ID: 512852
Sample Name: Antisocial.x86
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 13:37:09
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

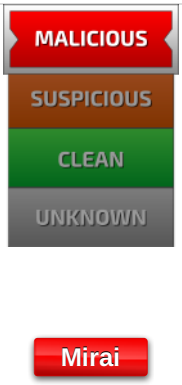
Linux Analysis Report Antisocial.x86

Overview

General Information

Sample Name:	Antisocial.x86
Analysis ID:	512852
MD5:	abf15f119a5fa68…
SHA1:	6531db808704d5..
SHA256:	e41b1347da792c..
Tags:	Mirai
Infos:	

Detection

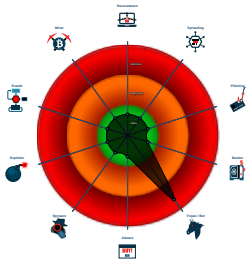


Score:	84
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Uses known network protocols on no…
- Machine Learning detection for samp…
- Connects to many ports of the same…
- Sample has stripped symbol table
- HTTP GET or POST without a user …
- Detected TCP or UDP traffic on non…
- Executes the "rm" command used to…

Classification



General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	512852
Start date:	01.11.2021
Start time:	13:37:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Antisocial.x86
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:	mal84.troj.linX86@0/1@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
  - Antisocial.x86 (PID: 5225, Parent: 5102, MD5: abf15f119a5fa686f85e3a9ce8f57cdc) Arguments: /tmp/Antisocial.x86
    - Antisocial.x86 New Fork (PID: 5226, Parent: 5225)
      - Antisocial.x86 New Fork (PID: 5237, Parent: 5226)
      - Antisocial.x86 New Fork (PID: 5238, Parent: 5226)
        - Antisocial.x86 New Fork (PID: 5239, Parent: 5238)
          - Antisocial.x86 New Fork (PID: 5250, Parent: 5239)
          - Antisocial.x86 New Fork (PID: 5251, Parent: 5239)
          - Antisocial.x86 New Fork (PID: 5252, Parent: 5239)
          - Antisocial.x86 New Fork (PID: 5253, Parent: 5239)
        - Antisocial.x86 New Fork (PID: 5240, Parent: 5238)
        - Antisocial.x86 New Fork (PID: 5242, Parent: 5238)
        - Antisocial.x86 New Fork (PID: 5244, Parent: 5238)
        - Antisocial.x86 New Fork (PID: 5246, Parent: 5238)
    - Antisocial.x86 New Fork (PID: 5227, Parent: 5225)
    - Antisocial.x86 New Fork (PID: 5228, Parent: 5225)
      - Antisocial.x86 New Fork (PID: 5229, Parent: 5228)
        - Antisocial.x86 New Fork (PID: 5241, Parent: 5229)
        - Antisocial.x86 New Fork (PID: 5243, Parent: 5229)
        - Antisocial.x86 New Fork (PID: 5245, Parent: 5229)
        - Antisocial.x86 New Fork (PID: 5247, Parent: 5229)
      - Antisocial.x86 New Fork (PID: 5230, Parent: 5228)
      - Antisocial.x86 New Fork (PID: 5231, Parent: 5228)
      - Antisocial.x86 New Fork (PID: 5232, Parent: 5228)
      - Antisocial.x86 New Fork (PID: 5234, Parent: 5228)
- dash New Fork (PID: 5268, Parent: 4332)
  - cat (PID: 5268, Parent: 4332, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.zwbUWO1Xs3
- dash New Fork (PID: 5269, Parent: 4332)
  - head (PID: 5269, Parent: 4332, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5270, Parent: 4332)
  - tr (PID: 5270, Parent: 4332, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5271, Parent: 4332)
  - cut (PID: 5271, Parent: 4332, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5272, Parent: 4332)
  - cat (PID: 5272, Parent: 4332, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.zwbUWO1Xs3
- dash New Fork (PID: 5273, Parent: 4332)
  - head (PID: 5273, Parent: 4332, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5274, Parent: 4332)
  - tr (PID: 5274, Parent: 4332, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5275, Parent: 4332)
  - cut (PID: 5275, Parent: 4332, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5276, Parent: 4332)
  - rm (PID: 5276, Parent: 4332, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.zwbUWO1Xs3 /tmp/tmp.7ybUxelKh4 /tmp/tmp.tWQiSu25Ld
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Antisocial.x86	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

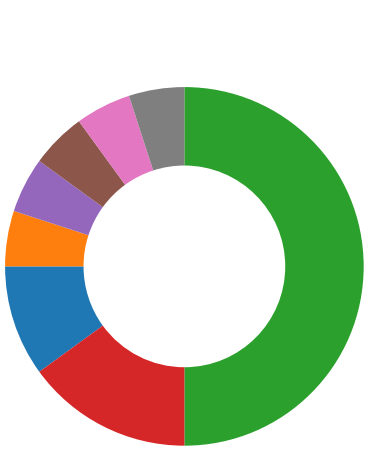
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5250.1.000000001a887bdc.000000001843e942.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5237.1.000000001a887bdc.000000001843e942.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5240.1.000000001a887bdc.000000001843e942.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5226.1.000000001a887bdc.000000001843e942.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5230.1.000000001a887bdc.000000001843e942.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Click to see the 3 entries				

Jbx Signature Overview



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

Connects to many ports of the same IP (likely port scanning)

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

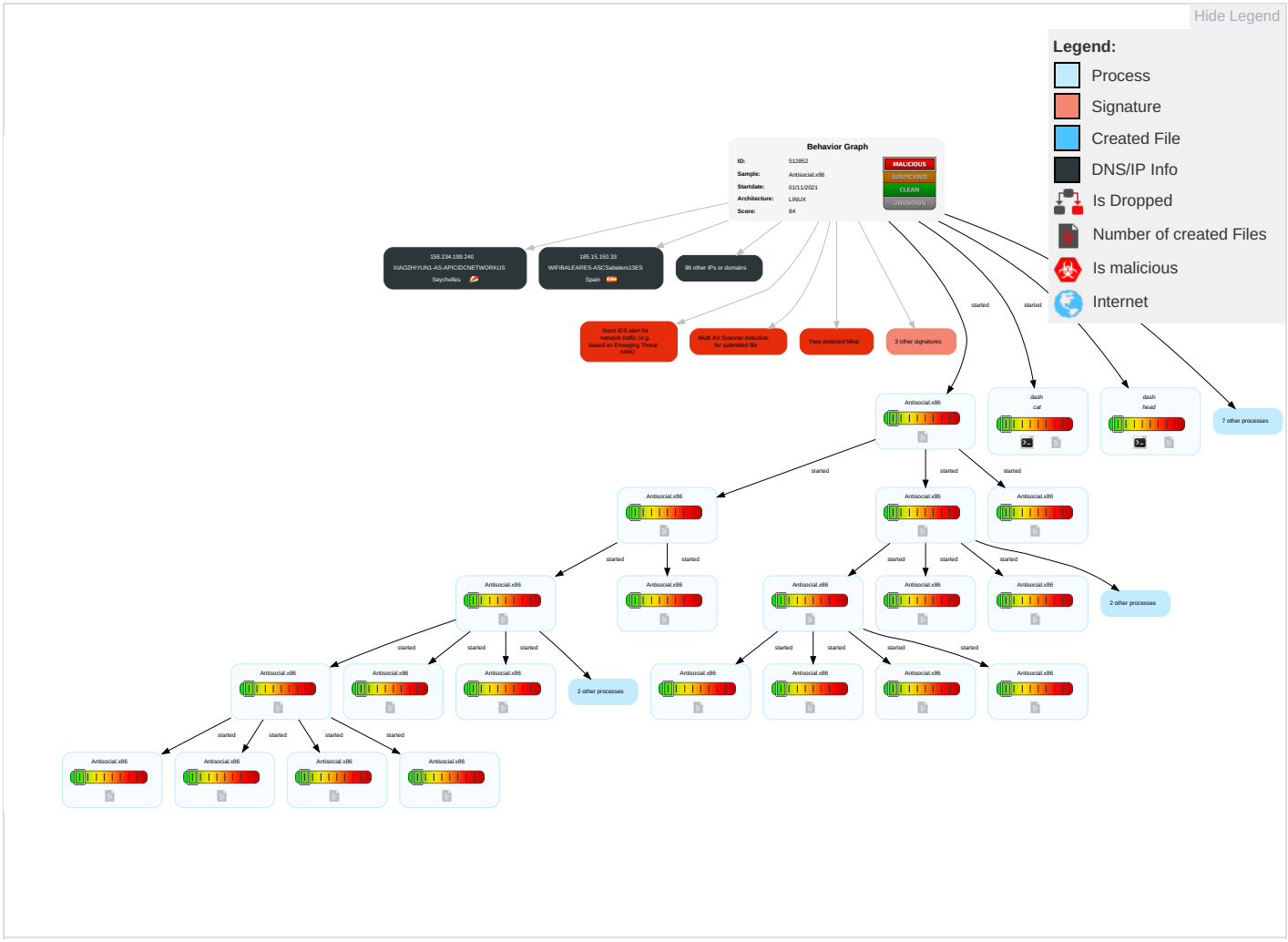
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	File Deletion 1	OS Credential Dumping	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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Antisocial.x86	56%	ReversingLabs	Linux.Trojan.Mirai	
Antisocial.x86	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:52869/picdesc.xml	0%	Avira URL Cloud	safe	
http://127.0.0.1:52869/wanipcn.xml	0%	Avira URL Cloud	safe	
http://194.87.42.3/Anti_Bins/Antisocial.mips	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:52869/picdesc.xml	true	• Avira URL Cloud: safe	unknown
http://127.0.0.1:52869/wanipcn.xml	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.128.94.101	unknown	Germany		202741	EDV-TEAM-OBERLANDDE	false
45.117.212.26	unknown	India		45194	SIPL-ASSysconInfowayPvtLtdIN	false
99.162.223.250	unknown	United States		7018	ATT-INTERNET4US	false
64.111.105.206	unknown	United States		26347	DREAMHOST-ASUS	false
91.19.189.233	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
19.85.187.31	unknown	United States		3	MIT-GATEWAYSUS	false
41.157.30.69	unknown	South Africa		37168	CELL-CZA	false
197.55.123.214	unknown	Egypt		8452	TE-ASTE-ASEG	false
45.111.37.172	unknown	Egypt		37069	MOBINILEG	false
216.67.126.193	unknown	United States		7782	ALSK-7782US	false
45.104.148.31	unknown	Egypt		37069	MOBINILEG	false
185.203.160.49	unknown	Iran (ISLAMIC Republic Of)		205837	SADADPSP-ASSadadProcessingModernServicesCompanyPJS	false
45.153.14.111	unknown	Russian Federation		208221	ORIONNET-BRKRU	false
63.62.160.86	unknown	United States		701	UUNETUS	false
91.49.236.110	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
177.62.126.180	unknown	Brazil		26599	TELEFONICABRASILSABR	false
91.163.145.63	unknown	France		12322	PROXADFR	false
197.12.117.159	unknown	Tunisia		37703	ATLAXTN	false
45.91.88.205	unknown	Romania		203020	HOSTROYALERO	false
185.106.143.31	unknown	Serbia		7979	SERVERS-COMUS	false
5.251.149.225	unknown	Kazakhstan		9198	KAZTELECOM-ASKZ	false
185.244.103.14	unknown	Estonia		202635	SERVERFARMEE	false
212.160.6.59	unknown	Poland		5617	TPNETPL	false
156.234.199.240	unknown	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	false
185.232.205.132	unknown	Spain		201942	SOLTIAES	false
91.95.68.164	unknown	Sweden		5617	TPNETPL	false
91.90.227.118	unknown	Latvia		24589	TELENETSIA-ASTelenetAUT-NUMpeeringspecificationobject	false
91.67.33.162	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
91.244.81.15	unknown	Russian Federation		197831	DISKUS-ASRU	false
41.148.196.223	unknown	South Africa		5713	SAIX-NETZA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.15.150.33	unknown	Spain		199930	WIFIBALEARES-ASCSabaters13ES	false
91.243.156.150	unknown	Spain		12479	UNI2-ASES	false
197.74.193.249	unknown	South Africa		16637	MTNNS-ASZA	false
91.11.116.189	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
119.172.19.38	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
141.88.148.250	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
178.87.239.143	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
45.20.50.217	unknown	United States		7018	ATT-INTERNET4US	false
156.43.68.69	unknown	United Kingdom		4211	ASN-MARICOPA1US	false
45.106.6.107	unknown	Egypt		37069	MOBINILEG	false
45.201.177.29	unknown	Seychelles		131178	KINGCORP-KHOpenNetISPCambodiaKH	false
91.32.221.2	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
45.111.37.151	unknown	Egypt		37069	MOBINILEG	false
91.186.75.37	unknown	Norway		56828	NORWEGIANHEALTHNETWORKNO	false
156.199.203.244	unknown	Egypt		8452	TE-ASTE-ASEG	false
185.166.97.74	unknown	Switzerland		8758	IWAYCH	false
45.50.203.110	unknown	United States		20001	TWC-20001-PACWESTUS	false
45.50.203.111	unknown	United States		20001	TWC-20001-PACWESTUS	false
143.160.177.92	unknown	South Africa		8094	PUKNETZA	false
38.112.91.39	unknown	United States		35884	SECUREDATA365-OH1US	false
91.112.149.146	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
45.244.195.57	unknown	Egypt		24863	LINKdotNET-ASEG	false
135.115.217.58	unknown	United States		10455	LUCENT-CIOUS	false
45.48.194.65	unknown	United States		20001	TWC-20001-PACWESTUS	false
193.79.200.215	unknown	Netherlands		702	UUNETUS	false
45.188.109.25	unknown	unknown		265607	CONECTAREDSADECVMX	false
45.91.88.227	unknown	Romania		203020	HOSTROYALERO	false
45.130.62.163	unknown	Israel		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
45.106.6.116	unknown	Egypt		37069	MOBINILEG	false
185.203.160.87	unknown	Iran (ISLAMIC Republic Of)		205837	SADADPSP-ASSadadProcessingModernServicesCompanyPJS	false
91.199.162.60	unknown	Germany		42652	DELUNETDE	false
221.60.149.251	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
45.202.220.126	unknown	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	false
142.34.24.35	unknown	Canada		27272	Q9-AS-CAL3CA	false
197.75.183.147	unknown	South Africa		16637	MTNNS-ASZA	false
41.117.228.167	unknown	South Africa		16637	MTNNS-ASZA	false
185.110.49.231	unknown	Poland		47544	IQPL-ASPL	false
128.122.29.218	unknown	United States		12	NYU-DOMAINUS	false
176.198.187.187	unknown	Germany		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
156.223.50.214	unknown	Egypt		8452	TE-ASTE-ASEG	false
67.236.61.9	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
185.45.66.61	unknown	Bulgaria		201200	SUPERHOSTING_ASBG	false
185.56.176.219	unknown	France		35600	ASN-VEDEGEFR	false
105.177.118.37	unknown	South Africa		16637	MTNNS-ASZA	false
45.229.91.225	unknown	Brazil		267106	NETFIBRATELECOMUNICACOESLTDA-MEBR	false
197.123.112.51	unknown	Egypt		36992	ETISALAT-MISREG	false
45.86.28.98	unknown	United Kingdom		9009	M247GB	false
41.197.85.149	unknown	Rwanda		36934	Broadband-Systems-CorporationRW	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
114.140.203.26	unknown	Taiwan; Republic of China (ROC)		9674	FET-TWFarEastToneTelecommunicationCoLtdTW	false
84.136.240.4	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
156.56.101.225	unknown	United States		87	INDIANA-ASUS	false
45.219.30.160	unknown	Morocco		36925	ASMediMA	false
57.37.96.242	unknown	Belgium		2686	ATGS-MMD-ASUS	false
157.136.46.228	unknown	France		2200	FR-RENATERReseauNationaldetelecommunicationspourlaTec	false
45.170.183.65	unknown	Brazil		268166	POINTTELECOMSERVICOSLTDABR	false
190.156.168.164	unknown	Colombia		10620	TelmexColombiaSACO	false
100.147.152.95	unknown	United States		21928	T-MOBILE-AS21928US	false
47.182.85.190	unknown	United States		5650	FRONTIER-FRTRUS	false
45.227.105.167	unknown	Brazil		267019	AHPROVEDORTELECOMBR	false
178.157.234.27	unknown	Denmark		43557	ASEMNETDK	false
45.222.24.183	unknown	South Africa		327849	ROCKETNETZA	false
45.150.101.191	unknown	Liechtenstein		47987	LOVESERVERSGB	false
185.68.214.201	unknown	Czech Republic		203208	CTU_AS4_2CZ	false
45.233.204.100	unknown	Brazil		267397	SKYNETARUJACOMUNICACOESEIRELIBR	false
192.91.253.232	unknown	United States		3356	LEVEL3US	false
185.102.18.28	unknown	Sweden		41753	TELELOCATIONSE	false
45.163.170.78	unknown	Brazil		268563	LIGNETSERVICOSDECOMUNICACAOMULTIMIDIAEIRELIBR	false
81.101.96.158	unknown	United Kingdom		5089	NTLGB	false
185.228.32.102	unknown	Austria		8540	AMANET-ASAT	false
45.219.30.151	unknown	Morocco		36925	ASMediMA	false

Runtime Messages

Command:	/tmp/Antisocial.x86
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	C7C - c
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.203.160.49	7NjQVwW7NZ	Get hash	malicious	Browse	
45.153.14.111	Antisocial.arm	Get hash	malicious	Browse	
45.128.94.101	Hilix.x86	Get hash	malicious	Browse	
45.117.212.26	Antisocial.arm	Get hash	malicious	Browse	
91.49.236.110	2S8N5fDSRs	Get hash	malicious	Browse	
41.157.30.69	nUDLlJvoP4	Get hash	malicious	Browse	
	FIBlU8JUAF	Get hash	malicious	Browse	
197.55.123.214	x86-20211013-0650	Get hash	malicious	Browse	
	17Rom1F3MY	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SIPL-ASSysconInfowayPvtLtdIN	BitmCvTrdO	Get hash	malicious	Browse	• 45.117.212.38
	UQnO4DB8Z1	Get hash	malicious	Browse	• 45.117.212.43
	lYmYPlzghQ	Get hash	malicious	Browse	• 45.117.212.43
	apep.x86	Get hash	malicious	Browse	• 103.76.76.166
	ivImhRZqGa	Get hash	malicious	Browse	• 103.76.76.167
	1alzsODTFe	Get hash	malicious	Browse	• 45.117.212.32
	5yjXpBEf1o	Get hash	malicious	Browse	• 160.22.32.93
	txYTweyXZ0	Get hash	malicious	Browse	• 160.22.254.152
	z0x3n.x86	Get hash	malicious	Browse	• 183.87.69.200
	arm-20211007-1206	Get hash	malicious	Browse	• 160.21.176.227
	e7HWBo7yQM	Get hash	malicious	Browse	• 160.20.5.38
	lessie.x86	Get hash	malicious	Browse	• 160.22.106.46
	17Rom1F3MY	Get hash	malicious	Browse	• 160.21.176.220
	Hilix.arm7	Get hash	malicious	Browse	• 45.117.212.13
	iuSFhE6G0p	Get hash	malicious	Browse	• 45.117.212.58
	re2.x86	Get hash	malicious	Browse	• 103.76.76.170
	Antisocial.arm	Get hash	malicious	Browse	• 45.117.212.26
	ZNobquzR0a	Get hash	malicious	Browse	• 160.22.254.118
	mips	Get hash	malicious	Browse	• 45.117.212.36
	jlKiz9kMcA	Get hash	malicious	Browse	• 160.21.176.245
ATT-INTERNET4US	Antisocial.arm	Get hash	malicious	Browse	• 99.161.94.81
	w66OTKGVFv	Get hash	malicious	Browse	• 75.45.81.104
	swOGb2sZYt	Get hash	malicious	Browse	• 45.20.156.207
	ydZLm6GD56	Get hash	malicious	Browse	• 13.41.205.23
	UQnO4DB8Z1	Get hash	malicious	Browse	• 45.30.40.102
	OhUy3woBmb	Get hash	malicious	Browse	• 172.185.62.64
	S8G5z3pdHw	Get hash	malicious	Browse	• 75.30.223.233
	9o6Z1wEokT	Get hash	malicious	Browse	• 12.207.216.252
	00hZyjOhZA	Get hash	malicious	Browse	• 70.250.254.60
	yxD7DmfG2j	Get hash	malicious	Browse	• 106.0.113.38
	V2WzER53Tt	Get hash	malicious	Browse	• 74.166.99.108
	a5nulABeSk	Get hash	malicious	Browse	• 108.64.172.130
	1bL17EUgTk	Get hash	malicious	Browse	• 107.193.164.34
	pTF1ilCUEm	Get hash	malicious	Browse	• 13.186.169.31
	032k4JmR0U	Get hash	malicious	Browse	• 70.142.13.244
	arm	Get hash	malicious	Browse	• 107.220.87.241
	x86	Get hash	malicious	Browse	• 108.213.51.215
	arm7	Get hash	malicious	Browse	• 104.58.236.145
	z0x3n.arm7	Get hash	malicious	Browse	• 45.21.146.181
	z0x3n.x86	Get hash	malicious	Browse	• 70.131.55.48
EDV-TEAM-OBERLANDDE	apep.arm7	Get hash	malicious	Browse	• 45.128.94.112
	Hilix.arm7	Get hash	malicious	Browse	• 45.128.94.119
	Hilix.x86	Get hash	malicious	Browse	• 45.128.94.101
	93T511Z3h8	Get hash	malicious	Browse	• 45.128.94.119
	Hilix.x86	Get hash	malicious	Browse	• 45.128.94.113
	ET42wHpzr3	Get hash	malicious	Browse	• 45.128.94.113

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fb4726d465c5f28b84cd6d14cedd13a7	1TnmkstVG8	Get hash	malicious	Browse	• 34.249.145.219
	10CV2biW2d	Get hash	malicious	Browse	• 34.249.145.219
	r7bQAtiN68	Get hash	malicious	Browse	• 34.249.145.219
	86wbpLsr78	Get hash	malicious	Browse	• 34.249.145.219
	zYEw8iWwGB	Get hash	malicious	Browse	• 34.249.145.219
	3QM8LROaOk	Get hash	malicious	Browse	• 34.249.145.219
	75OHlqPaRY	Get hash	malicious	Browse	• 34.249.145.219
	S0QgabliDO	Get hash	malicious	Browse	• 34.249.145.219
	vCLbAS7aPb	Get hash	malicious	Browse	• 34.249.145.219
	yzui4gwsrF	Get hash	malicious	Browse	• 34.249.145.219
	072FZHiMhs	Get hash	malicious	Browse	• 34.249.145.219

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sjZlfrpuyc	Get hash	malicious	Browse	• 34.249.145.219
	khoE2I8yer	Get hash	malicious	Browse	• 34.249.145.219
	wvsEoQ0khP	Get hash	malicious	Browse	• 34.249.145.219
	32	Get hash	malicious	Browse	• 34.249.145.219
	a-r.m-5.Sakura	Get hash	malicious	Browse	• 34.249.145.219
	NDYfrLSNFW	Get hash	malicious	Browse	• 34.249.145.219
	m-i.p-s.Sakura	Get hash	malicious	Browse	• 34.249.145.219
	6Qn1b9fB2C	Get hash	malicious	Browse	• 34.249.145.219
	ZSbDircdwC	Get hash	malicious	Browse	• 34.249.145.219

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):	6.4588282370976575
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	Antisocial.x86
File size:	58448
MD5:	abf15f119a5fa686f85e3a9ce8f57cdc
SHA1:	6531db808704d554554e9b696f965e94088fdd00
SHA256:	e41b1347da792c9718d4a65b26cdb2fdda54590f40a4fa1441c7954f09545df4
SHA512:	ac28930a117bdb0b4486003d4f14e440d0c60dddc879a2542e1a1d9f6518c302cfbb7e09b056399f960d84dd2d83d9a0ccc5f4c1ee96d528e53011662c109df5
SSDEEP:	1536:TjkZoZPif+ODr/5K9IMG/CtZZDKuihKuH0iM4/cndhaSML4o++++++++++++++:KoZ4+ODr/4IdCLcuihKuH44/Yzi++++y
File Content Preview:	.ELF.....d...4.....4. ...(.....`...`.....).....Q.td.....U..S.....w....h....s...[]...$.....U.....=.b...t..5....$`.....$`.....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:	58048
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	0xbd96	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x8053e46	0xbe46	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x8053e60	0xbe60	0x1d20	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x8056000	0xe000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8056008	0xe008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x8056020	0xe020	0x260	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x8056280	0xe280	0x2680	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0xe280	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	0xdb80	0xdb80	4.1302	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0xe000	0x8056000	0x8056000	0x280	0x2900	2.1765	0x6	RW	0x1000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

TCP Packets

HTTP Request Dependency Graph

- 127.0.0.1:52869

System Behavior

Analysis Process: Antisocial.x86 PID: 5225 Parent PID: 5102

General

Start time:	13:37:53
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	/tmp/Antisocial.x86
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5226 Parent PID: 5225

General

Start time:	13:37:53
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5237 Parent PID: 5226

General

Start time:	13:37:58
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5238 Parent PID: 5226

General

Start time:	13:37:58
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5239 Parent PID: 5238

General

Start time:	13:37:58
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5250 Parent PID: 5239

General

Start time:	13:38:03
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5251 Parent PID: 5239

General

Start time:	13:38:03
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5252 Parent PID: 5239

General

Start time:	13:38:03
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5253 Parent PID: 5239

General

Start time:	13:38:03
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5240 Parent PID: 5238

General

Start time:	13:37:58
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5242 Parent PID: 5238

General

Start time:	13:37:58
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5244 Parent PID: 5238

General

Start time:	13:37:58
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5246 Parent PID: 5238

General

Start time:	13:37:58
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5227 Parent PID: 5225

General

Start time:	13:37:53
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5228 Parent PID: 5225

General

Start time:	13:37:53
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5229 Parent PID: 5228

General

Start time:	13:37:53
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5241 Parent PID: 5229

General

Start time:	13:37:58
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5243 Parent PID: 5229

General

Start time:	13:37:58
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5245 Parent PID: 5229

General

Start time:	13:37:58
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5247 Parent PID: 5229

General

Start time:	13:37:58
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes

MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5230 Parent PID: 5228

General

Start time:	13:37:53
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5231 Parent PID: 5228

General

Start time:	13:37:53
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5232 Parent PID: 5228

General

Start time:	13:37:53
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: Antisocial.x86 PID: 5234 Parent PID: 5228

General

Start time:	13:37:53
Start date:	01/11/2021
Path:	/tmp/Antisocial.x86
Arguments:	n/a
File size:	58448 bytes
MD5 hash:	abf15f119a5fa686f85e3a9ce8f57cdc

Analysis Process: dash PID: 5268 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/dash

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

Analysis Process: cat PID: 5268 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.zwbUWO1Xs3
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5269 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5269 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5270 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5270 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
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: 5271 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5271 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: 5272 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5272 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.zwbUWO1Xs3
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5273 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5273 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5274 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5274 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
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: 5275 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5275 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
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: 5276 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5276 Parent PID: 4332

General

Start time:	13:38:28
Start date:	01/11/2021
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.zwbUWO1Xs3 /tmp/tmp.7ybUxelKh4 /tmp/tmp.tWQiSu25Ld
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read