ID: 508203
Sample Name: KPz4ERtS9a
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 09:39:09
Date: 24/10/2021
Version: 33.0.0 White Diamond

Table of Contents

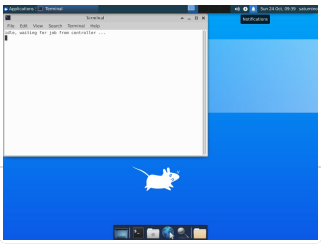
Linux Analysis Report KPz4ERtS9a

Overview

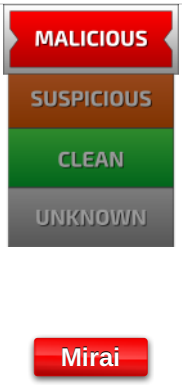
General Information

Sample Name:	KPz4ERtS9a
Analysis ID:	508203
MD5:	066901d9ef64208.
SHA1:	b012217d9b8e1a..
SHA256:	3a0dd755b8ef388.
Tags:	32 elf intel mirai
Infos:	

Most interesting Screenshot:



Detection

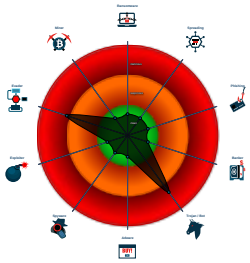


Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Sample deletes itself
- Uses known network protocols on no...
- Machine Learning detection for samp...
- Yara signature match
- Sample has stripped symbol table
- Detected TCP or UDP traffic on non...
- Executes the "rm" command used to...

Classification



General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	508203
Start date:	24.10.2021
Start time:	09:39:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KPz4ERtS9a
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.evad.lin@0/1@1/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- KPz4ERtS9a (PID: 5216, Parent: 5110, MD5: 066901d9ef64208c0daf3e6f428f7185) Arguments: /tmp/KPz4ERtS9a
  - KPz4ERtS9a New Fork (PID: 5217, Parent: 5216)
  - KPz4ERtS9a New Fork (PID: 5218, Parent: 5216)
- dash New Fork (PID: 5240, Parent: 4331)
- cat (PID: 5240, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.txS7eGBKCG
- dash New Fork (PID: 5241, Parent: 4331)
- head (PID: 5241, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5242, Parent: 4331)
- tr (PID: 5242, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5243, Parent: 4331)
- cut (PID: 5243, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5244, Parent: 4331)
- cat (PID: 5244, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.txS7eGBKCG
- dash New Fork (PID: 5245, Parent: 4331)
- head (PID: 5245, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5246, Parent: 4331)
- tr (PID: 5246, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5247, Parent: 4331)
- cut (PID: 5247, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5248, Parent: 4331)
- rm (PID: 5248, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.txS7eGBKCG /tmp/tmp.JsHkh9sVIe /tmp/tmp.UY8RlWyiII
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
KPz4ERtS9a	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x10bac:$xo1: \x19;.=885{azd • 0x10c1c:$xo1: \x19;.=885{azd • 0x10c80:$xo1: \x19;.=885{azd • 0x10cec:$xo1: \x19;.=885{azd • 0x10d58:$xo1: \x19;.=885{azd • 0x10e4c:$xo1: \x19;.=885{azd • 0x10f60:$xo1: \x175 366;uotj • 0x10fd0:$xo1: \x175 366;uotj • 0x11040:$xo1: \x175 366;uotj • 0x110b0:$xo1: \x175 366;uotj • 0x11120:$xo1: \x175 366;uotj • 0x11198:$xo1: \x19;.=885{azd • 0x111dc:$xo1: \x19;.=885{azd • 0x11228:$xo1: \x19;.=885{azd • 0x11284:$xo1: \x19;.=885{azd • 0x112cc:$xo1: \x19;.=885{azd • 0x11318:$xo1: \x19;.=885{azd • 0x1135c:$xo1: \x19;.=885{azd

PCAP (Network Traffic)

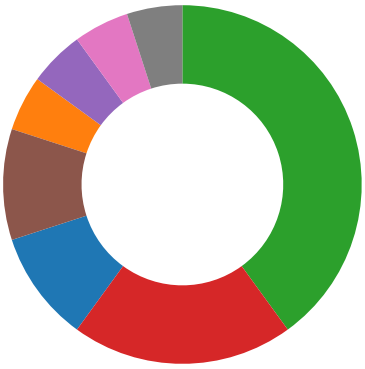
Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5216.1.0000000051390be1.000000002d48251b.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x5d0:$xo1: \x175 366;uotj • 0x648:$xo1: \x175 366;uotj • 0x6c0:$xo1: \x175 366;uotj • 0x738:$xo1: \x175 366;uotj • 0x7b0:$xo1: \x175 366;uotj • 0x830:$xo1: \x19;.=885{azd • 0x8a0:$xo1: \x19;.=885{azd • 0x908:$xo1: \x19;.=885{azd • 0x978:$xo1: \x19;.=885{azd • 0x9e8:$xo1: \x19;.=885{azd • 0xae8:$xo1: \x19;.=885{azd • 0xba0:$xo1: \x19;.=885{azd • 0xbe8:$xo1: \x19;.=885{azd • 0xc38:$xo1: \x19;.=885{azd • 0xc98:$xo1: \x19;.=885{azd • 0xce0:$xo1: \x19;.=885{azd • 0xd00:$xo1: \x19;.=885{azd • 0xd50:$xo1: \x19;.=885{azd • 0xd98:$xo1: \x19;.=885{azd • 0xdf8:$xo1: \x19;.=885{azd

Source	Rule	Description	Author	Strings
5216.1.000000001a887bdc.0000000019a04c35.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x10bac:$xo1: \x19;.=885{azd • 0x10c1c:$xo1: \x19;.=885{azd • 0x10c80:$xo1: \x19;.=885{azd • 0x10cec:$xo1: \x19;.=885{azd • 0x10d58:$xo1: \x19;.=885{azd • 0x10e4c:$xo1: \x19;.=885{azd • 0x10f60:$xo1: \x175 366;uotj • 0x10fd0:$xo1: \x175 366;uotj • 0x11040:$xo1: \x175 366;uotj • 0x110b0:$xo1: \x175 366;uotj • 0x11120:$xo1: \x175 366;uotj • 0x11198:$xo1: \x19;.=885{azd • 0x111dc:$xo1: \x19;.=885{azd • 0x11228:$xo1: \x19;.=885{azd • 0x11284:$xo1: \x19;.=885{azd • 0x112cc:$xo1: \x19;.=885{azd • 0x11318:$xo1: \x19;.=885{azd • 0x1135c:$xo1: \x19;.=885{azd

Jbx Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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:

Sample deletes itself

Uses known network protocols on non-standard ports

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

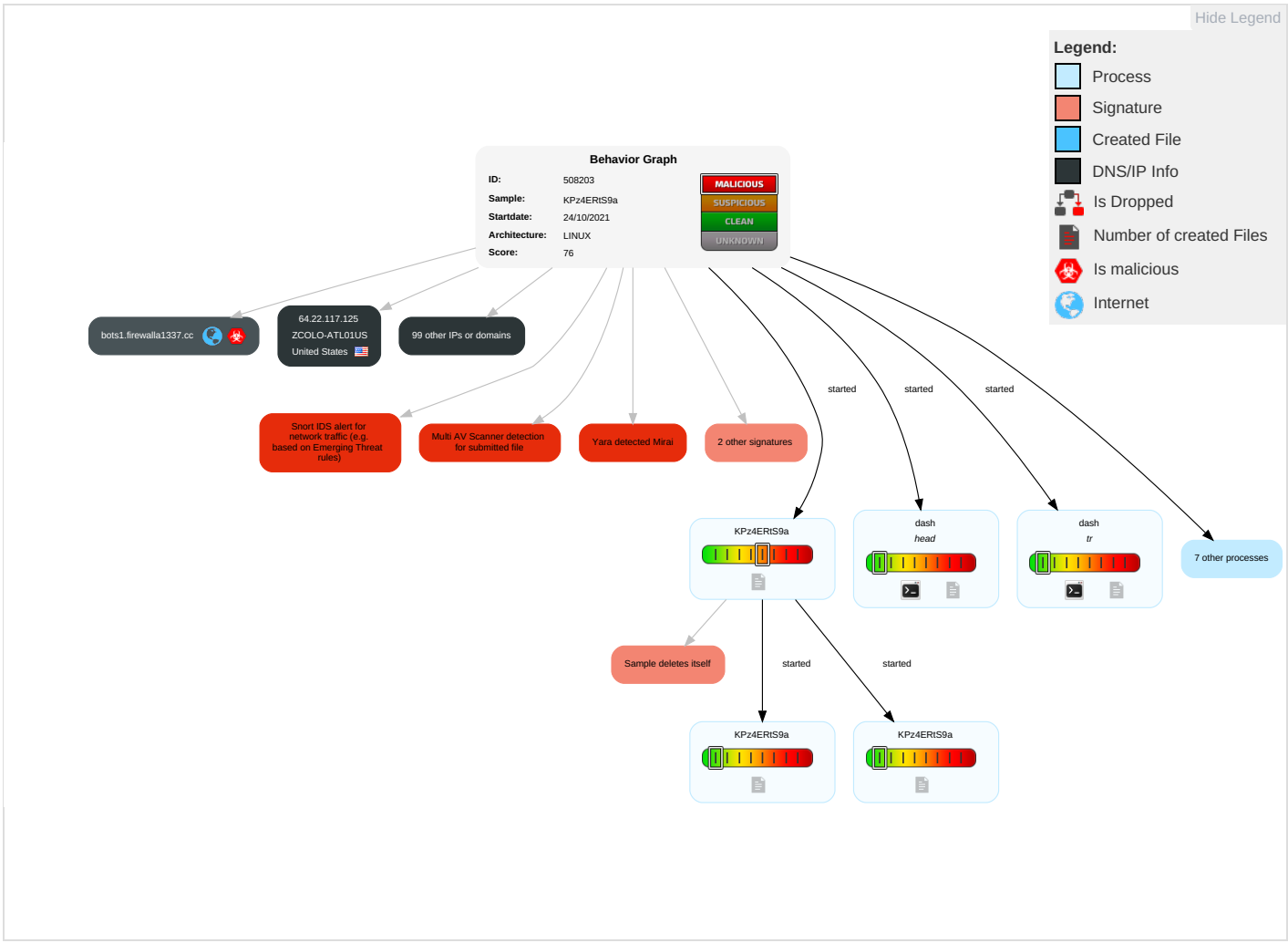
Mitre Att&ck Matrix

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	File Deletion 1 1	OS Credential Dumping	System Service Discovery	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 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	Non-Standard Port 1 1	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	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

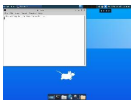
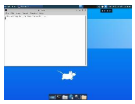
Behavior Graph

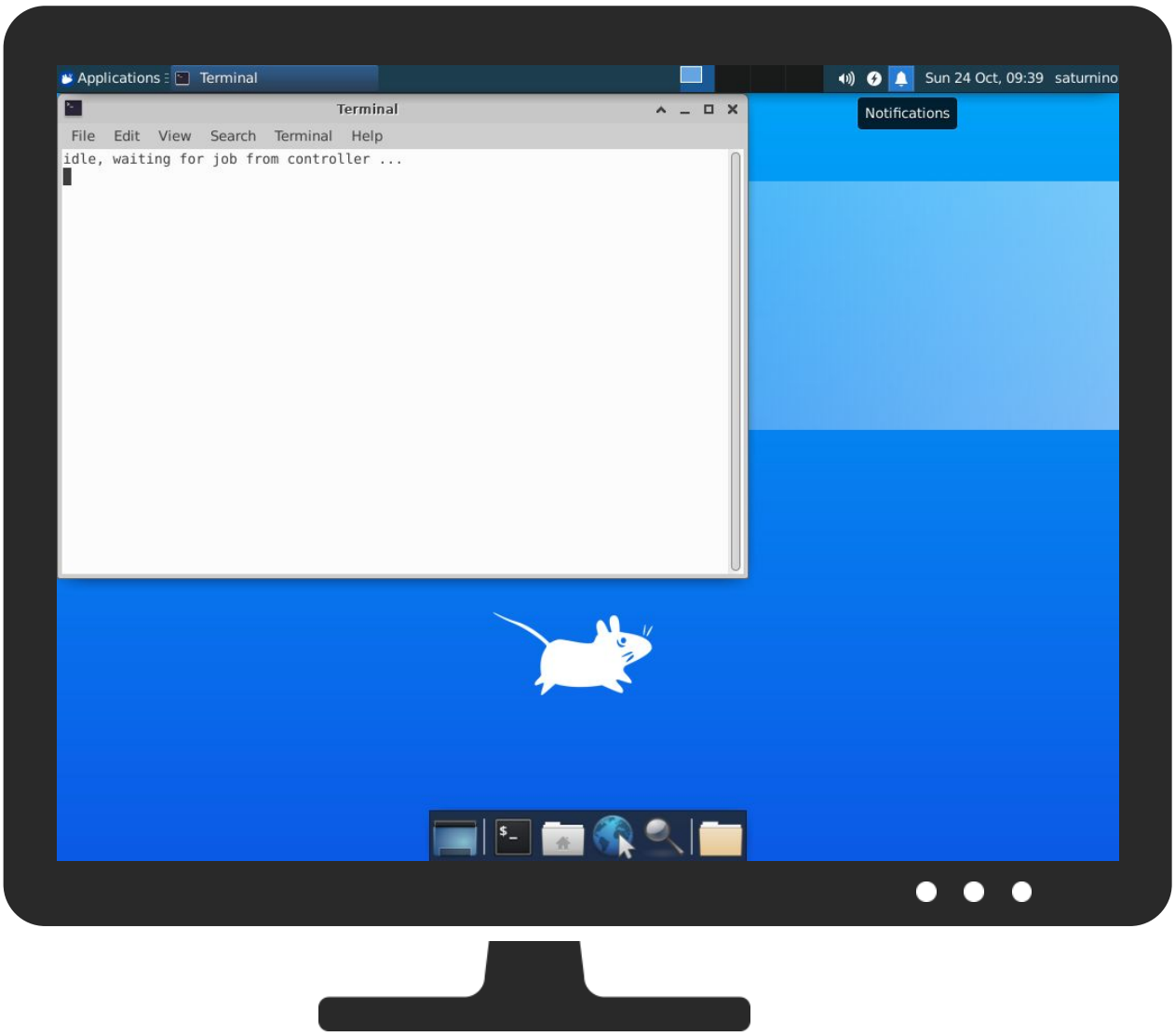


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
KPz4ERtS9a	52%	Virustotal		Browse
KPz4ERtS9a	40%	Metadefender		Browse
KPz4ERtS9a	68%	ReversingLabs	Linux.Trojan.Mirai	
KPz4ERtS9a	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
bots1.firewalla1337.cc	8%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bots1.firewalla1337.cc	107.189.1.185	true	true	• 8%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
206.61.188.190	unknown	United States		11280	SNAPPYDSL-ASN1US	false
154.109.4.238	unknown	Tunisia		37693	TUNISIANATN	false
87.136.201.29	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
96.155.237.246	unknown	United States		7922	COMCAST-7922US	false
114.53.103.116	unknown	Korea Republic of		18302	SKG_NW-AS-KRSKTelecomKR	false
76.15.172.29	unknown	United States		12271	TWC-12271-NYCUS	false
69.119.173.255	unknown	United States		6128	CABLE-NET-1US	false
49.216.216.28	unknown	Taiwan; Republic of China (ROC)		24158	TAIWANMOBILE-ASTaiwanMobileCoLtdTW	false
183.243.36.155	unknown	China		56048	CMNET-BEIJING-APChinaMobileCommunicaitonsCorporationCN	false
19.249.21.160	unknown	United States		3	MIT-GATEWAYSUS	false
182.200.28.120	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
25.88.36.74	unknown	United Kingdom		7922	COMCAST-7922US	false
222.12.163.129	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
86.17.238.169	unknown	United Kingdom		5089	NTLGB	false
192.154.238.237	unknown	United States		64200	VIVIDHOSTINGUS	false
20.169.237.13	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
36.20.185.59	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
198.65.209.238	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
136.173.114.39	unknown	Luxembourg		43375	EP-ASEU	false
70.176.178.96	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
111.205.148.181	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
182.104.254.37	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
141.30.26.199	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
135.122.218.248	unknown	United States		18676	AVAYAUS	false
4.107.107.55	unknown	United States		3356	LEVEL3US	false
176.149.9.225	unknown	France		5410	BOUYGTEL-ISPFR	false
2.222.21.137	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
103.157.51.89	unknown	unknown		134687	TWIDC-AS-APTWIDCLimitedHK	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
167.108.230.242	unknown	Uruguay		6057	AdministracionNacionaldeTelecomunicacionesUY	false
25.195.155.27	unknown	United Kingdom		7922	COMCAST-7922US	false
122.255.10.218	unknown	Sri Lanka		18001	DIALOG-ASDialogAxiataPLCLK	false
42.243.149.119	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
19.55.221.32	unknown	United States		3	MIT-GATEWAYSUS	false
173.66.71.172	unknown	United States		701	UUNETUS	false
131.87.85.231	unknown	United States		27046	DNIC-ASBLK-27032-27159US	false
113.68.61.110	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
17.54.245.74	unknown	United States		714	APPLE-ENGINEERINGUS	false
163.57.235.167	unknown	unknown		2516	KDDIKDDICORPORATIONJP	false
190.101.117.123	unknown	Chile		22047	VTRBANDAANCHASACL	false
199.121.191.229	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
12.138.97.107	unknown	United States		7018	ATT-INTERNET4US	false
103.159.224.199	unknown	unknown		134687	TWIDC-AS-APTWIDCLimitedHK	false
63.80.5.76	unknown	United States		701	UUNETUS	false
13.213.91.126	unknown	United States		16509	AMAZON-02US	false
143.23.212.59	unknown	United States		11003	PANDGUS	false
57.234.176.245	unknown	Belgium		2686	ATGS-MMD-ASUS	false
111.80.249.216	unknown	Taiwan; Republic of China (ROC)		2510	INFOWEBFUJITSULIMITEDJP	false
40.131.167.177	unknown	United States		7029	WINDSTREAMUS	false
196.51.223.15	unknown	South Africa		37518	FIBERGRIDSC	false
149.64.54.60	unknown	United States		188	SAIC-ASUS	false
211.110.246.116	unknown	Korea Republic of		18302	SKG_NW-AS-KRSKTelecomKR	false
153.31.237.205	unknown	United States		25996	FBICJISUS	false
42.130.115.68	unknown	China		4249	LILLY-ASUS	false
198.61.186.238	unknown	United States		19994	RACKSPACEUS	false
64.192.132.233	unknown	United States		33548	UNWIRED-NOCUS	false
49.52.78.12	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
179.188.242.121	unknown	Brazil		27715	LocawebServicosdeInternetSABR	false
8.36.137.236	unknown	United States		3356	LEVEL3US	false
152.170.97.196	unknown	Argentina		10318	TelecomArgentinaSAAR	false
64.95.129.152	unknown	United States		395424	LOGMEIN-EMEA-1US	false
194.25.238.144	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
105.237.52.13	unknown	South Africa		16637	MTNNS-ASZA	false
87.35.240.228	unknown	Ireland		1213	HEANETIE	false
213.37.228.51	unknown	Spain		12357	COMUNITELSPAINES	false
191.14.68.220	unknown	Brazil		26599	TELEFONICABRASILSABR	false
161.87.168.175	unknown	Netherlands		14298	EPA-NETUS	false
174.40.48.84	unknown	United States		6167	CELLCO-PARTUS	false
209.63.110.87	unknown	United States		7385	ALLSTREAMUS	false
203.51.120.80	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
31.219.164.78	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
187.177.237.196	unknown	Mexico		6503	AxtelSABdeCVMX	false
35.176.86.255	unknown	United States		16509	AMAZON-02US	false
179.62.170.72	unknown	Argentina		27983	RedIntercableDigitalSAAR	false
82.148.164.138	unknown	Norway		29300	AS-DIRECTCONNECTNO	false
105.179.46.23	unknown	unknown		37228	Olleh-Rwanda-NetworksRW	false
221.200.240.250	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
191.201.125.63	unknown	Brazil		26599	TELEFONICABRASILSABR	false
202.109.79.52	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
174.162.235.66	unknown	United States		7922	COMCAST-7922US	false
165.223.234.228	unknown	United States		3550	ERX-PHILNETAteneodeManilaUniversityPH	false
149.131.179.149	unknown	United States		33022	WELLESLEY-COLLEGEUS	false
213.215.187.119	unknown	Italy		8220	COLTCOLTTechnologyServicesGroupLimitedGB	false
42.204.186.200	unknown	China		7641	CHINABTNChinaBroadcastingTVNetCN	false
200.252.67.136	unknown	Brazil		4230	CLAROSABR	false
141.239.2.110	unknown	United States		36149	HAWAIIAN-TELCOMUS	false
211.41.228.38	unknown	Korea Republic of		9943	KNCTV-ASKangNamCableTVKR	false
65.239.163.61	unknown	United States		701	UUNETUS	false
151.58.79.95	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
25.148.142.254	unknown	United Kingdom		7922	COMCAST-7922US	false
92.179.237.117	unknown	France		12479	UNI2-ASES	false
196.146.184.1	unknown	Egypt		36935	Vodafone-EG	false
25.158.212.76	unknown	United Kingdom		7922	COMCAST-7922US	false
203.147.5.113	unknown	Thailand		7616	JINET-BKK-AS-APJasmineInternetCoLtdTH	false
185.21.26.85	unknown	Italy		199324	DODONETDODONETSRL-dodonetnetwork-httpwwwdodone	false
60.252.146.232	unknown	China		17968	DQTNETDaqingzhongjipetroleumtelecommunicationconstructi	false
64.22.117.125	unknown	United States		7226	ZCOLO-ATL01US	false
150.98.213.183	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
13.133.76.171	unknown	United States		7018	ATT-INTERNET4US	false
132.150.213.184	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
125.51.29.222	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false

Runtime Messages

Command:	/tmp/KPz4ERtS9a
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	InfectedNight did its job
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.65.209.238	PSLItQP6x7	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bots1.firewalla1337.cc	UNNEIaOxVM	Get hash	malicious	Browse	• 107.189.1.185
	ATc5uxXITp	Get hash	malicious	Browse	• 107.189.1.185
	il32XbklZm	Get hash	malicious	Browse	• 107.189.1.185
	IN7REq0Jv5	Get hash	malicious	Browse	• 107.189.1.185

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HDgtpV43hX	Get hash	malicious	Browse	• 107.189.1.185
	B2WBaqkm8k	Get hash	malicious	Browse	• 107.189.1.185
	7SerHvEAjE	Get hash	malicious	Browse	• 107.189.1.185
	i686	Get hash	malicious	Browse	• 107.189.1.185
	m5DozqUO2t	Get hash	malicious	Browse	• 107.189.1.185
	avxeC9Wssi	Get hash	malicious	Browse	• 107.189.1.185
	ayx5kFWYmZ	Get hash	malicious	Browse	• 107.189.1.185
	p4vXpD0P73	Get hash	malicious	Browse	• 107.189.1.185
	j3LQELTT0m	Get hash	malicious	Browse	• 107.189.1.185
	BLBHEA8knd	Get hash	malicious	Browse	• 107.189.1.185
	mips	Get hash	malicious	Browse	• 107.189.1.185
	x86_64	Get hash	malicious	Browse	• 107.189.1.185
	arm	Get hash	malicious	Browse	• 107.189.1.185
	Ynffczq7m4	Get hash	malicious	Browse	• 107.189.1.185
	BqfM9JwIC5	Get hash	malicious	Browse	• 107.189.1.185
	7bkrFirKok	Get hash	malicious	Browse	• 107.189.1.185

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TUNISIANATN	apep.x86	Get hash	malicious	Browse	• 197.16.172.171
	F3br85KuNX	Get hash	malicious	Browse	• 197.21.89.15
	zYMp3detVO	Get hash	malicious	Browse	• 102.108.21 1.181
	Tf9ATzpdKR	Get hash	malicious	Browse	• 154.104.70.32
	JYWllP5wHP	Get hash	malicious	Browse	• 197.23.201.48
	arm7	Get hash	malicious	Browse	• 41.228.193.68
	x86	Get hash	malicious	Browse	• 197.16.42.199
	FWsCarsq8Q	Get hash	malicious	Browse	• 197.20.132.151
	sora.arm7	Get hash	malicious	Browse	• 154.110.23 6.111
	sora.arm	Get hash	malicious	Browse	• 102.107.16 3.127
	iSdOB1UKQv	Get hash	malicious	Browse	• 102.175.134.3
	Kot3UfQMDm	Get hash	malicious	Browse	• 102.106.77.222
	arm	Get hash	malicious	Browse	• 197.23.213.125
	x86	Get hash	malicious	Browse	• 197.17.114.178
	arm	Get hash	malicious	Browse	• 197.19.205.253
	7vmT7Q2se0	Get hash	malicious	Browse	• 196.177.53.174
	x86.light	Get hash	malicious	Browse	• 197.19.253.162
	x86	Get hash	malicious	Browse	• 197.19.253.174
	lCTNXNa4Bo	Get hash	malicious	Browse	• 197.19.50.8
	UniRHdW5VC	Get hash	malicious	Browse	• 197.19.129.118
DTAGInternetserviceprovideroperationsDE	apep.arm	Get hash	malicious	Browse	• 31.238.199.244
	db0fa4b8db0333367e9bda3ab68b8042.x86	Get hash	malicious	Browse	• 79.208.52.225
	MjqRJNVy8K	Get hash	malicious	Browse	• 93.230.53.41
	6NzbU4oW61	Get hash	malicious	Browse	• 80.128.31.249
	Rpl2Twyrts	Get hash	malicious	Browse	• 93.249.80.159
	MPnFvlsvJp	Get hash	malicious	Browse	• 84.141.10.139
	sora.arm	Get hash	malicious	Browse	• 217.83.112.79
	R9kV5GcwPz	Get hash	malicious	Browse	• 194.25.238.156
	DPJPYxGxfI	Get hash	malicious	Browse	• 79.213.41.48
	4RBTXTxBnt	Get hash	malicious	Browse	• 79.222.243.3
	T4xP1S9Fhz	Get hash	malicious	Browse	• 79.241.253.30
	hWT9RJDotD	Get hash	malicious	Browse	• 2.169.202.35
	gKCq4VLpjL	Get hash	malicious	Browse	• 93.254.185.68
	UYnpKcFZ2s	Get hash	malicious	Browse	• 31.224.103.37
	jvilYCvWBc	Get hash	malicious	Browse	• 79.252.137.231
	zYMp3detVO	Get hash	malicious	Browse	• 80.128.233.103
	lQKil1R7D9	Get hash	malicious	Browse	• 87.152.228.70
	oH6qNmnFRP	Get hash	malicious	Browse	• 80.137.89.134
	b3astmode.arm	Get hash	malicious	Browse	• 217.226.14 3.197
	b3astmode.arm7	Get hash	malicious	Browse	• 93.202.104.141
SNAPPYDSL-ASN1US	sora.arm	Get hash	malicious	Browse	• 206.61.188.185

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fb4726d465c5f28b84cd6d14cedd13a7	vCLbAS7aPb	Get hash	malicious	Browse	• 54.171.230.55
	yzui4gwsrF	Get hash	malicious	Browse	• 54.171.230.55
	072FZHiMhs	Get hash	malicious	Browse	• 54.171.230.55
	sjZlfrpuyc	Get hash	malicious	Browse	• 54.171.230.55
	khoE2l8yer	Get hash	malicious	Browse	• 54.171.230.55
	wvsEoQ0khP	Get hash	malicious	Browse	• 54.171.230.55
	32	Get hash	malicious	Browse	• 54.171.230.55
	a-r.m-5.Sakura	Get hash	malicious	Browse	• 54.171.230.55
	NDYfrLSNFW	Get hash	malicious	Browse	• 54.171.230.55
	m-i.p-s.Sakura	Get hash	malicious	Browse	• 54.171.230.55
	6Qn1b9fB2C	Get hash	malicious	Browse	• 54.171.230.55
	ZSbDircdwC	Get hash	malicious	Browse	• 54.171.230.55
	s0bi9t	Get hash	malicious	Browse	• 54.171.230.55
	E7VXPEy1i2	Get hash	malicious	Browse	• 54.171.230.55
	JIMFLthThO	Get hash	malicious	Browse	• 54.171.230.55
	[cpu]	Get hash	malicious	Browse	• 54.171.230.55
	vC6OApPu6u	Get hash	malicious	Browse	• 54.171.230.55
	i686	Get hash	malicious	Browse	• 54.171.230.55
	4f0PBbcOBI	Get hash	malicious	Browse	• 54.171.230.55
	7iw4z5l41w	Get hash	malicious	Browse	• 54.171.230.55

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:P2lnI+5MsqqzNLz+FRNScHUBfRau95++sZzR5woLB1Fh0VTGTl/X5kURn:OZ8uNLzDc0pR75+9Zz/woFmIT52URn
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 LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.394763938732628
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	KPz4ERtS9a
File size:	74512

General

MD5:	066901d9ef64208c0daf3e6f428f7185
SHA1:	b012217d9b8e1a80a8d077cfdabcef03a12d15af
SHA256:	3a0dd755b8ef388ccb5dcdfc94a543450a8974830b87f0ea284c9de7356d1bef
SHA512:	10e417881e4a6805b7861c3d1c707c6b4d82d23b16c94355de36ffb62aabbe8033d033dddfae6e0185a5db5424326a6a520a4b25b3adbf8e56ee824ef58fb636
SSDEEP:	1536:RwyXAG59RrNQadk8+5SCH/WzEe9PSXtkaK1Dr5ZprWwrLr/ai6d:BXAG3RrNQwk55SCH/WzEcqtkr1DtHWWk
File Content Preview:	.ELF.....d...4....!.....4. ...(..... ... .@...@.....Q.td.....U..S..... w....h.....[]...$.....U.....=@....t..5....$.....$.....u..... ..t....h .....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x8048164
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	74112
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

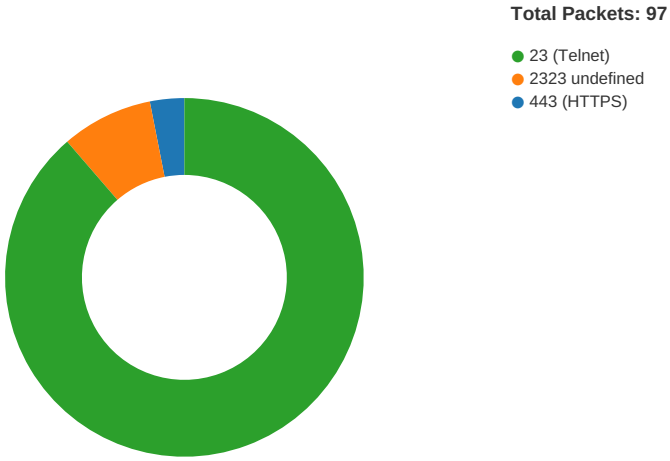
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8048094	0x94	0x1c	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x80480b0	0xb0	0xff36	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x8057fe6	0xffe6	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x8058000	0x10000	0x1920	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x805a000	0x12000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x805a008	0x12008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x805a020	0x12020	0x120	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x805a140	0x12140	0x800	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0x12140	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	0x8048000	0x8048000	0x11920	0x11920	3.9608	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0x12000	0x805a000	0x805a000	0x140	0x940	2.5092	0x6	RW	0x1000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 24, 2021 09:39:52.366121054 CEST	192.168.2.23	1.1.1.1	0xfbf4	Standard query (0)	bots1.fire walla1337.cc	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 24, 2021 09:39:52.391582012 CEST	1.1.1.1	192.168.2.23	0xfbf4	No error (0)	bots1.fire walla1337.cc		107.189.1.185	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: KPz4ERtS9a PID: 5216 Parent PID: 5110

General

Start time:	09:39:51
Start date:	24/10/2021
Path:	/tmp/KPz4ERtS9a
Arguments:	/tmp/KPz4ERtS9a
File size:	74512 bytes
MD5 hash:	066901d9ef64208c0daf3e6f428f7185

File Activities

File Deleted

Analysis Process: KPz4ERtS9a PID: 5217 Parent PID: 5216

General

Start time:	09:39:51
Start date:	24/10/2021
Path:	/tmp/KPz4ERtS9a
Arguments:	n/a

File size:	74512 bytes
MD5 hash:	066901d9ef64208c0daf3e6f428f7185

Analysis Process: KPz4ERtS9a PID: 5218 Parent PID: 5216

General

Start time:	09:39:51
Start date:	24/10/2021
Path:	/tmp/KPz4ERtS9a
Arguments:	n/a
File size:	74512 bytes
MD5 hash:	066901d9ef64208c0daf3e6f428f7185

Analysis Process: dash PID: 5240 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5240 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.txS7eGBKCG
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5241 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5241 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5242 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5242 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
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: 5243 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5243 Parent PID: 4331

General

Start time:	09:40:01

Start date:	24/10/2021
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: 5244 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5244 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.txS7eGBKCG
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5245 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5245 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
Path:	/usr/bin/head
Arguments:	head -n 10

File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5246 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5246 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
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: 5247 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5247 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
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: 5248 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5248 Parent PID: 4331

General

Start time:	09:40:01
Start date:	24/10/2021
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.txS7eGBKCG /tmp/tmp.JsHkh9sVIe /tmp/tmp.UY8RlWyiII
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read