKLM\System\CurrentControlSet\Services\Topip\Parameters\Interfaces\(d2f9c HKLM\System\CurrentControlSet\Services\Topip\Parameters\Interfaces\(d2f9c	5ef-d666-11ec-8c42-806e8/6e6963) Warre Server 5ef-d666-11ec-8c42-806e8/6e6963) Vhane Server		264 264
HKLM\System\CurrentControlSet\Services\Topip\Parameters\Interfaces\(d29c	5ef-d666-11ec-8c42-806e9f6e6963)\RegisterAdapterName		264

## Figure 16 ProcMon Filter Name

💐 Pro	cess Monitor - Sysinti	ernals: w	ww.sysinternals.co	m						- 0	×
File	Edit Event Filter	Tools	Options Help								
G 6		🗢	A 🚯 🔳	A 5	<b>此 3 4 3 Ⅲ</b>						
Time .	Process Name	PID	Operation		Path		Result	Detail	User	Command Line	
9:45:5.	MyDoom exe	4600	TCP Reconnect		DESKTOP-OKR609Q:49875 -> 1.9.168.192 in-addr.arpa.amt	2	SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binartes\MyDoo	om exe"
9:45:5.	MyDoom.exe	4600	TCP Reconnect		DESKTOP-OKR609Q:49876 -> 1.9.168.192.in-addr.arpa.http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60.	. "C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om exe"
9.45.5	MyDoom exe	4600	TCP Reconnect		DESKTOP-OKR609Q 49878 -> 1.9.168.192 in-addr.arpa.amtp	2	SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	. "C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om exe*
9:45:5.	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49879 -> 1.9.168.192.in-addr.arpa.antp		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	. "C:\Users\calli\Samples\MyDoom\Binaries\MyDoo	om exe"
9:45:5.	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49880 -> 1.9.168.192.in-addr.arpa:amb		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	. "C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om exe"
9:45:5.	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49883 -> 1.9.168.192 in-addr.arpa:amb	2	SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoi	om exe"
9:45:5.	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49886 -> 1.9.168.192 in-addr arpa http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	. "C:\Users\calli\Samples\MyDoom\Binaries\MyDoi	om exe"
9:45:5	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49884 -> 1.9.168.192.in-addr.arpa.http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om exe"
9:45:5	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49885 -> 1.9.168.192 in-addr.arpa.http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\calli\Samples\MyDoom\Binaries\MyDoo	om exe"
9.45.5.	MyDoom.exe	1308	ATCP Reconnect		DESKTOP-OKR609Q:49887-> 1.9.168.192 in-addr.arpa.http		SUCCESS	Length: 0, seqnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDor	om.exe"
9.45.5	MyDoom exe	1308	TCP Reconnect		DESKTOP-OKR609Q 49888 -> 1.9.168.192 in-addr.arpa.http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om exe"
9:45:5	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49889 -> 1.9.168.192 in-addr.arpa.http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60.	. "C:\Users\call\Samples\MyDoom\Binaries\MyDor	om exe"
9:45:5.	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49890 -> 1.9.168.192.in-addr.arpa.http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Semples\MyDoom\Binaries\MyDoo	om.exe"
9:45:5.	MyDoom exe	4600	TCP Reconnect		DESKTOP-OKR609Q:49878 -> 1.9.168.192.in-addr.arpa.smt		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\calli\Satiples\MyDoom\Binaries\MyDoo	om exe"
9:45:5	MyDoom exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49891 -> 1.9.168.192 in-addr.arpa.http		SUCCESS	Length: 0, seqnum:	DESKTOP-OKR60	. "C:\Users\calli\Samples\MyDoom\Binaries\MyDoo	om exe"
9:45:5.	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49892 -> 1.9.168.192 in-addr.arpa.smb	2	SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	am.exe"
9:45:5	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49893 -> 1.9.168.192 in-addr.arpa.smtp	9	SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om exe"
9.45.5	MyDoom exe	1308	TCP Reconnect		DESKTOP-OKR609Q-49894 -> 1.9.168.192 in-addr.arpa.smtp	2	SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om.exe"
9:45:5	MyDoom exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49895 -> 1.9.168.192 in-addr arpa ant		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\calli\Samples\MyDoom\Binaries\MyDoo	om.exe"
9 45:5	MyDoom exe	1308	TCP Reconnect		DESKTOP-OKR609Q-49879 -> 1.9.168.192 in addr arps ant		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C \Users\call\Samples\MyDoom\Binates\MyDo	om exe"
9:45:5.	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49880 -> 1.9.168.192.in-addr.arpa.smtp	2	SUCCESS	Length: 0, seqnum:	DESKTOP-OKR60	. "C:\Users\call\Samples\MyDoom\Binartes\MyDoo	om exe"
9:46:0.	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q 49896 -> 1.9.168.192 in-addr.arpa.smb	2	SUCCESS	Length: 0, seqnum:	DESKTOP-OKR60.	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om exe"
9:46:0	MyDoom.exe	1308	A TCP Reconnect		DESKTOP-OKR609Q-49883 -> 1.9.168.192 in-addr.arpa.antp	5	SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om exe*
9:46:0	MyDoom.exe	4600	TCP Reconnect		DESKTOP-OKR609Q:49897 -> 1.9.168.192 in-addr.arpa.amt	2	SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\calli\Samples\MyDoom\Binaries\MyDoo	om.exe"
9.46:0.	MyDoom.exe	4600	TCP Reconnect		DESKTOP-OKR609Q-49898 -> 1.9.168.192 in-addr.arpa.antp		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60.	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om exe"
9:46:0.	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q-49886 -> 1.9.168.192 in-addr.arpa.http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om.exe"
9.46.0	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49884 -> 1.9.168.192 in addr arpa http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om.exe"
9:46:0.	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49885 -> 1.9.168.192.in-addr.arpa.http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om.exe"
9:46:0	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49887 -> 1.9.168.192.in-addr.arpa.http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60.	"C:\Users\calli\Samples\MyDoom\Binaries\MyDoo	om.exe"
9:46:0	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49888 -> 1.9.168.192 in addr arpa http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om.exe"
9:46:0	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49889 -> 1.9.168.192 in-addr arpa http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om.exe"
9:46:0	MyDoom exe	4600	TCP Reconnect		DESKTOP-OKR609Q:49899 -> 1.9.168.192.in-addr.arpa.antp		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om exe"
9:46:0.	MyDoom.exe	4600	TCP Reconnect		DESKTOP-OKR609Q:49900 -> 1.9.168.192 in-addr.arpa.antp	2	SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om.exe"
9:46:0	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49890 -> 1.9.168.192 in-addr arpa http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om.exe"
9:46:0	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49891 -> 1.9.168.192 in-addr.arpa.http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\calli\Samples\MyDoom\Binaries\MyDor	om.exe"
9:46:0	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49892 -> 1.9.168.192.in-addr.arpa:smtp	3	SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om exe*
9:46:0.	MyDoom.exe	4600	TCP Reconnect		DESKTOP-OKR609Q:49901-> 1.9.168.192.in-addr.arpa.http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om.exe"
9:46:0.	MyDoom.exe	4600	TCP Reconnect		DESKTOP-OKR609Q:49902 -> 1.9.168.192 in-addr.arpa.http		SUCCESS	Length: 0, seqnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om.exe"
9:46:0	MyDoom exe	4600	TCP Reconnect		DESKTOP-OKR609Q:49903 -> 1.9.168.192 in-addr.arpa.http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\calli\Samples\MyDoom\Binaries\MyDoo	om.exe"
9:46:0	MyDoom.exe	4600	TCP Reconnect		DESKTOP-OKR609Q:49904 -> 1.9.168.192 in addr.arpa.http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binartes\MyDo	om.exe"
9:46:0	MyDoom.exe	4600	TCP Reconnect		DESKTOP-OKR609Q:49905 -> 1.9.168.192.in-addr.arpa.http		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om.exe"
9:46:0	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49893 -> 1.9.168.192 in-addr.arpa.antp	D.S.	SUCCESS	Length: 0, seqnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om.exe"
9:46:0.	MyDoom.exe	4600	TCP Reconnect		DESKTOP-OKR609Q 49906 -> 1.9.168.192 in-addr.arpa.http		SUCCESS	Length: 0, seqnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDoo	om.exe"
9:46:0	MyDoom exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49894 -> 1.9.168.192 in-addr.arpa.tmtp		SUCCESS	Length: 0, segnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binarles\MyDoo	om.exe"
9.46.0	MyDoom.exe	1308	TCP Reconnect		DESKTOP-OKR609Q:49895 -> 1.9.168.192 in-addr.arpa.smtp	2	SUCCESS	Length: 0, seqnum:	DESKTOP-OKR60	"C:\Users\call\Samples\MyDoom\Binaries\MyDo	om.exe"
9:46:0	MyDoom.exe	4600	TCP Reconnect		DESKTOP-OKR609Q-49907 -> 1 9.168.192 in-addr.aroa http:		SUCCESS	Length: 0. seanum:	DESKTOP-OKR60	"C:\Users\call\Samples\MvDoom\Binaries\MvDo	om.exe" "

Figure 17 ProcMon Filter TCP

olumn: Path ~	
Value	Count
C:\Users\calli\AppData\Local\Temp	223
C:\Users\calli\Samples\MyDoom\Binaries\MyDoom.exe	k 119
C:\Users\calli\AppData\Local\Temp\zincite.log	117
C:\Windows\SysWOW64\phoneinfo.dll	78
C:\Windows\SysWOW64\wshgos.dll	32
C:\Windows\SysWOW64\mswsock.dll	21
C:\Windows\SysWOW64\KemelBase.dll	20
C:\Windows\SysWOW64\tzres.dll	16
C:\Users\calli	13
C:\Users\calli\AppData\Local	13
C:\Windows\SysWOW64\bcrypt.dll	9
C:\Windows\SysWOW64\dhcpcsvc.dl	9
C:\Windows\SysWOW64\dhcpcsvc6.dll	9
C:\Windows\SysWOW64\dnsapi.dll	9
C:\Windows\SysWOW64\dwmapi.dll	9
C:\Windows\SysWOW64\FWPUCLNT.DLL	9
C:\Windows\SysWOW64\iertutil.dll	9
C:\Windows\SysWOW64\IPHLPAPI.DLL	9
C:\Windows\SysWOW64\mslso.dll	9
C:\Windows\SysWOW64\NapiNSP.dll	9
C:\Windows\SysWOW64\nlaapi.dll	9
C:\Windows\SysWOW64\oleaut32.dll	9
C:\Windows\SysWOW64\OnDemandConnRouteHelpe	r.dl 9
C:\Windows\SysWOW64\pnrpnsp.dll	9
C:\Windows\SysWOW64\rasadhlp.dll	9
C:\Windows\SysWOW64\urfmon.dll	9
C:\Windows\SysWOW64\uxtheme.dll	9
C:\Windows\SysWOW64\winhttp.dll	9
C:\Windows\SysWOW64\wininet.dll	9
C:\Windows\SysWOW64\winnsi.dll	9
C:\Windows\SysWOW64\winmr.dll	9
C:\Windows\SysWOW64\en-US\tzres.dll.mui	8
C:\Users\calli\AppData\Local\Microsoft\Windows\Hist	ory 7
C:\Users\calli\AppData\Local\Microsoft\Windows\INet	Cookies 7
C:\Users\calli\AppData\Local\Temp\tmp1131.tmp	6
C:\Users\calli\AppData\Local\Temp\tmp1C38.tmp	6
C:\Users\calli\AppData\Local\Temp\tmp22CD.tmp	6
C:\Users\calli\AppData\Local\Temp\tmp235B.tmp	6
C:\Users\calli\AppData\Local\Temp\tmp2F85.tmp	6

Figure 18 ProcMon Filter CreateFile

## **ApateDNS**

ApateDNS helps malware analysts by setting up a fake DNS server on the local host (Figure 19). This redirects all the DNS requests from the binary to a console where the researcher can monitor the outbound connection requests.

## Findings

As expected, the binary created thousands of DNS requests. These requests varied from search engine queries, MX hosts, and internal mail portals. Over a period of a few minutes nearly 1500 requests were made (Figure 20 DNS Requests).

## Analysis

DNS Hex View         DNS Requested         DNS Returned           000702         win1710.byt6.microsoft.com         FOUND           000842         win1710.byt6.microsoft.com         FOUND           000842         win1710.byt6.microsoft.com         FOUND           000842         win1710.byt6.microsoft.com         FOUND           000842         win1710.byt6.microsoft.com         FOUND           001025         az764295.vo.meecnd.net         FOUND           001034         win1710.byt6.microsoft.com         FOUND           001035         az764295.vo.meecnd.net         FOUND           001034         win1710.byt6.microsoft.com         FOUND           001135         win1710.byt6.microsoft.com         FOUND           001135         win1710.byt6.microsoft.com         FOUND           01135         win1710.byt6.microsoft.com         FOUND           01135         win1710.byt6.microsoft.com         FOUND           1135         win1710.byt6.microsoft.com         FOUND           0         server started at ee:66:49 successfully.         Stat Server           114         NtXDOMAIN's:         Stat Server         Stat Server           1250         main         Mix0.mix0.mix0.mix0.mix0.mix0.mix0.mix0.m				- 0	×
Time         Domain Requested         DNS Returned           000703         win1710/pv6/microsoft.com         FOUND           000842         win1710/pv6/microsoft.com         FOUND           000842         win1710/pv6/microsoft.com         FOUND           000842         win1710/pv6/microsoft.com         FOUND           000842         win1710/pv6/microsoft.com         FOUND           001025         az764255vo.meend.net         FOUND           001125         az764255vo.meend.net         FOUND           001113         win1710/pv6/microsoft.com         FOUND           11115         win1710/pv6/microsoft.com         FOUND           125ers/er started at 00:05:49 successfully.         Start Server           DNS Reply IP (Default: Current Gatway/ONS):         127.0.1         Start Server           12 dottoff crept1         foldel main au control c	Capture Window	V DNS Hex View			
00.07.02     win1710.pv6 microsoft.com     FOUND       00.07.03     win1710.pv6 microsoft.com     FOUND       00.08.04     win1710.pv6 microsoft.com     FOUND       00.08.04     win1710.pv6 microsoft.com     FOUND       00.08.04     win1710.pv6 microsoft.com     FOUND       00.08.02     win1710.pv6 microsoft.com     FOUND       00.010.6     win1710.pv6 microsoft.com     FOUND       00.10.25     az764255 vo meerd net     FOUND       00.10.25     az764255 vo meerd net     FOUND       00.10.25     az764255 vo meerd net     FOUND       00.11.5     win1710.pv6 microsoft.com     FOUND       00.11.5     win1710.pv6 microsoft.com     FOUND       00.11.5     win1710.pv6 microsoft.com     FOUND       01.11.5     win1710.pv6 microsoft.com     FOUND       01.11.5     win1710.pv6 microsoft.com     FOUND       01.11.5     win1710.pv6 microsoft.com     FOUND       11.11.5     win1710.pv6 microsoft.com     FOUND       12.11.5     win1710.pv6 microsoft.com     FOUND       13.11.5     win1710.pv6 microsoft.com     FOUND       14.11.5     win1710.pv6 microsoft.com     FOUND       15.11.5     win1710.pv6 microsoft.com     FOUND       14.11.5     win1710.pv6 microsoft.com     <	Time	Domain Requested		DNS Returned	^
000733     wn1710.pv6.microsoft.com     FOUND       000842     wn1710.pv6.microsoft.com     FOUND       000842     wn1710.pv6.microsoft.com     FOUND       000842     wn1710.pv6.microsoft.com     FOUND       001056     wn1710.pv6.microsoft.com     FOUND       001052     az764295.vo.mecnd.net     FOUND       00103     wn1710.pv6.microsoft.com     FOUND       00103     wn1710.pv6.microsoft.com     FOUND       00103     wn1710.pv6.microsoft.com     FOUND       00113     wn1710.pv6.microsoft.com     FOUND       00113     wn1710.pv6.microsoft.com     FOUND       00115     wn1710.pv6.microsoft.com     FOUND       01115     wn1710.pv6.microsoft.com     FOUND       1     Jusing 127.e.e.1.as return DNS IP!     FOUND       1     Server started at @e:es:#9 successfully.     Stat Server       1     Server started at @e:es:#9 successfully.     Stat Server       1     Server started at @e:es:#9 successfully.     Stat Server       1     DNS Reply IP (Default: Current Gatway/DNS):     127.0.1     Stat Server       1     driver started at @e:es:#9 successfully.     Stat Server     Stat Server       2     Server started at @e:es:#0 successfully.     Stat Server     Stat Server       1     Mot	00:07:02	win 1710.jpv6.microsoft.com		FOUND	
00.08.04         win1710.pw6.microsoft.com         FOUND           00.09.24         win1710.pw6.microsoft.com         FOUND           00.09.24         win1710.pw6.microsoft.com         FOUND           00.10.25         az764295.vo.msecnd.net         FOUND           00.10.25         az764295.vo.msecnd.net         FOUND           00.10.25         az764295.vo.msecnd.net         FOUND           00.11.5         win1710.pw6.microsoft.com         FOUND           1         start Servier         Start Servier         Start Servier           1         start Servier         Start Servier         Start Servier         Start Servier           1         start Servier         0         Start Servier         Start Servier           1         start Servier         0         Start Servier         Start Servier           1         start Servier         0         Start Servier         Start Servie	00:07:33	win 1710.jpv6.microsoft.com		FOUND	
20.08.42     wn1710.pv6 microsoft.com     FOUND       20.09.44     wn1710.pv6 microsoft.com     FOUND       20.09.06     win1710.pv6 microsoft.com     FOUND       20.10.25     az 76425 vo meech net     FOUND       20.11.58     win1710.pv6 microsoft.com     FOUND       20.11.59     win170.pv6 microsoft.com     FOUND       20.12.50     microsoft.com     FOUND       20.12.50     mal.x     O       20.12.50     mal.x     FOUND       20.12.50     mal.x     FOUND       20.12.50     mal.x	00:08:04	win 1710.jpv6.microsoft.com		FOUND	
20.09.24     win1710.pv6.microsoft.com     POUND       20.010.25     az764255 vo meend.net     POUND       20.010.39     win1710.pv6.microsoft.com     POUND       20.011.15     win1710.pv6.microsoft.com     POUND       20.012.15     win1710.pv6.microsoft.com     POUND       20.012.15     win1710.pv6.microsoft.com     POUND       20.012.15     Selected Interface:     Intell(R) PRO/1000 MT Network Connection.       20.012.15     POUND     POUND       20.012.15     Conture Requested     POUND       20.012.50     mal.n	00:08:42	win 1710.ipv6.microsoft.com		FOUND	
D0.006     win1710.py6microsoft.com     POUND       D0.1025     az764255 volumeend.net     POUND       D0.1025     az764255 volumeend.net     POUND       D0.1025     az764255 volumeend.net     POUND       D0.1025     az764255 volumeend.net     POUND       D0.1135     win1710.py6microsoft.com     POUND       D0.1115     win1710.py6microsoft.com     POUND       -1 Using 127.e.e.1 as return DNS IPI     POUND     POUND       -1 Using 127.e.e.1 as return DNS IPI     0     Server started at @0:06:49 successfully.       DNS Repky IP (Default: Current Gatway/DNS):     127.0.0.1     Server started at @0:06:49 successfully.       Selected Interface:     Intel(R) PRO/1000 MT Network Connection     Volume       rtd reputition compression	00:09:24	win 1710.jpv6.microsoft.com		FOUND	
00.10.25     az 764285 volmeend net     POUND       00.10.25     az 764285 volmeend net     POUND       00.10.39     win1710.pv6microsoft.com     POUND       00.11.15     win1710.pv6microsoft.com     POUND       00.11.15     win1710.pv6microsoft.com     POUND       01.11.15     win1710.pv6microsoft.com     POUND       01.11.15     win1710.pv6microsoft.com     POUND       10.11.15     win1710.pv6microsoft.com     POUND       11.15     win1710.pv6microsoft.com     POUND       11.15     win1710.pv6microsoft.com     POUND       11.15     win170.pv6microsoft.com     POUND       11.15     win170.pv6microsoft.com     POUND       11.15     win170.pv6microsoft.com     POUND <td>00:10:06</td> <td>win 1710. ipv6.microsoft.com</td> <td></td> <td>FOUND</td> <td></td>	00:10:06	win 1710. ipv6.microsoft.com		FOUND	
00.10.25     az 764295 vo meecnd net     POUND       00.10.23     win1710.pv5 microsoft.com     FOUND       00.11.15     win1710.pv5 microsoft.com     FOUND       00.11.15     win1710.pv5 microsoft.com     FOUND       01.11.5     win1710.pv5 microsoft.com     FOUND       1     using 127.e.e.1 as return DNS IP!     FOUND       1     DNS Set DI TAT.e.e.1 on Intel (8) FR0/1000 MT Network Connection.     FOUND       2     server started at 00:06:49 successfully.     Start Server       Set diagonal diagona diagonal diagonal diagonal diagonal diagonal diagonal di	0:10:25	az 764295 vo msecnd net		FOUND	
00.10.39       win1710.pv6.microsoft.com       FOUND         00.11.15       win1710.pv6.microsoft.com       FOUND         10.11.15       win1710.pv6.microsoft.com       Wintervector         10.11.15       win1710.pv6.microsoft.com       Istat Server         11.11.11       Server started at 00:06:49 successfully.       Istat Server         11.11.11       Selected Interface:       Intel(R) PR0/1000 MT Network Connection       vofterface         11.11.11       Selected Interface:       Intel(R) PR0/1000 MT Network Connection       vofterface         11.11.11       Selected Interface:       Intel(R) PR0/1000 MT Network Connection       FOUND         11.12.11       Intel R	0:10:25	az 764295.vo.msecnd.net		FOUND	
00:11:15       win1710.pv6.microsoft.com       FOUND         00:11:35       win1710.pv6.microsoft.com       FOUND         10:Using 127-0.0-1.as return DNS IP!       DNS set to 127.0.0.1 msture (R) FR0/1868 NT Network Connection.         10:Sending value       Sending value       Sending value         DNS Reply IP (Default: Current Gatway/DNS):       127.0.0.1       Sending value         # of NXDOMAIN's:       0       Sending value       Stort Server         Selected Interface:       Intel(R) PR0/1000 MT Network Connection       volume       Stort Server         rtil.cogistic arguit].intil.comines comines comprise compr	0:10:39	win 1710.jpv6.microsoft.com		FOUND	
20.11:58       win1710.bv6.microsoft.com       FOUND         1       Using 127.0.0.1 as return DNS IP!       FOUND         1       DNS Reply IP (Default: Current Gatway/DNS):       Trequest.         2       Server started at 00:06:49 successfully.       Start Server         DNS Reply IP (Default: Current Gatway/DNS):       127.0.0.1       Start Server         # of NXDOMAIN's:       0       Start Server       Stor Server         Selected Interface:       Intel(R) PRO/1000 MT Network Connection       V       Stor Server         rtd. cotorf organi.intel.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/one.com/	00:11:15	win 1710.jpv6.microsoft.com		FOUND	
USIGN 127.0.0.1 as return DNS IP! DNS Set to 127.0.0.1 on Intel(8) PRO/B808 MT Network Connection. Sending void DNS request. Server started at 00:06:49 successfully. DNS Reply IP (Default: Current Gatway/DNS): 127.0.1 # of NXDOMAIN's: 0 Selected Interface: Intel(R) PRO/1000 MT Network Connection Selected Interface: Intel(R) PRO/1000 MT Network Connection ApateDNS Capture Window DNS Requested 0:12:50 mail.u 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50 0:12:50	0:11:58	win 1710.jpv6.microsoft.com		FOUND	~
Tree Longer Free Comment Commentations Commentations Commentation  Tree Longer Free Comment Commentations Comment Com	DNS Reply # of NXDO	IP (Default: Current Gatway/DNS): MAIN's: terfano:	127.0.0.1 0	Start Ser Stop Ser	ver
M ApateDNS       -         Capture Window       DNS Hex View         Time       Domain Requested       DNS Returned         00:12:50       mainu       FOUND         00:12:50       126.com       FOUND         00:12:50       126.com       FOUND         00:12:50       nainu       FOUND         00:12:50       nainu       FOUND         00:12:50       mainu       FOUND         00:12:50       mainu       FOUND         00:12:50       mainu       FOUND         00:12:51       www.abavita.com       FOUND         00:12:51       search.lycos.com       FOUND         01:2:52       search.lycos.com       FOUND         10:12:51       single 127.0.0.1       Tittel 127.0.0.1         10:12:51       single 0.00       Tittel 127.0.0.1         10:12:51 <t< th=""><th>rtel.comietf.orgm</th><th>ail.intel.comairvana.comairvana.comairvana.c</th><th>comortel.comortel.comortel.comairvana.comairvana.commx.intel.comor adure teorete educe teorete educate alegene compil inserte</th><th>tel.comortel.comairvana</th><th>.comcisc</th></t<>	rtel.comietf.orgm	ail.intel.comairvana.comairvana.comairvana.c	comortel.comortel.comortel.comairvana.comairvana.commx.intel.comor adure teorete educe teorete educate alegene compil inserte	tel.comortel.comairvana	.comcisc
DNS Hex View           Time         Domain Requested         DNS Returned           00:12:50         mail ru         FOUND           00:12:50         mail ru         FOUND           00:12:50         126.com         FOUND           00:12:50         126.com         FOUND           00:12:50         mail ru         FOUND           00:12:50         mail ru         FOUND           00:12:51         www.google.com         FOUND           00:12:51         www.google.com         FOUND           00:12:51         mail.com         FOUND           00:12:51         mail.com         FOUND           00:12:51         mail.com         FOUND           00:12:51         map.com         FOUND           00:12:51         map.com         FOUND           00:12:51         map.com         FOUND           00:12:52         search.lycos.com         FOUND           00:12:51         map.com         FOUND           12:12:0:0:1         Istrict 12:7.0:0:1         Istrict 12:7.0:0:1	ApateDN	S			
Time         Domain Requested         DNS Returned           00:12:50         mail.ru         FOUND           00:12:50         mail.ru         FOUND           00:12:50         126.com         FOUND           00:12:50         126.com         FOUND           00:12:50         mail.ru         FOUND           00:12:51         www.abavita.com         FOUND           00:12:51         search.lycos.com         FOUND           00:12:51         search.lycos.com         FOUND           00:12:51         search.lycos.com         FOUND           00:12:51         search.lycos.com         FOUND           00:12:51         map.com         FOUND           00:12:52         search.lycos.com         FOUND           00:12:51         stage.tom.in.tetl(R) PRO/1000 MT Network Connection.           *1 Using 127:0:0:1         T37:0:0:1	Capture Windo			- 0	×
00:12:50         mail.ru         FOUND           00:12:50         126.com         FOUND           00:12:50         126.com         FOUND           00:12:50         126.com         FOUND           00:12:50         mail.ru         FOUND           00:12:50         mail.ru         FOUND           00:12:50         mail.ru         FOUND           00:12:51         www.abavita.com         FOUND           00:12:51         search.lycos.com         FOUND           00:12:51         smab.com         FOUND           00:12:52         search.lycos.com         FOUND           00:12:53         smab.com         FOUND           *) Is set to 127.0.0.1         Intel(R) PRO/1000 MT Network Connection.           *) Sending vulid DMS response of first request.         *)           *) Sending vulid DMS response of first request.         *)           *) Server started at 00:06:49 successfully.<		DNS Hex View		- 0	×
00:12:50         mail.u         FOUND           00:12:50         126.com         FOUND           00:12:50         126.com         FOUND           00:12:50         mail.u         FOUND           00:12:50         mail.u         FOUND           00:12:50         mail.u         FOUND           00:12:50         mail.u         FOUND           00:12:51         www.abavista.com         FOUND           00:12:51         search.lycos.com         FOUND           00:12:51         search.lycos.com         FOUND           00:12:51         search.lycos.com         FOUND           00:12:51         mmap.com         FOUND           00:12:51         search.lycos.com         FOUND           00:12:51         search.lycos.com         FOUND           00:12:51         mmap.com         FOUND           00:12:51         mmap.com         FOUND           00:12:58         mmap.com         FOUND           00:12:58         mmap.com         FOUND           +1         Using 127:0.0.1         istrict request.           +1         Sending valid DNS response of first request.         (*)           +1         Server started at @0:06:49 successfully.	Time	DNS Hex View Domain Requested		DNS Returned	×
00:12:50         126.com         FOUND           00:12:50         mairu         FOUND           00:12:50         mairu         FOUND           00:12:50         mairu         FOUND           00:12:51         www.google.com         FOUND           00:12:51         www.atavita.com         FOUND           00:12:51         www.atavita.com         FOUND           00:12:51         waw.atavita.com         FOUND           00:12:51         waw.atavita.com         FOUND           00:12:51         waw.atavita.com         FOUND           00:12:51         maa.com         FOUND           00:12:52         search.lycos.com         FOUND           00:12:58         maa.com         FOUND           00:12:58         maa.com         FOUND           00:12:59         maa.com         FOUND           00:12:58         maa.com         FOUND           00:12:58         maa.com         FOUND           12:12:0:0:1         Secoling valid DNS response of first request.         FOUND           *) Server started at 00:06:49 successfully.         127:0:0:1         Intervert Secoling valid	Time 00:12:50	DNS Hex View Domain Requested mail.ru		DNS Returned FOUND	×
D01250       126.com       FOUND         D01250       mairu       FOUND         D01250       mairu       FOUND         D01251       www.google.com       FOUND         D01251       www.google.com       FOUND         D01251       www.google.com       FOUND         D01251       search.yeloo.com       FOUND         D01252       search.yeloo.com       FOUND         D01252       search.yeloo.com       FOUND         001252       search.yeloo.com       FOUND         001252       search.yeloo.com       FOUND         001252       mag.com       FOUND         *) Using 127.0.0.1 an Intel(R) PR0/1000 NT Network Connection.       *         *) Server started at 00:06:49 successfully.       *         DNS Beek IP (Defa.it: Cummt Gisturar(DNS):       127.0.0.1	Time 00:12:50 00:12:50	DNS Hex View Domain Requested mail.ru mail.ru		DNS Returned FOUND FOUND	×
D01250       mairu       FOUND         D01251       www.google.com       FOUND         D01251       www.google.com       FOUND         D01251       www.google.com       FOUND         D01251       search.ycos.com       FOUND         D01252       search.ycos.com       FOUND         D01253       mmap.com       FOUND         001258       nmap.com       FOUND         001258       sreturn DNS IP!       *         *1 Using 127.0.0.1 as return DNS IP!       *         *1 Using 127.0.0.1 as return DNS IP!       *         *1 Sending valid DNS response of first request.       *         *1 Server started at 00:06:49 successfully.       *	Time 00:12:50 00:12:50 00:12:50	DNS Hex View Domain Requested mail.ru 126.com		DNS Returned FOUND FOUND FOUND	×
D01250       mairu       FOUND         D01251       www.google.com       FOUND         D01251       www.atavita.com       FOUND         D01251       search.lycos.com       FOUND         D01252       search.lycos.com       FOUND         D01253       mmap.com       FOUND         01254       mmap.com       FOUND         *1 Using 127.0.0.1 as return DNS IPI       *1         *1 Using 127.0.0.1 as return DNS IPI       **         *1 Using 127.0.0.1 as return DNS IPI       **         *1 Sending valid DNS response of first request.       **         *1 Server started at 00:06:49 successfully.       **	Time 00:12:50 00:12:50 00:12:50 00:12:50	W DNS Hex View Domain Requested mail.ru 126.com 126.com		DNS Returned FOUND FOUND FOUND FOUND	×
D0:12:51     www.google.com     FOUND       D0:12:51     wew.atavista.com     FOUND       D0:12:51     search.yoaco.com     FOUND       D0:12:52     search.yahoo.com     FOUND       00:12:53     mmap.com     FOUND       00:12:54     mmap.com     FOUND       00:12:58     mmap.com     FOUND       01:12:58     restrict.ext     FOUND       01:12:58     restrict.ext     FOUND       1:12:10:00     FOUND     FOUND       1:12:10:00     FOUND     FOUND	Time 00:12:50 00:12:50 00:12:50 00:12:50 00:12:50	DNS Hex View Domain Requested mail ru T26 com T26 com mail ru		DNS Returned FOUND FOUND FOUND FOUND FOUND	×
D0:12:51       www.atavista.com       FOUND         D0:12:51       search lycos.com       FOUND         D0:12:52       search lycos.com       FOUND         D0:12:53       nmap.com       FOUND         -1 USIng 127:0.0.1 as return DNS IP!       +         +1 USIng 127:0.0.1 as return DNS IP!       +         +2 USIng 127:0.0.1 as return DNS IP!       +         +3 Sending valid DNS response of first request.       +         +3 Server started at 00:06:49 successfully.       +	Time 00:12:50 00:12:50 00:12:50 00:12:50 00:12:50 00:12:50	w DNS Hex View Domain Requested mail.ru mail.ru 126.com 126.com mail.ru mail.r		DNS Returned     FOUND     FOUND     FOUND     FOUND     FOUND     FOUND     FOUND     FOUND	×
D01251       search.yoos.com       FOUND         D01252       search.yahoo.com       FOUND         D01258       immap.com       FOUND         *1 Using 127.0.0.1 as return DNS IP!       *1         *1 Using 127.0.0.1 as return DNS IP!       *1         *1 Sending valid DNS response of first request.       *1         *1 Server started at 00:06:49 successfully.       *1	Time 00:12:50 00:12:50 00:12:50 00:12:50 00:12:50 00:12:50 00:12:51	W DNS Hex View Domain Requested mail.ru mail.ru 126.com 126.com mail.ru mail.r		DNS Returned     FOUND     FOUND     FOUND     FOUND     FOUND     FOUND     FOUND     FOUND	×
UUILIZ search yahoo com FOUND 001258 mag com FOUND (*) Using 127.8.8.1 as return DNS IP! •) DNS set to 127.8.8.1 on Intel(R) PR0/1000 HT Network Connection. •) Sending vold DNS reports of first request. •) Server started at 00:06:49 successfully. DNS Beek IP (Defa.th Current Gaturar(DNS): 127.0.1	Time 00:12:50 00:12:50 00:12:50 00:12:50 00:12:50 00:12:50 00:12:51 00:12:51 00:12:51	DNS Hex View Domain Requested mail.ru mail.ru 126.com mail.ru		DNS Returned     FOUND	
UUIL258 nmap.com FOUND +) Using 127.0.0.1 as return DNS IP! +) DNS set to 127.0.0.1 on Intel(R) PRO/1000 HT Network Connection. +) Sending valid DNS response of first request. +) Server started at 00:06:49 successfully. DNS Beek IP (Defa.t: Current Gaturar(DNS): 127.0.1	Time 00:12:50 00:12:50 00:12:50 00:12:50 00:12:50 00:12:50 00:12:51 00:12:51 00:12:51 00:12:51	bonain Requested mail ru mail ru 126.com 126.com mail ru mail ru www.atavista.com search lycos.com		POIND FOUND FOUND FOUND FOUND FOUND FOUND FOUND FOUND FOUND	
DNS Banky IP (Dafault-Current Gaturary/DNS): 127.0.0.1	Time 00:12:50 00:12:50 00:12:50 00:12:50 00:12:50 00:12:51 00:12:51 00:12:51 00:12:51 00:12:52 00:12:58	DNS Hex View Domain Requested mail ru mail ru 126.com 126.com mail ru www.google.com www.atavista.com search lycos.com mae.com		DNS Returned     FOUND     FOUND	×
#of NXDOMAIN's: 0	Time 00:12:50 00:12:50 00:12:50 00:12:50 00:12:50 00:12:51 00:12:51 00:12:51 00:12:51 00:12:51 00:12:51 00:12:52 *] Using 12 *] Server s	DNS Hex View Domain Requested mail ru mail ru T26 com T26 com mail ru	1000 MT Network Connection. equest. ly.	DNS Returned FOUND FOUND FOUND FOUND FOUND FOUND FOUND FOUND FOUND	

Figure 19 Fake DNS Server

Selection View Go Run Terminal Help	Untitled-6 - MyDoom: Workspace (Workspace) - Visual Studio Code (Administrator)      Etatskpdungsog United 1      H      Transit		□□□□□08 - 01 ×
Allowing     and any set of the set of t	Bank provide and the second	2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2         2	2 control of the second of the
sets.ec.com.exe 57 lists.tepdump.org	37 sonic.net 37 us.lm.com	57 epilogue.com	57 andrew.cmu.edu
144	aoaioxxysz.net		
144	aoaioxxysz.net		
144	3 spam.raszi.hu		
144	+ aoaloxxysz.net		
144	aoaioxxysz.net		
144	aoaioxxysz.net		
144	juliangruber.com		
144	juliangruber.com		
145	juliangruber.com		
145	spam.raszi.hu		
145	aoaioxxysz.net		
145	juliangruber.com		
145	juliangruber.com		
145	5 juliangruber.com		
145	7 mx.aoaioxxysz.net		
145	mx.juliangruber.com		
145	<pre>mail.aoaioxxysz.net mail.juliangruber.com</pre>		
146	smtp.aoaioxxvsz.net		
146	2 smtp.juliangruber.com		
146	win1710.ipv6.microsoft.com		
146	1 hocevar.net		
146	5 hocevar.net		
146	hocevar.net		
146	nov avar nar		
146	hocevar.net		
146	hocevar.net		
146 146 147	hocevar.net hocevar.net hocevar.net win1710.ipv6.microsoft.com		

Figure 20 DNS Requests

## netstat

Netstat is a basic networking command line tool that is used to show connections and listening ports on a host.

## Findings

As indicated in the research, MyDoom creates a TCP listener that can be used to transfer files or command and control a large botnet of affected devices (Figure 21). Each variant opens a different port. As previously hypothesized, this further confirms that the sample is variant M (Port 1034).

# Analysis

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0:1034	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49670	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49671	0.0.0.0:0	LISTENING
TCP	127.0.0.1:55624	127.0.0.1:80	SYN_SENT
TCP	127.0.0.1:55625	127.0.0.1:80	SYN_SENT
TCP	127.0.0.1:55626	127.0.0.1:80	SYN_SENT
TCP	127.0.0.1:55627	127.0.0.1:80	SYN_SENT
TCP	127.0.0.1:55628	127.0.0.1:80	SYN_SENT
TCP	127.0.0.1:55629	127.0.0.1:80	SYN_SENT
TCP	127.0.0.1:55630	127.0.0.1:80	SYN_SENT
TCP	127.0.0.1:55631	127.0.0.1:80	SYN_SENT
TCP	169.254.214.217:5040	0.0.0.0:0	LISTENING
TCP	192.168.9.14:139	0.0.0.0:0	LISTENING
TCP	192.168.9.14:445	192.168.9.13:64321	ESTABLISHED
TCP	192.168.9.14:55477	16.50.1.85:1034	SYN_SENT
TCP	[::]:135	[::]:0	LISTENING
TCP	[::]:445	[::]:0	LISTENING
TCP	[::]:3389	[::]:0	LISTENING
TCP	[::]:49664	[::]:0	LISTENING
TCP	[::]:49665	[::]:0	LISTENING
TCP	[::]:49666	[::]:0	LISTENING
TCP	[::]:49667	[::]:0	LISTENING
TCP	[::]:49668	[::]:0	LISTENING
TCP	[::]:49669	[::]:0	LISTENING
TCP	[::]:49670	[::]:0	LISTENING
TCP	[::]:49671	[::]:0	LISTENING
UDP	0.0.0.0:53		
UDP	0.0.0.0:123		
UDP	0.0.0.0:500		
UDP	0.0.0.0:3389		
UDP	0.0.0.0:4500		
UDP	0.0.0.0:5050		
UDP	0.0.0.0:5353		
UDP	0.0.0.0:5355		
UDP	127 0 0 1-1900		

Figure 21 Backdoor Listener

# Advanced

## x32Debug

x32Debug is a dynamic debugging tool that can be used to step through a binary as well as provides the ability to manipulate the CPU, heap and stack in real time.

## Finding 1: DNS Query Algorithm

In the below analysis we can see the DNS requests being loaded into the stack before being registered in ApateDNS (Figure 22). This function is repeated numerous times as the binary makes its way through thousands of domains. With Wireshark, we can see each packet as the binary calls the GetHostByName API (Figure 23).

Ana	lysis	5										
Ӿ MyDoor	m.exe - PID: A	0C - Module: mydoom.exe - Thread: 2A	CC - x32dbg [Elevated]									- 🗆 ×
File View	Debug Trao	e Plugins Favourites Options Help	Aug 23 2019									
• • • •	+ II   † A	• 👒 🎍 🔋 🕰 📓 🦉 😸 🖉 🖋	# Aa 👗 📗 朢									
E CPU	🌳 Graph	Log Notes • Breakpoir	ts Memory Map	G Call Stack	SEH 🗵 Script	Symbols	Source	₽ References	😒 Threads	📥 Hand	les 👔 Trace	
		00506873	8500	test eax,eax	. [Kagethos toynali	••]		eax:&"alum.mit.	edu"	^ H1	de FPU	Alle Australia and all
( <b>9</b> .0)	, [,	005003#/         005003#/           0050087A         0050687C           0050087E         00506883           00506883         00506883           00506883         00506883           0050687E         00506883           00506883         00506883           00506884         00506884           00506885         00506884           00506884         00506884	8840 OC 800 800 8376 FF 75 02 3376 88C6 56 C3 55 88FC	<pre>mov eax,dword ptr mov eax,dword ptr mov esi,dword ptr Cmp esi,FFFFFF Imm mydoom,5006855 xor esi,esi mov eax,esi pop esi et push ebp mov ebp.esp</pre>	ds:[eax=C] ds:[eax] ds:[eax]			eax:&"alum.mit. eax:&"alum.mit. [eax]:"alum.mit eax:&"alum.mit.	.edu" [eax]:" .edu" [eax]:" .edu"		x         75570E0           x         75570E0           x         A8034C6E           x         00000000           P         77E6FB80           P         77E6FB80           I         FFFFFFF           I         77E6FDC4           P         00506877	ckerne132.1StrcatA> <dhstrcpy> "alum.mft.edu" mydoom.00506877</dhstrcpy>
		0050682 00506892 00506892 00506894 00506894 00506898 00506898 00506898	81EC 00010000 53 56 88F0 33C0 38F0 57	sub esp,100 push ebx mov esi mov esi,eax xor eax,eax cmp esi,eax push edi				eax:&"alum.mit. eax:&"alum.mit. eax:&"alum.mit. edi:"alum.mit.	. edu" . edu" . edu" edu"	EF ZF OF CF	LAGS 0000020 0 PF 0 AF 0 0 SF 0 DF 0 0 TF 0 IF 1 stError 00000 stStatus 0000	22 ) ) )000 (ERROR_SUCCESS) )000 (STATUS_INVALID_PARAMETER)
-	💽 ApateDN	00506898 NS	✓ 0F84 63010000	1e mydoom, 506004	- 0	$\times$				GS	0028 FS 005	3
	Capture Wind	ow DNS Hex View								cs	0023 55 0028	3
	Time	Domain Requested			DNS Returned	^				ST	(0) 0000000000 (1) 000000000000000000000000000000000000	0000000000 x87r0 Empty 0.00000000000000000 0000000000 x87r1 Empty 0.00000000000000000000000000000000000
	21:52:27	nmap.org			FOUND			D:'\r'		ST	(2) 0000000000 (3) 000000000000000000000000000000000000	0000000000 x87r2 Empty 0.00000000000000000000000000000000000
	21:52:27	lists.tcpdump.org			FOUND			A: '\n'		ST	(4) 0000000000 (5) 000000000000000000000000000000000000	0000000000 x87r4 Empty 0.00000000000000000000000000000000000
	21:52:27	lists.tcpdump.org			FOUND			20:' '		ST	(6) 000000000	0000000000 x87r6 Empty 0.00000000000000000000000000000000000
	21:52:27	nmap.org			FOUND			9:'\t'			(7) boodboodd	0000000000 x0/17 Empty 0.00000000000000000000
	21:52:31	ns.aus.com			FOUND					xe	7TW_0 3 (Empty	<pre>/) x87Tw_1 3 (Empty)</pre>
	21:52:47	alum mit edu			FOUND					~ ×8	7TW_2 3 (Empty	/) x87Tw_3 3 (Emptγ)
eax=00455	21:52:49	win1710.jpv6.microsoft.com			FOUND					> De	ault (stdcall)	▼ 5 \$ Unlocked
dword ptr	21:53:32	win1710.jpv6.microsoft.com			FOUND					2:	esp+8 7571E	260
.text:005	21:04:11	white to possible oscillation			POOND	~				4	[esp+10] 756D	6F68
Address 771E1000 771E1010 771E1020 771E1020 771E1030 771E1040 771E1050 771E1050 771E1080 771E1080 771E1080 771E1040	<pre>[+] Attempt [+] Using I [+] DNS set [+] Sending [+] Server</pre>	ing to find DNS by DHCP or static C P address 192.168.9.1 for DNS hepj to 127.08.0 to Intel(R) PRO/1000 valid DNS response of first reques started at 21:46:00 successfully.	NS. MT Network Connection t.					7756 7756 7766 7766 7766 7766 7766 7766	SFBE0 ≪A Strep (FBB4 (FBB5 (FBB6 (FBB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6 (FB6	2 755C7D 005073 7571E2 088CB3 756D6F 407975 6D756C 74696D 756465 000000 000000 000000 000000 000000	80 ke 21 re 10 re 10 ss 57 ss 51 ss 50 sss	ne132,755(788) (urn to mydoom.00506854
771E1080 771E10C0	DNS Rep	ly IP (Default: Current Gatway/DNS):			Start Serv	er		7760	FBE8	000000	00	
771E10D0 771E10E0	# of NXD	OMAIN's: 0	]					77E6 77E6	FBF4	000000	00	~
771E10F0	Selected	Interface: Inter	(R) PRO/1000 MT Network	k Connection V	Stop Sen	er		v <				>
Command:					-							Default 💌

Figure 22 DNS Requests

I I X	0 9 + + 5	¥ 🕴 📰 🔍 Q Q	11							
			-							-
Time	Source	Destination	Protocol	Length Info						
0 111.176904	127.0.0.1	127.0.0.1	DNS	81 Standard query response 0xf5f0 MX	alumni.rice.edu A 192	.168.9.1	1			
1 114.682690	127.0.0.1	127.0.0.1	DNS	59 Standard query 0x18d4 A sonic.net						
2 114.682833	127.0.0.1	127.0.0.1	DNS	75 Standard query response 0x18d4 A	sonic.net A 192.168.9.	1				
3 115.861588	127.0.0.1	127.0.0.1	DNS	59 Standard query 0x6d33 MX cisco.co	•					
4 115.861722	127.0.0.1	127.0.0.1	DNS	75 Standard query response 0x6d33 MX	cisco.com A 192.168.9	.1				
5 115.863244	127.0.0.1	127.0.0.1	DNS	64 Standard query 0x71c1 MX xlist.ag	cs.com					
6 115.863318	127.0.0.1	127.0.0.1	DNS	80 Standard query response 0x71c1 MX	xlist.agcs.com A 192.	168.9.1				
7 126.981463	127.0.0.1	127.0.0.1	DNS	69 Standard query 0xd9db A default.e	xp-tas.com					
8 126.981967	127.0.0.1	127.0.0.1	DNS	85 Standard query response Øxd9db A	default.exp-tas.com A	192.168.	.9.1			
79 128.091659	127.0.0.1	127.0.0.1	DNS	78 Standard query 0x1787 A update.co	de.visualstudio.com					
30 128.091844	127.0.0.1	127.0.0.1	DNS	94 Standard query response 0x1787 A	update.code.visualstud	io.com /	A 192.168.9.1			
31 129.442186	127.0.0.1	127.0.0.1	DNS	72 Standard query 0x0421 A az764295.	vo.msecnd.net					
32 129.442344	127.0.0.1	127.0.0.1	DNS	88 Standard query response 0x0421 A	az764295.vo.msecnd.net	A 192.1	168.9.1			
83 129.468608	127.0.0.1	127.0.0.1	DNS	72 Standard query 0x0421 A az764295.	vo.msecnd.net					
84 129.468746	127.0.0.1	127.0.0.1	DNS	88 Standard query response 0x0421 A	az764295.vo.msecnd.net	A 192.1	168.9.1			
85 130.038960	127.0.0.1	127.0.0.1	DNS	78 Standard query 0x3eb2 A dc.servic	es.visualstudio.com					
86 130.039110	127.0.0.1	127.0.0.1	DNS	94 Standard query response 0x3eb2 A	dc.services.visualstud	io.com #	A 192.168.9.1			
87 130.982190	127.0.0.1	127.0.0.1	DNS	78 Standard query 0xb10d A dc.servic	es.visualstudio.com					
estination Por	:: 52379			^	Null/Loopback					
ength: 57					0 1 1 1 1	111	1 1 1 1 1 1 15	16		
hecksum: 0x69b	[unverified]						East	mily		
Checksum Statu	:: Unverified]						T di	iiiiiy		
Stream index:	26]									
Timestamps]					Internet Protocol	Version 4	4			
DP payload (49	bytes)				0	11	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	16	31	
in Name System	(response)				Version Hea	der L I	offerentiated Services Fi		Total Length	
ransaction ID:	0xf5f0							-	. etai zargai	
lags: 0x8180 5	andard query resp	ponse, No error			1	Identifica	ation	Flags	Fragment Offset	
uestions: 1							153305	1000		
nswer RRs: 1					Time to Liv	/e	Protocol		Header Checksum	
uthority RRs:	,						(25)	2000		
dditional RRs:	0						Source	Address		
Jeries							-			
alumni.rice.e	du: type MX, clas	IS IN					Destinatio	on Addre	55	
swers					-					
equest In: 69					User Datagram P	rotocol				
1me: 0.000062	000 seconds]			~	0	111	1 1 1 1 1 1 1 15	16		

## Figure 23 DNS Packets

# Finding 2: Mass Mailer Algorithm

In the below analysis we can see where the binary calls the PostMessageA API (Figure 24). This call is repeated with each call to ESI, as the dereferenced memory location is loaded to this register on 005030FD.

Analysis		
MyDoom.exe - PID: 5578 - Module: mydoom.exe - Thread: Main Thread 5580 - x32dbg [Elevated]		– a x
File View Debug Trace Plugins Favourites Options Help Aug 23 2019		
		Annual Annual
Graph L2 Log L1 Notes Breakpoints Memory Map Caristack Sch 2 Scht 2 Symbols Source      O05030EF     C3     C3		Handles t' Trace     Hide FPU
consistency     consisten	edi:"LdrpInitializeProcess" edi:"LdrpInitializeProcess"	EAX 00000000 EBX 00000010 ECX 21380000 EDX 00000000 EDX 00000000 EDB 0019438
e 000104C 30 e 0000000 an 35 38115000 mov esi, dword ptr dis:[vd#nottvessageax] e 0000100 53 e 0000100 53 push ebx		ESP 00197A04 ESI 0024C000 EDI 771E69A4 "LdrpInitializeProcess"
e (03)33303 Be L2 public L4 e (03)3107 FF6 cublic est e (03)3100 S3 public est e (03)3100 S3 public est	edi:"LdrpInitializeProcess"	EIP 77280450 ntdl1.77280450 EFLAGS 00000246
OSSIDIC     O	edi:"LdrpInitializeProcess"	6 F 0 FF 0 0F 0 CF 0 TF 0 IF 1
e 00501112 53 push ebx e 00501113 66 02 push 2 e 0050113 55 57 push edi e 0050115 57 push edi	edi:"LdrpInitializeProcess"	LastError 00000000 (ERROR_SUCCESS) LastEratus CO000034 (STATUS_DBJECT_NAME_NOT_FOUND) GS 0028 FS 0053
e 00503118 Costal10 Se pop est pop edi pop edi pop est	edi:"LdrpInitializeProcess"	ES 002B DS 002B CS 0023 SS 002B
00000110         C3         Carbon           00000110         5405         54115000         Putch est (duard ptr ds: [dafredetindowde)]           00000123         64.000         Putch mydoom.5011A8           00000124         64.4115000         Putch mydoom.5011A8           00000125         64.4115000         Putch mydoom.5011A8           00000126         506         Putch mydoom.5012A8           00000127         506         Putch mydoom.500200	5011A8:"rctrl_renwnd32"	\$T(0)         000000000000000000000000000000000000
e 00593333 65.00 pc/sh 0 e 00593135 65 9c115000 pc/sh 0 e 00593136 FFD6 Call est e 0059313.C 50 pc/sh 0 pc/sh 0 call est	50119C:"ATH_Note"	x87TagWord FFFF x87Tw_0 3 (Empty) x87Tw_1 3 (Empty) x87Tw_2 3 (Empty) x87Tw_3 3 (Empty)
		> Default (stdcal)
Jump 15 taken myddom.05030119 : text:005030FA myddom.exe:\$30FA #24FA		1: esp+4] 77166944 "udrpInitial1zeProcess" 2: esp+8] 0024C000 3: esp+6] 0000010 4: esp+6] 00290656
🐖 Dump 1 🗰 Dump 2 🐖 Dump 3 🐖 Dump 4 🐖 Dump 5 👹 Watch 1 🖂 Locals 🤌 Struct	0019FA04 0019FA08	4592067E 771E69A4 "LdrpInitializeProcess"
Address   Mex   Me	<ul> <li>0019FADC</li> <li>0019FA10</li> <li>0019FA14</li> <li>0019FA18</li> <li>0019FA18</li> <li>0019FA20</li> <li>0019FA20</li> <li>0019FA26</li> <li>0019FA28</li> <li>0019FA28</li> <li>0019FA28</li> <li>0019FA20</li> </ul>	0026000 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 0052056 005205 005205 005205 005205 005205 005205 005205 005205 005205 005205 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00520 00500 00500 00500 00500 00500 00500 00500 00500 00500 00500 00500 00500 00500 00500 005000 005000 005000000
77141040         10         12         00         10         01         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00         <	(01) 9F A30           (01) 9F A34           (01) 9F A36           (01) 9F A3C           (01) 9F A3C           (01) 9F A3C           (01) 9F A3C           (01) 9F A40           (01) 9F A48	**728850         return to mtdll.7228563 from ntdll.7228424           00000000         Forefreere           00000000         ************************************
Command:		Default 🔻
Paused Breakpoint at 00503116 set!		Time Wasted Debugging: 0:10:38:31

Figure 24 PostMessageA Debug

# CONCLUSION

# **Potential Danger**

The MyDoom malware has successfully been used in email phishing campaigns as well as distributed denial of service attacks against large enterprises. Once a host is infected, the malware configures itself to launch automatically and can use a significant number of resources attempting to replicate. This can cause the local host to slow down, and some variants will additionally lock files to cause even more damage to the host. Additionally, a backdoor is created that can be later used to deliver more malware or command affected hosts to attack another organization.

# Malware Removal

The easiest way to detect and remove the MyDoom malware is to ensure your host has up to date antivirus software. Due to the age of this malware, most software will detect the hash, or signature of the file, as malicious. However, if the file is launched, it maintains persistence by modifying the registry and file system. System administrators should delete any unknown or suspicious startup tasks as well as the registry keys added from the RegShot Analysis.

It is important to note that this malware is typically delivered via social engineering techniques. With these types of attacks, prevention is key. To properly mitigate against this malware, a robust security awareness program should be implemented alongside signature-based detection.



1. Strings

- 2. FLOSS
- 3. UPX
- 4. PE View
- 5. PEiD
- 6. Resource Hacker
- 7. Virus Total
- 8. Ida Pro
- 9. RegShot
- 10. Process Monitor
- 11. ApateDNS
- 12. Netstat
- 13. Wireshark
- 14. X32Debug

# APPENDIX B – REFERENCES

1. <u>MyDoom Wikipedia</u>

- <u>https://www.f-secure.com/v-descs/novarg.shtml</u>
- 3. https://www.youtube.com/watch?v=cRH-khasTfg