ID: 679506
Sample Name: Nmg21us74l
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 22:22:16
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

Nmg21us74l

Overview

General Information

Sample Name:	Nmg21us74l
Analysis ID:	679506
MD5:	01ec15a16805e0..
SHA1:	d9ea867164e9ad.
SHA256:	a3946c00d0daf5..
Tags:	32 arm elf mirai
Infos:	

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

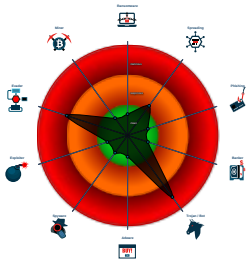
Mirai

Score:	88
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample deletes itself
- Uses known network protocols on n…
- Yara signature match
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Tries to connect to HTTP servers, b…

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:	35.0.0 Citrine
Analysis ID:	679506
Start date and time: 05/08/202222:22:16	2022-08-05 22:22:16 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Nmg21us74l
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:	mal88.troj.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/Nmg21us74l
PID:	6230
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	BEASTMODE-BITCHES@@"""""/p

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- Nmg21us74l (PID: 6230, Parent: 6123, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/Nmg21us74l
  - Nmg21us74l New Fork (PID: 6234, Parent: 6230)
  - Nmg21us74l New Fork (PID: 6236, Parent: 6230)
  - Nmg21us74l New Fork (PID: 6238, Parent: 6230)
  - Nmg21us74l New Fork (PID: 6241, Parent: 6230)
    - Nmg21us74l New Fork (PID: 6250, Parent: 6241)
    - Nmg21us74l New Fork (PID: 6252, Parent: 6241)
    - Nmg21us74l New Fork (PID: 6253, Parent: 6241)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Nmg21us74l	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0xeb14:$x1: POST /cdn-cgi/ • 0xefd0:$s1: LCOGQGPTGP
Nmg21us74l	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0xeb14:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
Nmg21us74l	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	

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
6234.1.00007f86f4017000.00007f86f4027000.r-x.sdmp	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0xeb14:$x1: POST /cdn-cgi/ • 0xefd0:$s1: LCOGQGPTGP
6234.1.00007f86f4017000.00007f86f4027000.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0xeb14:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
6234.1.00007f86f4017000.00007f86f4027000.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
6230.1.00007f86f4017000.00007f86f4027000.r-x.sdmp	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0xeb14:$x1: POST /cdn-cgi/ • 0xefd0:$s1: LCOGQGPTGP
6230.1.00007f86f4017000.00007f86f4027000.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0xeb14:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
Click to see the 7 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

Networking

Uses known network protocols on non-standard ports

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Sample deletes itself

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

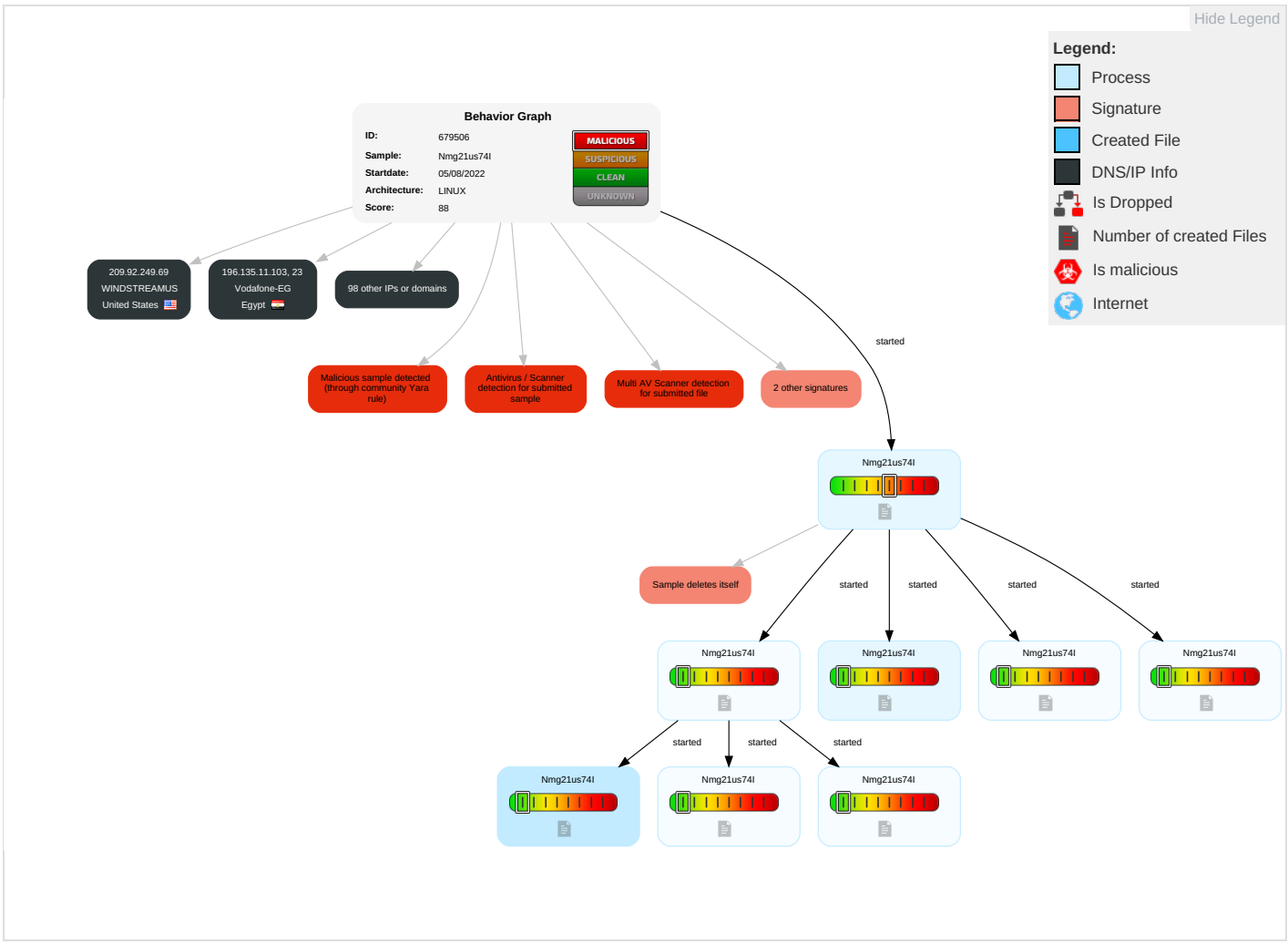
Mitre Att&ck Matrix

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 File Deletion	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
Nmg21us74l	58%	Virustotal		Browse
Nmg21us74l	68%	ReversingLabs	Linux.Trojan.Mirai	
Nmg21us74l	100%	Avira	LINUX/Mirai.bonb	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

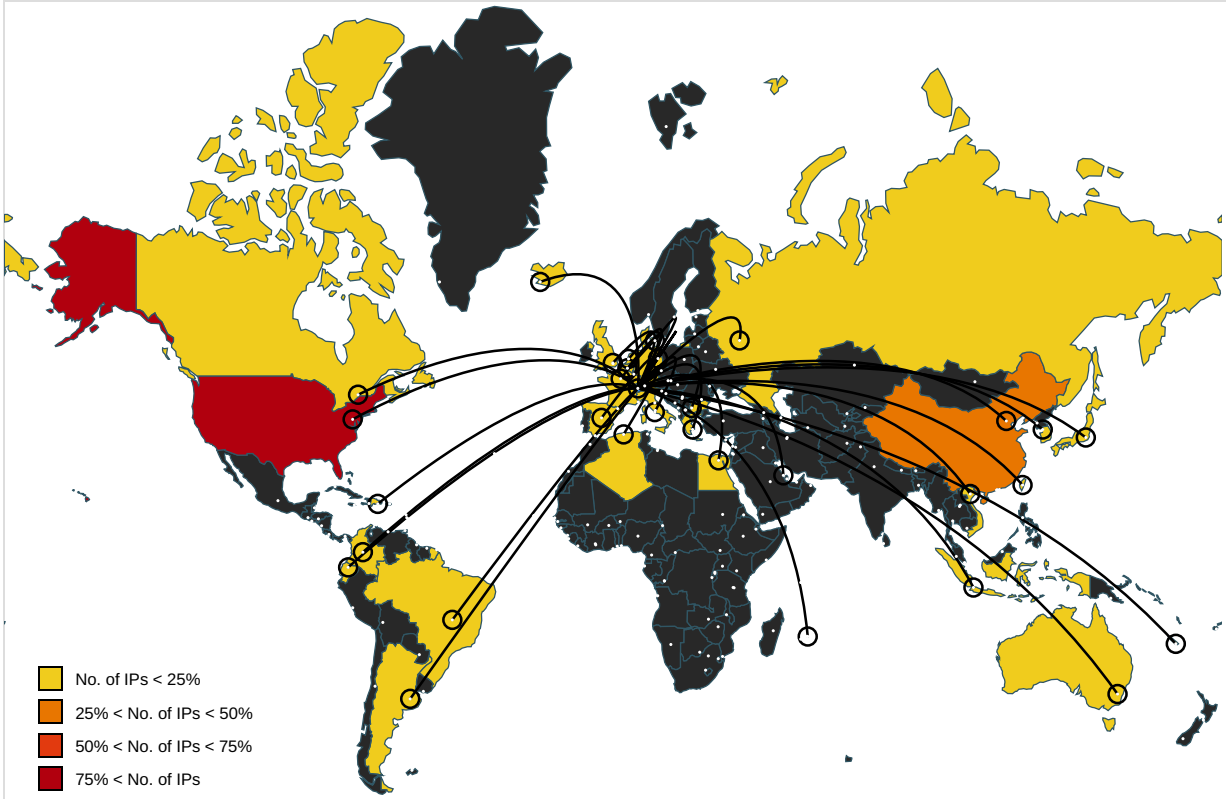
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
105.22.224.11	unknown	Mauritius		37100	SEACOM-ASMU	false
245.116.1.135	unknown	Reserved		unknown	unknown	false
222.233.103.170	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
246.9.2.21	unknown	Reserved		unknown	unknown	false
157.3.239.204	unknown	Japan		7671	MCNETNTTSmartConnectCorporationJP	false
108.178.45.135	unknown	United States		32475	SINGLEHOP-LLCUS	false
18.229.102.137	unknown	United States		16509	AMAZON-02US	false
32.160.66.218	unknown	United States		2686	ATGS-MMD-ASUS	false
53.16.36.106	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
76.28.59.66	unknown	United States		7922	COMCAST-7922US	false
121.92.158.157	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
223.201.67.26	unknown	China		4782	GSNETDataCommunicationBusinessGroupTW	false
246.109.35.181	unknown	Reserved		unknown	unknown	false
141.52.191.37	unknown	Germany		34878	KITKarlsruheInstituteofTechnologyDE	false
77.69.178.110	unknown	Bahrain		5416	InternetServiceProviderBH	false
133.192.104.39	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
32.48.63.177	unknown	United States		7018	ATT-INTERNET4US	false
75.36.168.76	unknown	United States		7018	ATT-INTERNET4US	false
100.173.129.169	unknown	United States		21928	T-MOBILE-AS21928US	false
141.227.0.199	unknown	France		21070	TOTALFR	false
120.169.246.82	unknown	Indonesia		4761	INDOSAT-INP-APINDOSATInternetNetworkProviderID	false
209.92.249.69	unknown	United States		7029	WINDSTREAMUS	false
54.140.144.36	unknown	United States		14618	AMAZON-AESUS	false
111.231.40.22	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
254.106.28.224	unknown	Reserved		unknown	unknown	false
166.117.52.131	unknown	United States		58681	NSWPOLSERV-AS-APNewSouthWalesPoliceAU	false
196.135.11.103	unknown	Egypt		36935	Vodafone-EG	false
104.80.152.99	unknown	United States		16625	AKAMAI-ASUS	false
98.173.208.29	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
179.53.118.76	unknown	Dominican Republic		6400	CompaniaDominicanadeTelefonosSADO	false
90.192.140.251	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
16.11.95.214	unknown	United States		unknown	unknown	false
186.178.15.174	unknown	Ecuador		28006	CORPORACIONNACIONALDETELECOMUNICACIONES-CNTEPEC	false
13.71.171.245	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
94.146.159.116	unknown	Denmark		9158	TELENOR_DANMARK_ASDK	false
118.150.116.140	unknown	Taiwan; Republic of China (ROC)		18419	DADA-AS-TWDaDaBroadbandLTDTW	false
170.131.82.35	unknown	United States		13954	STAPLESUS	false
89.248.107.35	unknown	Spain		48348	CLOUDBUILDERSES	false
197.53.119.202	unknown	Egypt		8452	TE-ASTE-ASEG	false
57.5.138.225	unknown	Belgium		2686	ATGS-MMD-ASUS	false
191.153.57.180	unknown	Colombia		26611	COMCELSACO	false
93.123.76.73	unknown	Bulgaria		43561	NET1-ASBG	false
208.41.137.69	unknown	United States		4565	MEGAPATH2-US	false
197.161.195.3	unknown	Egypt		24863	LINKdotNET-ASEG	false
220.65.188.96	unknown	Korea Republic of		9316	DACOM-PUBNETPLUS-AS-KRDACOM-PUBNETPLUSKR	false
81.211.32.43	unknown	Russian Federation		3216	SOVAM-ASRU	false
117.142.30.125	unknown	China		56040	CMNET-GUANGDONG-APChinaMobilecommunicationscorporation	false
203.54.162.175	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
88.125.239.228	unknown	France		12322	PROXADFR	false
210.84.92.204	unknown	Australia		703	UUNETUS	false
73.233.169.114	unknown	United States		7922	COMCAST-7922US	false
51.14.10.117	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
124.28.140.227	unknown	Korea Republic of		23578	NAMDONGNET-AS-KRTBROADSaeromNamdongSeohaebroadcastingKR	false
162.119.15.38	unknown	United States		3379	KAISER-NCALUS	false
185.41.237.242	unknown	Belgium		199942	CHEOPSBE	false
45.1.177.213	unknown	United States		7377	UCSDUS	false
43.110.214.123	unknown	Japan		4249	LILLY-ASUS	false
14.245.235.120	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
111.208.128.52	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
72.137.191.183	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
160.39.196.228	unknown	United States		14	COLUMBIA-GWUS	false
181.104.155.22	unknown	Argentina		6147	TelefonicadelPeruSAAPE	false
82.221.170.8	unknown	Iceland		30818	IS-ADVANIA-TRANSITIS	false
66.141.134.12	unknown	United States		7018	ATT-INTERNET4US	false
121.137.201.237	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
172.7.251.188	unknown	United States		7018	ATT-INTERNET4US	false
252.163.150.243	unknown	Reserved		unknown	unknown	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
122.114.141.69	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
153.161.19.176	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
124.94.70.87	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
75.50.159.107	unknown	United States		7018	ATT-INTERNET4US	false
162.5.54.167	unknown	United States		33348	PIERCE-COUNTYUS	false
201.68.106.106	unknown	Brazil		27699	TELEFONICABRASILSABR	false
44.78.82.191	unknown	United States		7377	UCSDUS	false
67.0.96.13	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
244.53.184.180	unknown	Reserved		unknown	unknown	false
151.168.66.12	unknown	United States		45025	EDN-ASUA	false
112.107.186.81	unknown	Korea Republic of		6619	SAMSUNGSDS-AS-KRSamsungSDSIncKR	false
145.22.219.194	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
61.230.253.244	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
35.25.130.31	unknown	United States		36375	UMICH-AS-5US	false
72.155.239.236	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
87.203.200.222	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	false
69.234.250.41	unknown	China		7018	ATT-INTERNET4US	false
36.96.13.140	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
9.215.94.18	unknown	United States		3356	LEVEL3US	false
213.121.90.101	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
152.50.33.117	unknown	United States		81	NCRENUS	false
194.194.0.57	unknown	European Union		2686	ATGS-MMD-ASUS	false
243.144.161.246	unknown	Reserved		unknown	unknown	false
159.86.109.59	unknown	United Kingdom		1945	FR-LYRESLyonRechercheetEnseignementSuperieurLyRESE	false
75.10.61.95	unknown	United States		7018	ATT-INTERNET4US	false
113.20.55.68	unknown	New Caledonia		45461	TELENET-AS-APTeleNetNC	false
117.71.137.154	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
182.9.51.16	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
93.56.245.69	unknown	Italy		12874	FASTWEBIT	false
24.75.110.232	unknown	United States		3356	LEVEL3US	false
121.45.181.169	unknown	Australia		4739	INTERNODE-ASInternodePtyLtdAU	false
112.167.3.3	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
197.204.101.39	unknown	Algeria		36947	ALGTEL-ASDZ	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, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	6.056530017553513
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	Nmg21us74I
File size:	63948
MD5:	01ec15a16805e0b57d0ef42097dca5ec
SHA1:	d9ea867164e9ad0c1901b85c8f18174743e1a0b4
SHA256:	a3946c00d0daf54a7e99a22e731dbc7977936ef6c9591dd0ae2a45632626b357
SHA512:	d00a10fb66a353b990d03e0493b049f922b3c736ccfb88e40b4da84a398a48c99b2115f5eb2185ebf08bb062511927db0003ad567859ab47d2c25816eba28912
SSDEEP:	768:zHnEczUZv4tZy6hQfyjXI8CMRxYVsx/DeiZvspz1Y3W7wCVy/Jx+5H8hG1rmCd/4:rEFZEZyjyj48NCiZvsphYceZWTMWCBW
TLSH:	D453F8827D81AA16C7C05777FE1F018D3319A798E0EA73438C191BA17ACED1F0D6B65A
File Content Preview:	.ELF...a.....(.....4...<.....4. ...(.....,.....Q.td.....-...L."....:.....0@-.\P...0....S.0...P@...0... ....R.....0...0.....0... ....R..... 0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x8190
Flags:	0x2
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	63548

ELF header

Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

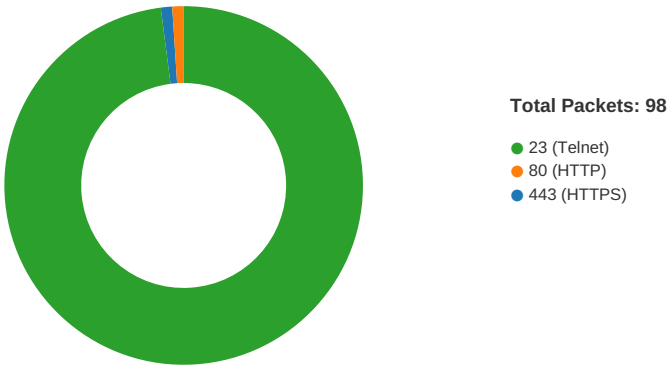
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0xea50	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x16b00	0xeb00	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x16b14	0xeb14	0xab8	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x1f5d0	0xf5d0	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x1f5d8	0xf5d8	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x1f5e4	0xf5e4	0x218	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x1f7fc	0xf7fc	0x578	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xf7fc	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	0x8000	0x8000	0xf5cc	0xf5cc	6.0810	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0xf5d0	0x1f5d0	0x1f5d0	0x22c	0x7a4	2.9355	0x6	RW	0x8000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: Nmg21us74l PID: 6230, Parent PID: 6123

General

Start time:	22:23:04
Start date:	05/08/2022
Path:	/tmp/Nmg21us74l

Arguments:	/tmp/Nmg21us74l
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Deleted

File Read

Directory Deleted

Analysis Process: Nmg21us74l PID: **6234**, Parent PID: **6230**

General

Start time:	22:23:07
Start date:	05/08/2022
Path:	/tmp/Nmg21us74l
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: Nmg21us74l PID: **6236**, Parent PID: **6230**

General

Start time:	22:23:07
Start date:	05/08/2022
Path:	/tmp/Nmg21us74l
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Nmg21us74l PID: **6238**, Parent PID: **6230**

General

Start time:	22:23:07
Start date:	05/08/2022
Path:	/tmp/Nmg21us74l
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Nmg21us74l PID: **6241**, Parent PID: **6230**

General

Start time:	22:23:07
Start date:	05/08/2022
Path:	/tmp/Nmg21us74l
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: Nmg21us74l PID: **6250**, Parent PID: **6241**

General

Start time:	22:23:14

Start date:	05/08/2022
Path:	/tmp/Nmg21us74l
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: Nmg21us74l PID: **6252**, Parent PID: **6241**

General

Start time:	22:23:14
Start date:	05/08/2022
Path:	/tmp/Nmg21us74l
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Nmg21us74l PID: **6253**, Parent PID: **6241**

General

Start time:	22:23:14
Start date:	05/08/2022
Path:	/tmp/Nmg21us74l
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1