ID: 626460
Sample Name: uuC6SqiHEK
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 03:44:04
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

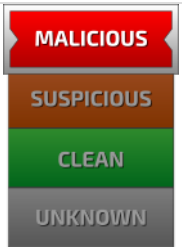
uuC6SqiHEK

Overview

General Information

Sample Name:	uuC6SqiHEK
Analysis ID:	626460
MD5:	772945ce381f38..
SHA1:	62c42fe68280e6..
SHA256:	cfcdff7a98c3829...
Tags:	32 elf mips mirai
Infos:	

Detection



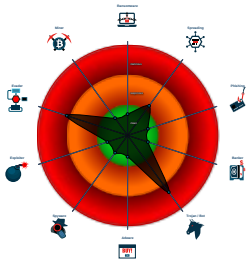
Mirai

Score:	64
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 contains only a LOAD segm...
- 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...
- Sample listens on a socket
- Sample tries to kill a process (SIGK...

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.

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626460
Start date and time: 14/05/202203:44:04	2022-05-14 03:44:04 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	uuC6SqiHEK
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.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/uuC6SqiHEK
PID:	6223
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- uuC6SqiHEK (PID: 6223, Parent: 6122, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/uuC6SqiHEK
  - uuC6SqiHEK New Fork (PID: 6225, Parent: 6223)
    - uuC6SqiHEK New Fork (PID: 6326, Parent: 6225)
    - uuC6SqiHEK New Fork (PID: 6328, Parent: 6225)
      - uuC6SqiHEK New Fork (PID: 6330, Parent: 6328)
        - uuC6SqiHEK New Fork (PID: 6343, Parent: 6330)
        - uuC6SqiHEK New Fork (PID: 6345, Parent: 6330)
      - uuC6SqiHEK New Fork (PID: 6332, Parent: 6328)
      - uuC6SqiHEK New Fork (PID: 6333, Parent: 6328)
    - uuC6SqiHEK New Fork (PID: 6226, Parent: 6223)
    - uuC6SqiHEK New Fork (PID: 6227, Parent: 6223)
      - uuC6SqiHEK New Fork (PID: 6231, Parent: 6227)
        - uuC6SqiHEK New Fork (PID: 6337, Parent: 6231)
        - uuC6SqiHEK New Fork (PID: 6339, Parent: 6231)
      - uuC6SqiHEK New Fork (PID: 6233, Parent: 6227)
      - uuC6SqiHEK New Fork (PID: 6234, Parent: 6227)
- **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

Networking

Uses known network protocols on non-standard ports

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

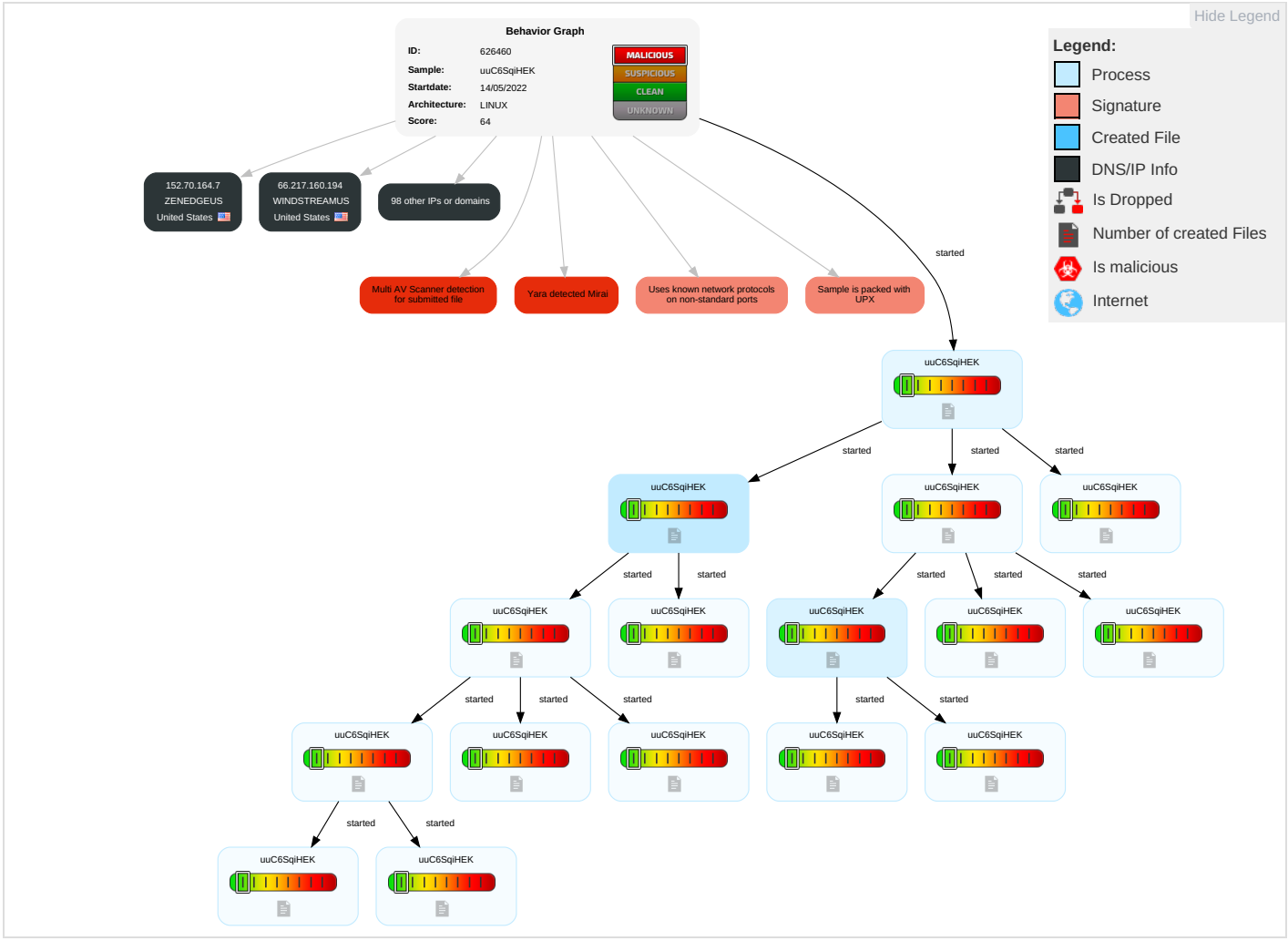
Mitre Att&ck Matrix

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	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
uuC6SqiHEK	43%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

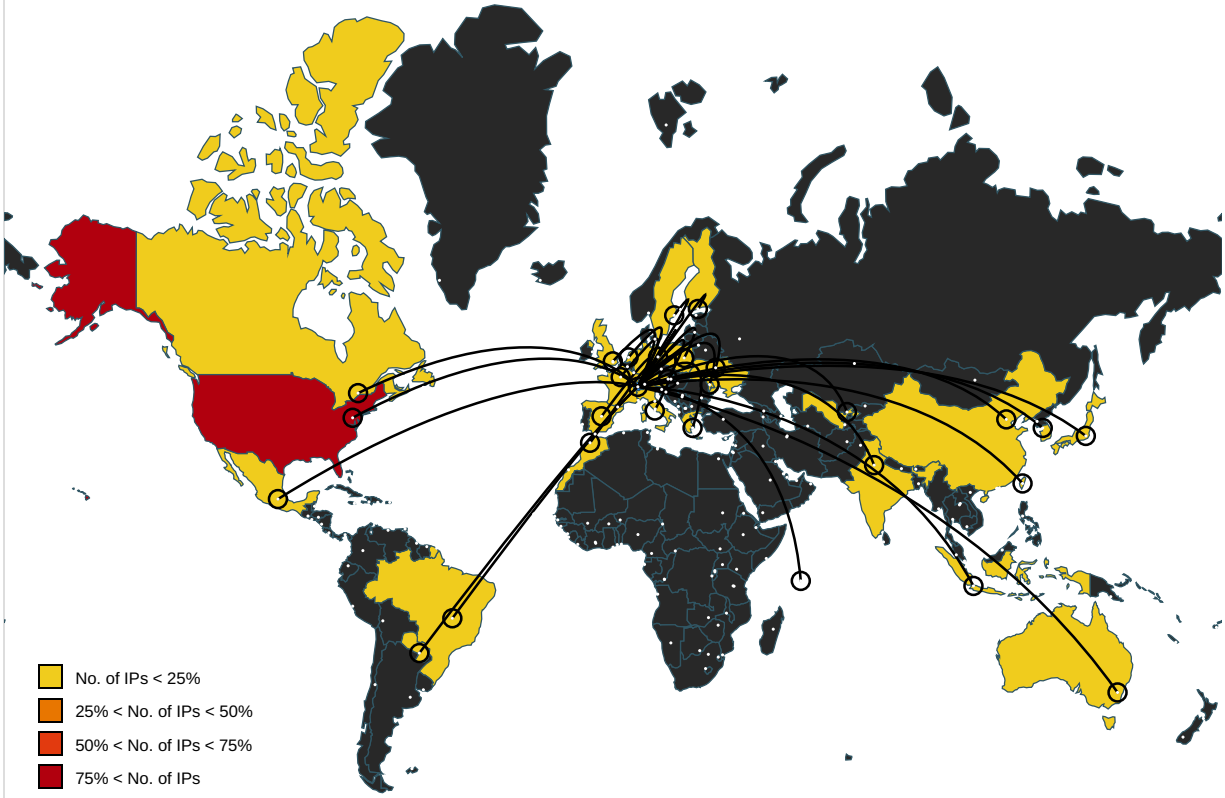
Domains and IPs

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
106.74.102.98	unknown	China		133118	UNICOM-CNChinaUnicomIPnetworkCN	false
16.145.233.90	unknown	United States		unknown	unknown	false
103.48.197.179	unknown	India		133982	EXCITEL-AS-INExcitelBroadbandPrivateLimitedIN	false
94.65.166.89	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	false
4.85.99.192	unknown	United States		3356	LEVEL3US	false
244.229.95.159	unknown	Reserved		unknown	unknown	false
198.43.106.103	unknown	United States		8038	6CONNECTUS	false
183.193.97.71	unknown	China		24400	CMNET-V4SHANGHAI-AS-APShanghaiMobileCommunicationsCoLt	false
199.69.193.131	unknown	United States		7018	ATT-INTERNET4US	false
212.49.48.110	unknown	Poland		3327	CITICCITICTelecomCPCNetherlandsBVEE	false
79.52.33.177	unknown	Italy		3269	ASN-IBSNAZIT	false
67.191.151.129	unknown	United States		7922	COMCAST-7922US	false
221.60.81.122	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
159.56.8.217	unknown	United States		11351	TWC-11351-NORTHEASTUS	false
253.158.26.187	unknown	Reserved		unknown	unknown	false
152.70.164.7	unknown	United States		393676	ZENEDGEUS	false
14.46.92.98	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
87.208.121.119	unknown	Netherlands		13127	VERSATELASfortheTrans-EuropeanTele2IPTransportbackbo	false
146.30.9.7	unknown	United States		197938	TRAVIANGAMESDE	false
13.225.38.199	unknown	United States		16509	AMAZON-02US	false
252.118.152.132	unknown	Reserved		unknown	unknown	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
220.134.72.61	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
167.147.188.217	unknown	Canada		25899	LSNETUS	false
133.252.162.131	unknown	Japan		7687	D-CRUISENETTOYOTADIGITALCRUISEINCORPORATEDJP	false
68.46.131.251	unknown	United States		7922	COMCAST-7922US	false
158.178.211.155	unknown	United Kingdom		15830	EQUINIX-CONNECT-EMEAGB	false
201.161.230.122	unknown	Mexico		28549	CableyComunicacionde CampecheSAdeCVMX	false
66.217.160.194	unknown	United States		7029	WINDSTREAMUS	false
159.82.197.236	unknown	United States		16928	UTCNETUS	false
161.108.200.94	unknown	United States		3955	WANG-US-1US	false
40.207.222.239	unknown	United States		4249	LILLY-ASUS	false
251.107.145.150	unknown	Reserved		unknown	unknown	false
247.21.116.49	unknown	Reserved		unknown	unknown	false
88.8.231.68	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
112.175.44.193	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
37.110.208.188	unknown	Uzbekistan		41202	UNITELUZ	false
91.175.167.230	unknown	France		12322	PROXADFR	false
101.107.22.252	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
117.89.208.53	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
249.17.141.60	unknown	Reserved		unknown	unknown	false
208.122.146.58	unknown	United States		46476	TTUHSCUS	false
60.238.28.32	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
177.250.111.169	unknown	Paraguay		27866	COPACOPY	false
104.214.47.103	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
174.14.19.141	unknown	United States		6327	SHAWCA	false
193.16.95.100	unknown	Germany		9145	EWETELCloppenburgerStrasse310DE	false
87.85.42.151	unknown	United Kingdom		4589	EASYNETEasynetGlobalServicesEU	false
198.8.229.114	unknown	United States		13540	LIBERTY-MUTUALUS	false
100.184.225.176	unknown	United States		21928	T-MOBILE-AS21928US	false
141.203.224.250	unknown	Austria		6720	MAGWIENAT	false
138.216.43.88	unknown	Finland		1759	TSF-IP-CORETeliaFinlandOyjEU	false
39.192.61.34	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
70.186.61.172	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
173.157.32.247	unknown	United States		10507	SPCSUS	false
255.56.80.239	unknown	Reserved		unknown	unknown	false
90.110.42.134	unknown	France		3215	FranceTelecom-OrangeFR	false
24.27.166.110	unknown	United States		10796	TWC-10796-MIDWESTUS	false
64.61.215.85	unknown	United States		32946	RPU-1892US	false
97.170.127.8	unknown	United States		6167	CELLCO-PARTUS	false
42.195.247.73	unknown	China		4249	LILLY-ASUS	false
193.66.92.128	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
98.39.11.74	unknown	United States		7922	COMCAST-7922US	false
162.173.110.34	unknown	United States		21928	T-MOBILE-AS21928US	false
65.11.58.74	unknown	United States		16509	AMAZON-02US	false
115.103.189.181	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
78.218.113.35	unknown	France		12322	PROXADFR	false
170.174.149.73	unknown	United States		11685	HNBCOL-ASUS	false
250.102.71.130	unknown	Reserved		unknown	unknown	false
97.173.157.158	unknown	United States		6167	CELLCO-PARTUS	false
251.153.15.216	unknown	Reserved		unknown	unknown	false
202.124.2.146	unknown	Japan		18126	CTCXChubuTelecommunicationsCompanyIncJP	false
172.75.225.48	unknown	United States		11426	TWC-11426-CAROLINASUS	false
157.54.61.122	unknown	United States		3598	MICROSOFT-CORP-ASUS	false
142.165.15.143	unknown	Canada		803	SASKTELCA	false
116.240.246.240	unknown	Australia		9443	VOCUS-RETAIL-AUVocusRetailAU	false
20.229.247.194	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
96.120.35.241	unknown	United States		7922	COMCAST-7922US	false
54.118.15.136	unknown	United States		16509	AMAZON-02US	false
31.226.141.94	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
206.171.177.30	unknown	United States		7018	ATT-INTERNET4US	false
17.93.233.237	unknown	United States		714	APPLE-ENGINEERINGUS	false
87.80.16.160	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
117.246.144.137	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
187.46.78.46	unknown	Brazil		26615	TIMSABR	false
39.145.157.157	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
105.77.140.180	unknown	Morocco		36884	MAROCCONNECTMA	false
37.246.127.6	unknown	Moldova Republic of		57598	FIBERHOP-ASNMD	false
93.77.136.84	unknown	Ukraine		25229	VOLIA-ASUA	false
184.9.206.96	unknown	United States		7011	FRONTIER-AND-CITIZENSUS	false
79.73.27.61	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	false
81.170.168.42	unknown	Sweden		8473	BAHNHOFhttpwwwbahnhofnetSE	false
171.29.63.199	unknown	United Kingdom		34457	AMB-GENERALIDE	false
204.176.239.53	unknown	United States		701	UUNETUS	false
19.1.83.197	unknown	United States		3	MIT-GATEWAYSUS	false
130.190.252.22	unknown	France		1942	FR-TIGRETOileInformatiqueGRENobloiseEU	false
113.109.71.95	unknown	China		4816	CHINANET-IDC-GDChinaTelecomGroupCN	false
156.226.9.176	unknown	Seychelles		135357	SKHT-ASShenzhenKatherineHengTechnologyInformationCo	false
155.58.195.100	unknown	United States		23366	LSUHEALTHSCIENCESCTRUS	false
36.46.16.113	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
201.115.242.113	unknown	Mexico		8151	UninetSAdeCVMX	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, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.87857528714088
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	uuC6SqiHEK
File size:	27244
MD5:	772945ce381f38c38472a94893995e6f
SHA1:	62c42fe68280e67aa016afa49f844da73a1d2df1
SHA256:	cfcdff7a98c3829650988decae442e8daaf67cb471d13048ad0d578d8c5f63cf
SHA512:	a2d3b5264ed4754a4c639fa28dc1076f98e99d3b3e4ce25dcfe99e4335842186b431ff11011617e9a27a02e5148c92f3721aa3b6010902763724958791a17bd4
SSDEEP:	768:MLCUFskb2Jgls/E2+OocrfJiHNjfmQ2q7IoqdBqWn:oCrJgHiOJrfwmQrctH
TLSH:	91C2E1DFB49A38C5CD1C5CBC219D5AD115B992C7334A8F0837502DCDA57645FB8AC8B8
File Content Preview:	.ELF.....V..4.....4. ...(.....Ei..Ei.....E...E.....tUPX!d.....T...T.....T.....?.E.h;....#.....b.L#4E..,....M..D{c...j;.D .A....~.....hE.:.O.....L..N.7g..\....R.....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x105608
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2
Section Header Offset:	0

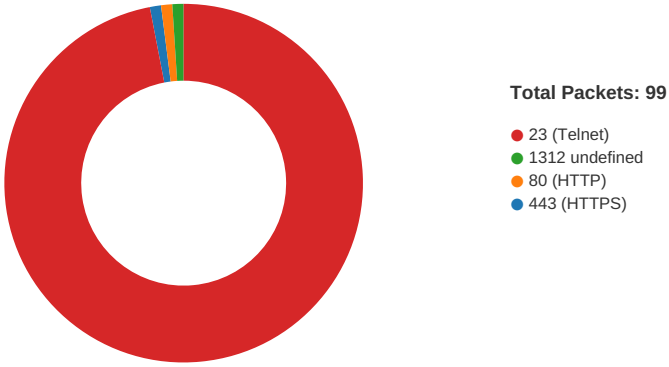
ELF header	
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

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	0x6945	0x6945	4.1994	0x5	R E	0x10000		
LOAD	0x18c0	0x4518c0	0x4518c0	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: uuC6SqiHEK PID: 6223, Parent PID: 6122

General

Start time:	03:44:50
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	/tmp/uuC6SqiHEK
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: uuC6SqiHEK PID: 6225, Parent PID: 6223

General

Start time:	03:44:50
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK

Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: uuC6SqiHEK PID: **6326**, Parent PID: **6225**

General

Start time:	03:47:42
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: uuC6SqiHEK PID: **6328**, Parent PID: **6225**

General

Start time:	03:47:42
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: uuC6SqiHEK PID: **6330**, Parent PID: **6328**

General

Start time:	03:47:42
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: uuC6SqiHEK PID: **6343**, Parent PID: **6330**

General

Start time:	03:47:47
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: uuC6SqiHEK PID: **6345**, Parent PID: **6330**

General

Start time:	03:47:47
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: uuC6SqiHEK PID: **6332**, Parent PID: **6328**

General	
Start time:	03:47:42
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: uuC6SqiHEK PID: **6333**, Parent PID: **6328**

General	
Start time:	03:47:42
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: uuC6SqiHEK PID: **6226**, Parent PID: **6223**

General	
Start time:	03:44:50
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: uuC6SqiHEK PID: **6227**, Parent PID: **6223**

General	
Start time:	03:44:50
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: uuC6SqiHEK PID: **6231**, Parent PID: **6227**

General	
Start time:	03:44:50
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Directory Enumerated

Analysis Process: uuC6SqiHEK PID: **6337**, Parent PID: **6231**

General	
Start time:	03:47:43
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	n/a
File size:	5773336 bytes

MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: uuC6SqiHEK PID: **6339**, Parent PID: **6231**

General

Start time:	03:47:43
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: uuC6SqiHEK PID: **6233**, Parent PID: **6227**

General

Start time:	03:44:51
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: uuC6SqiHEK PID: **6234**, Parent PID: **6227**

General

Start time:	03:44:51
Start date:	14/05/2022
Path:	/tmp/uuC6SqiHEK
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9