ID: 679266
Sample Name: VefqQeU0Xt
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 13:55:02
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

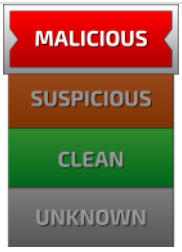
VefqQeU0Xt

Overview

General Information

Sample Name:	VefqQeU0Xt
Analysis ID:	679266
MD5:	b8ec31b1eff948a..
SHA1:	5590da71a98232.
SHA256:	f67ac47d33f3681..
Tags:	32 arm elf mirai
Infos:	

Detection



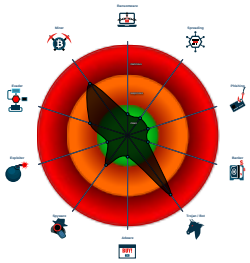
Mirai

Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Searches for CPU information (likely…
- Uses known network protocols on n…
- Executes the "grep" command used…
- Executes the "wget" command typic…
- Reads system information from the …
- Uses the "uname" system call to qu…
- Executes the "uname" command us…
- 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.

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:	679266
Start date and time: 05/08/202213:55:02	2022-08-05 13:55:02 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VefqQeU0Xt
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:	mal72.troj.mine.lin@0/4@0/0

Warnings

Runtime Messages

Command:	/tmp/VefqQeU0Xt
PID:	6253
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**
- systemd New Fork (PID: 6200, Parent: 1)
- 50-motd-news (PID: 6200, Parent: 1, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/update-motd.d/50-motd-news --force
  - 50-motd-news New Fork (PID: 6221, Parent: 6200)
  - mktemp (PID: 6221, Parent: 6200, MD5: e117ed1c2172d436fa31cc9d263131e8) Arguments: mktemp
  - 50-motd-news New Fork (PID: 6222, Parent: 6200)
  - mktemp (PID: 6222, Parent: 6200, MD5: e117ed1c2172d436fa31cc9d263131e8) Arguments: mktemp
  - 50-motd-news New Fork (PID: 6223, Parent: 6200)
  - mktemp (PID: 6223, Parent: 6200, MD5: e117ed1c2172d436fa31cc9d263131e8) Arguments: mktemp
  - 50-motd-news New Fork (PID: 6224, Parent: 6200)
    - 50-motd-news New Fork (PID: 6225, Parent: 6224)
    - dpkg (PID: 6225, Parent: 6224, MD5: 5e18156b434fc45062eec2f28b9147be) Arguments: dpkg -l wget
    - dpkg-query (PID: 6225, Parent: 6224, MD5: bf81745ea62201f11bc674cc7c1935fc) Arguments: dpkg-query --list -- wget
    - 50-motd-news New Fork (PID: 6226, Parent: 6224)
    - awk (PID: 6226, Parent: 6224, MD5: 7e9b2ed1272331cfbd2aac2e5eb3f84b) Arguments: awk "$1 == \"ii\" { print($3); exit(0); }"
  - 50-motd-news New Fork (PID: 6228, Parent: 6200)
    - 50-motd-news New Fork (PID: 6229, Parent: 6228)
    - 50-motd-news New Fork (PID: 6230, Parent: 6228)
    - sed (PID: 6230, Parent: 6228, MD5: 885062561f66aa1d4af4c54b9e7cc81a) Arguments: sed -e "s/ /\\/g"
  - 50-motd-news New Fork (PID: 6231, Parent: 6200)
  - uname (PID: 6231, Parent: 6200, MD5: 4ac7c634c5bec95753c480e9d421dcc2) Arguments: uname -o
  - 50-motd-news New Fork (PID: 6232, Parent: 6200)
  - uname (PID: 6232, Parent: 6200, MD5: 4ac7c634c5bec95753c480e9d421dcc2) Arguments: uname -r
  - 50-motd-news New Fork (PID: 6233, Parent: 6200)
  - uname (PID: 6233, Parent: 6200, MD5: 4ac7c634c5bec95753c480e9d421dcc2) Arguments: uname -m
  - 50-motd-news New Fork (PID: 6234, Parent: 6200)
  - uname (PID: 6234, Parent: 6200, MD5: 4ac7c634c5bec95753c480e9d421dcc2) Arguments: uname -m
  - 50-motd-news New Fork (PID: 6235, Parent: 6200)
    - 50-motd-news New Fork (PID: 6236, Parent: 6235)
    - grep (PID: 6236, Parent: 6235, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -m1 "^model name" /proc/cpuinfo
    - 50-motd-news New Fork (PID: 6237, Parent: 6235)
    - sed (PID: 6237, Parent: 6235, MD5: 885062561f66aa1d4af4c54b9e7cc81a) Arguments: sed -e "s/.*: //" -e s:\\s\\+:/:g
  - 50-motd-news New Fork (PID: 6238, Parent: 6200)
  - cloud-id (PID: 6238, Parent: 6200, MD5: 69f442c3e33b5f9a66b722c29ad89435) Arguments: /usr/bin/cloud-id
    - cloud-id New Fork (PID: 6243, Parent: 6238)
    - uname (PID: 6243, Parent: 6238, MD5: 4ac7c634c5bec95753c480e9d421dcc2) Arguments: uname -p
  - 50-motd-news New Fork (PID: 6244, Parent: 6200)
    - 50-motd-news New Fork (PID: 6245, Parent: 6244)
    - cut (PID: 6245, Parent: 6244, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -40 /tmp/tmp.ZtXsY8H9DY
    - 50-motd-news New Fork (PID: 6246, Parent: 6244)
    - tr (PID: 6246, Parent: 6244, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -c -d [:alnum:]
  - 50-motd-news New Fork (PID: 6247, Parent: 6200)
  - wget (PID: 6247, Parent: 6200, MD5: 996940118df7bb2aaa718589d4e95c08) Arguments: wget --timeout 60 -U "wget/1.20.3-1ubuntu1 Ubuntu/20.04.2/LTS GNU/Linux/5.4.0-72-generic/x86_64 Intel(R)/Xeon(R)/Silver/4210/CPU/@/2.20GHz cloud_id/none" -O- --content-on-error https://motd.ubuntu.com
  - 50-motd-news New Fork (PID: 6259, Parent: 6200)
  - cat (PID: 6259, Parent: 6200, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.EQLgjCNBFD
  - 50-motd-news New Fork (PID: 6260, Parent: 6200)
  - head (PID: 6260, Parent: 6200, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
  - 50-motd-news New Fork (PID: 6261, Parent: 6200)
  - tr (PID: 6261, Parent: 6200, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
  - 50-motd-news New Fork (PID: 6262, Parent: 6200)
  - cut (PID: 6262, Parent: 6200, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
  - 50-motd-news New Fork (PID: 6263, Parent: 6200)
  - cat (PID: 6263, Parent: 6200, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.EQLgjCNBFD
  - 50-motd-news New Fork (PID: 6264, Parent: 6200)
  - head (PID: 6264, Parent: 6200, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
  - 50-motd-news New Fork (PID: 6265, Parent: 6200)
  - tr (PID: 6265, Parent: 6200, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
  - 50-motd-news New Fork (PID: 6266, Parent: 6200)
  - cut (PID: 6266, Parent: 6200, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
  - 50-motd-news New Fork (PID: 6269, Parent: 6200)
  - rm (PID: 6269, Parent: 6200, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.EQLgjCNBFD /tmp/tmp.ONisxp5pqw /tmp/tmp.ZtXsY8H9DY
- VefqQeU0Xt (PID: 6253, Parent: 6122, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/VefqQeU0Xt
  - VefqQeU0Xt New Fork (PID: 6255, Parent: 6253)
    - VefqQeU0Xt New Fork (PID: 6257, Parent: 6255)
- **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

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Bitcoin Miner

Searches for CPU information (likely indicative for DDoS capability)

Networking

Uses known network protocols on non-standard ports

DDoS

Searches for CPU information (likely indicative for DDoS capability)

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

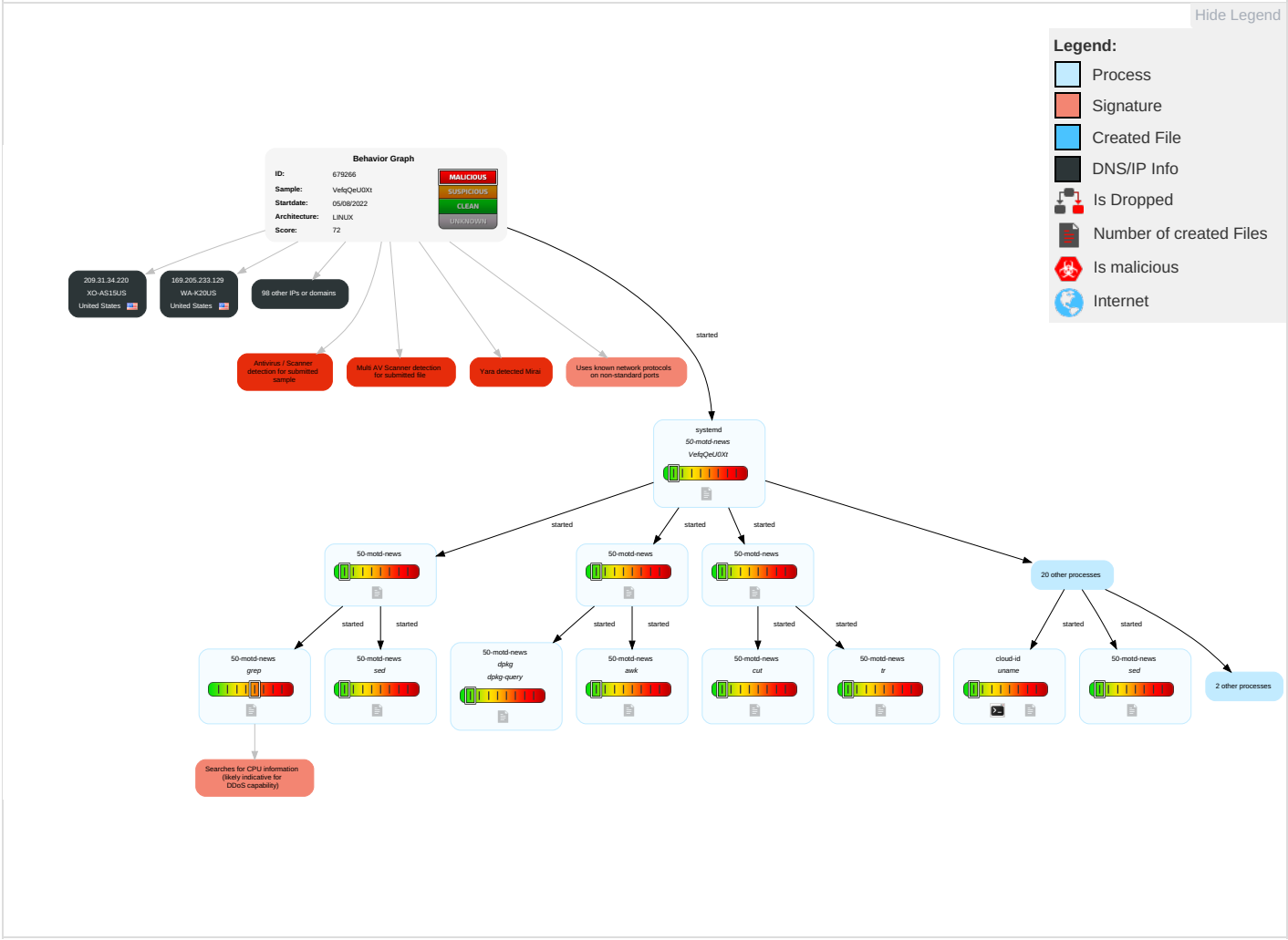
Mitre Att&ck Matrix

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	2 Command and Scripting Interpreter	Path Interception	Path Interception	1 Hide Artifacts	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	1 Jamming or Denial of Service	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 File Deletion	LSASS Memory	3 System Information 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 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
VefqQeU0Xt	50%	Virustotal		Browse
VefqQeU0Xt	52%	Metadefender		Browse
VefqQeU0Xt	48%	ReversingLabs	Linux.Trojan.Mirai	
VefqQeU0Xt	100%	Avira	LINUX/Mirai.evuay	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

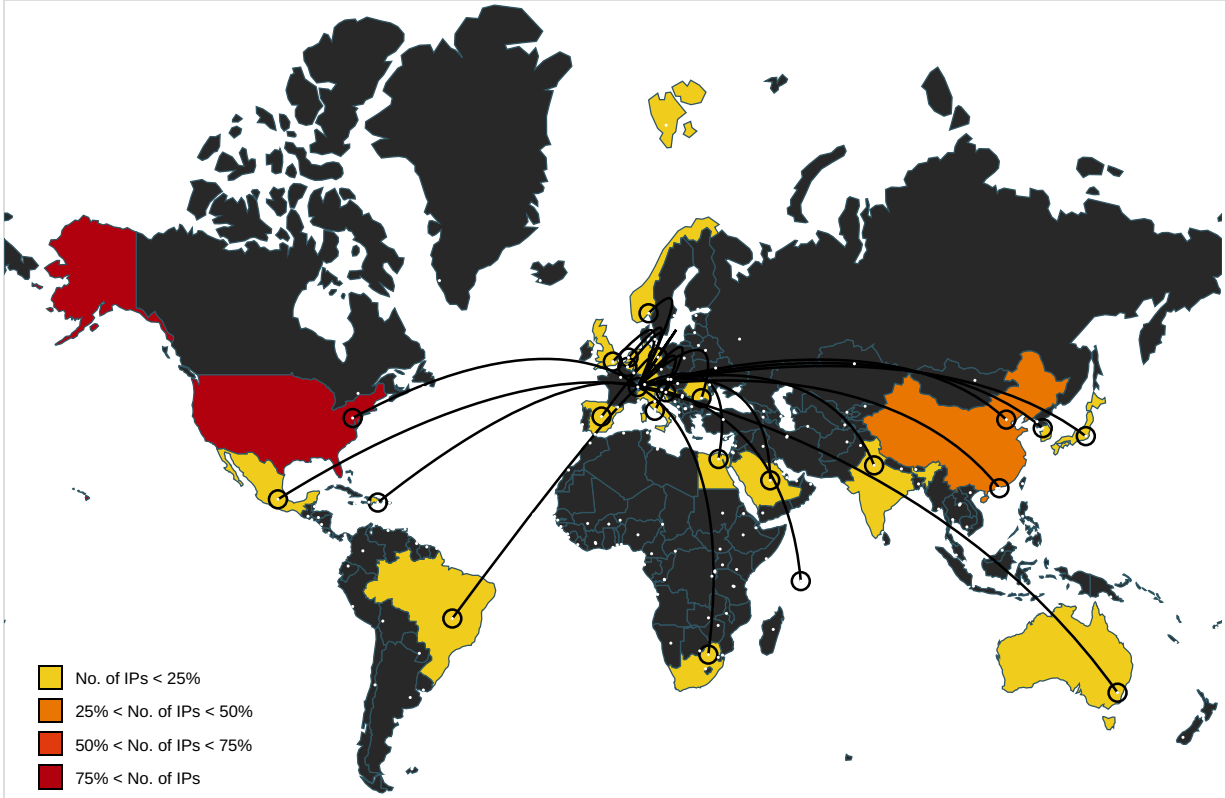
Domains and IPs

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
98.205.175.119	unknown	United States		7922	COMCAST-7922US	false
74.105.231.151	unknown	United States		701	UUNETUS	false
15.142.60.68	unknown	United States		5073	HPESUS	false
56.101.167.101	unknown	United States		2686	ATGS-MMD-ASUS	false
21.86.198.60	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
126.47.246.73	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
128.5.96.104	unknown	United States		3389	FORDSRL-ASUS	false
92.210.207.233	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
251.38.253.40	unknown	Reserved		unknown	unknown	false
209.31.34.220	unknown	United States		2828	XO-AS15US	false
189.138.184.246	unknown	Mexico		8151	UninetSAdeCVMX	false
79.115.120.145	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
115.35.234.224	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
179.52.79.6	unknown	Dominican Republic		6400	CompaniaDominicanadeTelefonosSADO	false
44.60.239.46	unknown	United States		7377	UCSDUS	false
175.36.15.194	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
217.151.153.64	unknown	Germany		9022	TWL-KOM-ASDonnersbergweg4DE	false
47.190.69.170	unknown	United States		5650	FRONTIER-FRTRUS	false
242.80.21.17	unknown	Reserved		unknown	unknown	false
1.45.73.121	unknown	China		45083	CHEERYZONEBeijingCheeryZoneScitechCoLtdCN	false
43.106.254.183	unknown	Japan		4249	LILLY-ASUS	false
188.54.137.99	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
89.164.32.20	unknown	Croatia (LOCAL Name: Hrvatska)		13046	ASN-ISKONHEPHR	false
251.176.62.50	unknown	Reserved		unknown	unknown	false
169.205.233.129	unknown	United States		10430	WA-K20US	false
199.241.205.94	unknown	United States		36529	AXXA-RACKCOUS	false
107.72.240.241	unknown	United States		7018	ATT-INTERNET4US	false
180.63.191.8	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
15.196.180.215	unknown	United States		7430	TANDEMUS	false
152.120.53.132	unknown	United States		2576	DOT-ASUS	false
66.186.165.62	unknown	United States		21547	OXNETUS	false
188.194.118.74	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
146.189.60.206	unknown	United States		1968	UMASSP-DOMUS	false
15.152.172.29	unknown	United States		71	HP-INTERNET-ASUS	false
61.235.174.146	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
12.245.37.186	unknown	United States		7018	ATT-INTERNET4US	false
151.65.106.122	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
106.162.29.233	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
66.1.102.108	unknown	United States		3651	SPRINT-BB6US	false
220.249.23.189	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
167.8.217.28	unknown	United States		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
48.184.111.104	unknown	United States		2686	ATGS-MMD-ASUS	false
197.132.217.115	unknown	Egypt		24835	RAYA-ASEG	false
169.202.199.165	unknown	South Africa		37611	AfrihostZA	false
182.82.174.104	unknown	China		23771	SXBCTV-APSXBCTVInternetServiceProviderCN	false
134.18.244.239	unknown	Australia		385	AFCONC-BLOCK1-ASUS	false
196.247.60.225	unknown	Seychelles		41564	AS41564SE	false
145.131.223.72	unknown	Netherlands		28685	ASN-ROUTITNL	false
91.44.2.107	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
86.86.132.45	unknown	Netherlands		1136	KPNKPNNationalEU	false
112.20.205.10	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
199.209.36.222	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
134.12.55.229	unknown	United States		270	AS270US	false
157.168.230.20	unknown	Switzerland		22192	SSHENETUS	false
253.216.122.239	unknown	Reserved		unknown	unknown	false
131.127.120.80	unknown	United States		668	DNIC-AS-00668US	false
166.146.116.6	unknown	United States		6167	CELLCO-PARTUS	false
153.15.14.86	unknown	Norway		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
53.193.209.203	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
58.167.228.180	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
177.72.19.16	unknown	unknown		262537	DataSafeITSolucoesemTecnologiaBR	false
80.33.186.77	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
212.137.210.222	unknown	United Kingdom		1273	CWVodafoneGroupPLCEU	false
203.137.219.160	unknown	Japan		4694	IDCFIDCFrontierIncJP	false
212.222.240.70	unknown	United Kingdom		3257	GTT-BACKBONEGTTDE	false
69.181.177.29	unknown	United States		7922	COMCAST-7922US	false
152.130.163.46	unknown	United States		29992	VA-TMP-COREUS	false
17.3.87.29	unknown	United States		714	APPLE-ENGINEERINGUS	false
217.46.188.101	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	false
27.59.44.110	unknown	India		45609	BHARTI-MOBILITY-AS-APBhartiAirtelLtdASforGPRSService	false
65.13.253.121	unknown	United States		7018	ATT-INTERNET4US	false
56.25.161.4	unknown	United States		2686	ATGS-MMD-ASUS	false
1.119.157.21	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
184.118.230.138	unknown	United States		7922	COMCAST-7922US	false
193.207.211.160	unknown	Italy		3269	ASN-IBSNAZIT	false
204.235.126.14	unknown	United States		30030	SIMPLEXITYUS	false
119.90.12.105	unknown	China		24143	CNNIC-QCN-APQingdaoCableTVNetworkCenterCN	false
61.130.143.143	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
57.254.163.62	unknown	Belgium		2686	ATGS-MMD-ASUS	false
22.180.220.222	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
22.216.57.76	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
200.19.1.255	unknown	Brazil		2716	UniversidadeFederaldoRioGrandedoSulBR	false
130.41.40.1	unknown	United States		243	HARRIS-ATD-ASUS	false
16.128.90.16	unknown	United States		unknown	unknown	false
18.232.167.114	unknown	United States		14618	AMAZON-AESUS	false
129.234.12.157	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
211.127.141.254	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
218.69.20.117	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
133.59.142.56	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
11.226.204.223	unknown	United States		3356	LEVEL3US	false
48.166.50.111	unknown	United States		2686	ATGS-MMD-ASUS	false
84.185.121.75	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
3.89.7.218	unknown	United States		14618	AMAZON-AESUS	false
161.81.250.8	unknown	Hong Kong		137872	PEOPLESPHONE-HKChinaMobileHongKongCompanyLimitedHK	false
59.55.32.214	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
150.223.227.59	unknown	China		58519	CHINATELECOM-CTCLOUDCloudComputingCorporationCN	false
54.2.225.241	unknown	United States		14618	AMAZON-AESUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
240.253.190.20	unknown	Reserved		unknown	unknown	false
75.179.52.87	unknown	United States		10796	TWC-10796-MIDWESTUS	false
27.167.147.1	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	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

/tmp/tmp.EQLgjCNBFD

/tmp/tmp.ONisxp5pqw

/tmp/tmp.ZtXsY8H9DY

/var/cache/motd-news

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	5.802220381620875
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	VefqQeU0Xt
File size:	37884
MD5:	b8ec31b1eff948abc9e797eb796d10cb
SHA1:	5590da71a98232aa873143780f4f9e36e1a8359a
SHA256:	f67ac47d33f3681cd957585c4338c43e939eb5fc0d8da4ac84aa33ccf52fcb1e
SHA512:	43662da6d6b544a3e34409b1e52f0147a4f74a27e3592d057f3913e888001ba1c8e8f2322ccd87eab2a56ff7d5926431d603b9be1807f68133b5a03ef8b43b0c
SSDEEP:	768:ZUcgPbzj5HoD2ogElo5fEFUsduP5KZ7m8LIZkk:Gcg8oDfYduxy7x
TLSH:	E903E784B9869A07CAD4537BFA1E42DD3B2573C8F2CE3313DE162F51368A92B0D6B145
File Content Preview:	.ELF...a.....(.....4...l.....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:	37484
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	0x8390	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x10440	0x8440	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x10454	0x8454	0x770	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x19000	0x9000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x19008	0x9008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x19014	0x9014	0x218	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x1922c	0x922c	0x2d0	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x922c	0x3e	0x0	0x0		0	0	1

Program Segments

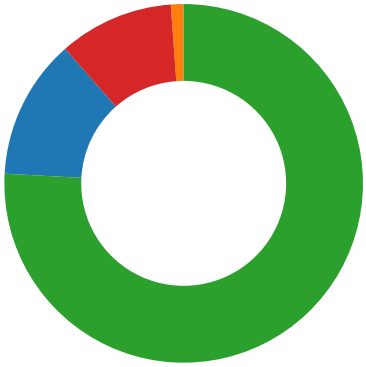
Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0x8bc4	0x8bc4	5.9377	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0x9000	0x19000	0x19000	0x22c	0x4fc	2.9360	0x6	RW	0x8000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution

Total Packets: 87

- 2323 undefined
- 23 (Telnet)
- 5556 undefined
- 443 (HTTPS)



TCP Packets

System Behavior

Analysis Process: systemd PID: 6200, Parent PID: 1

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: 50-motd-news PID: 6200, Parent PID: 1

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	/etc/update-motd.d/50-motd-news --force
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: 50-motd-news PID: 6221, Parent PID: 6200

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mktemp PID: 6221, Parent PID: 6200

General

Start time:	13:55:43
Start date:	05/08/2022

Path:	/usr/bin/mktemp
Arguments:	mktemp
File size:	47448 bytes
MD5 hash:	e117ed1c2172d436fa31cc9d263131e8

File Activities

File Read

Analysis Process: 50-motd-news PID: **6222**, Parent PID: **6200**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mktemp PID: **6222**, Parent PID: **6200**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/usr/bin/mktemp
Arguments:	mktemp
File size:	47448 bytes
MD5 hash:	e117ed1c2172d436fa31cc9d263131e8

File Activities

File Read

Analysis Process: 50-motd-news PID: **6223**, Parent PID: **6200**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mktemp PID: **6223**, Parent PID: **6200**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/usr/bin/mktemp
Arguments:	mktemp
File size:	47448 bytes
MD5 hash:	e117ed1c2172d436fa31cc9d263131e8

File Activities

File Read

Analysis Process: 50-motd-news PID: **6224**, Parent PID: **6200**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news

Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: 50-motd-news PID: **6225**, Parent PID: **6224**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/usr/bin/dpkg
Arguments:	dpkg -l wget
File size:	309944 bytes
MD5 hash:	5e18156b434fc45062eec2f28b9147be

File Activities

File Read

Directory Enumerated

Analysis Process: dpkg-query PID: **6225**, Parent PID: **6224**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/usr/bin/dpkg-query
Arguments:	dpkg-query --list -- wget
File size:	166488 bytes
MD5 hash:	bf81745ea62201f11bc674cc7c1935fc

File Activities

File Read

Directory Enumerated

Analysis Process: 50-motd-news PID: **6226**, Parent PID: **6224**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: awk PID: **6226**, Parent PID: **6224**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/usr/bin/awk
Arguments:	awk "$1 == \"ii\" { print($3); exit(0); }"
File size:	711136 bytes

MD5 hash:	7e9b2ed1272331cfbd2aac2e5eb3f84b

File Activities

File Read

Analysis Process: 50-motd-news PID: **6228**, Parent PID: **6200**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: 50-motd-news PID: **6229**, Parent PID: **6228**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: 50-motd-news PID: **6230**, Parent PID: **6228**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sed PID: **6230**, Parent PID: **6228**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/usr/bin/sed
Arguments:	sed -e "s/ /\\/g"
File size:	121288 bytes
MD5 hash:	885062561f66aa1d4af4c54b9e7cc81a

File Activities

File Read

Analysis Process: 50-motd-news PID: **6231**, Parent PID: **6200**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: uname PID: **6231**, Parent PID: **6200**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/usr/bin/uname
Arguments:	uname -o
File size:	39288 bytes
MD5 hash:	4ac7c634c5bec95753c480e9d421dcc2

File Activities

File Read

Analysis Process: 50-motd-news PID: 6232, Parent PID: 6200

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: uname PID: 6232, Parent PID: 6200

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/usr/bin/uname
Arguments:	uname -r
File size:	39288 bytes
MD5 hash:	4ac7c634c5bec95753c480e9d421dcc2

File Activities

File Read

Analysis Process: 50-motd-news PID: 6233, Parent PID: 6200

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: uname PID: 6233, Parent PID: 6200

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/usr/bin/uname
Arguments:	uname -m
File size:	39288 bytes
MD5 hash:	4ac7c634c5bec95753c480e9d421dcc2

File Activities

File Read

Analysis Process: 50-motd-news PID: 6234, Parent PID: 6200

General	
Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: uname PID: **6234**, Parent PID: **6200**

General	
Start time:	13:55:43
Start date:	05/08/2022
Path:	/usr/bin/uname
Arguments:	uname -m
File size:	39288 bytes
MD5 hash:	4ac7c634c5bec95753c480e9d421dcc2

File Activities

File Read

Analysis Process: 50-motd-news PID: **6235**, Parent PID: **6200**

General	
Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: 50-motd-news PID: **6236**, Parent PID: **6235**

General	
Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: **6236**, Parent PID: **6235**

General	
Start time:	13:55:43
Start date:	05/08/2022
Path:	/usr/bin/grep
Arguments:	grep -m1 "^model name" /proc/cpuinfo
File size:	199136 bytes
MD5 hash:	1e6ebb9dd094f774478f72727bdba0f5

File Activities

File Read

Analysis Process: 50-motd-news PID: **6237**, Parent PID: **6235**

General	
Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news

Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: sed PID: **6237**, Parent PID: **6235**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/usr/bin/sed
Arguments:	sed -e "s/.*: //" -e s:\\s\\+:/:g
File size:	121288 bytes
MD5 hash:	885062561f66aa1d4af4c54b9e7cc81a

File Activities

File Read

Analysis Process: 50-motd-news PID: **6238**, Parent PID: **6200**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cloud-id PID: **6238**, Parent PID: **6200**

General

Start time:	13:55:43
Start date:	05/08/2022
Path:	/usr/bin/cloud-id
Arguments:	/usr/bin/cloud-id
File size:	5490352 bytes
MD5 hash:	69f442c3e33b5f9a66b722c29ad89435

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: cloud-id PID: **6243**, Parent PID: **6238**

General

Start time:	13:55:48
Start date:	05/08/2022
Path:	/usr/bin/cloud-id
Arguments:	n/a
File size:	5490352 bytes
MD5 hash:	69f442c3e33b5f9a66b722c29ad89435

File Activities

Directory Enumerated

Analysis Process: uname PID: **6243**, Parent PID: **6238**

General

Start time:	13:55:48
Start date:	05/08/2022

Path:	/usr/bin/uname
Arguments:	uname -p
File size:	39288 bytes
MD5 hash:	4ac7c634c5bec95753c480e9d421dcc2

File Activities

File Read

Analysis Process: 50-motd-news PID: **6244**, Parent PID: **6200**

General

Start time:	13:55:49
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: 50-motd-news PID: **6245**, Parent PID: **6244**

General

Start time:	13:55:49
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: **6245**, Parent PID: **6244**

General

Start time:	13:55:49
Start date:	05/08/2022
Path:	/usr/bin/cut
Arguments:	cut -c -40 /tmp/tmp.ZtXsY8H9DY
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: 50-motd-news PID: **6246**, Parent PID: **6244**

General

Start time:	13:55:49
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: **6246**, Parent PID: **6244**

General

Start time:	13:55:49
Start date:	05/08/2022
Path:	/usr/bin/tr
Arguments:	tr -c -d [:alnum:]
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: 50-motd-news PID: **6247**, Parent PID: **6200**

General

Start time:	13:55:49
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: wget PID: **6247**, Parent PID: **6200**

General

Start time:	13:55:49
Start date:	05/08/2022
Path:	/usr/bin/wget
Arguments:	wget --timeout 60 -U "wget/1.20.3-1ubuntu1 Ubuntu/20.04.2/LTS GNU/Linux/5.4.0-72-generic/x86_64 Intel(R)/Xeon(R)/Silver/4210/CPU/@/2.20GHz cloud_id/none" -O- --content-on-error https://motd.ubuntu.com
File size:	548568 bytes
MD5 hash:	996940118df7bb2aaa718589d4e95c08

File Activities

File Read

File Written

Analysis Process: 50-motd-news PID: **6259**, Parent PID: **6200**

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: **6259**, Parent PID: **6200**

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.EQLgjCNBFD
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: 50-motd-news PID: **6260**, Parent PID: **6200**

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes

MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: **6260**, Parent PID: **6200**

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: 50-motd-news PID: **6261**, Parent PID: **6200**

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: **6261**, Parent PID: **6200**

General

Start time:	13:55:50
Start date:	05/08/2022
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: 50-motd-news PID: **6262**, Parent PID: **6200**

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: **6262**, Parent PID: **6200**

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: 50-motd-news PID: 6263, Parent PID: 6200

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 6263, Parent PID: 6200

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.EQLgjCNBFD
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: 50-motd-news PID: 6264, Parent PID: 6200

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 6264, Parent PID: 6200

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: 50-motd-news PID: 6265, Parent PID: 6200

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 6265, Parent PID: 6200

General

Start time:	13:55:50
Start date:	05/08/2022
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: 50-motd-news PID: **6266**, Parent PID: **6200**

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: **6266**, Parent PID: **6200**

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

File Written

Analysis Process: 50-motd-news PID: **6269**, Parent PID: **6200**

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/etc/update-motd.d/50-motd-news
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **6269**, Parent PID: **6200**

General

Start time:	13:55:50
Start date:	05/08/2022
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.EQLgjCNBFD /tmp/tmp.ONisxp5pqw /tmp/tmp.ZtXsY8H9DY
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: VefqQeU0Xt PID: **6253**, Parent PID: **6122**

General	
Start time:	13:55:49
Start date:	05/08/2022
Path:	/tmp/VefqQeU0Xt
Arguments:	/tmp/VefqQeU0Xt
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: VefqQeU0Xt PID: **6255**, Parent PID: **6253**

General	
Start time:	13:55:49
Start date:	05/08/2022
Path:	/tmp/VefqQeU0Xt
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: VefqQeU0Xt PID: **6257**, Parent PID: **6255**

General	
Start time:	13:55:49
Start date:	05/08/2022
Path:	/tmp/VefqQeU0Xt
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1