ID: 635411
Sample Name: 5zKnElN0F2
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 21:16:42
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

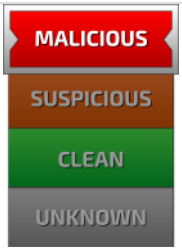
5zKnElN0F2

Overview

General Information

Sample Name:	5zKnElN0F2
Analysis ID:	635411
MD5:	d74bf4db8e2e43..
SHA1:	5de6b4e1a4b1f8..
SHA256:	c0b3f4b9a9a579..
Tags:	32 elf mirai powerpc
Infos:	

Detection



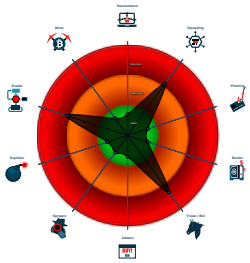
Mirai

Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Uses known network protocols on n…
- Sample tries to kill multiple process…
- Sample contains only a LOAD segm…
- Yara signature match
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might not execute correctly on this machine.

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:	635411
Start date and time: 27/05/202221:16:42	2022-05-27 21:16:42 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5zKnElN0F2
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:	mal68.spre.troj.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/5zKnElN0F2
PID:	6225
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infected
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- 5zKnElN0F2 (PID: 6225, Parent: 6126, MD5: ae65271c943d3451b7f026d1fadccea6) Arguments: /tmp/5zKnElN0F2
  - 5zKnElN0F2 New Fork (PID: 6227, Parent: 6225)
  - 5zKnElN0F2 New Fork (PID: 6229, Parent: 6225)
    - 5zKnElN0F2 New Fork (PID: 6233, Parent: 6229)
    - 5zKnElN0F2 New Fork (PID: 6236, Parent: 6229)
      - 5zKnElN0F2 New Fork (PID: 6238, Parent: 6236)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
5zKnElN0F2	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x9154:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x91c3:$s2: $Id: UPX • 0x9174:$s3: $Info: This file is packed with the UPX executable packer

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

Networking

Uses known network protocols on non-standard ports

System Summary

Sample tries to kill multiple processes (SIGKILL)

Data Obfuscation

Sample is packed with UPX

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

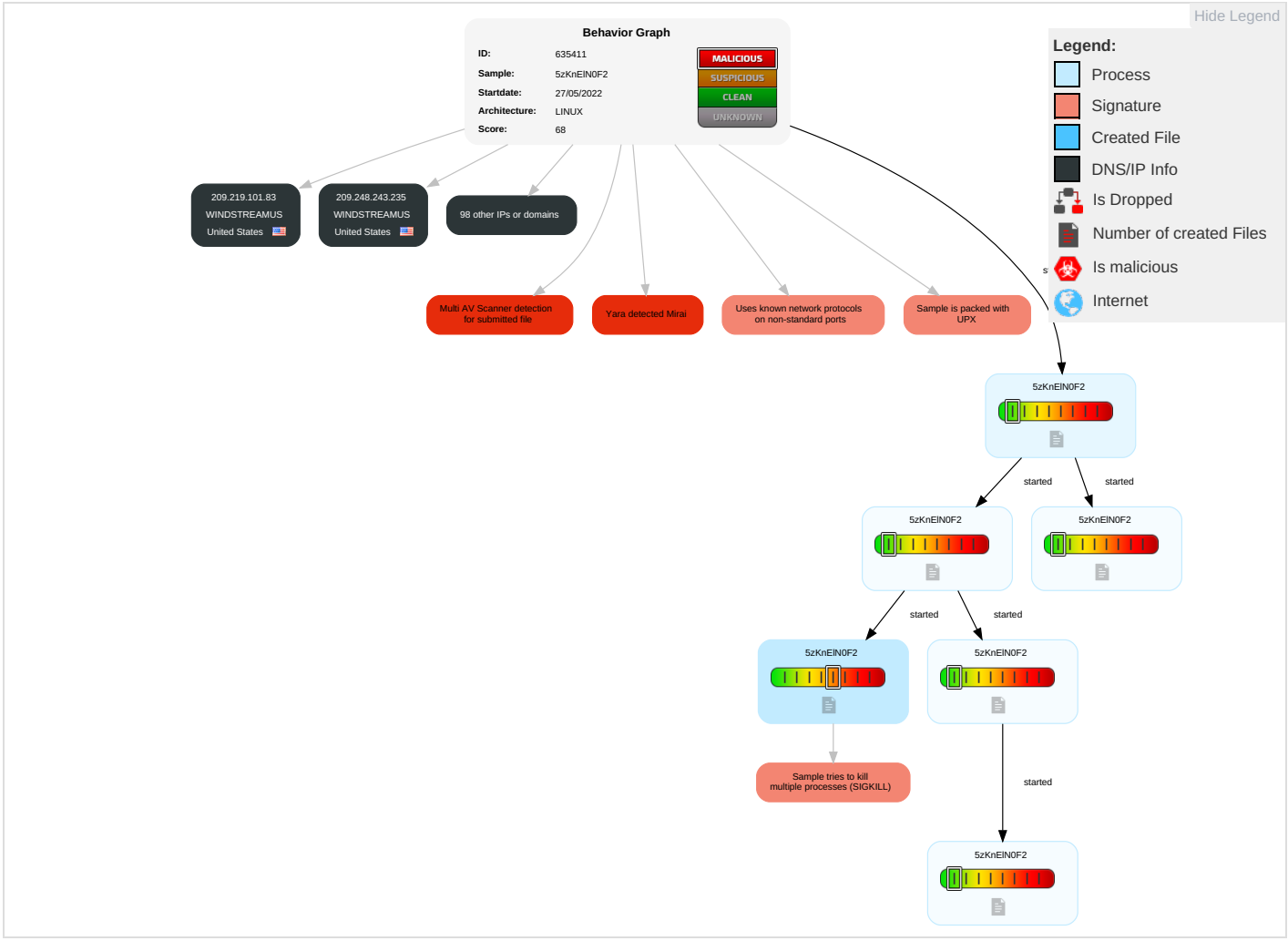
Mitre Att&ck Matrix

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	1 Obfuscated Files or Information	1 OS Credential Dumping	1 1 Security Software 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	1 Service Stop
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
5zKnElN0F2	30%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

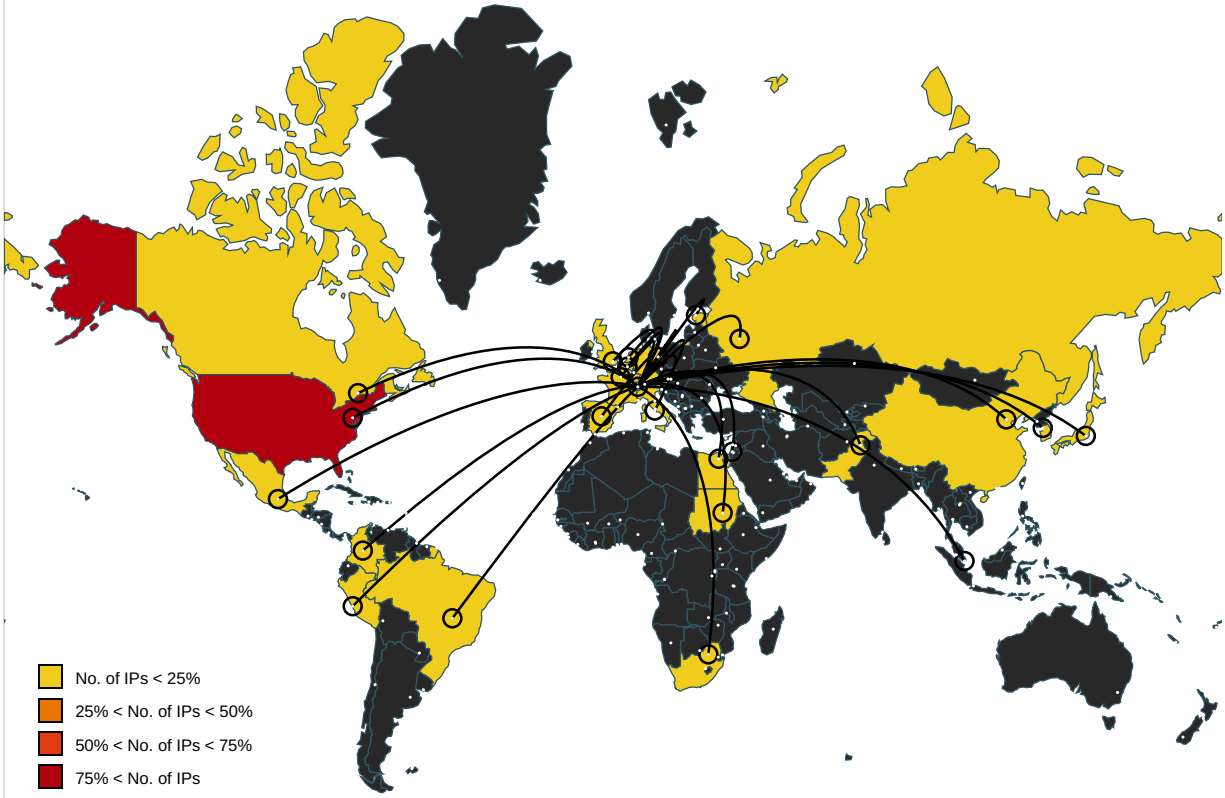
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
248.213.59.144	unknown	Reserved		unknown	unknown	false
251.130.127.226	unknown	Reserved		unknown	unknown	false
88.75.6.154	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
152.40.102.106	unknown	United States		53785	UNC-GREENSBOROUS	false
152.38.121.52	unknown	United States		81	NCRENUS	false
202.218.0.155	unknown	Japan		4694	IDCFIDCFrontierIncJP	false
85.84.124.101	unknown	Spain		12338	EUSKALTELES	false
181.242.239.177	unknown	Colombia		26611	COMCELSACO	false
166.17.196.160	unknown	United States		206	CSC-IGN-AMERUS	false
6.71.232.135	unknown	United States		1479	DNIC-ASBLK-01478-01479US	false
215.140.101.179	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
131.67.195.233	unknown	United States		138	DNIC-AS-00138US	false
216.47.114.137	unknown	United States		397187	NHN-GLOBALUS	false
175.44.191.61	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
57.95.244.181	unknown	Belgium		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
182.181.115.112	unknown	Pakistan		45595	PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	false
147.36.189.252	unknown	United States		1559	DNIC-ASBLK-01550-01601US	false
16.163.191.244	unknown	United States		unknown	unknown	false
102.125.211.85	unknown	Sudan		36972	MTNSD	false
242.207.165.243	unknown	Reserved		unknown	unknown	false
220.146.79.49	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
59.204.179.210	unknown	China		2516	KDDIKDDICORPORATIONJP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
176.67.118.196	unknown	Palestinian Territory Occupied		51407	MADA-ASPS	false
95.225.107.120	unknown	Italy		3269	ASN-IBSNAZIT	false
7.179.30.152	unknown	United States		3356	LEVEL3US	false
209.248.243.235	unknown	United States		7029	WINDSTREAMUS	false
21.7.113.27	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
17.3.87.47	unknown	United States		714	APPLE-ENGINEERINGUS	false
72.97.169.89	unknown	United States		22394	CELLCOUS	false
57.141.231.103	unknown	Belgium		2686	ATGS-MMD-ASUS	false
91.220.89.64	unknown	Austria		51767	JOHANNITER-UNFALL-HILFEAT	false
11.33.204.40	unknown	United States		3356	LEVEL3US	false
70.30.247.30	unknown	Canada		577	BACOMCA	false
98.19.126.216	unknown	United States		7029	WINDSTREAMUS	false
173.7.4.52	unknown	United States		10507	SPCSUS	false
64.123.49.206	unknown	United States		7018	ATT-INTERNET4US	false
71.161.139.71	unknown	United States		701	UUNETUS	false
221.27.57.106	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
57.252.101.85	unknown	Belgium		2686	ATGS-MMD-ASUS	false
221.239.50.117	unknown	China		17638	CHINATELECOM-TJ-AS-APASNforTIANJINProvincialNetofCT	false
60.26.69.53	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
67.116.193.63	unknown	United States		7018	ATT-INTERNET4US	false
160.184.16.245	unknown	South Africa		36903	MT-MPLSMA	false
251.16.126.103	unknown	Reserved		unknown	unknown	false
193.245.180.21	unknown	Belgium		3549	LVLT-3549US	false
8.188.45.192	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
125.143.119.66	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
152.31.80.240	unknown	United States		6559	NCIHUS	false
12.92.121.104	unknown	United States		7018	ATT-INTERNET4US	false
215.126.53.189	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
3.131.241.119	unknown	United States		16509	AMAZON-02US	false
191.92.238.155	unknown	Colombia		27831	ColombiaMovilCO	false
24.26.58.217	unknown	United States		10796	TWC-10796-MIDWESTUS	false
63.72.64.154	unknown	United States		701	UUNETUS	false
9.115.4.121	unknown	United States		3356	LEVEL3US	false
57.25.76.38	unknown	Belgium		2686	ATGS-MMD-ASUS	false
167.38.155.197	unknown	Canada		2665	CDAGOVNCA	false
163.151.39.36	unknown	United States		36161	WESTCHESTERCOUNTY-NYUS	false
82.224.120.126	unknown	France		12322	PROXADFR	false
53.72.59.103	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
171.130.11.59	unknown	United States		9874	STARHUB-MOBILEStarHubLtdSG	false
215.91.18.89	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
25.254.25.135	unknown	United Kingdom		199055	UKCLOUD-ASGB	false
71.192.101.169	unknown	United States		7922	COMCAST-7922US	false
85.196.199.247	unknown	Estonia		61307	EE-AS-STVEE	false
91.250.181.214	unknown	Spain		12479	UNI2-ASES	false
215.55.124.124	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
109.218.10.173	unknown	France		3215	FranceTelecom-OrangeFR	false
100.188.108.206	unknown	United States		21928	T-MOBILE-AS21928US	false
181.66.216.170	unknown	Peru		6147	TelefonicadelPeruSAAPE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.107.223.195	unknown	United States		3	MIT-GATEWAYSUS	false
119.80.115.135	unknown	China		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
176.151.103.215	unknown	France		5410	BOUYGTEL-ISPFR	false
96.105.107.122	unknown	United States		7922	COMCAST-7922US	false
160.95.83.51	unknown	United States		217	UMN-SYSTEMUS	false
209.219.101.83	unknown	United States		7029	WINDSTREAMUS	false
159.197.33.178	unknown	United Kingdom		1273	CWVodafoneGroupPLCEU	false
141.238.20.159	unknown	United States		395015	SUNY-FREDONIAUS	false
100.63.227.120	unknown	United States		701	UUNETUS	false
163.226.55.140	unknown	Japan		24297	FCNUniversityPublicCorporationOsakaJP	false
189.166.254.5	unknown	Mexico		8151	UninetSAdeCVMX	false
130.247.179.246	unknown	United States		786	JANETJiscServicesLimitedGB	false
40.196.42.224	unknown	United States		4249	LILLY-ASUS	false
134.214.79.249	unknown	France		2060	FR-RENATERRENATER_ASNBLOCK1EU	false
244.140.81.28	unknown	Reserved		unknown	unknown	false
86.176.103.153	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
145.208.19.23	unknown	Netherlands		1101	IP-EEND-ASIP-EENDBVNL	false
113.105.159.164	unknown	China		134763	CT-DONGGUAN-IDCCHINANETGuangdongprovincenetworkCN	false
105.91.86.94	unknown	Egypt		36992	ETISALAT-MISREG	false
12.141.232.110	unknown	United States		7018	ATT-INTERNET4US	false
31.172.254.55	unknown	United Kingdom		34920	SIMPLY-ROMFORDGB	false
76.144.187.104	unknown	United States		7922	COMCAST-7922US	false
4.0.229.194	unknown	United States		3356	LEVEL3US	false
48.35.173.172	unknown	United States		2686	ATGS-MMD-ASUS	false
170.178.42.2	unknown	United States		11685	HNBCOL-ASUS	false
61.207.245.49	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
195.189.238.150	unknown	Russian Federation		41654	INETRARU	false
1.5.141.51	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
186.224.149.70	unknown	Brazil		28580	CILNETComunicacaoeInformaticaLTDABR	false
255.150.73.125	unknown	Reserved		unknown	unknown	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 MSB executable, PowerPC or cisco 4500, version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.9643107024054975
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	5zKnElN0F2
File size:	39372
MD5:	d74bf4db8e2e43cbdc9c527ec15356b0
SHA1:	5de6b4e1a4b1f896ec6b3b6b473c8afb4d6f40a1
SHA256:	c0b3f4b9a9a57965c0429b5199e634012e223a4617a13a89dc5e2508085e5575
SHA512:	d262f391e46bf85eabadd74dfc74d78a2eb1fd25d32b45b8f9b6e2cbaeed624a1a32237897014bf26346bbbe27d71e0a3a5d7fad1d12dbcbfc86086b5fb22a1f
SSDEEP:	768:FdCZnhT/jFCaEQd4RC8he9+QZu3ckO7jTlZKhnHdM9i285BE4uVcqgw09M:O5hnFOQURhCZtB7j/oHdAijQ4u+qgw0W
TLSH:	F903F1BDD0B90DC1EB6BED6C8C77C2A82EE15F9AF2E6CDA4329C6F5149060395345D40
File Content Preview:	.ELF.....4.....4. ... (.....dt.Q.....UPX!.....E...E.....W.....?.E.h4...@b.....d/%.....)..2x....F...NUu....]<fh.u...B.

Static ELF Info

ELF header

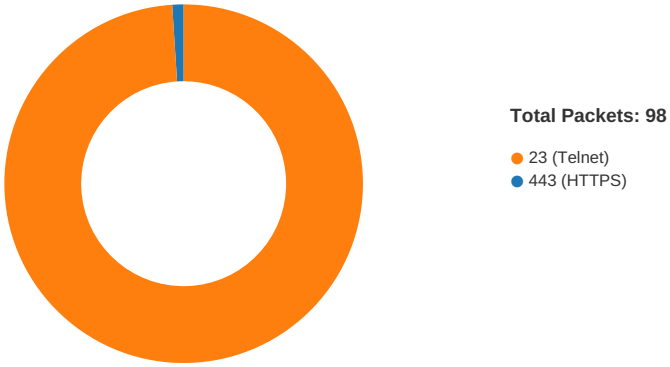
Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	PowerPC
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0x1086d8
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x100000	0x100000	0x98c0	0x98c0	4.1310	0x5	R E	0x10000		
LOAD	0xa6e0	0x1002a6e0	0x1002a6e0	0x0	0x0	0.0000	0x6	RW	0x10000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: 5zKnElN0F2 PID: 6225, Parent PID: 6126

General

Start time:	21:17:29
Start date:	27/05/2022
Path:	/tmp/5zKnElN0F2
Arguments:	/tmp/5zKnElN0F2
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Analysis Process: 5zKnElN0F2 PID: 6227, Parent PID: 6225

General

Start time:	21:17:29
Start date:	27/05/2022
Path:	/tmp/5zKnElN0F2
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: 5zKnElN0F2 PID: 6229, Parent PID: 6225

General

Start time:	21:17:29
Start date:	27/05/2022
Path:	/tmp/5zKnElN0F2
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: 5zKnElN0F2 PID: **6233**, Parent PID: **6229**

General

Start time:	21:17:29
Start date:	27/05/2022
Path:	/tmp/5zKnElN0F2
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: 5zKnElN0F2 PID: **6236**, Parent PID: **6229**

General

Start time:	21:17:29
Start date:	27/05/2022
Path:	/tmp/5zKnElN0F2
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: 5zKnElN0F2 PID: **6238**, Parent PID: **6236**

General

Start time:	21:17:29
Start date:	27/05/2022
Path:	/tmp/5zKnElN0F2
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6