ID: 512845
Sample Name: w66OTKGVFv
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 13:24:13
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

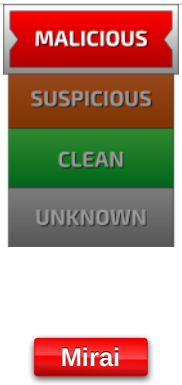
Linux Analysis Report w66OTKGVFv

Overview

General Information

Sample Name:	w66OTKGVFv
Analysis ID:	512845
MD5:	392f09a2ade70a6.
SHA1:	fe2543dea574c38.
SHA256:	f79a9bc14990a8a.
Tags:	32 elf mips mirai
Infos:	

Detection

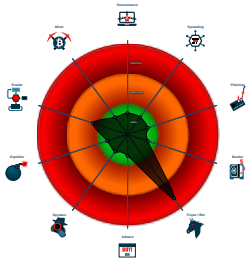


Score:	80
Range:	0 - 100
Whitelisted:	false

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...
- Tries to connect to HTTP servers, b...
- Detected TCP or UDP traffic on non...

Classification



Analysis Advice

- **Some HTTP requests failed (404). It is likely the sample will exhibit less behavior**
- **Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures**
- **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:	512845
Start date:	01.11.2021
Start time:	13:24:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	w66OTKGVFv
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:	mal80.troj.lin@0/0@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
  - w66OTKGVFv (PID: 5247, Parent: 5121, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/w66OTKGVFv
    - w66OTKGVFv New Fork (PID: 5249, Parent: 5247)
      - w66OTKGVFv New Fork (PID: 5268, Parent: 5249)
      - w66OTKGVFv New Fork (PID: 5269, Parent: 5249)
        - w66OTKGVFv New Fork (PID: 5272, Parent: 5269)
          - w66OTKGVFv New Fork (PID: 5292, Parent: 5272)
          - w66OTKGVFv New Fork (PID: 5293, Parent: 5272)
          - w66OTKGVFv New Fork (PID: 5296, Parent: 5272)
          - w66OTKGVFv New Fork (PID: 5297, Parent: 5272)
        - w66OTKGVFv New Fork (PID: 5276, Parent: 5269)
        - w66OTKGVFv New Fork (PID: 5280, Parent: 5269)
        - w66OTKGVFv New Fork (PID: 5285, Parent: 5269)
        - w66OTKGVFv New Fork (PID: 5287, Parent: 5269)
    - w66OTKGVFv New Fork (PID: 5250, Parent: 5247)
    - w66OTKGVFv New Fork (PID: 5252, Parent: 5247)
      - w66OTKGVFv New Fork (PID: 5255, Parent: 5252)
        - w66OTKGVFv New Fork (PID: 5273, Parent: 5255)
        - w66OTKGVFv New Fork (PID: 5274, Parent: 5255)
        - w66OTKGVFv New Fork (PID: 5279, Parent: 5255)
        - w66OTKGVFv New Fork (PID: 5282, Parent: 5255)
      - w66OTKGVFv New Fork (PID: 5256, Parent: 5252)
      - w66OTKGVFv New Fork (PID: 5259, Parent: 5252)
      - w66OTKGVFv New Fork (PID: 5260, Parent: 5252)
      - w66OTKGVFv New Fork (PID: 5263, Parent: 5252)
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
w66OTKGVFv	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

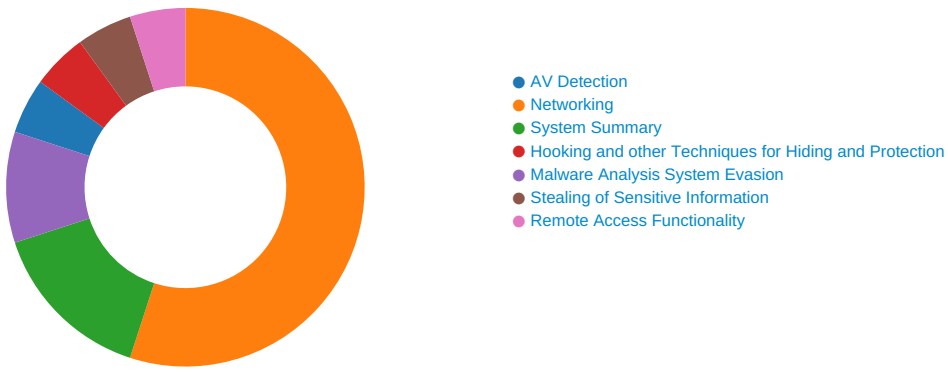
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5268.1.0000000009e3a5dd.000000007387e1a1.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5256.1.0000000009e3a5dd.000000007387e1a1.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5250.1.0000000009e3a5dd.000000007387e1a1.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5292.1.0000000009e3a5dd.000000007387e1a1.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5276.1.0000000009e3a5dd.000000007387e1a1.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

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

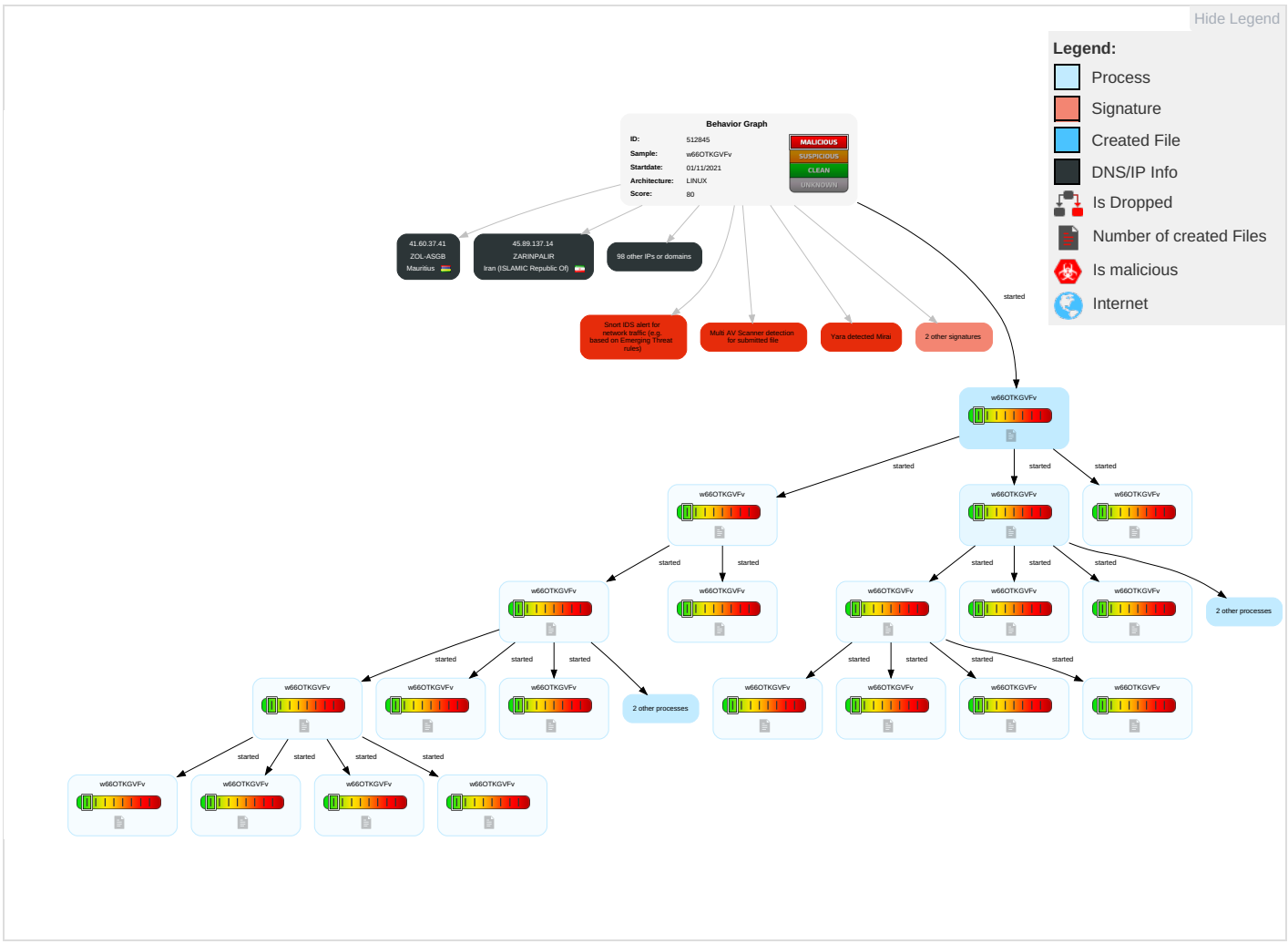
Mitre Att&ck Matrix

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	Direct Volume Access	OS Credential Dumping	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 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 2	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 3	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 2	Manipulate Device Communication		Manipula App Sto Ranking or Ratin

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
w66OTKGVFv	55%	Virustotal		Browse
w66OTKGVFv	51%	ReversingLabs	Linux.Trojan.Mirai	

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://127.0.0.1:52869/wanipcn.xml	0%	Virustotal		Browse
http://127.0.0.1:52869/wanipcn.xml	0%	Avira URL Cloud	safe	
http://194.87.42.3/Anti_Bins/Antisocial.mips	11%	Virustotal		Browse
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	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://127.0.0.1:52869/wanipcn.xml	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.19.109.161	unknown	United Kingdom		17804	LAODC-AS-APLaoDataCenterLA	false
42.25.79.214	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
156.246.150.168	unknown	Seychelles		328608	Africa-on-Cloud-ASZA	false
91.54.122.232	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
41.239.218.43	unknown	Egypt		8452	TE-ASTE-ASEG	false
185.41.19.222	unknown	Norway		199900	ASN-BEDSYSNO	false
148.176.105.99	unknown	United Kingdom		6400	CompaniaDominicanadeTelefonosSADO	false
91.52.65.169	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
166.141.255.180	unknown	United States		22394	CELLCOUS	false
185.50.154.156	unknown	United Kingdom		50203	UK-REYNOLDS-ASNGB	false
73.148.101.94	unknown	United States		7922	COMCAST-7922US	false
185.69.33.22	unknown	Netherlands		196826	PL-NETTELEKOM-ASNPL	false
123.192.31.28	unknown	Taiwan; Republic of China (ROC)		38841	KBRO-AS-TWkbroCOLtdTW	false
211.241.253.133	unknown	Korea Republic of		38661	HCLC-AS-KRpurplestonesKR	false
45.89.137.14	unknown	Iran (ISLAMIC Republic Of)		208675	ZARINPALIR	false
197.123.112.81	unknown	Egypt		36992	ETISALAT-MISREG	false
91.125.161.178	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	false
185.220.10.233	unknown	Spain		205390	TECTIQOM-ASDE	false
45.108.120.244	unknown	Egypt		37069	MOBINILEG	false
197.211.66.43	unknown	South Africa		29918	IMPOL-ASNZA	false
79.99.182.249	unknown	Turkey		44261	HDISIGORTA-ASNTR	false
185.138.105.212	unknown	France		39405	FULLSAVE-ASFR	false
209.19.202.117	unknown	United States		2828	XO-AS15US	false
45.246.175.189	unknown	Egypt		24863	LINKdotNET-ASEG	false
45.82.161.108	unknown	Lithuania		208862	SIRINFO-ASIT	false
45.50.203.142	unknown	United States		20001	TWC-20001-PACWESTUS	false
45.219.30.100	unknown	Morocco		36925	ASMediMA	false
144.248.130.52	unknown	Belgium		2611	BELNETBE	false
2.208.22.166	unknown	Germany		6805	TDDE-ASN1DE	false
45.94.158.147	unknown	Ukraine		56851	VPS-UA-ASUA	false
41.196.116.155	unknown	Egypt		24863	LINKdotNET-ASEG	false
91.19.165.60	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
91.49.236.104	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
13.137.183.110	unknown	United States		7018	ATT-INTERNET4US	false
147.16.177.236	unknown	United States		10796	TWC-10796-MIDWESTUS	false
91.112.149.135	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
45.145.30.159	unknown	Turkey		197328	INETLTDTR	false
48.64.241.83	unknown	United States		2686	ATGS-MMD-ASUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
88.199.11.246	unknown	Poland		20960	TKTELEKOM-ASPL	false
100.17.104.106	unknown	United States		701	UUNETUS	false
91.155.155.213	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
45.150.101.166	unknown	Liechtenstein		47987	LOVESERVERSGB	false
186.227.57.230	unknown	Brazil		53162	VOIPGLOBESERVICOSDECOMMULTIMIDIAVIAINTERNETBR	false
45.221.254.36	unknown	Benin		328092	SUD-TELCOM-ASBJ	false
45.130.62.153	unknown	Israel		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
91.52.65.198	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
91.48.246.208	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
174.177.52.210	unknown	United States		7922	COMCAST-7922US	false
185.57.166.109	unknown	Iran (ISLAMIC Republic Of)		49103	IR-ASRETELECOM-ASIR	false
115.132.43.20	unknown	Malaysia		4788	TMNET-AS-APTMNetInternetServiceProviderMY	false
45.50.203.115	unknown	United States		20001	TWC-20001-PACWESTUS	false
200.231.97.12	unknown	Brazil		4230	CLAROSABR	false
141.236.172.178	unknown	United States		5972	DNIC-ASBLK-05800-06055US	false
156.146.251.153	unknown	United States		1448	UNITED-BROADBANDUS	false
98.196.137.24	unknown	United States		7922	COMCAST-7922US	false
45.11.15.104	unknown	Netherlands		395800	GBTCLOUDUS	false
185.146.72.16	unknown	Russian Federation		41639	INCOMSV-ASRU	false
52.32.127.114	unknown	United States		16509	AMAZON-02US	false
97.40.37.7	unknown	United States		22394	CELLCOUS	false
91.72.218.214	unknown	United Arab Emirates		15802	DU-AS1AE	false
91.196.209.250	unknown	Spain		205295	ACCESSCABLEES	false
45.63.53.223	unknown	United States		20473	AS-CHOOPAUS	false
197.130.137.65	unknown	Morocco		6713	IAM-ASMA	false
69.230.36.218	unknown	United States		7018	ATT-INTERNET4US	false
91.120.127.62	unknown	Hungary		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
185.236.155.1	unknown	Bulgaria		41922	MIS70BG	false
156.8.202.250	unknown	South Africa		3741	ISZA	false
91.100.152.115	unknown	Denmark		15516	DK-DANSKKABELTVDK	false
91.244.81.34	unknown	Russian Federation		197831	DISKUS-ASRU	false
221.160.166.188	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
91.74.182.158	unknown	United Arab Emirates		15802	DU-AS1AE	false
45.199.228.216	unknown	Seychelles		8100	ASN-QUADRANET-GLOBALUS	false
45.145.30.177	unknown	Turkey		197328	INETLTDTR	false
197.173.155.85	unknown	South Africa		37168	CELL-CZA	false
45.30.40.118	unknown	United States		7018	ATT-INTERNET4US	false
91.112.149.159	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
160.131.108.103	unknown	United States		8103	STATE-OF-FLAUS	false
197.211.66.60	unknown	South Africa		29918	IMPOL-ASNZA	false
45.115.168.110	unknown	India		59162	UPCSPL-AS-INUPCOMMUNICATIONSERVICESPVTLTDIN	false
91.210.131.86	unknown	Poland		44279	DCA-AS1PL	false
185.3.157.7	unknown	Czech Republic		210306	ADVNETCZ	false
185.42.252.15	unknown	Germany		202208	TEUTELDE	false
41.60.37.41	unknown	Mauritius		30969	ZOL-ASGB	false
98.169.101.209	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
176.168.181.246	unknown	France		5410	BOUYGTEL-ISPFR	false
72.194.18.218	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
189.72.70.138	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
45.20.156.206	unknown	United States		7018	ATT-INTERNET4US	false
70.2.128.100	unknown	United States		10507	SPCSUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.120.127.30	unknown	Hungary		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
45.62.111.92	unknown	Canada		25820	IT7NETCA	false
75.45.81.104	unknown	United States		7018	ATT-INTERNET4US	false
45.104.148.77	unknown	Egypt		37069	MOBINILEG	false
76.110.59.222	unknown	United States		7922	COMCAST-7922US	false
128.153.194.130	unknown	United States		92	CLARKSON-ASUS	false
91.74.182.148	unknown	United Arab Emirates		15802	DU-AS1AE	false
52.111.240.94	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
197.169.124.241	unknown	South Africa		37168	CELL-CZA	false
41.187.12.183	unknown	Egypt		20928	NOOR-ASEG	false
156.115.143.100	unknown	Switzerland		59630	NN_INSURANCE_EURASIA_NV_ITH-ASNL	false

Runtime Messages

Command:	/tmp/w66OTKGVFv
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
197.123.112.81	swOGb2sZYt	Get hash	malicious	Browse	
45.50.203.142	swOGb2sZYt	Get hash	malicious	Browse	
45.219.30.100	Iu8Qn68jzj	Get hash	malicious	Browse	
	sora.arm	Get hash	malicious	Browse	
156.246.150.168	U4r9W64doy	Get hash	malicious	Browse	
41.239.218.43	FD6qpyHOPI	Get hash	malicious	Browse	
45.89.137.14	KXM253rCpW	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
Africa-on-Cloud-ASZA	ydZLm6GD56	Get hash	malicious	Browse	• 45.203.157.220
	OhUy3woBmb	Get hash	malicious	Browse	• 45.206.90.63
	9o6Z1wEokT	Get hash	malicious	Browse	• 156.240.70.1
	00hZyjOhZA	Get hash	malicious	Browse	• 156.228.228.21
	mP1pg0ryFA	Get hash	malicious	Browse	• 156.228.63.83
	1bL17EUgTk	Get hash	malicious	Browse	• 45.197.161.70
	Ceji2MdFHD	Get hash	malicious	Browse	• 156.240.10.186
	Change Vessel Schedule Notice - KTX3-JVA261S.exe	Get hash	malicious	Browse	• 156.240.157.205
	CtTYTpaAKA.exe	Get hash	malicious	Browse	• 156.240.150.22
	LsSAq5zX9w.exe	Get hash	malicious	Browse	• 156.240.146.122
	Minutes of Meeting 23.10.2021.exe	Get hash	malicious	Browse	• 156.248.135.40
	b3astmode.arm	Get hash	malicious	Browse	• 45.206.20.134
	JYWllP5wHP	Get hash	malicious	Browse	• 156.246.150.186

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tqQd9hibj0	Get hash	malicious	Browse	• 156.228.38.66
	x86	Get hash	malicious	Browse	• 156.228.141.222
	arm	Get hash	malicious	Browse	• 156.228.38.63
	x86	Get hash	malicious	Browse	• 156.246.150.165
	sora.arm	Get hash	malicious	Browse	• 45.196.129.59
	8jfOcvTqQA	Get hash	malicious	Browse	• 154.200.75.0
	x86.light	Get hash	malicious	Browse	• 156.228.63.78
LAODC-AS-APLaoDataCenterLA	ydZLm6GD56	Get hash	malicious	Browse	• 185.19.109.122
	BitmCvTrdO	Get hash	malicious	Browse	• 185.19.109.135
	Hilix.arm7	Get hash	malicious	Browse	• 185.19.109.149
	93T511Z3h8	Get hash	malicious	Browse	• 185.19.109.112
	i686	Get hash	malicious	Browse	• 185.19.109.133
	Antisocial.arm	Get hash	malicious	Browse	• 185.19.109.153
	BcOfN2cD3e	Get hash	malicious	Browse	• 185.19.109.165
	RIy8RQn22Y	Get hash	malicious	Browse	• 185.19.109.168
	G7eLqVZPgX	Get hash	malicious	Browse	• 185.19.109.121
	UguI8hPCWh	Get hash	malicious	Browse	• 185.19.109.140
	QIJ16axero	Get hash	malicious	Browse	• 185.19.109.119
	4kWyL2w4wQ	Get hash	malicious	Browse	• 185.19.109.118
	http://bayimg.com	Get hash	malicious	Browse	• 185.109.87.28
SKTELECOM-NET-ASSKTelecomKR	yxD7DmfG2j	Get hash	malicious	Browse	• 42.18.100.211
	arm7	Get hash	malicious	Browse	• 27.168.251.60
	S13B4aCa4E	Get hash	malicious	Browse	• 42.43.212.29
	Tsunami.arm7	Get hash	malicious	Browse	• 42.17.201.113
	KXAJjgoH22	Get hash	malicious	Browse	• 223.38.129.85
	PpZvxl4DJg	Get hash	malicious	Browse	• 223.58.206.43
	arm7	Get hash	malicious	Browse	• 223.36.30.149
	JUZVpUSH0W	Get hash	malicious	Browse	• 180.132.24.17
	2pPPNW1XSo	Get hash	malicious	Browse	• 27.170.232.254
	S1WMHUXAQU	Get hash	malicious	Browse	• 27.165.123.157
	5mLAGfiGBf	Get hash	malicious	Browse	• 27.161.81.36
	st2AAeCXsR	Get hash	malicious	Browse	• 223.48.101.224
	yZ7D7o1Z7p	Get hash	malicious	Browse	• 223.39.144.208
	eNrYzJWFvB	Get hash	malicious	Browse	• 27.171.83.144
	x86_64	Get hash	malicious	Browse	• 223.39.36.73
	vLqyyo55oA	Get hash	malicious	Browse	• 223.63.186.8
	KfvEoN0wIw	Get hash	malicious	Browse	• 123.229.178.121
	Xb1sM3W7BK	Get hash	malicious	Browse	• 27.177.194.0
	txwaNf62fv	Get hash	malicious	Browse	• 223.52.33.62
	nLfUJu0kEA	Get hash	malicious	Browse	• 223.39.73.91

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

General

File type:	ELF 32-bit LSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.557165221244349
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	w66OTKGVFv
File size:	85612
MD5:	392f09a2ade70a6281ed7919a9cf1ef0
SHA1:	fe2543dea574c383d83e6f5c14a952cba5f7fba8
SHA256:	f79a9bc14990a8a97de98c21adf4ad65c83aacc12718cb3a26a28f0fbdf54fd8
SHA512:	a13b6dd8486f2edecc92e3db25ccb9d71dbc7c1b3e2866858b0ec2e35703a76cfd4b229968ba49f0e09716a5936db2eb9fc40384a8a7343bfd602f0d9ccf935e
SSDEEP:	1536:Z5nFmqc0mLCAGekcQ3M58fzGlvGTZx71gWG4H:Z5n82mL0CiqGT3
File Content Preview:	.ELF.....`.@.4...<L.....4. ...(.....@...@..=.. .=.....@...@E..@E..... /.....Q.td.....<...'!.....'.....<...'!... .....9'.. .....`#9

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	85052
Section Header Size:	40
Number of Section Headers:	14
Header String Table Index:	13

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x122b0	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x4123d0	0x123d0	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x412430	0x12430	0x19c0	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x454000	0x14000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x454008	0x14008	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x454014	0x14014	0x404	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x454420	0x14420	0x3a0	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x4547c0	0x147c0	0x418	0x4	0x10000003	WA	0	0	16
.sbss	NOBITS	0x454bd8	0x14bd8	0x24	0x0	0x10000003	WA	0	0	4
.bss	NOBITS	0x454c00	0x14bd8	0x2320	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x828	0x14bd8	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x14bd8	0x64	0x0	0x0		0	0	1

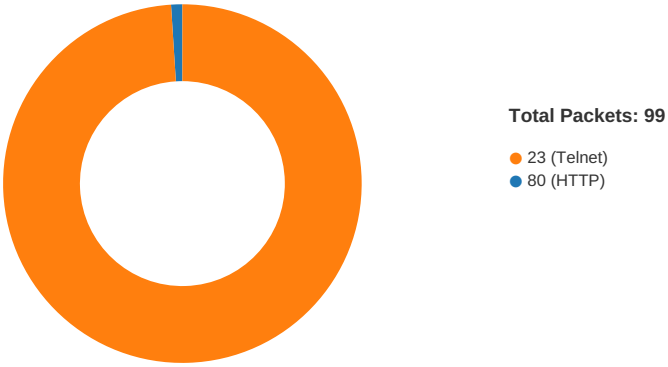
Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x13df0	0x13df0	3.5967	0x5	R E	0x10000		.init .text .fini .rodata

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x14000	0x454000	0x454000	0xbd8	0x2f20	2.9281	0x6	RW	0x10000		.ctors .dtors .data.rel.ro .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

HTTP Request Dependency Graph

- 127.0.0.1:52869

System Behavior

Analysis Process: w66OTKGVFv PID: 5247 Parent PID: 5121

General

Start time:	13:24:58
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	/tmp/w66OTKGVFv
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: w66OTKGVFv PID: 5249 Parent PID: 5247

General

Start time:	13:24:59
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5268 Parent PID: 5249

General

Start time:	13:25:04
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5269 Parent PID: 5249

General

Start time:	13:25:04
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5272 Parent PID: 5269

General

Start time:	13:25:04
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5292 Parent PID: 5272

General

Start time:	13:25:09
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5293 Parent PID: 5272

General

Start time:	13:25:09
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5296 Parent PID: 5272

General

Start time:	13:25:09
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5297 Parent PID: 5272

General

Start time:	13:25:09
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5276 Parent PID: 5269

General

Start time:	13:25:04
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5280 Parent PID: 5269

General

Start time:	13:25:04
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5285 Parent PID: 5269

General

Start time:	13:25:04
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5287 Parent PID: 5269

General

Start time:	13:25:04
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5250 Parent PID: 5247

General

Start time:	13:24:59
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5252 Parent PID: 5247

General

Start time:	13:24:59
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5255 Parent PID: 5252

General

Start time:	13:24:59
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5273 Parent PID: 5255

General

Start time:	13:25:04
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5274 Parent PID: 5255

General

Start time:	13:25:04
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5279 Parent PID: 5255

General

Start time:	13:25:04
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5282 Parent PID: 5255

General

Start time:	13:25:04
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5256 Parent PID: 5252

General

Start time:	13:24:59
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes

MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5259 Parent PID: 5252

General

Start time:	13:24:59
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5260 Parent PID: 5252

General

Start time:	13:24:59
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: w66OTKGVFv PID: 5263 Parent PID: 5252

General

Start time:	13:24:59
Start date:	01/11/2021
Path:	/tmp/w66OTKGVFv
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9