ID: 507413
Sample Name: MPnFvIsvJp
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 08:23:59
Date: 22/10/2021
Version: 33.0.0 White Diamond

Table of Contents

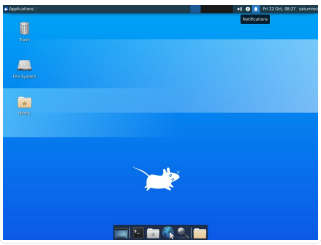
Linux Analysis Report MPnFvIsvJp

Overview

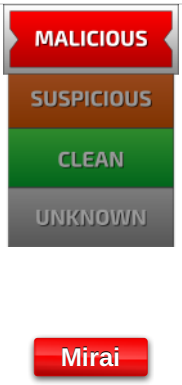
General Information

Sample Name:	MPnFvIsvJp
Analysis ID:	507413
MD5:	2af6167aa24d06f..
SHA1:	24092366777f504.
SHA256:	4c6ea0ba603fe0b.
Tags:	32 elf mirai powerpc
Infos:	

Most interesting Screenshot:



Detection

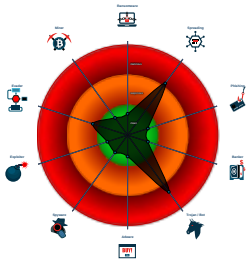


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Sample tries to kill many processes...
- Sample has stripped symbol table
- 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...
- Executes the "rm" command used to...
- Sample listens on a socket
- Sample tries to kill a process (SIGK...

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:	33.0.0 White Diamond
Analysis ID:	507413
Start date:	22.10.2021
Start time:	08:23:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MPnFvIsvJp
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.spre.troj.lin@0/3@0/0
Warnings:	Show All

Process Tree

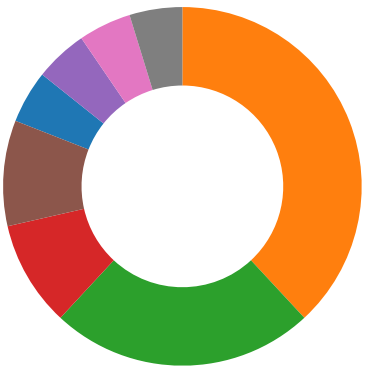
- **system is lnxubuntu20**
- dash New Fork (PID: 5213, Parent: 4342)
  - cat (PID: 5213, Parent: 4342, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.nd5wZIclrj
- dash New Fork (PID: 5214, Parent: 4342)
  - head (PID: 5214, Parent: 4342, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5215, Parent: 4342)
  - tr (PID: 5215, Parent: 4342, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5216, Parent: 4342)
  - cut (PID: 5216, Parent: 4342, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5217, Parent: 4342)
  - cat (PID: 5217, Parent: 4342, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.nd5wZIclrj
- dash New Fork (PID: 5218, Parent: 4342)
  - head (PID: 5218, Parent: 4342, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5219, Parent: 4342)
  - tr (PID: 5219, Parent: 4342, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5220, Parent: 4342)
  - cut (PID: 5220, Parent: 4342, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5221, Parent: 4342)
  - rm (PID: 5221, Parent: 4342, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.nd5wZIclrj /tmp/tmp.zShyQQ7qTu /tmp/tmp.3SdD1ZBLJc
  - MPnFvIsvJp (PID: 5267, Parent: 5124, MD5: ae65271c943d3451b7f026d1fadccea6) Arguments: /tmp/MPnFvIsvJp
    - MPnFvIsvJp New Fork (PID: 5270, Parent: 5267)
    - MPnFvIsvJp New Fork (PID: 5271, Parent: 5267)
    - MPnFvIsvJp New Fork (PID: 5272, Parent: 5267)
      - MPnFvIsvJp New Fork (PID: 5276, Parent: 5272)
      - MPnFvIsvJp New Fork (PID: 5277, Parent: 5272)
      - MPnFvIsvJp New Fork (PID: 5281, Parent: 5272)
- systemd New Fork (PID: 5307, Parent: 1)
  - sshd (PID: 5307, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5308, Parent: 1)
  - sshd (PID: 5308, 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



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

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

System Summary:

Sample tries to kill many processes (SIGKILL)

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

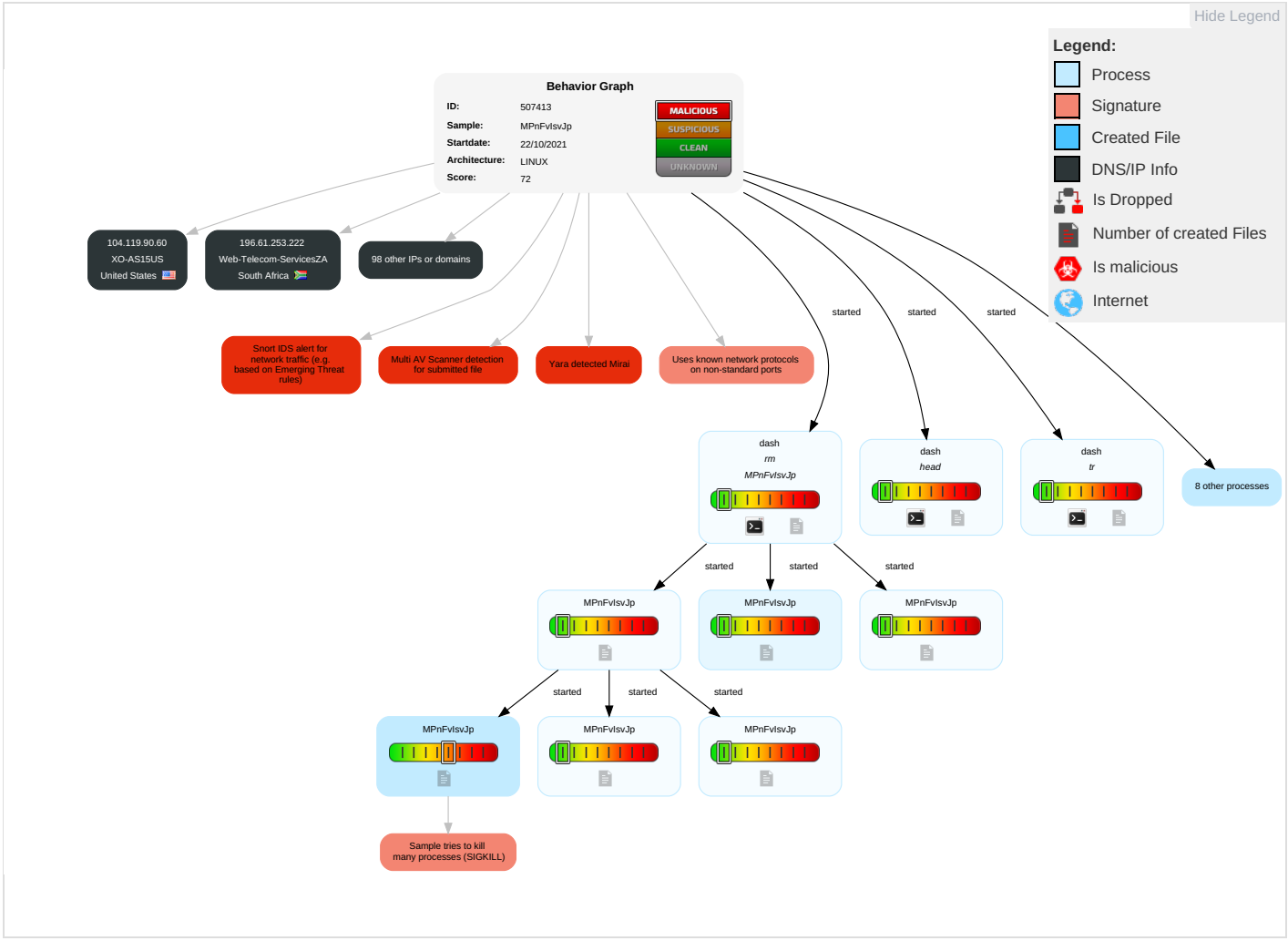
Mitre Att&ck Matrix

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	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

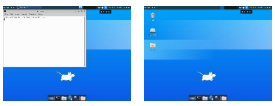
Behavior Graph

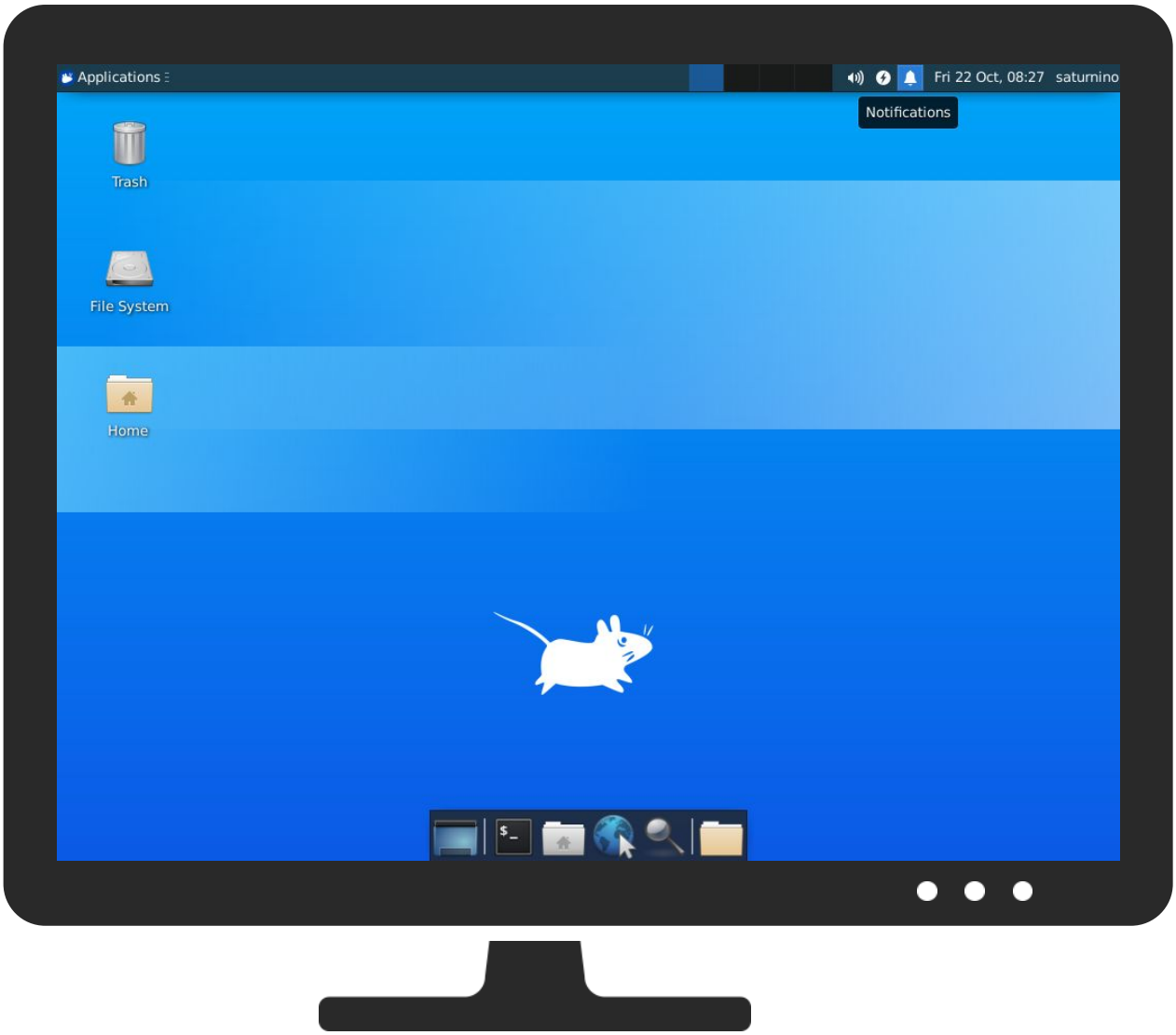


Screenshots

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
MPnFvIsvJp	50%	Virustotal		Browse
MPnFvIsvJp	58%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
53.112.165.99	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
162.249.159.72	unknown	United States		12177	ETS-TELEPHONE-COMPANYUS	false
38.189.106.217	unknown	United States		174	COGENT-174US	false
146.117.193.114	unknown	unknown		17477	MCT-SYDNEYMacquarieTelecomAU	false
197.45.56.18	unknown	Egypt		8452	TE-ASTE-ASEG	false
79.112.91.127	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
159.230.61.6	unknown	United States		4922	SHENTELUS	false
104.119.90.60	unknown	United States		2828	XO-AS15US	false
73.210.5.139	unknown	United States		7922	COMCAST-7922US	false
185.13.32.132	unknown	Russian Federation		46844	ST-BGPUS	false
95.195.139.140	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
109.142.99.132	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
84.141.10.139	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
2.144.217.201	unknown	Iran (ISLAMIC Republic Of)		44244	IRANCELL-ASIR	false
254.124.160.89	unknown	Reserved		unknown	unknown	false
157.72.111.104	unknown	Japan		131932	JEIS-NETJREastInformationSystemsCompanyJP	false
166.2.57.61	unknown	United States		4152	USDA-1US	false
196.98.136.157	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
105.214.52.124	unknown	South Africa		16637	MTNNS-ASZA	false
76.177.163.230	unknown	United States		10796	TWC-10796-MIDWESTUS	false
18.69.142.225	unknown	United States		3	MIT-GATEWAYSUS	false
47.253.16.98	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
222.209.131.174	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
118.144.105.142	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
73.26.71.206	unknown	United States		7922	COMCAST-7922US	false
216.44.168.130	unknown	United States		22691	ISPNET-1US	false
207.34.254.92	unknown	Canada		852	ASN852CA	false
109.236.158.185	unknown	Germany		62023	NYNEXDE	false
4.26.92.139	unknown	United States		3356	LEVEL3US	false
78.143.58.117	unknown	Germany		34309	LINK11Link11GmbHDE	false
158.255.70.161	unknown	France		39104	OXEVAFR	false
249.229.94.227	unknown	Reserved		unknown	unknown	false
118.28.147.193	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
121.127.142.57	unknown	Korea Republic of		9756	CHEONANVITSSEN-AS-KRTbroadChungbuBroadcastingCoKR	false
82.231.167.86	unknown	France		12322	PROXADFR	false
90.252.197.202	unknown	United Kingdom		5378	VodafoneGB	false
207.176.202.218	unknown	United States		3491	BTN-ASNUS	false
18.30.10.250	unknown	United States		3	MIT-GATEWAYSUS	false
223.8.151.73	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
192.20.120.58	unknown	United States		14153	EDGECAST-IRUS	false
200.167.253.216	unknown	Brazil		4230	CLAROSABR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
86.68.72.129	unknown	France		15557	LDCOMNETFR	false
213.146.201.32	unknown	Portugal		5626	ONIInternetServiceProviderPT	false
83.45.140.221	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
152.26.195.240	unknown	United States		81	NCRENUS	false
221.0.56.164	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
133.55.183.163	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
2.17.213.1	unknown	European Union		16625	AKAMAI-ASUS	false
248.29.159.14	unknown	Reserved		unknown	unknown	false
41.152.76.213	unknown	Egypt		36992	ETISALAT-MISREG	false
201.19.52.194	unknown	Brazil		7738	TelemarNorteLesteSABR	false
240.42.170.232	unknown	Reserved		unknown	unknown	false
139.156.150.80	unknown	Netherlands		2497	IIJInternetInitiativeJapanIncJP	false
118.64.199.38	unknown	China		4713	OCNNTTCommunicationsCorporationJP	false
121.145.80.39	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
98.59.61.81	unknown	United States		7922	COMCAST-7922US	false
196.61.253.222	unknown	South Africa		328029	Web-Telecom-ServicesZA	false
205.153.15.252	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
223.10.93.212	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
223.93.79.103	unknown	China		56041	CMNET-ZHEJIANG-APChinaMobilecommunicationscorporationC	false
175.12.84.190	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
183.25.200.23	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
93.137.66.222	unknown	Croatia (LOCAL Name: Hrvatska)		5391	T-HTCroatianTelecomIncHR	false
189.40.178.46	unknown	Brazil		26615	TIMSABR	false
180.140.66.56	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
203.176.141.81	unknown	Cambodia		38235	MEKONGNET-ADC-AS-APANGKORDATACOMMUNICATIONKH	false
45.146.92.203	unknown	Germany		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
19.197.93.3	unknown	United States		3	MIT-GATEWAYSUS	false
212.191.184.166	unknown	Poland		16283	LODMAN-AS2MetropolitanAreaNetworkLODMANPL	false
60.23.101.154	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
73.49.124.155	unknown	United States		7922	COMCAST-7922US	false
142.212.99.59	unknown	Canada		13576	SDNW-13576US	false
79.106.115.210	unknown	Albania		42313	ALBTELECOM-ASAL	false
32.251.50.182	unknown	United States		2686	ATGS-MMD-ASUS	false
253.83.161.80	unknown	Reserved		unknown	unknown	false
17.208.85.231	unknown	United States		714	APPLE-ENGINEERINGUS	false
174.105.227.80	unknown	United States		10796	TWC-10796-MIDWESTUS	false
250.12.81.189	unknown	Reserved		unknown	unknown	false
247.235.238.231	unknown	Reserved		unknown	unknown	false
78.254.217.14	unknown	France		12322	PROXADFR	false
216.239.120.101	unknown	United States		6623	CBSI-1US	false
243.115.4.52	unknown	Reserved		unknown	unknown	false
89.146.240.88	unknown	Germany		8495	INTERNET_AGFrankfurt-Munich-Stuttgart-Amsterdam-LondonDE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
221.170.37.56	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
73.191.86.218	unknown	United States		7922	COMCAST-7922US	false
94.11.229.252	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
1.201.22.138	unknown	Korea Republic of		38099	KAKAO-AS-KRKakaoCorpKR	false
31.156.41.151	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
211.43.179.175	unknown	Korea Republic of		7561	SAMSUNGELEC-AS-KRSamsungElectronicsCoKR	false
120.202.209.113	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
186.106.106.120	unknown	Chile		7418	TELEFONICACHILESACL	false
161.116.72.74	unknown	Spain		13041	CESCA-ACES	false
195.225.21.96	unknown	Norway		25148	BASEFARM-ASNOslo-NorwayNO	false
84.85.119.56	unknown	Netherlands		1136	KPNKPNNationalEU	false
184.169.138.101	unknown	United States		16509	AMAZON-02US	false
81.235.47.61	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
59.247.33.40	unknown	China		2516	KDDIKDDICORPORATIONJP	false
62.76.192.45	unknown	Russian Federation		200135	FLEXSOFT-ASRU	false
178.179.16.172	unknown	Russian Federation		25159	SONICDUO-ASRU	false
23.26.94.58	unknown	United States		11798	ACEDATACENTERS-AS-1US	false

Runtime Messages

Command:	/tmp/MPnFvIsvJp
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
95.195.139.140	ZIB8Eu6SUW	Get hash	malicious	Browse	
118.144.105.142	bqrHRKVNod	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAIMLER-ASITIGNGlobalNetworkDE	UYnpKcFZ2s	Get hash	malicious	Browse	• 53.55.173.225
	lQKil1R7D9	Get hash	malicious	Browse	• 53.191.190.232
	oH6qNmnFRP	Get hash	malicious	Browse	• 53.222.36.80
	Tf9ATzpdKR	Get hash	malicious	Browse	• 53.15.248.186
	b3astmode.arm	Get hash	malicious	Browse	• 53.94.68.130
	b3astmode.arm7	Get hash	malicious	Browse	• 53.229.195.214
	gjoqKYwnGG	Get hash	malicious	Browse	• 53.60.141.114
	hNsTaM2BAu	Get hash	malicious	Browse	• 53.209.76.80

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	iSdOB1UKQv	Get hash	malicious	Browse	• 53.6.170.177
	Kot3UfQMDm	Get hash	malicious	Browse	• 53.117.49.110
	kMn6L4fH2T	Get hash	malicious	Browse	• 53.231.244.12
	x86	Get hash	malicious	Browse	• 53.82.162.71
	arm7	Get hash	malicious	Browse	• 53.139.143.37
	arm7	Get hash	malicious	Browse	• 53.125.154.192
	GRPVtMlbK5	Get hash	malicious	Browse	• 53.251.116.245
	arm	Get hash	malicious	Browse	• 53.15.57.128
	S3LjnqUKlm	Get hash	malicious	Browse	• 53.190.194.162
	7vmT7Q2se0	Get hash	malicious	Browse	• 53.9.145.121
	ouMR5UDBpj	Get hash	malicious	Browse	• 53.178.98.137
	sora.arm	Get hash	malicious	Browse	• 53.240.30.150
COGENT-174US	T4xP1S9Fhz	Get hash	malicious	Browse	• 38.219.169.128
	cosvgegE1S	Get hash	malicious	Browse	• 204.240.223.118
	gKCq4VLpjL	Get hash	malicious	Browse	• 38.57.190.29
	mkRkjGXjDJ	Get hash	malicious	Browse	• 149.121.17.196
	zYMp3detVO	Get hash	malicious	Browse	• 204.7.106.123
	pLpqV3XZ76	Get hash	malicious	Browse	• 2.58.5.255
	ggtS1fKlqX	Get hash	malicious	Browse	• 198.242.181.102
	Tf9ATzpdKR	Get hash	malicious	Browse	• 38.83.11.68
	b3astmode.arm7	Get hash	malicious	Browse	• 38.10.205.211
	b3astmode.x86	Get hash	malicious	Browse	• 206.84.234.163
	sora.x86	Get hash	malicious	Browse	• 23.237.9.127
	sora.arm7	Get hash	malicious	Browse	• 206.7.224.111
	p6j5MzMpDW	Get hash	malicious	Browse	• 38.5.199.135
	tqQd9hibj0	Get hash	malicious	Browse	• 38.142.152.59
	gjoqKYwnGG	Get hash	malicious	Browse	• 38.174.109.106
	hNsTaM2BAu	Get hash	malicious	Browse	• 38.219.109.6
	Shipping_docs190dk0lwt837.exe	Get hash	malicious	Browse	• 154.23.172.72
	x86	Get hash	malicious	Browse	• 38.220.172.141
	arm	Get hash	malicious	Browse	• 38.250.166.201
	JuofJwjQMT	Get hash	malicious	Browse	• 38.218.17.35
ETS-TELEPHONE-COMPANYUS	Oro00CeYE0	Get hash	malicious	Browse	• 162.249.159.63
	1.sh	Get hash	malicious	Browse	• 162.217.40.164

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5308/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

/proc/5308/oom_score_adj	
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:DVdv:Jdv
MD5:	AF34BBE5A632AEFB5A6EDF64F8F26DA6
SHA1:	783857FEDC655D8822AED8FA0F1ABAA11B513FD9
SHA-256:	33B0D743AB15ABC049A46B5D5C68352F01F66D07AF7734E1F3AD459B4652C1C0
SHA-512:	0C13D42C8F6B55E2A344E7C90C80A62A3C70C377BF42586D4B527941D74C67ED735917F9E6905D354F18571FE00ECB2B8D0BF60CF8ABE0A6A7F23E79916EA40
Malicious:	false
Reputation:	low
Preview:	5308.

/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/woFmlT52URn
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, PowerPC or cisco 4500, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.25159913283433
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	MPnFvIsvJp
File size:	51604
MD5:	2af6167aa24d06f1795c507272d02916
SHA1:	24092366777f504a441a27f3555ca64e00719528
SHA256:	4c6ea0ba603fe0b1d8a97485afcf756d6e2a2630dfe18ee33353a17588924741
SHA512:	96c0db3f2db0c58cc109b4d3b99f087326091287f41041f420cf9039765a816a9a09115aa3e00413e64428cc6b2db177c03e7e2418b51adc64a71d65ec9694dc
SSDEEP:	768:opgPdUwOe1Po/7wni3RiAPSnPfDPKA2JjcRlgaizjrvVwipnpBX9QeA3:D1FOe1Po/kcExB9Mai6wvXeN3
File Content Preview:	.ELF.....4.....4. ...(.....t.....dt.Q.....!..|.....$H...H.....$8!. |...N.. .!..|.....?...../...@..\?.....+../...A..$8...})....N..

Static ELF Info

ELF header	
Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	PowerPC
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x100001f0
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	51124
Section Header Size:	40
Number of Section Headers:	12
Header String Table Index:	11

Sections

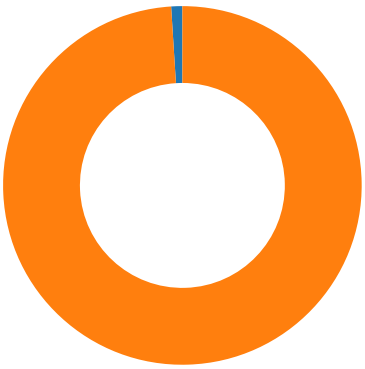
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10000094	0x94	0x24	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100000b8	0xb8	0xbef4	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x1000bfac	0xbfac	0x20	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1000bfcc	0xbfcc	0x624	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x1001c5f4	0xc5f4	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x1001c5fc	0xc5fc	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x1001c608	0xc608	0x140	0x0	0x3	WA	0	0	8
.sdata	PROGBITS	0x1001c748	0xc748	0x20	0x0	0x3	WA	0	0	4
.sbss	NOBITS	0x1001c768	0xc768	0x74	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x1001c7dc	0xc768	0x20c	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xc768	0x4b	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	0x10000000	0x10000000	0xc5f0	0xc5f0	4.0284	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xc5f4	0x1001c5f4	0x1001c5f4	0x174	0x3f4	0.3754	0x6	RW	0x10000		.ctors .dtors .data .sdata .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



Total Packets: 100

- 23 (Telnet)
- 1312 undefined

TCP Packets

System Behavior

Analysis Process: dash PID: 5213 Parent PID: 4342

General

Start time:	08:24:45
Start date:	22/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5213 Parent PID: 4342

General

Start time:	08:24:45
Start date:	22/10/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.nd5wZIclrj
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5214 Parent PID: 4342

General

Start time:	08:24:45
Start date:	22/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5214 Parent PID: 4342

General

Start time:	08:24:45
Start date:	22/10/2021
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5215 Parent PID: 4342

General

Start time:	08:24:45
Start date:	22/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5215 Parent PID: 4342

General

Start time:	08:24:45
Start date:	22/10/2021
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: 5216 Parent PID: 4342

General

Start time:	08:24:45
Start date:	22/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5216 Parent PID: 4342

General

Start time:	08:24:45
Start date:	22/10/2021
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: 5217 Parent PID: 4342

General

Start time:	08:24:46
Start date:	22/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5217 Parent PID: 4342

General

Start time:	08:24:46
Start date:	22/10/2021
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.nd5wZIclrj
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5218 Parent PID: 4342

General

Start time:	08:24:46
Start date:	22/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5218 Parent PID: 4342

General

Start time:	08:24:46
Start date:	22/10/2021
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5219 Parent PID: 4342

General

Start time:	08:24:46
Start date:	22/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5219 Parent PID: 4342

General

Start time:	08:24:46
Start date:	22/10/2021
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: 5220 Parent PID: 4342

General

Start time:	08:24:46
Start date:	22/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5220 Parent PID: 4342

General

Start time:	08:24:46
Start date:	22/10/2021
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: 5221 Parent PID: 4342

General

Start time:	08:24:46
Start date:	22/10/2021
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5221 Parent PID: 4342

General

Start time:	08:24:46
Start date:	22/10/2021
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.nd5wZIclrj /tmp/tmp.zShyQQ7qTu /tmp/tmp.3SdD1ZBLJc
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: MPnFvIsvJp PID: 5267 Parent PID: 5124

General

Start time:	08:24:56
Start date:	22/10/2021
Path:	/tmp/MPnFvIsvJp
Arguments:	/tmp/MPnFvIsvJp
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Analysis Process: MPnFvIsvJp PID: 5270 Parent PID: 5267

General

Start time:	08:24:57
Start date:	22/10/2021
Path:	/tmp/MPnFvIsvJp
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: MPnFvIsvJp PID: 5271 Parent PID: 5267

General

Start time:	08:24:57
Start date:	22/10/2021
Path:	/tmp/MPnFvIsvJp
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MPnFvIsvJp PID: 5272 Parent PID: 5267

General

Start time:	08:24:57
Start date:	22/10/2021
Path:	/tmp/MPnFvIsvJp
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MPnFvIsvJp PID: 5276 Parent PID: 5272

General

Start time:	08:24:57
Start date:	22/10/2021
Path:	/tmp/MPnFvIsvJp
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: MPnFvIsvJp PID: 5277 Parent PID: 5272

General

Start time:	08:24:57
Start date:	22/10/2021
Path:	/tmp/MPnFvIsvJp
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MPnFvIsvJp PID: 5281 Parent PID: 5272

General

Start time:	08:24:57
Start date:	22/10/2021
Path:	/tmp/MPnFvIsvJp
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: systemd PID: 5307 Parent PID: 1

General

Start time:	08:25:11
Start date:	22/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5307 Parent PID: 1

General

Start time:	08:25:11
Start date:	22/10/2021
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: 5308 Parent PID: 1

General

Start time:	08:25:11
Start date:	22/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5308 Parent PID: 1

General

Start time:	08:25:11
Start date:	22/10/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated