

ID: 626597
Sample Name: Malware
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 15:12:04
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Linux Analysis Report Malware 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Analysis Advice 3
General Information 3
Runtime Messages 3
Process Tree 4
Yara Signatures 4
Initial Sample 4
Memory Dumps 4
Snort Signatures 4
Joe Sandbox Signatures 4
AV Detection 4
Mitre Att&ck Matrix 4
Malware Configuration 5
Behavior Graph 5
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 5
Domains 5
URLs 6
Domains and IPs 6
Contacted Domains 6
World Map of Contacted IPs 6
Public IPs 6
Joe Sandbox View / Context 6
IPs 6
Domains 6
ASNs 6
JA3 Fingerprints 7
Dropped Files 7
Created / dropped Files 7
Static File Info 7
General 7
Static ELF Info 7
ELF header 7
Sections 7
Program Segments 8
Dynamic Tags 8
Symbols 9
Network Behavior 14
Network Port Distribution 14
TCP Packets 14
System Behavior 14
Analysis Process: Malware PID: 6222, Parent PID: 6125 14
General 14
File Activities 14
File Read 14

Copyright Joe Security LLC 2022

Linux Analysis Report

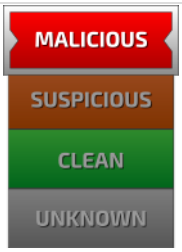
Malware

Overview

General Information

Sample Name:	Malware
Analysis ID:	626597
MD5:	686a654a185db3.
SHA1:	fe3168d630ccb6…
SHA256:	74ef6cc38f5a1a8..
Tags:	BFPDoor elf
Infos:	YARA

Detection

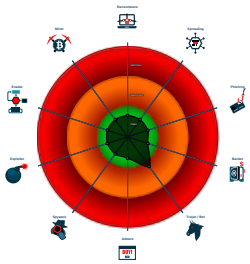


Score:	52
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Machine Learning detection for sam…
- Tries to connect to HTTP servers, b…
- Yara signature match

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. The sample is likely an old dropper which does no longer work.

Non-zero exit code suggests an error during the execution. Lookup the error code for hints.

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626597
Start date and time: 14/05/202215:12:04	2022-05-14 15:12:04 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Malware
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal52.lin@0/0@0/0

Runtime Messages

Command:	/tmp/Malware
PID:	6222
Exit Code:	1
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	/tmp/Malware: /lib/x86_64-linux-gnu/libc.so.6: version `GLIBC_2.34' not found (required by /tmp/Malware)

Copyright Joe Security LLC 2022

Process Tree

- **system is lnxubuntu20**
  - Malware (PID: 6222, Parent: 6125, MD5: 686a654a185db3f40514966d1409b2b1) Arguments: /tmp/Malware
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Malware	APT_MAL_LNX_RedMenshen_BPFDoor_Controller_May22_3	Detects BPFDoor implants used by Chinese actor Red Menshen	Florian Roth	• 0x6080:$s1: hald-addon-acpi: listening on acpi kernel interface /proc/acpi/event • 0x6035:$s2: /sbin/mingetty /dev • 0x60e6:$s3: pickup -l -t fifo -u
Malware	APT_MAL_LNX_RedMenshen_BPFDoor_Controller_Generic_May22_1	Detects BPFDoor malware	Florian Roth	• 0x2865:$op1: C6 80 01 01 00 00 00 48 8B 45 D8 0F B6 90 01 01 00 00 48 8B 45 D8 88 90 00 01 00 00 C6 45 F6 00 0F B6 45 F6 88 45 • 0x2861:$op5: 48 8B 45 D8 C6 80 01 01 00 00 00 48 8B 45 D8 0F B6 90 01 01 00 00 48 8B 45 D8 88 90 00 01 00 00 C6 45 F6 00 0F B6 45

Memory Dumps

Source	Rule	Description	Author	Strings
6222.1.00000000517089bc.000000004d171c55.rw-.sdmp	APT_MAL_LNX_RedMenshen_BPFDoor_Controller_May22_3	Detects BPFDoor implants used by Chinese actor Red Menshen	Florian Roth	• 0x80:$s1: hald-addon-acpi: listening on acpi kernel interface /proc/acpi/event • 0x35:$s2: /sbin/mingetty /dev • 0xe6:$s3: pickup -l -t fifo -u

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Mitre Att&ck Matrix

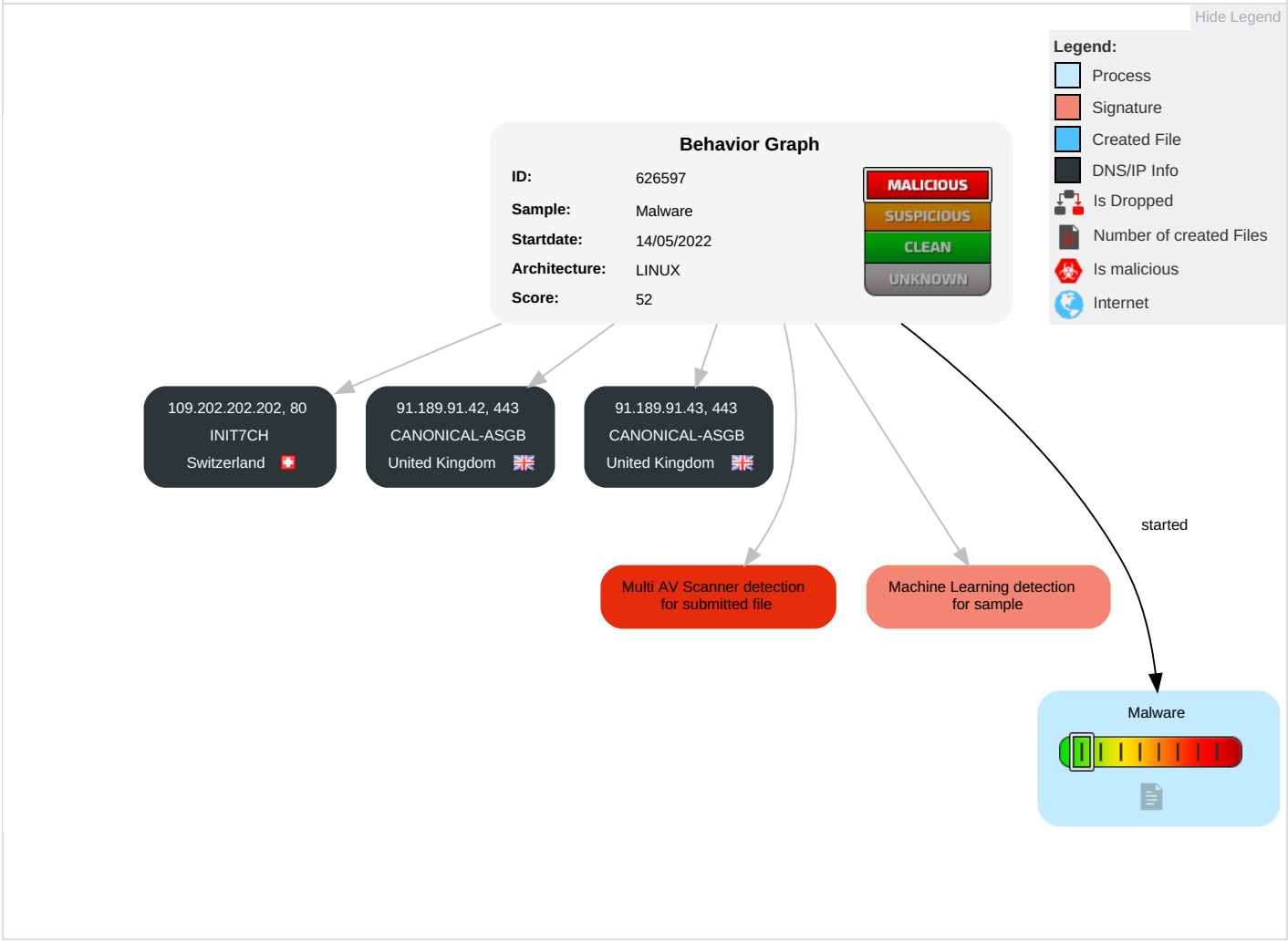
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Copyright Joe Security LLC 2022

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Malware	40%	Virustotal		Browse
Malware	46%	ReversingLabs	Linux.Backdoor.Bpfdoor	
Malware	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

Copyright Joe Security LLC 2022

URLs

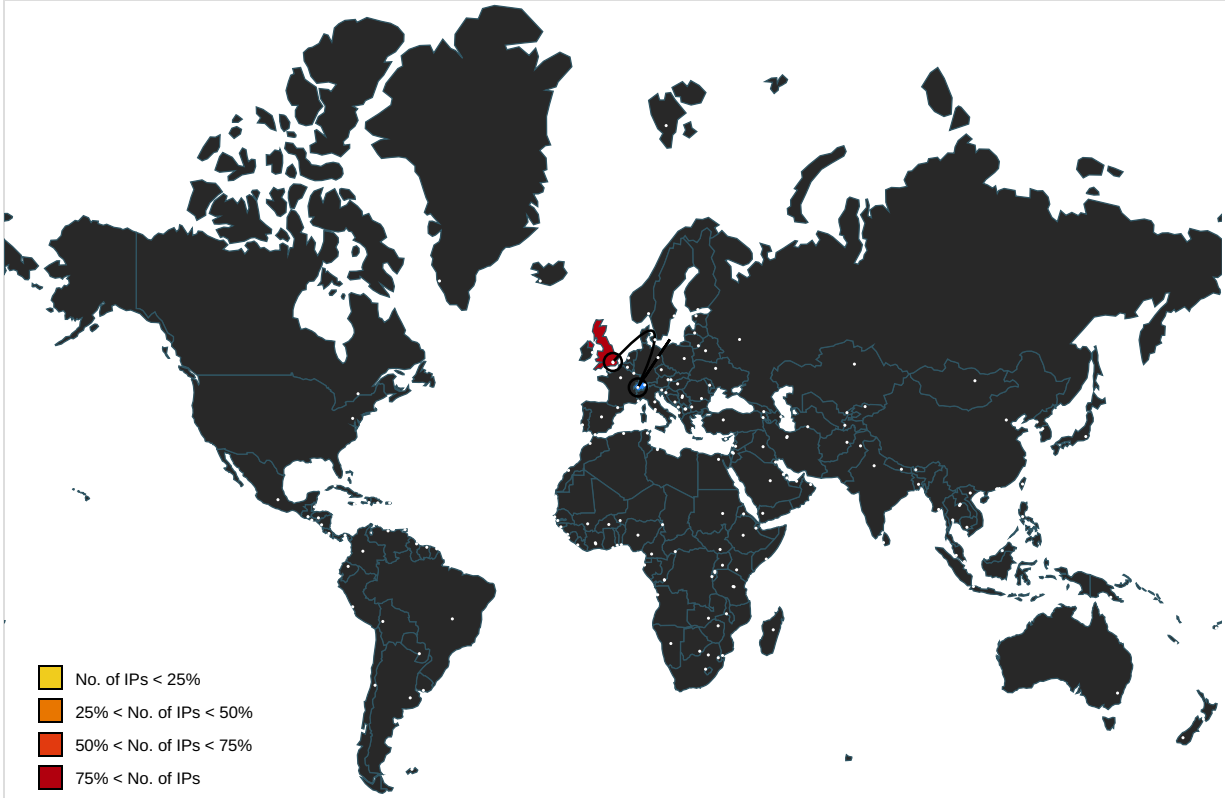
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	false
91.189.91.42	unknown	United Kingdom		41231	CANONICAL-ASGB	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

Copyright Joe Security LLC 2022

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=baa0c7d6b74504b26c1eef16043a52af235bbac1, for GNU/Linux 3.2.0, not stripped
Entropy (8bit):	3.988288057662513
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 49.77% • ELF Executable and Linkable format (generic) (4004/1) 49.46% • Lumena CEL bitmap (63/63) 0.78%
File name:	Malware
File size:	35704
MD5:	686a654a185db3f40514966d1409b2b1
SHA1:	fe3168d630ccb61559c06b6b0ab68d5cfa1c1a8f
SHA256:	74ef6cc38f5a1a80148752b63c117e6846984debd2af806c65887195a8eccc56
SHA512:	def8ba24db0072def2bcc208c1fc01ad54f1ce9321d23d42352df0b6f73fe2a3f31942bccae24aae2097d212644acae7f28512cc63123b408f5351e31e9dfbe1
SSDEEP:	768:DvqoAYwIg4QoAYwIg4QbTLD7zrjbTLD7zrjbTLD7zrjbTLD7zrjOm+Wu0jIEYvA+:DgTpzJ
TLSH:	10F2841EF391CE3CC8C9A2312ECBD5705170B0B4AB32211B379167BB3AA679D5979E11
File Content Preview:	.ELF.....>.....'.....@.....@.8...@.....@.....@.....@..... ....

Static ELF Info

ELF header

Class:	ELF64
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Advanced Micro Devices X86-64
Version Number:	0x1
Type:	DYN (Shared object file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x2700
Flags:	0x0
ELF Header Size:	64
Program Header Offset:	64
Program Header Size:	56
Number of Program Headers:	13
Section Header Offset:	33720
Section Header Size:	64
Number of Section Headers:	31
Header String Table Index:	30

Sections

Copyright Joe Security LLC 2022

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.interp	PROGBITS	0x318	0x318	0x1c	0x0	0x2	A	0	0	1
.note.gnu.property	NOTE	0x338	0x338	0x30	0x0	0x2	A	0	0	8
.note.gnu.build-id	NOTE	0x368	0x368	0x24	0x0	0x2	A	0	0	4
.note.ABI-tag	NOTE	0x38c	0x38c	0x20	0x0	0x2	A	0	0	4
.gnu.hash	GNU_HASH	0x3b0	0x3b0	0x34	0x0	0x2	A	6	0	8
.dynsym	DYNSYM	0x3e8	0x3e8	0x5e8	0x18	0x2	A	7	1	8
.dynstr	STRTAB	0x9d0	0x9d0	0x21c	0x0	0x2	A	0	0	1
.gnu.version	VERSYM	0xbec	0xbec	0x7e	0x2	0x2	A	6	0	2
.gnu.version_r	VERNEED	0xc70	0xc70	0x50	0x0	0x2	A	7	1	8
.rela.dyn	RELA	0xcc0	0xcc0	0xd8	0x18	0x2	A	6	0	8
.rela.plt	RELA	0xd98	0xd98	0x510	0x18	0x42	AI	6	24	8
.init	PROGBITS	0x2000	0x2000	0x1b	0x0	0x6	AX	0	0	4
.plt	PROGBITS	0x2020	0x2020	0x370	0x10	0x6	AX	0	0	16
.plt.got	PROGBITS	0x2390	0x2390	0x10	0x10	0x6	AX	0	0	16
.plt.sec	PROGBITS	0x23a0	0x23a0	0x360	0x10	0x6	AX	0	0	16
.text	PROGBITS	0x2700	0x2700	0x2962	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x5064	0x5064	0xd	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x6000	0x6000	0x156	0x0	0x2	A	0	0	8
.eh_frame_hdr	PROGBITS	0x6158	0x6158	0xfc	0x0	0x2	A	0	0	4
.eh_frame	PROGBITS	0x6258	0x6258	0x3c0	0x0	0x2	A	0	0	8
.init_array	INIT_ARRAY	0x7c10	0x6c10	0x8	0x8	0x3	WA	0	0	8
.fini_array	FINI_ARRAY	0x7c18	0x6c18	0x8	0x8	0x3	WA	0	0	8
.dynamic	DYNAMIC	0x7c20	0x6c20	0x1f0	0x10	0x3	WA	7	0	8
.got	PROGBITS	0x7e10	0x6e10	0x1f0	0x8	0x3	WA	0	0	8
.data	PROGBITS	0x8000	0x7000	0x10	0x0	0x3	WA	0	0	8
.bss	NOBITS	0x8020	0x7010	0x4c8	0x0	0x3	WA	0	0	32
.comment	PROGBITS	0x0	0x7010	0x26	0x1	0x30	MS	0	0	1
.symtab	SYMTAB	0x0	0x7038	0xba0	0x18	0x0		29	24	8
.strtab	STRTAB	0x0	0x7bd8	0x6c1	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x8299	0x11a	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
PHDR	0x40	0x40	0x40	0x2d8	0x2d8	1.4984	0x4	R	0x8		
INTERP	0x318	0x318	0x318	0x1c	0x1c	3.9408	0x4	R	0x1	/lib64/ld-linux-x86-64.so.2	.interp
LOAD	0x0	0x0	0x0	0x12a8	0x12a8	2.2135	0x4	R	0x1000		.interp .note.gnu.property .note.gnu.build-id .note.ABI-tag .gnu.hash .dynsym .dynstr .gnu.version .gnu.version_r .rela.dyn .rela.plt
LOAD	0x2000	0x2000	0x2000	0x3071	0x3071	2.7806	0x5	R E	0x1000		.init .plt .plt.got .plt.sec .text .fini
LOAD	0x6000	0x6000	0x6000	0x618	0x618	3.9149	0x4	R	0x1000		.rodata .eh_frame_hdr .eh_frame
LOAD	0x6c10	0x7c10	0x7c10	0x400	0x8d8	1.2825	0x6	RW	0x1000		.init_array .fini_array .dynamic .got .data .bss
DYNAMIC	0x6c20	0x7c20	0x7c20	0x1f0	0x1f0	1.1215	0x6	RW	0x8		.dynamic
NOTE	0x338	0x338	0x338	0x30	0x30	1.6272	0x4	R	0x8		.note.gnu.property
NOTE	0x368	0x368	0x368	0x44	0x44	2.4132	0x4	R	0x4		.note.gnu.build-id .note.ABI-tag
LOOS+474e553	0x338	0x338	0x338	0x30	0x30	1.6272	0x4	R	0x8		.note.gnu.property
GNU_EH_FRAME	0x6158	0x6158	0x6158	0xfc	0xfc	2.0044	0x4	R	0x4		.eh_frame_hdr
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x10		
GNU_RELRO	0x6c10	0x7c10	0x7c10	0x3f0	0x3f0	1.2909	0x4	R	0x1		.init_array .fini_array .dynamic .got

Dynamic Tags

Type	Meta	Value	Tag
DT_NEEDED	sharedlib	libc.so.6	0x1
DT_INIT	value	0x2000	0xc
DT_FINI	value	0x5064	0xd
DT_INIT_ARRAY	value	0x7c10	0x19
DT_INIT_ARRAYSZ	bytes	8	0x1b
DT_FINI_ARRAY	value	0x7c18	0x1a
DT_FINI_ARRAYSZ	bytes	8	0x1c
DT_GNU_HASH	value	0x3b0	0x6ffffef5
DT_STRTAB	value	0x9d0	0x5
DT_SYMTAB	value	0x3e8	0x6
DT_STRSZ	bytes	540	0xa
DT_SYMENT	bytes	24	0xb
DT_DEBUG	value	0x0	0x15
DT_PLTGOT	value	0x7e10	0x3
DT_PLTRELSZ	bytes	1296	0x2
DT_PLTREL	pltrel	DT_RELA	0x14
DT_JMPREL	value	0xd98	0x17
DT_RELA	value	0xcc0	0x7
DT_RELASZ	bytes	216	0x8
DT_RELAENT	bytes	24	0x9
DT_FLAGS	value	0x8	0x1e
DT_FLAGS_1	value	0x8000001	0x6ffffffb
DT_VERNEED	value	0xc70	0x6ffffffe
DT_VERNEEDNUM	value	1	0x6fffffff
DT_VERSYM	value	0xbec	0x6ffffff0
DT_RELACOUNT	value	3	0x6ffffff9
DT_NULL	value	0x0	0x0

Symbols

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
			.dynsym	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
_ITM_deregisterTMCloneTable			.dynsym	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
_ITM_registerTMCloneTable			.dynsym	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
__cxa_atexit	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
__cxa_finalize	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
__environ	GLIBC_2.2.5	libc.so.6	.dynsym	0x8020	8	OBJECT	<unknown>	DEFAULT	26
__gmon_start__			.dynsym	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
__libc_start_main	GLIBC_2.34	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
__stack_chk_fail	GLIBC_2.4	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
_environ	GLIBC_2.2.5	libc.so.6	.dynsym	0x8020	8	OBJECT	<unknown>	DEFAULT	26
_exit	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
accept	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
access	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
bind	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
chdir	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
close	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
connect	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF

Copyright Joe Security LLC 2022

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
dup2	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
environ	GLIBC_2.2.5	libc.so.6	.dynsym	0x8020	8	OBJECT	<unknown>	DEFAULT	26
execve	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
exit	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
fork	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
free	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
getpid	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
getuid	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
grantpt	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
htons	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
inet_ntoa	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
ioctl	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
kill	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
listen	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
malloc	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
memchr	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
memcmp	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
memcpy	GLIBC_2.14	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
memset	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
ntohs	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
open	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
prctl	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
ptsname	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
rand	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
read	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
recvfrom	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
select	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
sendto	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
setsid	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
setsockopt	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
signal	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
sleep	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
snprintf	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
socket	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
srand	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF

Copyright Joe Security LLC 2022

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
strcpy	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
strlen	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
strncpy	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
system	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
time	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
unlink	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
unlockpt	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
utimes	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
vhangup	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
waitpid	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
write	GLIBC_2.2.5	libc.so.6	.dynsym	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
Red Menshen BPFDoor Source Code( ).c	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
Scrt1.o	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
_DYNAMIC	GLIBC_2.2.5	libc.so.6	.symtab	0x7c20	0	OBJECT	<unknown>	DEFAULT	23
_GLOBAL_OFFSET_TABLE_	GLIBC_2.2.5	libc.so.6	.symtab	0x7e10	0	OBJECT	<unknown>	DEFAULT	24
_IO_stdin_used			.symtab	0x6000	4	OBJECT	<unknown>	DEFAULT	18
_ITM_deregisterTMCloneTable			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
_ITM_registerTMCloneTable			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
__FRAME_END__	GLIBC_2.2.5	libc.so.6	.symtab	0x6614	0	OBJECT	<unknown>	DEFAULT	20
__GNU_EH_FRAME_HDR	GLIBC_2.2.5	libc.so.6	.symtab	0x6158	0	NOTYPE	<unknown>	DEFAULT	19
__TMC_END__			.symtab	0x8010	0	OBJECT	<unknown>	HIDDEN	25
__abi_tag	GLIBC_2.2.5	libc.so.6	.symtab	0x38c	32	OBJECT	<unknown>	DEFAULT	4
__bss_start			.symtab	0x8010	0	NOTYPE	<unknown>	DEFAULT	26
__cxa_atexit@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
__cxa_finalize@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
__data_start			.symtab	0x8000	0	NOTYPE	<unknown>	DEFAULT	25
__do_global_dtors_aux			.symtab	0x27a0	0	FUNC	<unknown>	DEFAULT	16
__do_global_dtors_aux_fini_array_entry	GLIBC_2.2.5	libc.so.6	.symtab	0x7c18	0	OBJECT	<unknown>	DEFAULT	22
__dso_handle			.symtab	0x8008	0	OBJECT	<unknown>	HIDDEN	25
__environ@GLIBC_2.2.5			.symtab	0x8020	8	OBJECT	<unknown>	DEFAULT	26
__frame_dummy_init_array_entry	GLIBC_2.2.5	libc.so.6	.symtab	0x7c10	0	OBJECT	<unknown>	DEFAULT	21
__gmon_start__			.symtab	0x0	0	NOTYPE	<unknown>	DEFAULT	SHN_UNDEF
__libc_start_main@GLIBC_2.34	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
__stack_chk_fail@GLIBC_2.4	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
_edata	GLIBC_2.2.5	libc.so.6	.symtab	0x8010	0	NOTYPE	<unknown>	DEFAULT	25
_end			.symtab	0x84e8	0	NOTYPE	<unknown>	DEFAULT	26
_exit@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
_fini	GLIBC_2.2.5	libc.so.6	.symtab	0x5064	0	FUNC	<unknown>	HIDDEN	17
_init			.symtab	0x2000	0	FUNC	<unknown>	HIDDEN	12
_start			.symtab	0x2700	38	FUNC	<unknown>	DEFAULT	16
accept@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF

Copyright Joe Security LLC 2022

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
access@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
argv0			.symtab	0x82b8	8	OBJECT	<unknown>	DEFAULT	26
atexit	GLIBC_2.2.5	libc.so.6	.symtab	0x5050	18	FUNC	<unknown>	DEFAULT	16
b	GLIBC_2.2.5	libc.so.6	.symtab	0x3e90	262	FUNC	<unknown>	DEFAULT	16
bind@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
cfg	GLIBC_2.2.5	libc.so.6	.symtab	0x8040	548	OBJECT	<unknown>	DEFAULT	26
chdir@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
close@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
completed.0	GLIBC_2.2.5	libc.so.6	.symtab	0x8028	1	OBJECT	<unknown>	DEFAULT	26
connect@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
cread	GLIBC_2.2.5	libc.so.6	.symtab	0x2a99	96	FUNC	<unknown>	DEFAULT	16
crtstuff.c	GLIBC_2.34	libc.so.6	.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
crtstuff.c	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FILE	<unknown>	DEFAULT	SHN_ABS
crypt_ctx			.symtab	0x82c0	258	OBJECT	<unknown>	DEFAULT	26
cwrite	GLIBC_2.2.5	libc.so.6	.symtab	0x29fb	158	FUNC	<unknown>	DEFAULT	16
data_start	GLIBC_2.14	libc.so.6	.symtab	0x8000	0	NOTYPE	<unknown>	DEFAULT	25
decrypt_ctx	GLIBC_2.2.5	libc.so.6	.symtab	0x83e0	258	OBJECT	<unknown>	DEFAULT	26
deregister_tm_clones	GLIBC_2.2.5	libc.so.6	.symtab	0x2730	0	FUNC	<unknown>	DEFAULT	16
dup2@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
environ@GLIBC_2.2.5			.symtab	0x8020	8	OBJECT	<unknown>	DEFAULT	26
execve@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
exit@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
fork@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
frame_dummy	GLIBC_2.2.5	libc.so.6	.symtab	0x27e0	0	FUNC	<unknown>	DEFAULT	16
free@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
getpid@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
getshell			.symtab	0x4003	1065	FUNC	<unknown>	DEFAULT	16
getuid@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
godpid	GLIBC_2.2.5	libc.so.6	.symtab	0x826c	4	OBJECT	<unknown>	DEFAULT	26
grantpt@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
htons@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
inet_ntoa@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
init_signal	GLIBC_2.2.5	libc.so.6	.symtab	0x2bc8	46	FUNC	<unknown>	DEFAULT	16
ioctl@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
kill@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
listen@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
logon			.symtab	0x352c	142	FUNC	<unknown>	DEFAULT	16
main			.symtab	0x4d23	800	FUNC	<unknown>	DEFAULT	16
malloc@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
memchr@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
memcmp@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
memcpy@GLIBC_2.14			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
memset@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF

Copyright Joe Security LLC 2022

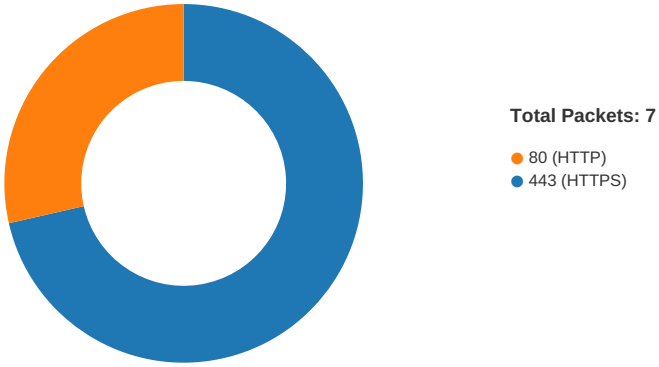
Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
mon	GLIBC_2.2.5	libc.so.6	.symtab	0x2ede	212	FUNC	<unknown>	DEFAULT	16
ntohs@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
on_terminate	GLIBC_2.4	libc.so.6	.symtab	0x2bb1	23	FUNC	<unknown>	DEFAULT	16
open@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
open_tty	GLIBC_2.2.5	libc.so.6	.symtab	0x2dad	125	FUNC	<unknown>	DEFAULT	16
packet_loop			.symtab	0x35ba	2262	FUNC	<unknown>	DEFAULT	16
pid_path			.symtab	0x8280	50	OBJECT	<unknown>	DEFAULT	26
prctl@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
ptsname@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
pty	GLIBC_2.2.5	libc.so.6	.symtab	0x8264	4	OBJECT	<unknown>	DEFAULT	26
ptym_open			.symtab	0x2c30	201	FUNC	<unknown>	DEFAULT	16
ptys_open			.symtab	0x2cf9	180	FUNC	<unknown>	DEFAULT	16
rand@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
rc4			.symtab	0x28f9	258	FUNC	<unknown>	DEFAULT	16
rc4_init			.symtab	0x281d	220	FUNC	<unknown>	DEFAULT	16
read@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
recvfrom@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
register_tm_clones	GLIBC_2.2.5	libc.so.6	.symtab	0x2760	0	FUNC	<unknown>	DEFAULT	16
remove_pid	GLIBC_2.2.5	libc.so.6	.symtab	0x2af9	31	FUNC	<unknown>	DEFAULT	16
select@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
sendto@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
set_proc_name	GLIBC_2.2.5	libc.so.6	.symtab	0x2fb2	615	FUNC	<unknown>	DEFAULT	16
setsid@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
setsockopt@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
setup_time	GLIBC_2.2.5	libc.so.6	.symtab	0x2b18	105	FUNC	<unknown>	DEFAULT	16
shell			.symtab	0x442c	2295	FUNC	<unknown>	DEFAULT	16
sig_child			.symtab	0x2bf6	58	FUNC	<unknown>	DEFAULT	16
signal@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
sleep@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
snprintf@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
socket@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
srand@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
strcpy@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
strlen@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
strncpy@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
system@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
terminate	GLIBC_2.2.5	libc.so.6	.symtab	0x2b81	48	FUNC	<unknown>	DEFAULT	16
time@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
to_open			.symtab	0x3219	787	FUNC	<unknown>	DEFAULT	16
try_link	GLIBC_2.2.5	libc.so.6	.symtab	0x2e2a	180	FUNC	<unknown>	DEFAULT	16
tty	GLIBC_2.2.5	libc.so.6	.symtab	0x8268	4	OBJECT	<unknown>	DEFAULT	26
unlink@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
unlockpt@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF

Copyright Joe Security LLC 2022

Name	Version Info Name	Version Info File Name	Section Name	Value	Size	Symbol Type	Symbol Bind	Symbol Visibility	Ndx
utimes@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
vhangup@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
w			.symtab	0x3f96	109	FUNC	<unknown>	DEFAULT	16
waitpid@GLIBC_2.2.5			.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
write@GLIBC_2.2.5	GLIBC_2.2.5	libc.so.6	.symtab	0x0	0	FUNC	<unknown>	DEFAULT	SHN_UNDEF
xchg			.symtab	0x27e9	52	FUNC	<unknown>	DEFAULT	16

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: Malware PID: **6222**, Parent PID: **6125**

General

Start time:	15:12:52
Start date:	14/05/2022
Path:	/tmp/Malware
Arguments:	/tmp/Malware
File size:	35704 bytes
MD5 hash:	686a654a185db3f40514966d1409b2b1

File Activities

File Read