ID: 553499
Sample Name: UnHAnaAW.x86
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 03:04:38
Date: 15/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

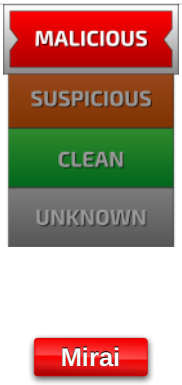
Linux Analysis Report UnHAnaAW.x86

Overview

General Information

Sample Name:	UnHAnaAW.x86
Analysis ID:	553499
MD5:	2fbd7450e710106.
SHA1:	981cf3e75f77074..
SHA256:	f28f21fb731b222…
Tags:	Mirai
Infos:	

Detection

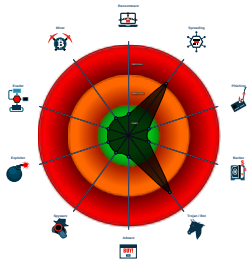


Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Uses known network protocols on no…
- Machine Learning detection for samp…
- Sample tries to kill multiple processe…
- Sample has stripped symbol table
- HTTP GET or POST without a user …
- Enumerates processes within the "p…
- Detected TCP or UDP traffic on non…
- Executes the "rm" command used to…

Classification



Analysis Advice

Some HTTP requests failed (404). It is likely the sample will exhibit less behavior

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553499
Start date:	15.01.2022
Start time:	03:04:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	UnHAnaAW.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:	mal76.spre.troj.linX86@0/1@0/0
Warnings:	Show All

Process Tree

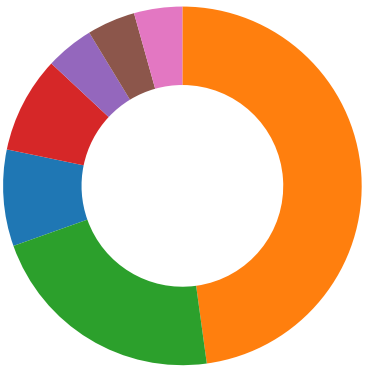
- **system is lnxubuntu20**
- dash New Fork (PID: 5184, Parent: 4331)
- cat (PID: 5184, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.zD6SFGNQb7
- dash New Fork (PID: 5185, Parent: 4331)
- head (PID: 5185, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5186, Parent: 4331)
- tr (PID: 5186, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5187, Parent: 4331)
- cut (PID: 5187, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5190, Parent: 4331)
- cat (PID: 5190, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.zD6SFGNQb7
- dash New Fork (PID: 5191, Parent: 4331)
- head (PID: 5191, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5192, Parent: 4331)
- tr (PID: 5192, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5193, Parent: 4331)
- cut (PID: 5193, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5194, Parent: 4331)
- rm (PID: 5194, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.zD6SFGNQb7 /tmp/tmp.MPIRMYR9iI /tmp/tmp.rMRfKpgfLJ
- UnHAnaAW.x86 (PID: 5222, Parent: 5106, MD5: 2fbd7450e710106e40f973c15359d94a) Arguments: /tmp/UnHAnaAW.x86
  - UnHAnaAW.x86 New Fork (PID: 5223, Parent: 5222)
  - UnHAnaAW.x86 New Fork (PID: 5224, Parent: 5222)
  - UnHAnaAW.x86 New Fork (PID: 5225, Parent: 5222)
    - UnHAnaAW.x86 New Fork (PID: 5226, Parent: 5225)
    - UnHAnaAW.x86 New Fork (PID: 5227, Parent: 5225)
    - UnHAnaAW.x86 New Fork (PID: 5228, Parent: 5225)
    - UnHAnaAW.x86 New Fork (PID: 5229, Parent: 5225)
    - UnHAnaAW.x86 New Fork (PID: 5230, Parent: 5225)
    - UnHAnaAW.x86 New Fork (PID: 5231, Parent: 5225)
- **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

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

System Summary:

Sample tries to kill multiple 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

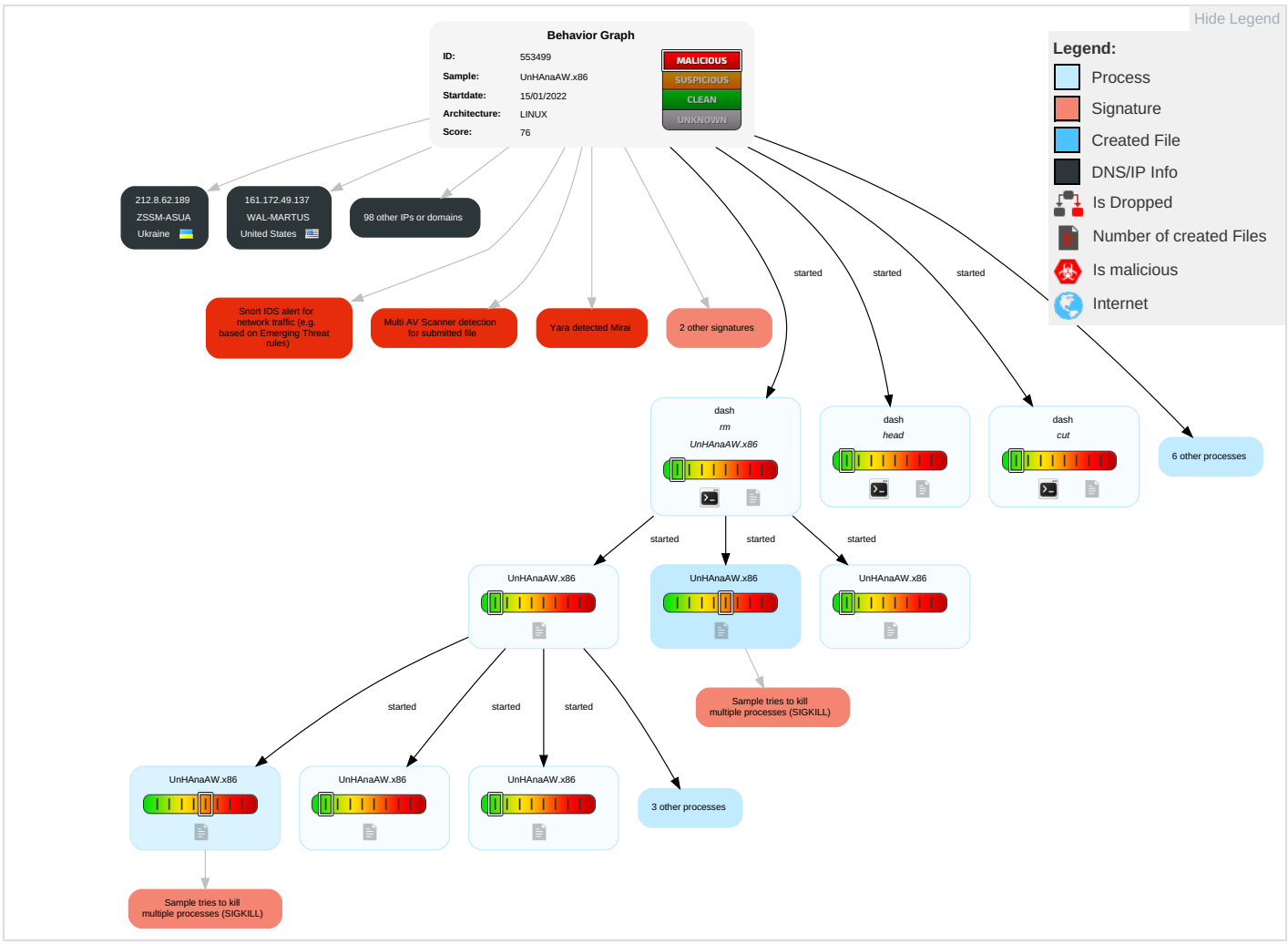
Mitre Att&ck Matrix

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	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 4	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 5	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Ingress Tool Transfer 4	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
UnHAnaAW.x86	56%	Virustotal		Browse
UnHAnaAW.x86	60%	ReversingLabs	Linux.Trojan.Mirai	
UnHAnaAW.x86	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://95.181.161.119/bins/x86	0%	Avira URL Cloud	safe	
http://95.181.161.119/zyxel.sh;	0%	Avira URL Cloud	safe	
http://192.168.0.14:80/cgi-bin/ViewLog.asp	0%	Virustotal		Browse
http://192.168.0.14:80/cgi-bin/ViewLog.asp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://192.168.0.14:80/cgi-bin/ViewLog.asp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
183.162.114.95	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
41.143.204.132	unknown	Morocco		36903	MT-MPLSMA	false
94.81.248.212	unknown	Italy		3269	ASN-IBSNAZIT	false
85.108.172.24	unknown	Turkey		9121	TTNETTR	false
32.108.18.108	unknown	United States		2688	ATGS-MMD-ASUS	false
159.210.217.171	unknown	Italy		131090	CAT-IDC-4BYTENET-AS-APCATTELECOMPublicCompanyLtdCATT	false
128.246.74.142	unknown	Germany		209781	BASF-LUDWIGSHAFENDE	false
85.246.119.54	unknown	Portugal		3243	MEO-RESIDENCIALPT	false
95.215.48.43	unknown	Ukraine		48882	OPTIMA-SHID-ASUA	false
94.64.142.135	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	false
205.9.96.150	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
161.172.49.137	unknown	United States		10695	WAL-MARTUS	false
31.199.232.10	unknown	Italy		3269	ASN-IBSNAZIT	false
31.100.145.19	unknown	United Kingdom		12576	EELtdGB	false
85.124.31.216	unknown	Austria		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
95.51.134.80	unknown	Poland		5617	TPNETPL	false
176.252.26.170	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
197.120.220.111	unknown	Egypt		36992	ETISALAT-MISREG	false
85.157.241.243	unknown	Finland		15527	ANVIASilmukkatie6VaasaFinlandFI	false
85.50.194.182	unknown	Spain		12479	UNI2-ASES	false
31.59.81.101	unknown	Iran (ISLAMIC Republic Of)		31549	RASANAIR	false
112.252.196.37	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
207.197.18.234	unknown	United States		3851	NSHE-NEVADANETUS	false
85.140.83.179	unknown	Russian Federation		39001	MTSRU	false
220.116.183.170	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
94.171.13.63	unknown	Netherlands		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
62.68.231.179	unknown	Egypt		24835	RAYA-ASEG	false
173.214.157.199	unknown	United States		16700	ROSENET-1US	false
95.217.66.167	unknown	Germany		24940	HETZNER-ASDE	false
112.80.112.4	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
85.119.64.1	unknown	Turkey		15924	BORUSANTELEKOM-ASTR	false
112.168.231.13	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
48.64.241.50	unknown	United States		2686	ATGS-MMD-ASUS	false
62.44.89.188	unknown	United Kingdom		5413	AS5413GB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.218.240.62	unknown	Denmark		197288	STOFANETDK	false
85.251.57.32	unknown	Spain		12357	COMUNITELSPAINES	false
171.226.193.180	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	false
41.206.191.242	unknown	South Africa		6453	AS6453US	false
31.220.220.243	unknown	United Kingdom		42689	GLIDEGB	false
205.162.203.241	unknown	United States		11404	AS-WAVE-1US	false
157.121.78.209	unknown	United States		2514	INFOSPHERENTTPCCommunicationsIncJP	false
85.112.35.33	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
94.8.166.137	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
197.252.76.136	unknown	Sudan		15706	SudatelSD	false
95.24.169.220	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
85.196.204.174	unknown	Estonia		61307	EE-AS-STVEE	false
94.67.223.113	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	false
64.157.90.134	unknown	United States		3064	AFFINITY-FTLUS	false
85.205.176.70	unknown	Germany		12663	VODAFONE-GROUPIT	false
85.206.15.28	unknown	Lithuania		8764	TELIA-LIETUVALT	false
95.28.117.17	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
94.224.166.163	unknown	Belgium		6848	TELENET-ASBE	false
31.14.164.20	unknown	Syrian Arab Republic		29256	INT-PDN-STE-ASSTEPDNInternalASSY	false
95.51.134.96	unknown	Poland		5617	TPNETPL	false
41.245.154.150	unknown	Nigeria		328050	Intercellular-Nigeria-ASNG	false
62.39.77.39	unknown	France		29322	STREAMWIDE-ASThecompanySTREAMWIDElocatedinParisFranc	false
62.40.187.78	unknown	Austria		8339	KABSI-ASAT	false
197.103.64.230	unknown	South Africa		3741	ISZA	false
156.115.143.157	unknown	Switzerland		59630	NN_INSURANCE_EURASIA_NV_ITH-ASNL	false
136.21.200.189	unknown	United States		60311	ONEFMCH	false
31.91.17.4	unknown	United Kingdom		12576	EELtdGB	false
31.161.195.254	unknown	Netherlands		1136	KPNKPNNationalEU	false
85.64.123.38	unknown	Israel		1680	NV-ASNCELLCOMltdIL	false
94.85.243.31	unknown	Italy		3269	ASN-IBSNAZIT	false
212.8.62.189	unknown	Ukraine		9202	ZSSM-ASUA	false
95.215.48.60	unknown	Ukraine		48882	OPTIMA-SHID-ASUA	false
95.94.139.71	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
94.94.61.76	unknown	Italy		3269	ASN-IBSNAZIT	false
146.55.160.218	unknown	United States		1483	DNIC-AS-01483US	false
31.46.162.107	unknown	Hungary		5483	MAGYAR-TELEKOM-MAIN-ASMagyarTelekomNyrtHU	false
90.27.204.130	unknown	France		3215	FranceTelecom-OrangeFR	false
95.111.20.237	unknown	Bulgaria		35141	MEGALANBG	false
62.153.147.111	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
31.143.175.13	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
104.204.57.212	unknown	United States		19397	ACN-DIGITAL-PHONEUS	false
157.37.178.135	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
31.66.126.243	unknown	United Kingdom		12576	EELtdGB	false
104.62.108.192	unknown	United States		7018	ATT-INTERNET4US	false
112.91.103.34	unknown	China		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
62.235.224.87	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
107.10.100.22	unknown	United States		10796	TWC-10796-MIDWESTUS	false
38.199.28.199	unknown	United States		174	COGENT-174US	false
167.171.172.39	unknown	United States		11101	PALMETTOHEALTHASUS	false
184.105.254.45	unknown	United States		23250	BPS-STAGINGUS	false
78.141.232.146	unknown	Netherlands		20473	AS-CHOOPAUS	false
94.175.48.233	unknown	United Kingdom		5089	NTLGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
197.173.180.16	unknown	South Africa		37168	CELL-CZA	false
216.28.163.240	unknown	United States		174	COGENT-174US	false
88.189.112.235	unknown	France		12322	PROXADFR	false
39.199.223.197	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
88.139.140.68	unknown	France		8228	CEGETEL-ASFR	false
31.61.72.78	unknown	Poland		5617	TPNETPL	false
62.202.185.171	unknown	Switzerland		12684	SES-LUX-ASLU	false
95.205.130.87	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
84.188.59.213	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
99.10.28.94	unknown	United States		7018	ATT-INTERNET4US	false
78.141.232.150	unknown	Netherlands		20473	AS-CHOOPAUS	false
94.42.225.74	unknown	Poland		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
31.137.99.217	unknown	Netherlands		15480	VFNL-ASVodafoneNLAutonomousSystemNL	false
157.184.0.159	unknown	United States		22192	SSHENETUS	false

Runtime Messages

Command:	/tmp/UnHAnaAW.x86
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infected By Cult
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/var/cache/motd-news	
Process:	/usr/bin/cut
File Type:	ASCII text

/var/cache/motd-news	
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):	6.372181051106509
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	UnHAnaAW.x86
File size:	74512
MD5:	2fbd7450e710106e40f973c15359d94a
SHA1:	981cf3e75f770741b2c8287fd080e0bdd31b17f2
SHA256:	f28f21fb731b222ba26788a21c5d8f9547c55e3a1703204fb634c7cdf12f75b4
SHA512:	5098684ea0b96cd2e663374b7eee3fdece6170c6eca0edecd7e11f17eb198cd97191c572a8e8aeb0876cc8a99ce45962ee82d55ab5baa5ea3cf78a5beecf76e8
SSDEEP:	1536:zyJOnlDu2LkjVvUPYDaGiYPnvMqOyJTtWtSM0dsjB6CifGqhKlK9m8C9nndN:zyJOnlDu2LkjVvUPcSUnk1SZdsjflHl9
File Content Preview:	.ELF.....d...4....!.....4. ...(.....`...`.....@.....Q.td.....U..S.....w....h....#...[]...$.....U.....=@....t..5....$.....$.....u.....t....h`.....

Static ELF Info

ELF header

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

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8048094	0x94	0x1c	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x80480b0	0xb0	0x10746	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x80587f6	0x107f6	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x8058820	0x10820	0x1340	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x805a000	0x12000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x805a008	0x12008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x805a020	0x12020	0x120	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x805a140	0x12140	0x6a0	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0x12140	0x3e	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8048000	0x8048000	0x11b60	0x11b60	3.8370	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0x12000	0x805a000	0x805a000	0x140	0x7e0	2.5037	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

- 192.168.0.14:80

System Behavior

Analysis Process: dash PID: 5184 Parent PID: 4331

General

Start time:	03:05:15
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5184 Parent PID: 4331

General

Start time:	03:05:15
Start date:	15/01/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.zD6SFGNQb7
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5185 Parent PID: 4331

General

Start time:	03:05:15
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5185 Parent PID: 4331

General

Start time:	03:05:15
Start date:	15/01/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5186 Parent PID: 4331

General

Start time:	03:05:15
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5186 Parent PID: 4331

General

Start time:	03:05:15
Start date:	15/01/2022
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: 5187 Parent PID: 4331

General

Start time:	03:05:15
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5187 Parent PID: 4331

General

Start time:	03:05:15
Start date:	15/01/2022
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: 5190 Parent PID: 4331

General

Start time:	03:05:16
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5190 Parent PID: 4331

General

Start time:	03:05:16
Start date:	15/01/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.zD6SFGNQb7
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5191 Parent PID: 4331

General

Start time:	03:05:16
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5191 Parent PID: 4331

General

Start time:	03:05:16
Start date:	15/01/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5192 Parent PID: 4331

General

Start time:	03:05:16
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5192 Parent PID: 4331

General

Start time:	03:05:16
Start date:	15/01/2022
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: 5193 Parent PID: 4331

General

Start time:	03:05:16
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5193 Parent PID: 4331

General

Start time:	03:05:16
Start date:	15/01/2022
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: 5194 Parent PID: 4331

General

Start time:	03:05:16
Start date:	15/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5194 Parent PID: 4331

General

Start time:	03:05:16
Start date:	15/01/2022
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.zD6SFGNQb7 /tmp/tmp.MPIRMYR9iI /tmp/tmp.rMRfKpgfLJ
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: UnHAnaAW.x86 PID: 5222 Parent PID: 5106

General

Start time:	03:05:20
Start date:	15/01/2022
Path:	/tmp/UnHAnaAW.x86
Arguments:	/tmp/UnHAnaAW.x86
File size:	74512 bytes
MD5 hash:	2fbd7450e710106e40f973c15359d94a

Analysis Process: UnHAnaAW.x86 PID: 5223 Parent PID: 5222

General

Start time:	03:05:20
Start date:	15/01/2022
Path:	/tmp/UnHAnaAW.x86
Arguments:	n/a
File size:	74512 bytes
MD5 hash:	2fbd7450e710106e40f973c15359d94a

File Activities

File Read

Directory Enumerated

Analysis Process: UnHAnaAW.x86 PID: 5224 Parent PID: 5222

General

Start time:	03:05:20
Start date:	15/01/2022
Path:	/tmp/UnHAnaAW.x86
Arguments:	n/a
File size:	74512 bytes
MD5 hash:	2fbd7450e710106e40f973c15359d94a

Analysis Process: UnHAnaAW.x86 PID: 5225 Parent PID: 5222

General

Start time:	03:05:20
Start date:	15/01/2022
Path:	/tmp/UnHAnaAW.x86
Arguments:	n/a
File size:	74512 bytes
MD5 hash:	2fbd7450e710106e40f973c15359d94a

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

General

Start time:	03:05:20

Start date:	15/01/2022
Path:	/tmp/UnHAnaAW.x86
Arguments:	n/a
File size:	74512 bytes
MD5 hash:	2fbd7450e710106e40f973c15359d94a

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

General

Start time:	03:05:20
Start date:	15/01/2022
Path:	/tmp/UnHAnaAW.x86
Arguments:	n/a
File size:	74512 bytes
MD5 hash:	2fbd7450e710106e40f973c15359d94a

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

General

Start time:	03:05:20
Start date:	15/01/2022
Path:	/tmp/UnHAnaAW.x86
Arguments:	n/a
File size:	74512 bytes
MD5 hash:	2fbd7450e710106e40f973c15359d94a

Analysis Process: UnHAnaAW.x86 PID: 5229 Parent PID: 5225

General

Start time:	03:05:20
Start date:	15/01/2022
Path:	/tmp/UnHAnaAW.x86
Arguments:	n/a
File size:	74512 bytes
MD5 hash:	2fbd7450e710106e40f973c15359d94a

File Activities

File Read

Directory Enumerated

Analysis Process: UnHAnaAW.x86 PID: 5230 Parent PID: 5225

General

Start time:	03:05:20
Start date:	15/01/2022
Path:	/tmp/UnHAnaAW.x86
Arguments:	n/a
File size:	74512 bytes
MD5 hash:	2fbd7450e710106e40f973c15359d94a

Analysis Process: UnHAnaAW.x86 PID: 5231 Parent PID: 5225

General

Start time:	03:05:20
Start date:	15/01/2022
Path:	/tmp/UnHAnaAW.x86
Arguments:	n/a
File size:	74512 bytes
MD5 hash:	2fbd7450e710106e40f973c15359d94a