ID: 635907
Sample Name: x86
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 06:58:45
Date: 30/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Linux Analysis Report x86 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Analysis Advice 3
General Information 3
Warnings 3
Runtime Messages 3
Process Tree 4
Yara Signatures 4
PCAP (Network Traffic) 4
Snort Signatures 4
Joe Sandbox Signatures 4
AV Detection 4
Networking 4
Hooking and other Techniques for Hiding and Protection 4
Stealing of Sensitive Information 4
Remote Access Functionality 4
Mitre Att&ck Matrix 4
Malware Configuration 5
Behavior Graph 5
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 6
Dropped Files 6
Domains 6
URLs 6
Domains and IPs 6
Contacted Domains 6
World Map of Contacted IPs 6
Public IPs 6
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 10
General 10
Static ELF Info 10
ELF header 10
Sections 10
Program Segments 10
Network Behavior 11
Network Port Distribution 11
TCP Packets 11
System Behavior 11
Analysis Process: x86 PID: 6221, Parent PID: 6129 11
General 11
Analysis Process: x86 PID: 6222, Parent PID: 6221 11
General 11
Analysis Process: x86 PID: 6223, Parent PID: 6221 11
General 11
Analysis Process: x86 PID: 6225, Parent PID: 6223 11
General 12
File Activities 12
File Read 12
Analysis Process: x86 PID: 6233, Parent PID: 6225 12
General 12
Analysis Process: x86 PID: 6234, Parent PID: 6233 12
General 12
Analysis Process: x86 PID: 6226, Parent PID: 6223 12
General 12
Analysis Process: x86 PID: 6227, Parent PID: 6226 12
General 12

Linux Analysis Report

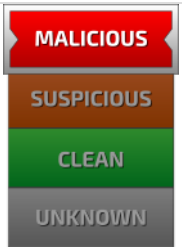
x86

Overview

General Information

Sample Name:	x86
Analysis ID:	635907
MD5:	bef642eeed970f7.
SHA1:	baaa1dc20118f9..
SHA256:	10f35885f96f694..
Infos:	

Detection



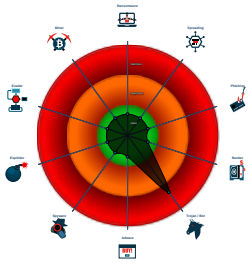
Mirai

Score:	64
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Mirai
- Machine Learning detection for sam…
- Uses known network protocols on n…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…
- Sample has stripped symbol table

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.

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635907
Start date and time: 30/05/202206:58:45	2022-05-30 06:58:45 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	x86
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:	mal64.troj.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/x86
PID:	6221
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	''
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- x86 (PID: 6221, Parent: 6129, MD5: bef642eeed970f7c3ee944a513ea4c88) Arguments: /tmp/x86
  - x86 New Fork (PID: 6222, Parent: 6221)
  - x86 New Fork (PID: 6223, Parent: 6221)
    - x86 New Fork (PID: 6225, Parent: 6223)
      - x86 New Fork (PID: 6233, Parent: 6225)
        - x86 New Fork (PID: 6234, Parent: 6233)
    - x86 New Fork (PID: 6226, Parent: 6223)
      - x86 New Fork (PID: 6227, Parent: 6226)
- **cleanup**

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Uses known network protocols on non-standard ports

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

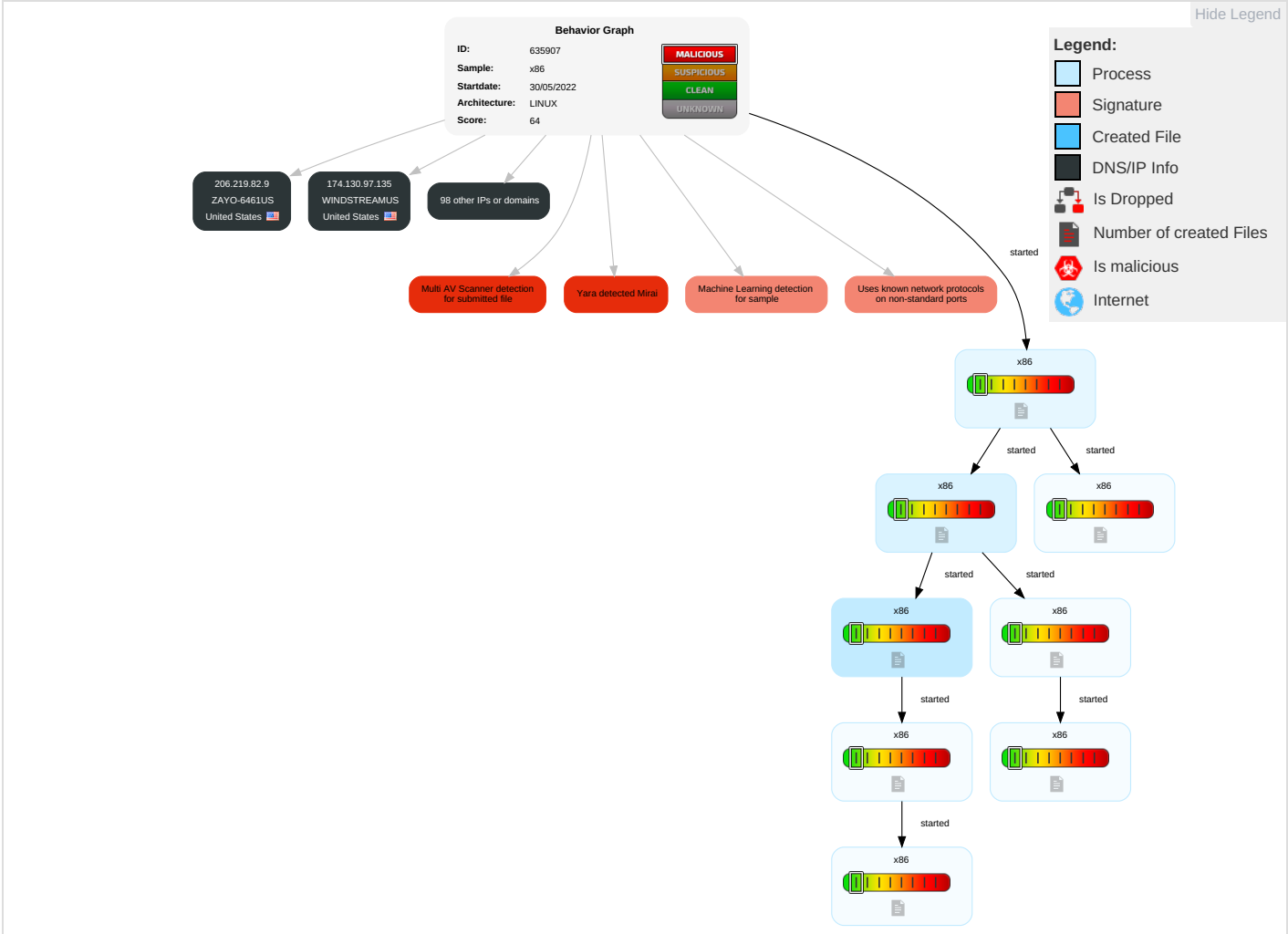
Mitre Att&ck Matrix

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 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
x86	46%	Virustotal		Browse
x86	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

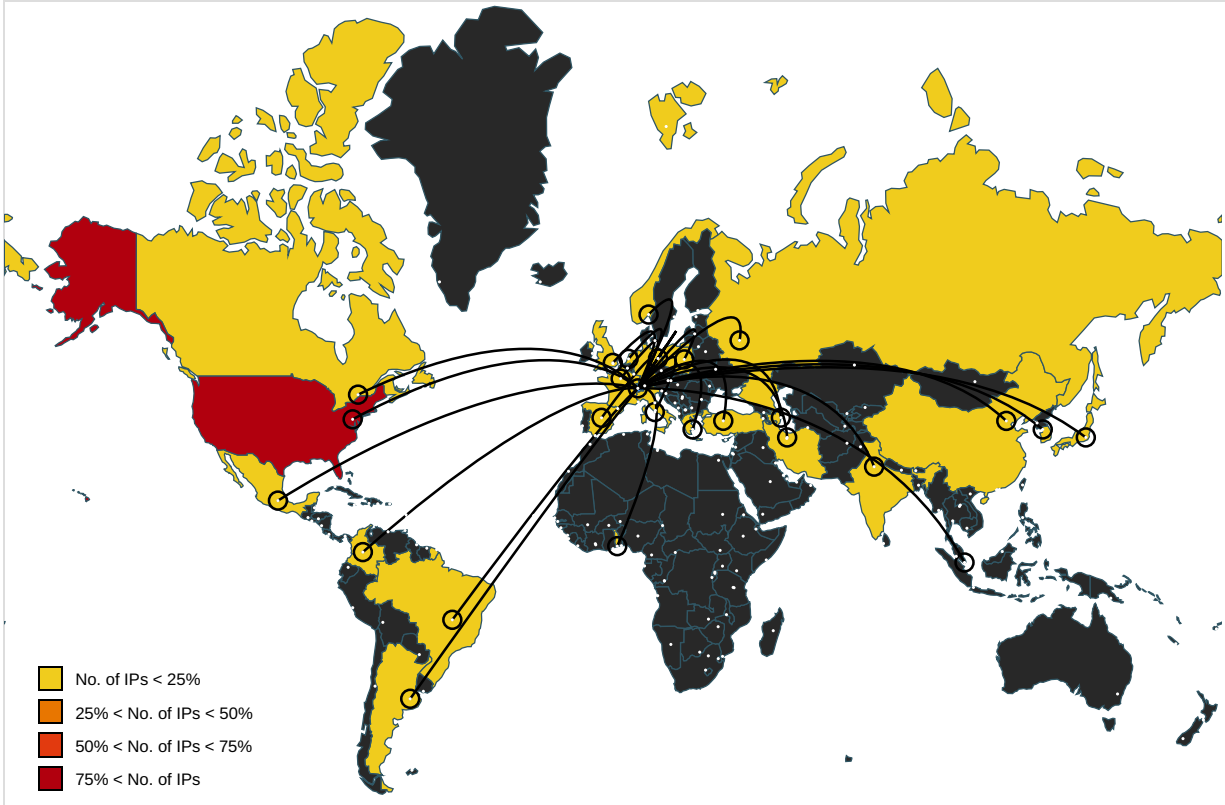
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
71.82.186.46	unknown	United States		20115	CHARTER-20115US	false
8.188.166.156	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
222.18.102.174	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
163.69.133.211	unknown	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
161.199.170.152	unknown	United States		27311	AS27311US	false
97.195.248.46	unknown	United States		6167	CELLCO-PARTUS	false
167.127.239.68	unknown	United States		11520	ALLSTATE-INSURANCE-COUS	false
115.107.38.68	unknown	China		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	false
173.66.71.180	unknown	United States		701	UUNETUS	false
24.45.250.77	unknown	United States		6128	CABLE-NET-1US	false
92.184.111.45	unknown	France		3215	FranceTelecom-OrangeFR	false
61.106.99.55	unknown	Korea Republic of		17839	DREAMPLUS-AS-KRLGHelloVisionCorpKR	false
98.112.164.94	unknown	United States		7018	ATT-INTERNET4US	false
223.217.50.228	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
112.183.28.110	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
183.23.36.205	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
161.145.179.44	unknown	United States		263740	CorporacionLaceibanetsocietyHN	false
171.188.4.179	unknown	United States		9874	STARHUB-MOBILEStarHubLtdSG	false
66.126.55.147	unknown	United States		22352	APPLIED-TECHNOLOGYUS	false
206.219.82.9	unknown	United States		6461	ZAYO-6461US	false
1.68.163.174	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
141.89.138.125	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
139.182.115.224	unknown	United States		2152	CSUNET-NWUS	false
63.100.146.131	unknown	United States		701	UUNETUS	false
116.40.101.173	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
166.111.47.118	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
73.99.131.134	unknown	United States		7922	COMCAST-7922US	false
71.75.173.83	unknown	United States		11426	TWC-11426-CAROLINASUS	false
20.231.62.15	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
220.79.231.181	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
130.146.219.140	unknown	Netherlands		6908	DATAHOPDatahop-SixDegreesGB	false
18.252.179.134	unknown	United States		16509	AMAZON-02US	false
174.130.97.135	unknown	United States		7029	WINDSTREAMUS	false
168.5.246.18	unknown	United States		8	RICE-ASUS	false
103.223.165.48	unknown	China		135445	IDNIC-AIRPAY-AS-IDPTAirpayInternationalIndonesiaID	false
63.202.183.61	unknown	United States		7018	ATT-INTERNET4US	false
196.170.140.141	unknown	Togo		24691	TOGOTEL-ASTogoTelecomTogoTG	false
181.45.1.154	unknown	Argentina		27747	TelecentroSAAR	false
206.9.140.116	unknown	United States		5006	VOYANTUS	false
109.174.181.139	unknown	United Kingdom		4589	EASYNETEasynetGlobalServicesEU	false
182.134.160.88	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
95.183.142.116	unknown	Turkey		8517	ULAKNETTR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
9.100.126.155	unknown	United States		3356	LEVEL3US	false
34.96.75.202	unknown	United States		15169	GOOGLEUS	false
169.80.122.10	unknown	United States		37611	AfrihostZA	false
212.229.189.169	unknown	United Kingdom		6659	NEXINTO-DE	false
193.122.239.176	unknown	United States		31898	ORACLE-BMC-31898US	false
199.98.250.141	unknown	United States		174	COGENT-174US	false
152.247.120.26	unknown	Brazil		26599	TELEFONICABRASILSABR	false
98.175.159.226	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
149.64.54.62	unknown	United States		188	SAIC-ASUS	false
185.91.208.162	unknown	Azerbaijan		198193	ASN-TCABLEES	false
54.109.99.197	unknown	United States		16509	AMAZON-02US	false
91.211.55.231	unknown	Russian Federation		48494	MKNET-ASCZ	false
9.195.199.9	unknown	United States		3356	LEVEL3US	false
114.108.48.50	unknown	Korea Republic of		23563	VITSSEN-SUWON-AS-KRTbroadSuwonBroadcastingCorporationK	false
218.72.121.235	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
18.133.194.252	unknown	United States		16509	AMAZON-02US	false
157.21.250.131	unknown	United States		53446	EVMSUS	false
38.118.59.140	unknown	United States		174	COGENT-174US	false
184.98.240.213	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
176.86.239.65	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
203.101.40.148	unknown	India		24560	AIRTELBROADBAND-AS-APBhartiAirtelLtdTelemediaServices	false
216.137.217.153	unknown	United States		11090	MTAONLINE-ASUS	false
89.67.99.51	unknown	Poland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
183.152.181.199	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
39.3.14.235	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
185.203.160.88	unknown	Iran (ISLAMIC Republic Of)		205837	SADADPSP-ASSadadProcessingModernServicesCompanyPJS	false
90.34.68.223	unknown	France		3215	FranceTelecom-OrangeFR	false
187.213.164.208	unknown	Mexico		8151	UninetSAdeCVMX	false
200.172.238.44	unknown	Brazil		4230	CLAROSABR	false
61.73.112.244	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
81.148.253.114	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
45.173.39.97	unknown	Brazil		268790	DEBORAALINEALMEIDA-MEBR	false
131.215.33.187	unknown	United States		31	CITUS	false
112.183.28.147	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
99.55.160.90	unknown	United States		7018	ATT-INTERNET4US	false
108.30.94.26	unknown	United States		701	UUNETUS	false
136.94.212.177	unknown	United States		60311	ONEFMCH	false
115.6.239.91	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
42.170.152.249	unknown	China		4249	LILLY-ASUS	false
77.19.124.127	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
209.210.62.8	unknown	United States		396033	BFDX515US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.210.46.1	unknown	Greece		29247	COSMOTE-GRCosmoteMobileTelecommunicationsSAGR	false
85.103.175.203	unknown	Turkey		9121	TTNETTR	false
125.137.19.174	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
213.23.15.125	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
191.154.239.239	unknown	Colombia		26611	COMCELSACO	false
153.248.18.11	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
179.185.213.56	unknown	Brazil		18881	TELEFONICABRASILSAB R	false
84.223.116.24	unknown	Italy		8612	TISCALI-IT	false
94.9.108.60	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
203.190.179.96	unknown	Singapore		7552	VIETEL-AS-APViettelGroupVN	false
158.113.125.249	unknown	United States		49278	NORDEFNO	false
42.30.66.52	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
128.83.226.100	unknown	United States		18	UTEXASUS	false
218.209.89.102	unknown	Korea Republic of		23563	VITSSEN-SUWON-AS-KRTbroadSuwonBroadcastingCorporationK	false
98.67.105.92	unknown	United States		11351	TWC-11351-NORTHEASTUS	false
161.26.142.204	unknown	United States		1916	AssociacaoRedeNacionaldeEnsinoePesquisaBR	false
131.141.109.74	unknown	Canada		74	SSC-299-Z-74CA	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.483956231146537
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	x86
File size:	55332
MD5:	bef642eeed970f7c3ee944a513ea4c88
SHA1:	baaa1dc20118f95134cb1ca1fa0c32ad49ed8eeb
SHA256:	10f35885f96f694fbf6239de4f4e400367cdb0201bd6b4a6fa85b3cc609de22e
SHA512:	11e9b343e7c658355d22ea542808b0f1bcb191cc4537296d4ea3ceac1a564b0c1fa283f831054a029451207a5cfae41939231aab73ac9f737036aea887f3b8f1
SSDEEP:	768:cRe7+KeFlsC1pDU/4p+gP0JrTS/+Q+Y7RamvmxDOKUKICkmT1:WI+KidsP0JK/+Qh7RasmxiKFsm
TLSH:	60433A85D6DBF9F2E85104BC30A9AB72DF33F53AA871D9DBE39D24229C06201D20635D
File Content Preview:	.ELF.....d...4.....4. ...(.....c...c.....k.....Q.td.....U..S.....h....C... []...$.....U.....=`f...t..5.....c.....c.....u.....t....h.S.....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x8048164
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	54932
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

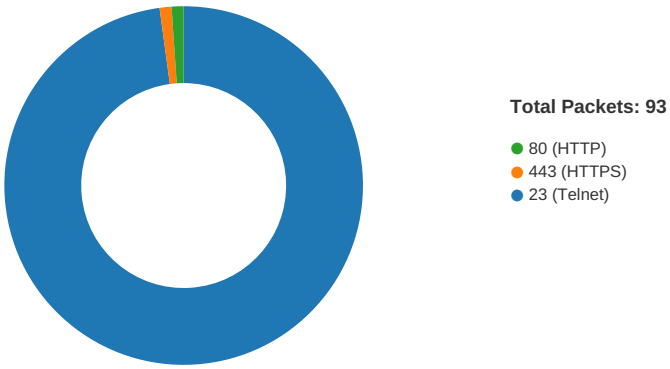
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8048094	0x94	0x1c	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x80480b0	0xb0	0xc366	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x8054416	0xc416	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x8054440	0xc440	0xf40	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x8056384	0xd384	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x805638c	0xd38c	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x80563c0	0xd3c0	0x294	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x8056660	0xd654	0x6904	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0xd654	0x3e	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
LOAD	0x0	0x8048000	0x8048000	0xd380	0xd380	3.6131	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0xd384	0x8056384	0x8056384	0x2d0	0x6be0	2.0811	0x6	RW	0x1000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: x86 PID: **6221**, Parent PID: **6129**

General

Start time:	06:59:34
Start date:	30/05/2022
Path:	/tmp/x86
Arguments:	/tmp/x86
File size:	55332 bytes
MD5 hash:	bef642eeed970f7c3ee944a513ea4c88

Analysis Process: x86 PID: **6222**, Parent PID: **6221**

General

Start time:	06:59:34
Start date:	30/05/2022
Path:	/tmp/x86
Arguments:	n/a
File size:	55332 bytes
MD5 hash:	bef642eeed970f7c3ee944a513ea4c88

Analysis Process: x86 PID: **6223**, Parent PID: **6221**

General

Start time:	06:59:34
Start date:	30/05/2022
Path:	/tmp/x86
Arguments:	n/a
File size:	55332 bytes
MD5 hash:	bef642eeed970f7c3ee944a513ea4c88

Analysis Process: x86 PID: **6225**, Parent PID: **6223**

General

Start time:	06:59:34
Start date:	30/05/2022
Path:	/tmp/x86
Arguments:	n/a
File size:	55332 bytes
MD5 hash:	bef642eeed970f7c3ee944a513ea4c88

File Activities

File Read

Analysis Process: x86 PID: **6233**, Parent PID: **6225**

General

Start time:	06:59:41
Start date:	30/05/2022
Path:	/tmp/x86
Arguments:	n/a
File size:	55332 bytes
MD5 hash:	bef642eeed970f7c3ee944a513ea4c88

Analysis Process: x86 PID: **6234**, Parent PID: **6233**

General

Start time:	06:59:41
Start date:	30/05/2022
Path:	/tmp/x86
Arguments:	n/a
File size:	55332 bytes
MD5 hash:	bef642eeed970f7c3ee944a513ea4c88

Analysis Process: x86 PID: **6226**, Parent PID: **6223**

General

Start time:	06:59:34
Start date:	30/05/2022
Path:	/tmp/x86
Arguments:	n/a
File size:	55332 bytes
MD5 hash:	bef642eeed970f7c3ee944a513ea4c88

Analysis Process: x86 PID: **6227**, Parent PID: **6226**

General

Start time:	06:59:34
Start date:	30/05/2022
Path:	/tmp/x86
Arguments:	n/a
File size:	55332 bytes
MD5 hash:	bef642eeed970f7c3ee944a513ea4c88