ID: 679269
Sample Name: Smqw34mNlm
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 14:02:57
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

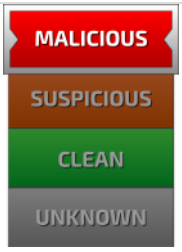
Smqw34mNlm

Overview

General Information

Sample Name:	Smqw34mNlm
Analysis ID:	679269
MD5:	280c087a0073bd..
SHA1:	0c650be334cc8f…
SHA256:	8b5fc53ad49b00..
Tags:	64 elf mirai
Infos:	

Detection



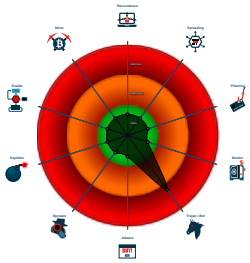
Mirai

Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Machine Learning detection for sam…
- Yara signature match
- Sample has stripped symbol table
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…
- Sample listens on a socket

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:	35.0.0 Citrine
Analysis ID:	679269
Start date and time: 05/08/202214:02:57	2022-08-05 14:02:57 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Smqw34mNlm
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:	mal76.troj.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/Smqw34mNlm
PID:	6223
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	your device just got infected to a bootnoot
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- Smqw34mNlm (PID: 6223, Parent: 6122, MD5: 280c087a0073bd36784e8af0b7254670) Arguments: /tmp/Smqw34mNlm
  - Smqw34mNlm New Fork (PID: 6224, Parent: 6223)
    - Smqw34mNlm New Fork (PID: 6225, Parent: 6224)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Smqw34mNlm	Linux_Trojan_Gafgyt_9e9530a7	unknown	unknown	• 0x5634:$a: F6 48 63 FF B8 36 00 00 00 0F 05 48 3D 00 F0 FF FF 48 89 C3
Smqw34mNlm	Linux_Trojan_Gafgyt_807911a2	unknown	unknown	• 0x5e23:$a: FE 48 39 F3 0F 94 C2 48 83 F9 FF 0F 94 C0 84 D0 74 16 4B 8D
Smqw34mNlm	Linux_Trojan_Gafgyt_d4227dbf	unknown	unknown	• 0x4d2e:$a: FF 48 81 EC D0 00 00 00 48 8D 84 24 E0 00 00 00 48 89 54 24 30 C7 04 24 18 00 • 0x4e64:$a: FF 48 81 EC D0 00 00 00 48 8D 84 24 E0 00 00 00 48 89 54 24 30 C7 04 24 18 00
Smqw34mNlm	Linux_Trojan_Gafgyt_620087b9	unknown	unknown	• 0x59e3:$a: 48 89 D8 48 83 C8 01 EB 04 48 8B 76 10 48 3B 46 08 72 F6 48 8B
Smqw34mNlm	Linux_Trojan_Gafgyt_0cd591cd	unknown	unknown	• 0x5272:$a: 4E F8 48 8D 4E D8 49 8D 42 E0 48 83 C7 03 EB 6B 4C 8B 46 F8 48 8D

Click to see the 3 entries

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
6223.1.0000000000400000.0000000000409000.r-x.sdmp	Linux_Trojan_Gafgyt_9e9530a7	unknown	unknown	• 0x5634:$a: F6 48 63 FF B8 36 00 00 00 0F 05 48 3D 00 F0 FF FF 48 89 C3
6223.1.0000000000400000.0000000000409000.r-x.sdmp	Linux_Trojan_Gafgyt_807911a2	unknown	unknown	• 0x5e23:$a: FE 48 39 F3 0F 94 C2 48 83 F9 FF 0F 94 C0 84 D0 74 16 4B 8D
6223.1.0000000000400000.0000000000409000.r-x.sdmp	Linux_Trojan_Gafgyt_d4227dbf	unknown	unknown	• 0x4d2e:$a: FF 48 81 EC D0 00 00 00 48 8D 84 24 E0 00 00 00 48 89 54 24 30 C7 04 24 18 00 • 0x4e64:$a: FF 48 81 EC D0 00 00 00 48 8D 84 24 E0 00 00 00 48 89 54 24 30 C7 04 24 18 00
6223.1.0000000000400000.0000000000409000.r-x.sdmp	Linux_Trojan_Gafgyt_620087b9	unknown	unknown	• 0x59e3:$a: 48 89 D8 48 83 C8 01 EB 04 48 8B 76 10 48 3B 46 08 72 F6 48 8B
6223.1.0000000000400000.0000000000409000.r-x.sdmp	Linux_Trojan_Gafgyt_0cd591cd	unknown	unknown	• 0x5272:$a: 4E F8 48 8D 4E D8 49 8D 42 E0 48 83 C7 03 EB 6B 4C 8B 46 F8 48 8D

Click to see the 3 entries

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

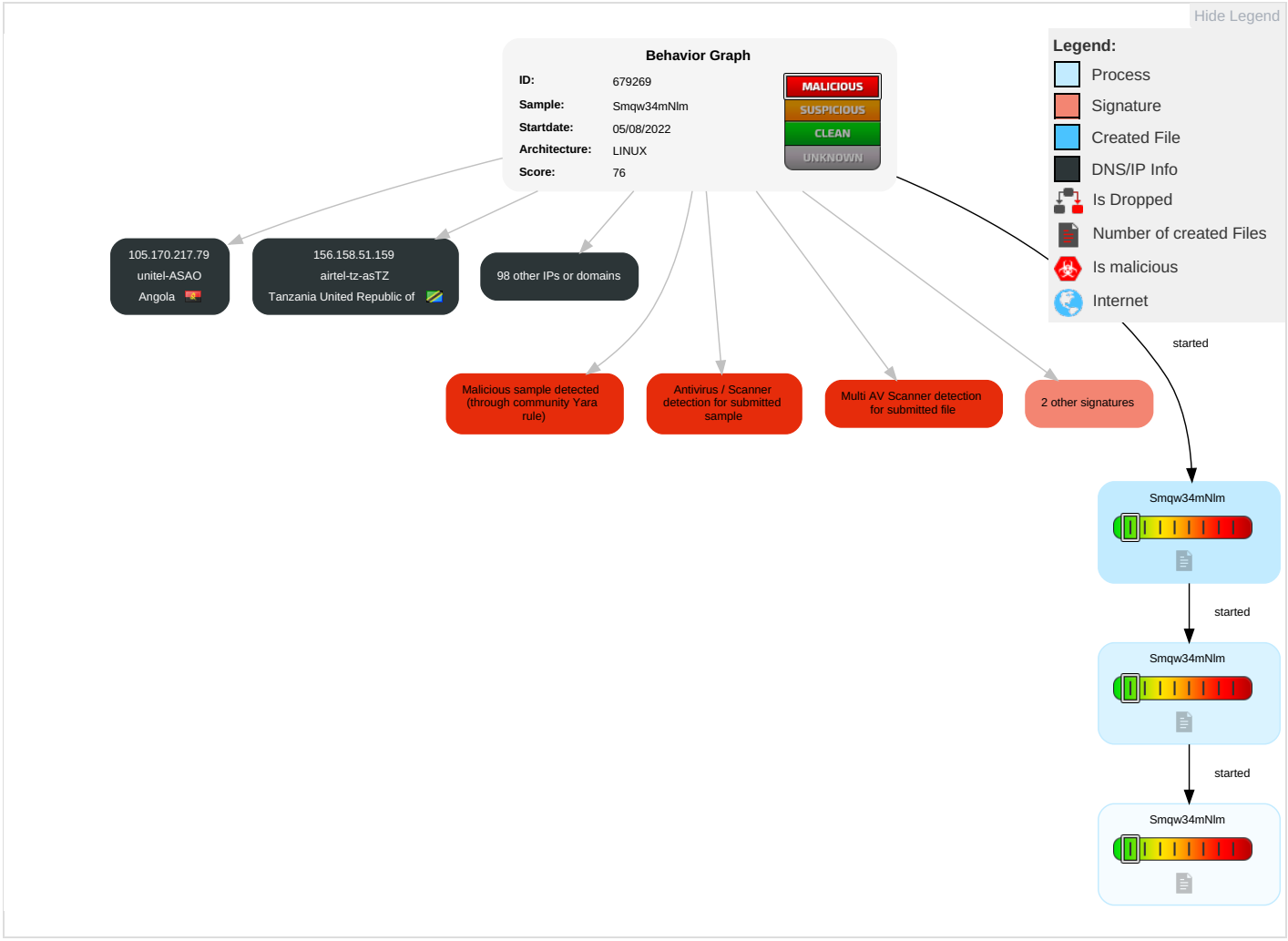
Mitre Att&ck Matrix

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 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
Smqw34mNlm	38%	Virustotal		Browse
Smqw34mNlm	77%	ReversingLabs	Linux.Trojan.Mirai	
Smqw34mNlm	100%	Avira	LINUX/Mirai.zxjge	
Smqw34mNlm	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

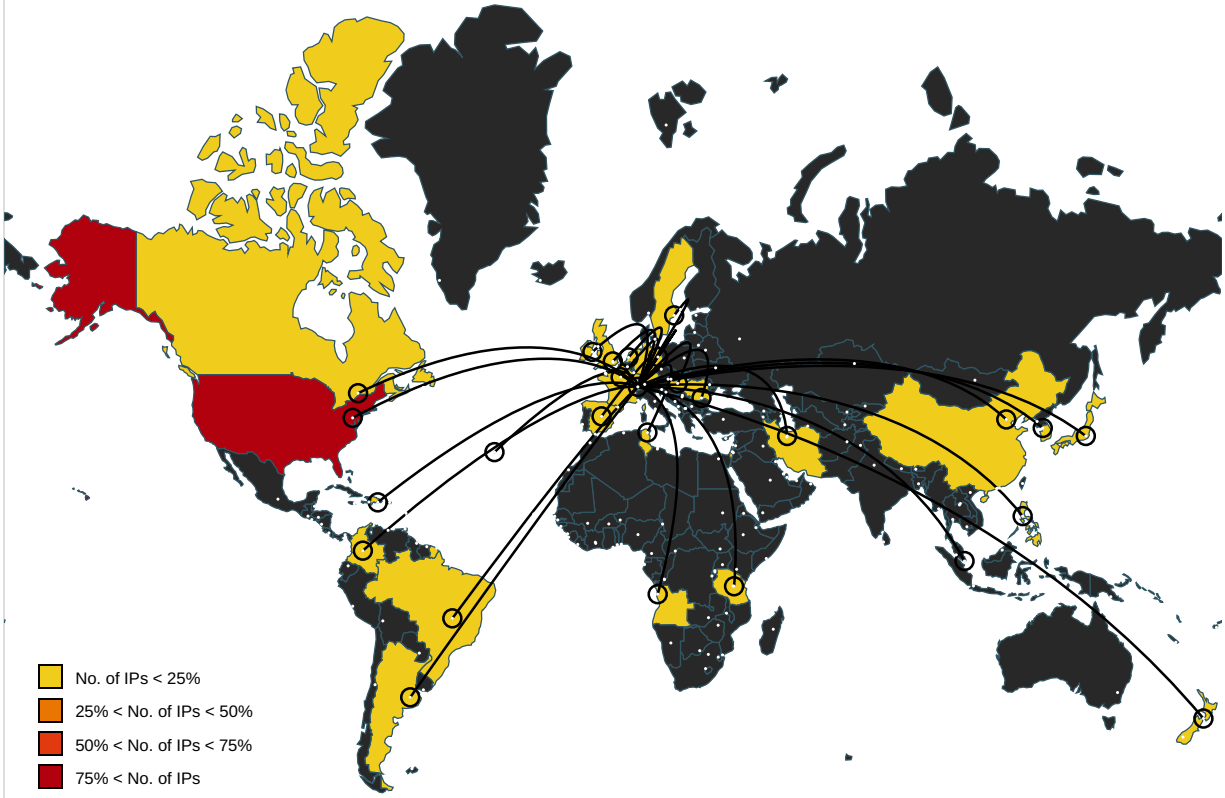
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
130.41.108.217	unknown	United States		243	HARRIS-ATD-ASUS	false
105.170.217.79	unknown	Angola		37119	unitel-ASAO	false
172.95.97.83	unknown	United States		5650	FRONTIER-FRTRUS	false
24.119.32.80	unknown	United States		11492	CABLEONEUS	false
30.69.36.129	unknown	United States		7922	COMCAST-7922US	false
75.58.102.119	unknown	United States		7018	ATT-INTERNET4US	false
245.241.93.17	unknown	Reserved		unknown	unknown	false
252.212.204.109	unknown	Reserved		unknown	unknown	false
108.17.85.21	unknown	United States		701	UUNETUS	false
125.84.43.238	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
74.39.32.134	unknown	United States		7011	FRONTIER-AND-CITIZENSUS	false
81.248.152.139	unknown	France		3215	FranceTelecom-OrangeFR	false
56.243.22.28	unknown	United States		2686	ATGS-MMD-ASUS	false
82.163.179.146	unknown	United Kingdom		34119	WILDCARD-ASWildcardUKLimitedGB	false
59.204.179.226	unknown	China		2516	KDDIKDDICORPORATIONJP	false
6.204.135.131	unknown	United States		3356	LEVEL3US	false
120.73.155.204	unknown	Korea Republic of		9761	KUMHO-ASKUMHOKR	false
116.203.175.100	unknown	Germany		24940	HETZNER-ASDE	false
21.113.206.71	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
86.122.212.76	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
102.241.140.246	unknown	Tunisia		36926	CKL1-ASNKE	false
99.243.147.138	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
93.173.74.246	unknown	Israel		1680	NV-ASNCELLCOMltdIL	false
251.168.78.125	unknown	Reserved		unknown	unknown	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.182.151.38	unknown	United States		7018	ATT-INTERNET4US	false
108.137.250.74	unknown	United States		16509	AMAZON-02US	false
216.157.141.99	unknown	United States		64200	VIVIDHOSTINGUS	false
21.235.122.143	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
87.40.33.219	unknown	Ireland		1213	HEANETIE	false
13.64.110.77	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
46.164.101.132	unknown	Iran (ISLAMIC Republic Of)		21283	A1SI-ASA1SlovenijaSI	false
252.168.83.145	unknown	Reserved		unknown	unknown	false
47.70.101.167	unknown	United States		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
243.151.202.251	unknown	Reserved		unknown	unknown	false
223.175.71.94	unknown	Korea Republic of		17853	LGTELECOM-AS-KRLGTELECOMKR	false
241.120.231.67	unknown	Reserved		unknown	unknown	false
205.23.67.181	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
163.242.135.255	unknown	Germany		668	DNIC-AS-00668US	false
4.88.72.209	unknown	United States		3356	LEVEL3US	false
48.88.173.146	unknown	United States		2686	ATGS-MMD-ASUS	false
65.223.235.70	unknown	United States		14251	MLSLIUS	false
184.221.32.102	unknown	United States		10507	SPCSUS	false
2.202.172.190	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
15.181.88.203	unknown	United States		5073	HPESUS	false
155.46.249.142	unknown	United States		24324	KORDIA-TRANSIT-AS-APKordiaLimitedNZ	false
81.137.110.100	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
13.185.138.46	unknown	United States		7018	ATT-INTERNET4US	false
206.139.179.160	unknown	United States		701	UUNETUS	false
199.10.82.74	unknown	United States		397086	LAYER-HOST-HOUSTONUS	false
132.202.39.111	unknown	Canada		10754	GOV-FRB-BOGUS	false
72.127.213.109	unknown	United States		22394	CELLCOUS	false
190.109.191.109	unknown	Colombia		27695	EDATELSAESPCO	false
173.140.11.76	unknown	United States		10507	SPCSUS	false
156.158.51.159	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
25.54.136.191	unknown	United Kingdom		7922	COMCAST-7922US	false
93.246.95.232	unknown	Germany		3320	DTAGInternetserviceproviderationsDE	false
52.107.25.220	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
45.185.84.70	unknown	Brazil		269408	EdmilsondeLimaAraujo-meBR	false
55.35.146.194	unknown	United States		322	DNIC-ASBLK-00306-00371US	false
76.58.177.92	unknown	United States		18494	CENTURYLINK-LEGACY-EMBARQ-WRBGUS	false
89.141.144.186	unknown	Spain		12430	VODAFONE_ESES	false
24.57.77.34	unknown	Canada		7992	COGECOWAVECA	false
212.84.77.133	unknown	United Kingdom		198382	FIRSTEASY-ASGB	false
100.88.99.186	unknown	Reserved		701	UUNETUS	false
152.0.104.82	unknown	Dominican Republic		6400	CompaniaDominicanadeTelefonosSADO	false
240.228.111.21	unknown	Reserved		unknown	unknown	false
222.159.198.164	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
40.102.64.11	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
181.87.83.61	unknown	Argentina		7303	TelecomArgentinaSAAR	false
54.51.52.171	unknown	United States		14618	AMAZON-AESUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
8.222.140.99	unknown	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
138.99.105.43	unknown	Brazil		52764	DeltaBroadbandTelecomProvedoresdeInternetLtdBR	false
162.202.25.19	unknown	United States		7018	ATT-INTERNET4US	false
136.74.244.2	unknown	United States		60311	ONEFMCH	false
250.177.253.177	unknown	Reserved		unknown	unknown	false
71.233.212.132	unknown	United States		7922	COMCAST-7922US	false
96.195.149.26	unknown	United States		7922	COMCAST-7922US	false
5.234.141.95	unknown	Iran (ISLAMIC Republic Of)		58224	TCIIR	false
133.125.49.232	unknown	Japan		7684	SAKURA-ASAKURAInternetIncJP	false
26.138.209.53	unknown	United States		7922	COMCAST-7922US	false
243.182.99.116	unknown	Reserved		unknown	unknown	false
49.227.44.247	unknown	New Zealand		9500	VODAFONE-TRANSIT-ASVodafoneNZLtdNZ	false
8.123.122.28	unknown	United States		3356	LEVEL3US	false
13.20.238.138	unknown	United States		395959	XEROX-ELLUS	false
46.107.141.193	unknown	Hungary		5483	MAGYAR-TELEKOM-MAIN-ASMagyarTelekomNyrtHU	false
186.234.255.181	unknown	Brazil		19089	UOLDIVEOSABR	false
69.166.99.217	unknown	United States		26527	LIGHTWAVE-NETWORKSUS	false
177.203.221.213	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
40.216.186.116	unknown	United States		4249	LILLY-ASUS	false
133.106.140.194	unknown	Japan		138384	RMNI-AS-APRakutenMobileNetworkIncJP	false
137.8.149.51	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
216.110.27.234	unknown	United States		36070	NCHCORPUS	false
82.75.178.20	unknown	Netherlands		33915	TNF-ASNL	false
38.77.254.22	unknown	United States		395719	EMERALDUS	false
152.14.250.158	unknown	United States		11442	NCSUUS	false
34.142.42.124	unknown	United States		2686	ATGS-MMD-ASUS	false
82.214.10.135	unknown	Sweden		42708	PORTLANEwwwportlanecomSE	false
124.105.52.172	unknown	Philippines		9299	IPG-AS-APPhilippineLongDistanceTelephoneCompanyPH	false
15.123.220.174	unknown	United States		13979	ATT-IPFRUS	false
107.111.117.130	unknown	United States		7018	ATT-INTERNET4US	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 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.764749674440205
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	Smqw34mNlm
File size:	38144
MD5:	280c087a0073bd36784e8af0b7254670
SHA1:	0c650be334cc8f692102e27d4a0e9ae3d97afd71
SHA256:	8b5fc53ad49b0005798e9fdd8a9738d798755ee6070b08d1fff41c848200548a
SHA512:	55d0b717f05af68ddf090e8423b6b296713ef8a63355c7818d077794b6b0082a220bb67782882ce5dde35b64836c66aadaad3b4cc06bee6fbb48c0a82645eee4
SSDEEP:	768:gl18lk3XKf9kLb5R3c97Clb6jrojNC5I:olHOo/q7CF6fB5I
TLSH:	020318132450C1FCD549C5705BBFA22BCA33F07D5235FA8A73A47E2A6E0BE311E1A849
File Content Preview:	.ELF.....>.....@.....@.....@.8...@.....@.....@.....@.....@.....P.....P.....@.....Q.td.....H. ..._.....w..H.....

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:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x400194
Flags:	0x0
ELF Header Size:	64
Program Header Offset:	64
Program Header Size:	56
Number of Program Headers:	3
Section Header Offset:	37504
Section Header Size:	64
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	0x4000e8	0xe8	0x13	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x400100	0x100	0x77e6	0x0	0x6	AX	0	0	16

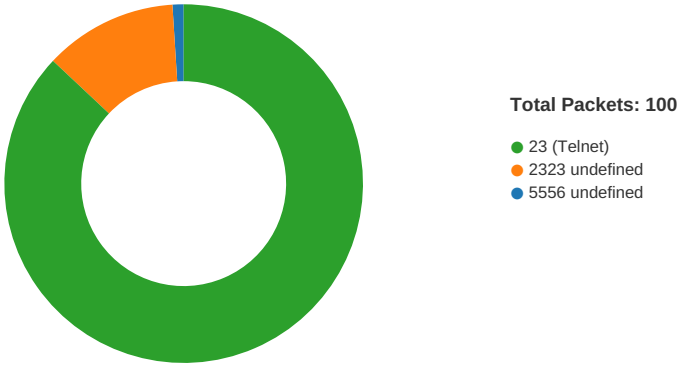
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.fini	PROGBITS	0x4078e6	0x78e6	0xe	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x407900	0x7900	0xc40	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x509000	0x9000	0x10	0x0	0x3	WA	0	0	8
.dtors	PROGBITS	0x509010	0x9010	0x10	0x0	0x3	WA	0	0	8
.data	PROGBITS	0x509040	0x9040	0x200	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x509240	0x9240	0xb68	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0x9240	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	0x400000	0x400000	0x8540	0x8540	6.1466	0x5	R E	0x100000		.init .text .fini .rodata
LOAD	0x9000	0x509000	0x509000	0x240	0xda8	2.8704	0x6	RW	0x100000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x8		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: Smqw34mNlm PID: 6223, Parent PID: 6122

General

Start time:	14:03:43
Start date:	05/08/2022
Path:	/tmp/Smqw34mNlm
Arguments:	/tmp/Smqw34mNlm
File size:	38144 bytes
MD5 hash:	280c087a0073bd36784e8af0b7254670

Analysis Process: Smqw34mNlm PID: 6224, Parent PID: 6223

General

Start time:	14:03:43

Start date:	05/08/2022
Path:	/tmp/Smqw34mNlm
Arguments:	n/a
File size:	38144 bytes
MD5 hash:	280c087a0073bd36784e8af0b7254670

Analysis Process: Smqw34mNlm PID: **6225**, Parent PID: **6224**

General

Start time:	14:03:43
Start date:	05/08/2022
Path:	/tmp/Smqw34mNlm
Arguments:	n/a
File size:	38144 bytes
MD5 hash:	280c087a0073bd36784e8af0b7254670