ID: 513323
Sample Name: zJk9UEOnQ7
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 02:34:42
Date: 02/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

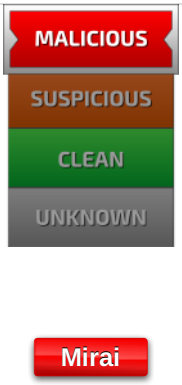
Linux Analysis Report zJk9UEOnQ7

Overview

General Information

Sample Name:	zJk9UEOnQ7
Analysis ID:	513323
MD5:	309bf4c5ed21406.
SHA1:	a22d7169e00733..
SHA256:	040224bd9ea2a0..
Tags:	32 elf mirai sparc
Infos:	

Detection

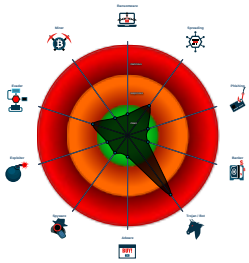


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Connects to many ports of the same...
- Sample has stripped symbol table
- HTTP GET or POST without a user ...
- Uses the "uname" system call to qu...
- Enumerates processes within the "p...
- Tries to connect to HTTP servers, b...
- Detected TCP or UDP traffic on non...

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work

Static ELF header machine description suggests that the sample might not execute correctly on this machine

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	513323
Start date:	02.11.2021
Start time:	02:34:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zJk9UEOnQ7
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.lin@0/3@0/0
Warnings:	Show All

Process Tree

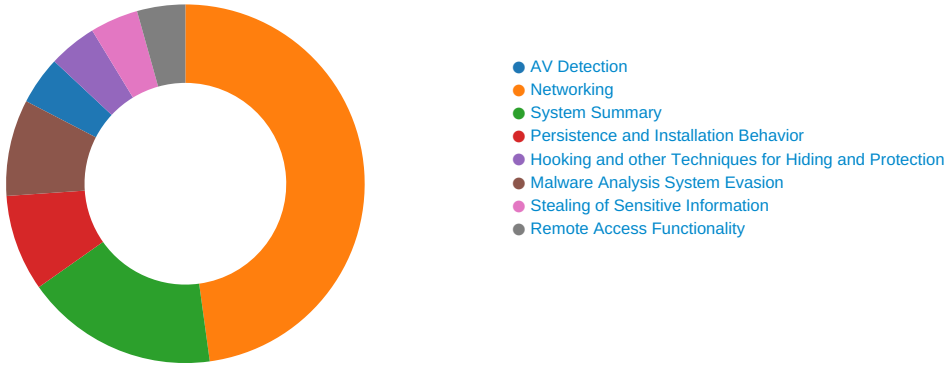
- **system is lnxubuntu20**
- dash New Fork (PID: 5205, Parent: 4331)
  - cat (PID: 5205, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.91tEJtbEWc
- dash New Fork (PID: 5206, Parent: 4331)
  - head (PID: 5206, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5207, Parent: 4331)
  - tr (PID: 5207, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5208, Parent: 4331)
  - cut (PID: 5208, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5209, Parent: 4331)
  - cat (PID: 5209, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.91tEJtbEWc
- dash New Fork (PID: 5210, Parent: 4331)
  - head (PID: 5210, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5211, Parent: 4331)
  - tr (PID: 5211, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5212, Parent: 4331)
  - cut (PID: 5212, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5213, Parent: 4331)
  - rm (PID: 5213, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.91tEJtbEWc /tmp/tmp.Zus0sicMvy /tmp/tmp.qH6x8mL5YT
  - zJk9UEOnQ7 (PID: 5241, Parent: 5107, MD5: 7dc1c0e23cd5e102bb12e5c29403410e) Arguments: /tmp/zJk9UEOnQ7
    - zJk9UEOnQ7 New Fork (PID: 5243, Parent: 5241)
      - zJk9UEOnQ7 New Fork (PID: 5285, Parent: 5243)
      - zJk9UEOnQ7 New Fork (PID: 5289, Parent: 5243)
        - zJk9UEOnQ7 New Fork (PID: 5292, Parent: 5289)
          - zJk9UEOnQ7 New Fork (PID: 5297, Parent: 5292)
          - zJk9UEOnQ7 New Fork (PID: 5301, Parent: 5292)
          - zJk9UEOnQ7 New Fork (PID: 5305, Parent: 5292)
          - zJk9UEOnQ7 New Fork (PID: 5308, Parent: 5292)
        - zJk9UEOnQ7 New Fork (PID: 5293, Parent: 5289)
        - zJk9UEOnQ7 New Fork (PID: 5296, Parent: 5289)
        - zJk9UEOnQ7 New Fork (PID: 5299, Parent: 5289)
        - zJk9UEOnQ7 New Fork (PID: 5302, Parent: 5289)
    - zJk9UEOnQ7 New Fork (PID: 5244, Parent: 5241)
    - zJk9UEOnQ7 New Fork (PID: 5245, Parent: 5241)
      - zJk9UEOnQ7 New Fork (PID: 5249, Parent: 5245)
        - zJk9UEOnQ7 New Fork (PID: 5280, Parent: 5249)
        - zJk9UEOnQ7 New Fork (PID: 5282, Parent: 5249)
        - zJk9UEOnQ7 New Fork (PID: 5284, Parent: 5249)
        - zJk9UEOnQ7 New Fork (PID: 5286, Parent: 5249)
      - zJk9UEOnQ7 New Fork (PID: 5250, Parent: 5245)
      - zJk9UEOnQ7 New Fork (PID: 5254, Parent: 5245)
      - zJk9UEOnQ7 New Fork (PID: 5256, Parent: 5245)
      - zJk9UEOnQ7 New Fork (PID: 5257, Parent: 5245)
- systemd New Fork (PID: 5279, Parent: 1)
  - sshd (PID: 5279, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5310, Parent: 1)
  - sshd (PID: 5310, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- **cleanup**

Yara Overview

PCAP (Network Traffic)

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

Jbx Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

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

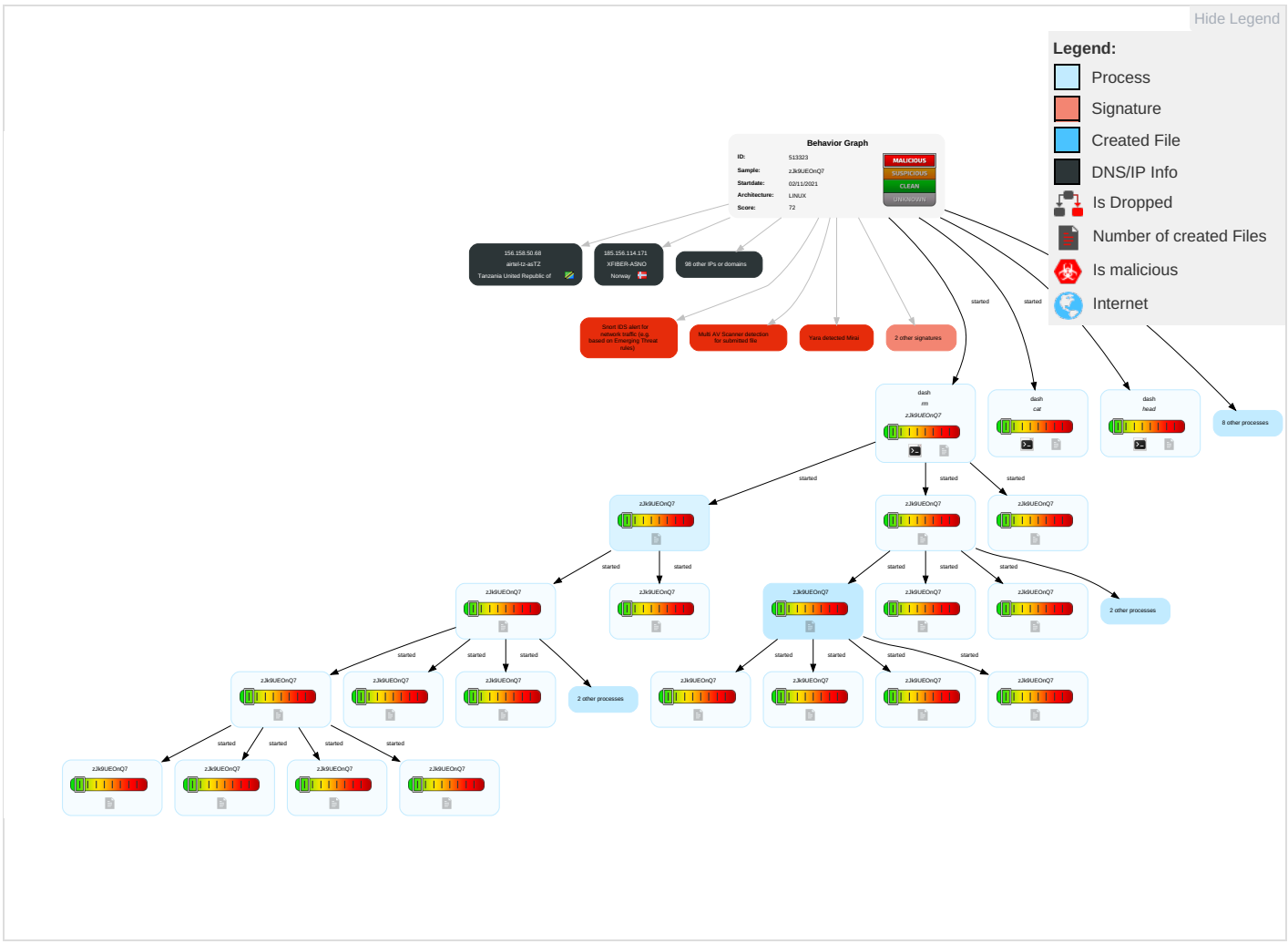
Mitre Att&ck Matrix

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 1	Security Software Discovery 1 1	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 Partitio
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 Lockou
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
zJk9UEOnQ7	52%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:52869/picdesc.xml	0%	Virustotal		Browse
http://127.0.0.1:52869/picdesc.xml	0%	Avira URL Cloud	safe	
http://37.0.9.202/bins/Hilix.mips	10%	Virustotal		Browse
http://37.0.9.202/bins/Hilix.mips	100%	Avira URL Cloud	malware	
http://127.0.0.1:52869/wanipcn.xml	0%	Avira URL Cloud	safe	

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	• 0%, Virustotal, Browse • 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
185.220.10.243	unknown	Spain		205390	TECTIQOM-ASDE	false
45.63.53.210	unknown	United States		20473	AS-CHOOPAUS	false
103.92.122.33	unknown	India		135718	DISHAWAVESINFONET-ASDISHAWAVESINFONET PVTLTDIN	false
177.200.187.233	unknown	Brazil		262526	TitaniaTelecomBR	false
45.130.62.177	unknown	Israel		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
185.114.210.159	unknown	Switzerland		199366	TTNETDCTR	false
45.199.228.247	unknown	Seychelles		8100	ASN-QUADRANET-GLOBALUS	false
45.21.146.145	unknown	United States		7018	ATT-INTERNET4US	false
105.103.188.148	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.143.201.55	unknown	Algeria		36891	ICOSNET-ASDZ	false
91.90.138.87	unknown	Israel		25046	CHECKPOINTIL	false
197.19.253.197	unknown	Tunisia		37693	TUNISIANATN	false
197.44.77.183	unknown	Egypt		8452	TE-ASTE-ASEG	false
185.38.220.159	unknown	Poland		56523	AMELEKTRONIKPL	false
68.49.212.219	unknown	United States		7922	COMCAST-7922US	false
45.153.14.26	unknown	Russian Federation		208221	ORIONNET-BRKRU	false
156.43.68.96	unknown	United Kingdom		4211	ASN-MARICOPA1US	false
172.255.87.27	unknown	United States		394380	LEASEWEB-USA-DAL-10US	false
45.246.175.184	unknown	Egypt		24863	LINKdotNET-ASEG	false
45.246.175.186	unknown	Egypt		24863	LINKdotNET-ASEG	false
185.203.160.64	unknown	Iran (ISLAMIC Republic Of)		205837	SADADPSP-ASSadadProcessingModern ServicesCompanyPJS	false
91.130.14.16	unknown	Austria		1257	TELE2EU	false
91.130.14.18	unknown	Austria		1257	TELE2EU	false
91.167.86.160	unknown	France		12322	PROXADFR	false
185.204.16.74	unknown	Czech Republic		200918	ORELSOFTCZ	false
185.21.99.33	unknown	Austria		49808	POWERSPEED-ASAT	false
185.166.97.85	unknown	Switzerland		8758	IWAYCH	false
91.167.86.167	unknown	France		12322	PROXADFR	false
91.178.113.232	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
164.85.190.86	unknown	Brazil		23074	PETROLEOBRASILEIROSA-PETROBRASBR	false
91.183.234.36	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
91.67.33.164	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
41.5.41.242	unknown	South Africa		29975	VODACOM-ZA	false
91.67.33.166	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
8.40.221.25	unknown	United States		394856	IPACCUS	false
45.44.104.180	unknown	Canada		54198	VIANETCA	false
185.78.7.94	unknown	United Kingdom		16030	ALTECOMES	false
91.163.145.86	unknown	France		12322	PROXADFR	false
45.237.182.82	unknown	Brazil		268283	NETWORKFIBERCOMERCIOESERVICOSDECOMUNICACAOBR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
92.212.74.4	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
91.219.76.54	unknown	Netherlands		51571	PROTECHNICSNL	false
59.1.116.39	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
45.221.254.31	unknown	Benin		328092	SUD-TELCOM-ASBJ	false
197.51.4.224	unknown	Egypt		8452	TE-ASTE-ASEG	false
91.184.212.207	unknown	Cyprus		35432	CABLENET-ASCY	false
45.50.54.54	unknown	United States		20001	TWC-20001-PACWESTUS	false
45.111.37.150	unknown	Egypt		37069	MOBINILEG	false
201.67.116.239	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
91.211.55.231	unknown	Russian Federation		48494	MKNET-ASCZ	false
45.145.30.185	unknown	Turkey		197328	INETLTDTR	false
66.55.202.243	unknown	United States		5760	BIDDEFORD1US	false
119.104.84.1	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
45.227.105.109	unknown	Brazil		267019	AHPROVEDORTELECOMBR	false
156.158.50.68	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
197.211.66.63	unknown	South Africa		29918	IMPOL-ASNZA	false
197.92.49.8	unknown	South Africa		10474	OPTINETZA	false
2.135.247.91	unknown	Kazakhstan		9198	KAZTELECOM-ASKZ	false
45.127.206.114	unknown	Indonesia		55699	STARNET-AS-IDPTCemerlangMultimediaID	false
45.106.6.117	unknown	Egypt		37069	MOBINILEG	false
96.78.116.253	unknown	United States		7922	COMCAST-7922US	false
89.61.196.207	unknown	Germany		5430	FREENETDEfreenetDatenkommunikationsGmbHDE	false
185.50.154.127	unknown	United Kingdom		50203	UK-REYNOLDS-ASNGB	false
24.29.246.12	unknown	United States		10796	TWC-10796-MIDWESTUS	false
91.100.152.119	unknown	Denmark		15516	DK-DANSKKABELTVDK	false
41.227.43.22	unknown	Tunisia		2609	TN-BB-ASTunisiaBackBoneASTN	false
45.94.158.129	unknown	Ukraine		56851	VPS-UA-ASUA	false
45.117.212.64	unknown	India		45194	SIPL-ASSysconInfowayPvtLtdIN	false
70.49.63.170	unknown	Canada		577	BACOMCA	false
160.181.79.212	unknown	South Africa		36903	MT-MPLSMA	false
140.123.127.169	unknown	Taiwan; Republic of China (ROC)		38844	NTNU-TWNationalTaiwanNormalUniversityTW	false
202.203.120.2	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
45.104.92.38	unknown	Egypt		37069	MOBINILEG	false
185.156.114.171	unknown	Norway		8896	XFIBER-ASNO	false
185.228.32.110	unknown	Austria		8540	AMANET-ASAT	false
45.104.148.70	unknown	Egypt		37069	MOBINILEG	false
183.236.151.32	unknown	China		56040	CMNET-GUANGDONG-APChinaMobilecommunicationscorporation	false
185.86.223.119	unknown	Iceland		200868	KAPALVAEDINGIS	false
45.30.40.163	unknown	United States		7018	ATT-INTERNET4US	false
126.11.178.137	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
41.3.151.166	unknown	South Africa		29975	VODACOM-ZA	false
91.66.119.226	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
45.91.88.230	unknown	Romania		203020	HOSTROYALERO	false
45.9.118.68	unknown	Netherlands		29066	VELIANET-ASvelianetInternetdiensteGmbHDE	false
103.200.224.62	unknown	China		134633	IDNIC-AHU-AS-IDDirektoratJenderalAdministrasiHukumUmum	false
45.48.194.85	unknown	United States		20001	TWC-20001-PACWESTUS	false
41.217.104.32	unknown	Nigeria		37340	SpectranetNG	false
91.198.173.169	unknown	Switzerland		43477	WIRBANK-ASSteinengraben12CH	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.73.200.152	unknown	United States		19318	IS-AS-1US	false
185.78.207.26	unknown	United Kingdom		8426	CLARANET-ASClaraNETLTDGB	false
185.171.27.35	unknown	Turkey		60721	BURSABILTR	false
185.156.114.187	unknown	Norway		8896	XFIBER-ASNO	false
185.248.70.63	unknown	Netherlands		202374	PREWESTNL	false
156.13.155.42	unknown	New Zealand		22192	SSHENETUS	false
185.19.109.116	unknown	United Kingdom		17804	LAODC-AS-APLaoDataCenterLA	false
156.49.160.41	unknown	Sweden		29975	VODACOM-ZA	false
185.25.208.150	unknown	United Kingdom		60804	SWISS-NETWORKCH	false
45.21.146.194	unknown	United States		7018	ATT-INTERNET4US	false
45.246.175.149	unknown	Egypt		24863	LINKdotNET-ASEG	false
45.242.108.56	unknown	Egypt		24863	LINKdotNET-ASEG	false
42.122.248.206	unknown	China		17638	CHINATELECOM-TJ-AS-APASNforTIANJINProvincialNetofCT	false

Runtime Messages

Command:	/tmp/zJk9UEOnQ7
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
197.19.253.197	zgV2Uq4fmu	Get hash	malicious	Browse	
91.130.14.18	z3hir.x86	Get hash	malicious	Browse	
	uh2jT4lQME	Get hash	malicious	Browse	
197.44.77.183	Vk3A1yJJMg	Get hash	malicious	Browse	
91.167.86.160	Antisocial.x86	Get hash	malicious	Browse	
185.204.16.74	QIJ16axero	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DISHAWAVESINFONET-ASDISHAWAVESINFONETPVTLTDIN	dark.x86	Get hash	malicious	Browse	• 103.92.122.37
	4NqKj5KARM	Get hash	malicious	Browse	• 103.101.56.111
	Clh974QBqG	Get hash	malicious	Browse	• 103.92.122.21
AS-CHOOPAUS	MePwVTNRoA	Get hash	malicious	Browse	• 45.32.45.171
	MkyxPXGeTq	Get hash	malicious	Browse	• 45.32.45.179
	TlhOKlVSwf	Get hash	malicious	Browse	• 45.32.45.176
	Hilix.arm	Get hash	malicious	Browse	• 45.63.53.230
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 149.28.253.196
	A3845D760F3394981F0E9B2330C279DB0534BEFAAA17C.exe	Get hash	malicious	Browse	• 149.28.253.196
	P8AVd483d7	Get hash	malicious	Browse	• 45.32.230.26
	eLL1MVwOME.exe	Get hash	malicious	Browse	• 149.28.171.238
	mxHkqAIYT0	Get hash	malicious	Browse	• 167.179.103.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	w66OTKGVFv	Get hash	malicious	Browse	• 45.63.53.223
	ydZLm6GD56	Get hash	malicious	Browse	• 45.63.53.239
	Zm1Oz6lCLO.exe	Get hash	malicious	Browse	• 216.128.137.31
	MBlIM3UCPz.exe	Get hash	malicious	Browse	• 216.128.137.31
	RYDdv7X9e8.exe	Get hash	malicious	Browse	• 216.128.137.31
	gPm4nLttxA.exe	Get hash	malicious	Browse	• 216.128.137.31
	BTKK4TcLar.exe	Get hash	malicious	Browse	• 216.128.137.31
	tVzelearRj.exe	Get hash	malicious	Browse	• 216.128.137.31
	4viHjPSIXn.exe	Get hash	malicious	Browse	• 216.128.137.31
	03DF381BD91F5CFC93785D4B9A809CDCF6E13E9023651.exe	Get hash	malicious	Browse	• 149.28.253.196
	RFQ DTD011121- FAMORITALIA.xlsx	Get hash	malicious	Browse	• 149.28.171.238
TECTIQOM-ASDE	w66OTKGVFv	Get hash	malicious	Browse	• 185.220.10.233
	swOGb2sZYt	Get hash	malicious	Browse	• 185.220.10.239
	R3Y21HxKFx	Get hash	malicious	Browse	• 185.220.10.214
	sora.x86	Get hash	malicious	Browse	• 185.220.10.229
	Hilix.arm7	Get hash	malicious	Browse	• 185.220.10.246
	Hilix.x86	Get hash	malicious	Browse	• 185.220.10.222
	2S8N5fDSRs	Get hash	malicious	Browse	• 185.220.10.209
	KXM253rCpW	Get hash	malicious	Browse	• 185.220.10.232
	Antisocial.arm	Get hash	malicious	Browse	• 185.220.10.205
	loligang.x86	Get hash	malicious	Browse	• 185.220.10.202
	B7Cm8HC6EZ	Get hash	malicious	Browse	• 185.220.10.241
	JVB30EDCaR	Get hash	malicious	Browse	• 185.220.10.246
	XhEdLIc8Vn	Get hash	malicious	Browse	• 185.220.10.252

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5310/oom_score_adj	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	6
Entropy (8bit):	1.7924812503605778
Encrypted:	false
SSDEEP:	3:ptn:Dn
MD5:	CBF282CC55ED0792C33D10003D1F760A
SHA1:	007DD8BD75468E6B7ABA4285E9B267202C7EAEED
SHA-256:	FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22
SHA-512:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	-1000.

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:DUF:y
MD5:	50A8E45270E16679E6A7AA0F75F0D0B8

/run/sshd.pid	
SHA1:	0413113B4F151E5CE15A9DE93BCBDAE262483544
SHA-256:	0FF7E248711867AD5A1BFA1F13922A0DE635C92A8ED527363E232827AB66C6C0
SHA-512:	9678C8EA37E8CAC932B8DA362E6990C0D251ED8D55EA88F0EE7746B7C892F03D626DAF2F88B8A7CB138BC01AD40BA03F5220AB5C83C9FB543DD23A16EF7D5DF
Malicious:	false
Reputation:	low
Preview:	5310.

/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 MSB executable, SPARC, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.179513692558146
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	zJk9UEOnQ7
File size:	63160
MD5:	309bf4c5ed21406e7014eb818dc1788f
SHA1:	a22d7169e00733c6de7a3ba69e8d05a38b635f13
SHA256:	040224bd9ea2a0069c349f9a514c3ccd977307f217516ecac9266897c1e6641d
SHA512:	613d2667cc9fbb4e6505140f06846886488add415f9ab115515242db2fadc8534dd3cd162f603f694bb0fe1c878938cb184f8702b4718a50f64d14289cabe286
SSDEEP:	1536:Z4b/GEEStcNEu6F+lnWgnE629to3s1xP8oHAHSN9:ipqNraez4focgSN9
File Content Preview:	.ELF.....4...(.....4. ...(.....,.....dt.Q.....@..(....@.8.....#.....`..`.....!....."...@....."........`.....$"..."...@.....`....

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	Sparc
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x101a4
Flags:	0x0

ELF header

ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	62760
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	0x10094	0x94	0x1c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100b0	0xb0	0xe058	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x1e108	0xe108	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1e120	0xe120	0x1198	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x2f2bc	0xf2bc	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x2f2c4	0xf2c4	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x2f2d0	0xf2d0	0x218	0x0	0x3	WA	0	0	8
.bss	NOBITS	0x2f4e8	0xf4e8	0x2f0	0x0	0x3	WA	0	0	8
.shstrtab	STRTAB	0x0	0xf4e8	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	0x10000	0x10000	0xf2b8	0xf2b8	3.6873	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xf2bc	0x2f2bc	0x2f2bc	0x22c	0x51c	1.5766	0x6	RW	0x10000		.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: dash PID: 5205 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5205 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.91tEJtbEWc
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5206 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5206 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5207 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5207 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
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: 5208 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5208 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: 5209 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5209 Parent PID: 4331

General

Start time:	02:35:21

Start date:	02/11/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.91tEJtbEWc
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5210 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5210 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5211 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5211 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
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: 5212 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5212 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
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: 5213 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5213 Parent PID: 4331

General

Start time:	02:35:21
Start date:	02/11/2021
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.91tEJtbEWc /tmp/tmp.Zus0sicMvy /tmp/tmp.qH6x8mL5YT

File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: zJk9UEOnQ7 PID: 5241 Parent PID: 5107

General

Start time:	02:35:24
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	/tmp/zJk9UEOnQ7
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Analysis Process: zJk9UEOnQ7 PID: 5243 Parent PID: 5241

General

Start time:	02:35:24
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Directory Enumerated

Analysis Process: zJk9UEOnQ7 PID: 5285 Parent PID: 5243

General

Start time:	02:35:33
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5289 Parent PID: 5243

General

Start time:	02:35:33
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5292 Parent PID: 5289

General

Start time:	02:35:33
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5297 Parent PID: 5292

General

Start time:	02:35:34
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5301 Parent PID: 5292

General

Start time:	02:35:34
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5305 Parent PID: 5292

General

Start time:	02:35:34
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5308 Parent PID: 5292

General

Start time:	02:35:34
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5293 Parent PID: 5289

General

Start time:	02:35:33
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5296 Parent PID: 5289

General

Start time:	02:35:34
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5299 Parent PID: 5289

General

Start time:	02:35:34
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5302 Parent PID: 5289

General

Start time:	02:35:34
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5244 Parent PID: 5241

General

Start time:	02:35:24
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5245 Parent PID: 5241

General

Start time:	02:35:24
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5249 Parent PID: 5245

General

Start time:	02:35:24
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Directory Enumerated

Analysis Process: zJk9UEOnQ7 PID: 5280 Parent PID: 5249

General

Start time:	02:35:33
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5282 Parent PID: 5249

General

Start time:	02:35:33
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5284 Parent PID: 5249

General

Start time:	02:35:33
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5286 Parent PID: 5249

General

Start time:	02:35:33
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5250 Parent PID: 5245

General

Start time:	02:35:24
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5254 Parent PID: 5245

General

Start time:	02:35:25
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5256 Parent PID: 5245

General

Start time:	02:35:25
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: zJk9UEOnQ7 PID: 5257 Parent PID: 5245

General

Start time:	02:35:25
Start date:	02/11/2021
Path:	/tmp/zJk9UEOnQ7
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: systemd PID: 5279 Parent PID: 1

General

Start time:	02:35:33
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5279 Parent PID: 1

General

Start time:	02:35:33
Start date:	02/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5310 Parent PID: 1

General

Start time:	02:35:35
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd

Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5310 Parent PID: 1

General

Start time:	02:35:35
Start date:	02/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated