ID: 553492
Sample Name: 52lN2HSY7O
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 01:33:11
Date: 15/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

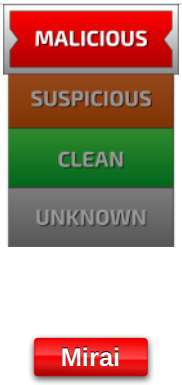
Linux Analysis Report 52lN2HSY7O

Overview

General Information

Sample Name:	52lN2HSY7O
Analysis ID:	553492
MD5:	e0db3c63694e83..
SHA1:	d04a564f43e9ed6.
SHA256:	da6d168edfc190e.
Tags:	32 elf mirai motorola
Infos:	

Detection

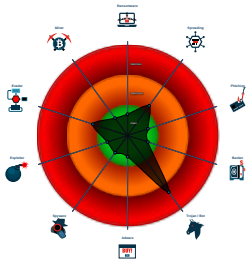


Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Sample has stripped symbol table
- 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...
- Executes the "rm" command used to...
- Sample listens on a socket
- Sample tries to kill a process (SIGK...

Classification



Analysis Advice

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

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553492
Start date:	15.01.2022
Start time:	01:33:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	52lN2HSY7O
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.troj.lin@0/1@0/0
Warnings:	Show All

Process Tree

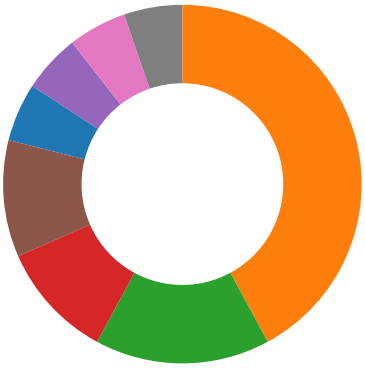
- **system is lnxubuntu20**
- dash New Fork (PID: 5186, Parent: 4331)
  - cat (PID: 5186, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.JmXH35JStJ
- dash New Fork (PID: 5187, Parent: 4331)
  - head (PID: 5187, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5188, Parent: 4331)
  - tr (PID: 5188, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5189, Parent: 4331)
  - cut (PID: 5189, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5190, Parent: 4331)
  - cat (PID: 5190, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.JmXH35JStJ
- dash New Fork (PID: 5191, Parent: 4331)
  - head (PID: 5191, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5192, Parent: 4331)
  - tr (PID: 5192, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5193, Parent: 4331)
  - cut (PID: 5193, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5194, Parent: 4331)
  - rm (PID: 5194, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.JmXH35JStJ /tmp/tmp.AdZnWFxIG7 /tmp/tmp.Bef8J1nfzZ
  - 52lN2HSY7O (PID: 5242, Parent: 5106, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/52lN2HSY7O
    - 52lN2HSY7O New Fork (PID: 5244, Parent: 5242)
      - 52lN2HSY7O New Fork (PID: 5343, Parent: 5244)
      - 52lN2HSY7O New Fork (PID: 5346, Parent: 5244)
        - 52lN2HSY7O New Fork (PID: 5350, Parent: 5346)
          - 52lN2HSY7O New Fork (PID: 5359, Parent: 5350)
          - 52lN2HSY7O New Fork (PID: 5361, Parent: 5350)
        - 52lN2HSY7O New Fork (PID: 5352, Parent: 5346)
        - 52lN2HSY7O New Fork (PID: 5354, Parent: 5346)
    - 52lN2HSY7O New Fork (PID: 5245, Parent: 5242)
    - 52lN2HSY7O New Fork (PID: 5247, Parent: 5242)
      - 52lN2HSY7O New Fork (PID: 5250, Parent: 5247)
        - 52lN2HSY7O New Fork (PID: 5342, Parent: 5250)
        - 52lN2HSY7O New Fork (PID: 5344, Parent: 5250)
      - 52lN2HSY7O New Fork (PID: 5251, Parent: 5247)
      - 52lN2HSY7O New Fork (PID: 5255, Parent: 5247)
- **cleanup**

Yara Overview

PCAP (Network Traffic)

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

Jbx Signature Overview



- AV Detection
- Networking
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

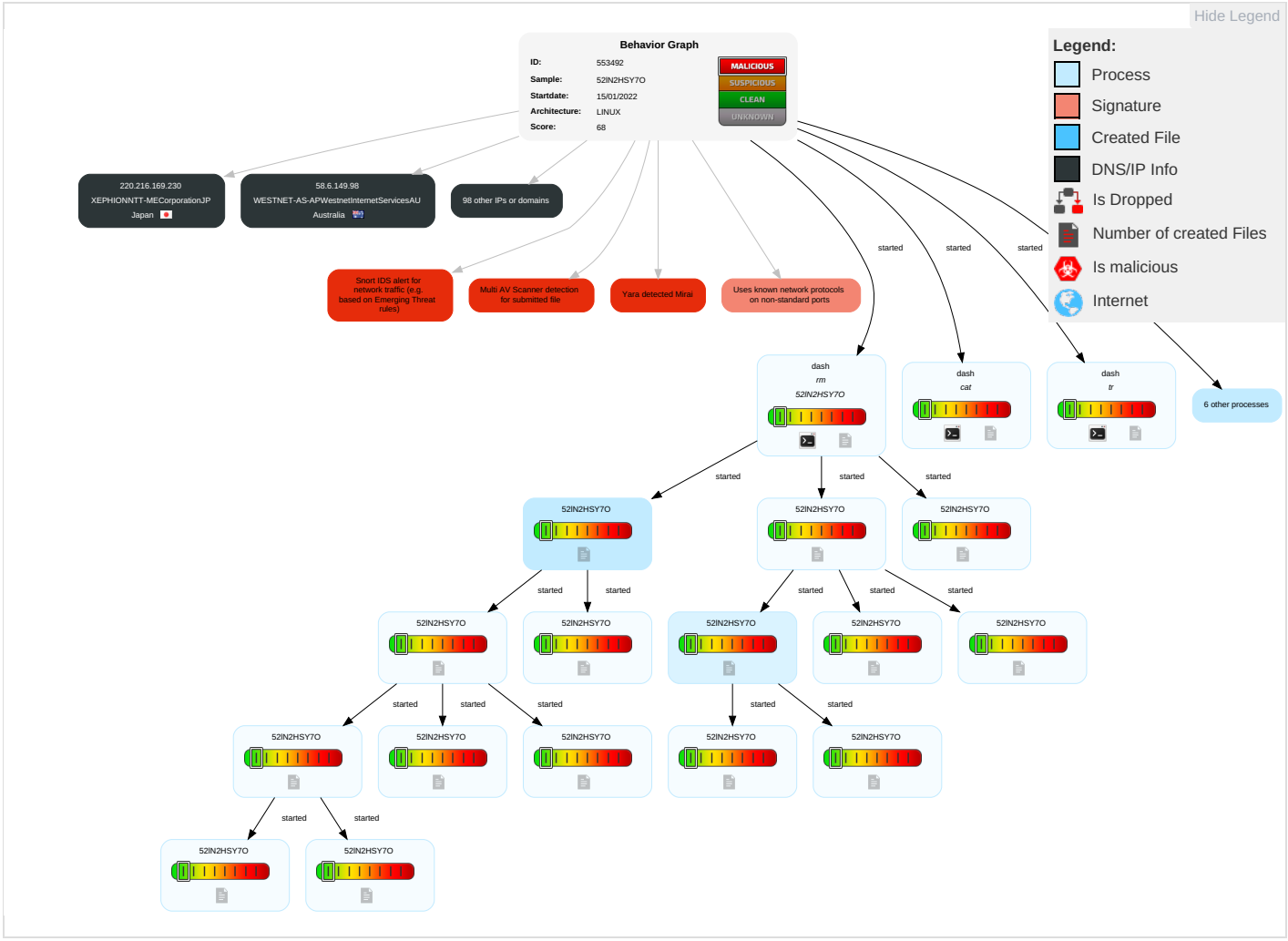
Mitre Att&ck Matrix

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	File Deletion 1	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitio
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	Non-Standard Port 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockou
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	Application Layer Protocol 1	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
52IN2HSY7O	56%	Virustotal		Browse
52IN2HSY7O	63%	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

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.110.235.164	unknown	United States		7018	ATT-INTERNET4US	false
113.121.141.255	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
177.11.31.210	unknown	Brazil		52754	GRUPOSHARKBR	false
27.110.107.33	unknown	Japan		23783	CNACableNetworksAkitaColtdJP	false
80.24.212.170	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
186.83.234.200	unknown	Colombia		10620	TelmexColombiaSACO	false
207.56.160.227	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
222.171.173.133	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
206.184.241.50	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
207.116.49.21	unknown	United States		6407	PRIMUS-AS6407CA	false
81.255.86.163	unknown	France		3215	FranceTelecom-OrangeFR	false
101.128.206.180	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
58.6.149.98	unknown	Australia		9543	WESTNET-AS-APWestnetInternetServicesAU	false
60.64.115.12	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
72.191.168.77	unknown	United States		11427	TWC-11427-TEXASUS	false
134.2.145.161	unknown	Germany		553	BELWUEBelWue-KoordinationEU	false
88.190.10.46	unknown	France		12322	PROXADFR	false
189.230.128.7	unknown	Mexico		8151	UninetSAdeCVMX	false
240.234.53.120	unknown	Reserved		unknown	unknown	false
200.228.138.0	unknown	Brazil		4230	CLAROSABR	false
245.90.212.44	unknown	Reserved		unknown	unknown	false
18.188.26.118	unknown	United States		16509	AMAZON-02US	false
121.55.215.27	unknown	Guam		3605	ERX-KUENTOS-ASGuamCablevisionLLCGU	false
175.240.25.72	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
247.205.244.162	unknown	Reserved		unknown	unknown	false
164.42.74.234	unknown	Puerto Rico		16649	IUPR-ASPR	false
53.228.90.236	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
96.25.164.173	unknown	United States		16625	AKAMAI-ASUS	false
99.10.28.76	unknown	United States		7018	ATT-INTERNET4US	false
116.40.43.10	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
159.52.118.79	unknown	Australia		4826	VOCUS-BACKBONE-ASVocusConnectInternationalBackboneAU	false
201.233.213.54	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	false
169.243.206.141	unknown	United States		47024	THE-METROHEALTH-SYSTEMUS	false
109.44.45.243	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
240.203.171.95	unknown	Reserved		unknown	unknown	false
150.253.133.66	unknown	United States		13445	13445US	false
253.47.120.163	unknown	Reserved		unknown	unknown	false
110.220.30.89	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
43.8.221.27	unknown	Japan		4249	LILLY-ASUS	false
203.120.137.187	unknown	Singapore		4628	PACIFICINTERNET-AS-APPacificInternetPteLtdSG	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
218.181.74.60	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
53.169.5.228	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
75.125.11.254	unknown	United States		36351	SOFTLAYERUS	false
101.215.253.239	unknown	India		58519	CHINATELECOM-CTCLOUDCloudComputingCorporationCN	false
156.7.48.65	unknown	United States		29975	VODACOM-ZA	false
117.178.243.226	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
161.78.252.141	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
240.160.53.154	unknown	Reserved		unknown	unknown	false
108.28.236.159	unknown	United States		701	UUNETUS	false
195.249.101.245	unknown	Denmark		3292	TDCTDCASDK	false
148.56.211.54	unknown	Spain		12430	VODAFONE_ESES	false
159.106.135.52	unknown	United States		16050	REUTERS-DOCKLANDS-RES-ASReutersDocklandsresiliancyGB	false
80.97.224.172	unknown	Romania		9050	RTDBucharestRomaniaRO	false
211.21.103.87	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
183.219.249.8	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
197.31.187.186	unknown	Tunisia		37492	ORANGE-TN	false
156.146.203.249	unknown	United States		1448	UNITED-BROADBANDUS	false
220.216.169.230	unknown	Japan		9595	XEPHIONNTT-MECorporationJP	false
198.196.224.109	unknown	United States		292	ESNET-WESTUS	false
153.239.66.159	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
220.216.56.40	unknown	Japan		10010	TOKAITOKAICommunicationsCorporationJP	false
124.225.208.91	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
105.143.72.239	unknown	Morocco		6713	IAM-ASMA	false
177.203.133.248	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
192.233.100.166	unknown	United States		3356	LEVEL3US	false
112.249.78.53	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
220.0.129.208	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
141.156.237.63	unknown	United States		701	UUNETUS	false
110.141.121.185	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
83.138.58.49	unknown	unknown		207642	LEONIXDATACENTERFR	false
31.114.146.114	unknown	United Kingdom		12576	EELtdGB	false
17.234.124.225	unknown	United States		714	APPLE-ENGINEERINGUS	false
146.136.220.194	unknown	Switzerland		559	SWITCHPeeringrequestspeeringswitchchEU	false
247.168.152.143	unknown	Reserved		unknown	unknown	false
87.198.117.230	unknown	Ireland		34245	MAGNET-ASIE	false
169.31.128.125	unknown	United States		37611	AfrihostZA	false
210.112.251.134	unknown	Korea Republic of		4663	ELIMNET-AS-KRELIMNETINCKR	false
58.114.227.42	unknown	Taiwan; Republic of China (ROC)		9416	MULTIMEDIA-AS-APHoshinMultimediaCenterIncTW	false
123.47.209.227	unknown	Korea Republic of		6619	SAMSUNGSDS-AS-KRSamsungSDSIncKR	false
243.219.250.131	unknown	Reserved		unknown	unknown	false
195.136.103.120	unknown	Poland		200539	INTELLYSPJ-ASINTELLYPL	false
40.192.134.233	unknown	United States		4249	LILLY-ASUS	false
254.52.94.164	unknown	Reserved		unknown	unknown	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
164.65.13.51	unknown	United States		1778	DNIC-AS-01778US	false
212.9.249.185	unknown	Ukraine		6703	ALKAR-ASUA	false
186.170.17.43	unknown	Colombia		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
133.27.156.188	unknown	Japan		38635	KEIO-NETKeioUniversityJP	false
155.232.197.139	unknown	South Africa		2018	TENET-1ZA	false
109.4.187.52	unknown	France		15557	LDCOMNETFR	false
99.189.112.218	unknown	United States		7018	ATT-INTERNET4US	false
184.6.30.97	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
186.37.158.45	unknown	Chile		27925	EntelPCSTelecomunicacionesSACL	false
109.1.194.240	unknown	France		15557	LDCOMNETFR	false
87.179.231.26	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
151.75.212.221	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
218.31.166.125	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
191.133.1.249	unknown	Brazil		26615	TIMSABR	false
186.235.64.46	unknown	Brazil		262725	RGSILVEIRALTDABR	false
158.197.0.29	unknown	Slovakia (SLOVAK Republic)		2607	SANETSlovakAcademicNetworkSK	false
154.145.140.146	unknown	Morocco		6713	IAM-ASMA	false

Runtime Messages

Command:	/tmp/52lN2HSY7O
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/var/cache/motd-news	
Process:	/usr/bin/cut
File Type:	ASCII text
Category:	dropped
Size (bytes):	191
Entropy (8bit):	4.515771857099866
Encrypted:	false
SSDEEP:	3:P2lnl+5MsqqzNLz+FRNScHUBfRau95++sZzR5woLB1Fh0VTGTl/X5kURn:OZ8uNLzDc0pR75+9Zz/woFmlT52URn
MD5:	DD514F892B5F93ED615D366E58AC58AF
SHA1:	BA75EDB3C2232CC260BC187F604DC8F25AA72C11
SHA-256:	F40D0DCE6E83DF74109FEF5E68E51CC255727783EEAE04C3E34677E23F7552CF
SHA-512:	9150BDE63F6C4850C5340D8877892B4D9BBF9EBDC98CDCF557A93FA304C1222CEE446418F5BE2ACCDBF38393778AFA5D4F3EDCB37A47BF57D3A4B2DEAD42A2D0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	* Super-optimized for small spaces - read how we shrank the memory. footprint of MicroK8s to make it the smallest full K8s around... https://ubuntu.com/blog/microk8s-memory-optimisation.

Static File Info

General

File type:	ELF 32-bit MSB executable, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.214678185526423
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	52lN2HSY7O
File size:	53052
MD5:	e0db3c63694e83c4ea4187a6fd40c9d2
SHA1:	d04a564f43e9ed664478443199b196d6cb191580
SHA256:	da6d168edfc190ef5f7a8ae9ad40de97ea559989c3f7421af1c9a0909522dbf4
SHA512:	540dd1a5feed9777760399c626a0ce4dfcee4bf3d39c5631765a7b949fa2084495cb458ee31efe017a161714090491...59d841abb5175df66ecbad22f53dcb7fbb
SSDEEP:	768:8CeKEfhe5XdrbejRIcfFMQ/5MdgFHj0iPuvWeffpqmUJTXr6Lu380D3:dsfIBZe5tJrFj0imvppqmUJP6Lc82
File Content Preview:	.ELF.....D...4.....4. ...(.....p..... .dt.Q.....NV..a....da.....N^NuNV..J9...lf>"y.... QJ.g.X.#.....N."y.... QJ.f.A.....J.g.Hy....N.X.....lN^NuNV..N^NuN

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MC68000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x80000144
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	52652
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

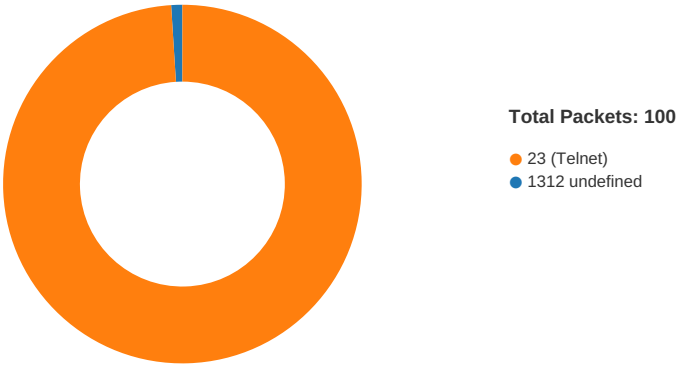
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0xc5d6	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x8000c67e	0xc67e	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x8000c68c	0xc68c	0x56c	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x8000ebfc	0xcbfc	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8000ec04	0xcc04	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x8000ec10	0xcc10	0x15c	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x8000ed6c	0xcd6c	0x23c	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xcd6c	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	0x80000000	0x80000000	0xcbf8	0xcbf8	4.2316	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0xcbfc	0x8000ebfc	0x8000ebfc	0x170	0x3ac	0.2775	0x6	RW	0x2000		.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: dash PID: 5186 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5186 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.JmXH35JStJ
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5187 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5187 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5188 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5188 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: 5189 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5189 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: 5190 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5190 Parent PID: 4331

General

Start time:	01:33:46

Start date:	15/01/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.JmXH35JStJ
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5191 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5191 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5192 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5192 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037

File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: 5193 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5193 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

File Written

Analysis Process: dash PID: 5194 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5194 Parent PID: 4331

General

Start time:	01:33:46
Start date:	15/01/2022
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.JmXH35JStJ /tmp/tmp.AdZnWFxIG7 /tmp/tmp.Bef8J1nfzZ

File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: 52lN2HSY7O PID: 5242 Parent PID: 5106

General

Start time:	01:33:51
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	/tmp/52lN2HSY7O
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: 52lN2HSY7O PID: 5244 Parent PID: 5242

General

Start time:	01:33:51
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: 52lN2HSY7O PID: 5343 Parent PID: 5244

General

Start time:	01:36:43
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 52lN2HSY7O PID: 5346 Parent PID: 5244

General

Start time:	01:36:43
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 52lN2HSY7O PID: 5350 Parent PID: 5346

General

Start time:	01:36:43
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 52lN2HSY7O PID: 5359 Parent PID: 5350

General

Start time:	01:36:48
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 52lN2HSY7O PID: 5361 Parent PID: 5350

General

Start time:	01:36:48
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 52lN2HSY7O PID: 5352 Parent PID: 5346

General

Start time:	01:36:43
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 52lN2HSY7O PID: 5354 Parent PID: 5346

General

Start time:	01:36:43
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 52lN2HSY7O PID: 5245 Parent PID: 5242

General

Start time:	01:33:51
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 52lN2HSY7O PID: 5247 Parent PID: 5242

General

Start time:	01:33:51
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 52lN2HSY7O PID: 5250 Parent PID: 5247

General

Start time:	01:33:51
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: 52lN2HSY7O PID: 5342 Parent PID: 5250

General

Start time:	01:36:43

Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 52lN2HSY7O PID: 5344 Parent PID: 5250

General

Start time:	01:36:43
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 52lN2HSY7O PID: 5251 Parent PID: 5247

General

Start time:	01:33:51
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: 52lN2HSY7O PID: 5255 Parent PID: 5247

General

Start time:	01:33:51
Start date:	15/01/2022
Path:	/tmp/52lN2HSY7O
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc