ID: 512678
Sample Name: OhUy3woBmb
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 10:19:29
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

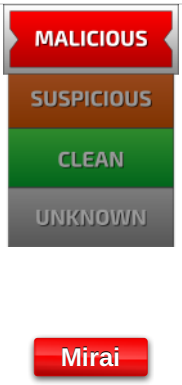
Linux Analysis Report OhUy3woBmb

Overview

General Information

Sample Name:	OhUy3woBmb
Analysis ID:	512678
MD5:	213da876cd489b..
SHA1:	2c155fc36dfcb27…
SHA256:	0a331e7b35913f9.
Tags:	32 elf mips mirai
Infos:	

Detection

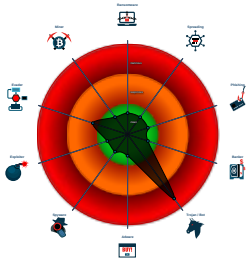


Score:	80
Range:	0 - 100
Whitelisted:	false

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

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:	512678
Start date:	01.11.2021
Start time:	10:19:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OhUy3woBmb
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**
- OhUy3woBmb (PID: 5254, Parent: 5137, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/OhUy3woBmb
  - OhUy3woBmb New Fork (PID: 5256, Parent: 5254)
    - OhUy3woBmb New Fork (PID: 5275, Parent: 5256)
    - OhUy3woBmb New Fork (PID: 5277, Parent: 5256)
      - OhUy3woBmb New Fork (PID: 5279, Parent: 5277)
        - OhUy3woBmb New Fork (PID: 5301, Parent: 5279)
        - OhUy3woBmb New Fork (PID: 5303, Parent: 5279)
        - OhUy3woBmb New Fork (PID: 5305, Parent: 5279)
        - OhUy3woBmb New Fork (PID: 5306, Parent: 5279)
      - OhUy3woBmb New Fork (PID: 5281, Parent: 5277)
      - OhUy3woBmb New Fork (PID: 5284, Parent: 5277)
      - OhUy3woBmb New Fork (PID: 5288, Parent: 5277)
      - OhUy3woBmb New Fork (PID: 5294, Parent: 5277)
  - OhUy3woBmb New Fork (PID: 5257, Parent: 5254)
  - OhUy3woBmb New Fork (PID: 5259, Parent: 5254)
    - OhUy3woBmb New Fork (PID: 5262, Parent: 5259)
      - OhUy3woBmb New Fork (PID: 5282, Parent: 5262)
      - OhUy3woBmb New Fork (PID: 5286, Parent: 5262)
      - OhUy3woBmb New Fork (PID: 5292, Parent: 5262)
      - OhUy3woBmb New Fork (PID: 5295, Parent: 5262)
    - OhUy3woBmb New Fork (PID: 5263, Parent: 5259)
    - OhUy3woBmb New Fork (PID: 5265, Parent: 5259)
    - OhUy3woBmb New Fork (PID: 5267, Parent: 5259)
    - OhUy3woBmb New Fork (PID: 5270, Parent: 5259)
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
OhUy3woBmb	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

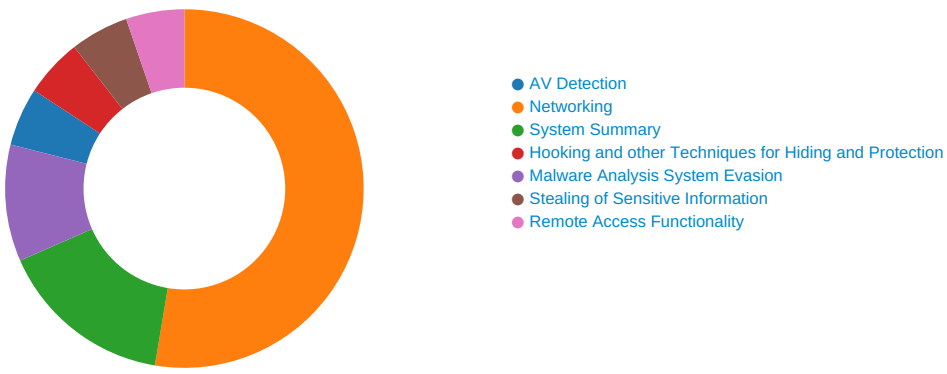
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5263.1.00000000f315aa15.000000006119b545.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5275.1.00000000f315aa15.000000006119b545.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5256.1.00000000f315aa15.000000006119b545.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5282.1.00000000f315aa15.000000006119b545.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5254.1.00000000f315aa15.000000006119b545.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

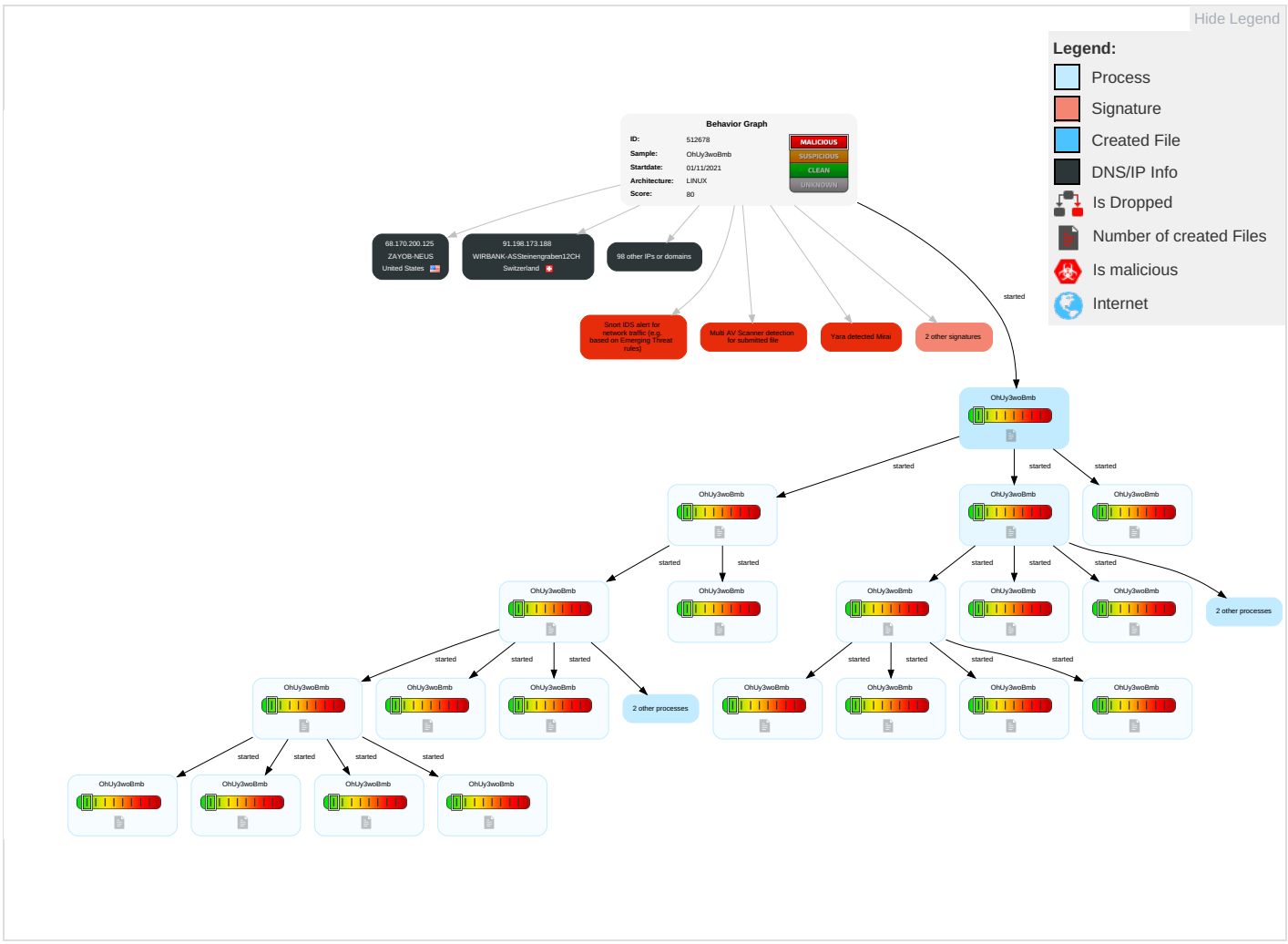
Mitre Att&ck Matrix

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 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
OhUy3woBmb	54%	Virustotal		Browse
OhUy3woBmb	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%	Avira URL Cloud	safe	
http://127.0.0.1:52869/wanipcn.xml	0%	Avira URL Cloud	safe	
http://194.87.42.3/Anti_Bins/Antisocial.mips	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
90.214.188.166	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
45.127.206.123	unknown	Indonesia		55699	STARNET-AS-IDPTCemerlangMultimediaID	false
45.50.54.76	unknown	United States		20001	TWC-20001-PACWESTUS	false
185.138.105.229	unknown	France		39405	FULLSAVE-ASFR	false
91.19.189.236	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
156.249.107.12	unknown	Seychelles		139086	ONL-HKOCEANNETWORKLIMITEDHK	false
50.64.199.136	unknown	Canada		6327	SHAWCA	false
91.72.131.142	unknown	United Arab Emirates		15802	DU-AS1AE	false
91.90.138.83	unknown	Israel		25046	CHECKPOINTIL	false
185.1.23.16	unknown	Russian Federation		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
91.54.23.23	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
109.254.119.164	unknown	Ukraine		20590	DEC-ASUA	false
35.201.141.234	unknown	United States		15169	GOOGLEUS	false
45.11.15.127	unknown	Netherlands		395800	GBTCLOUDUS	false
185.110.49.228	unknown	Poland		47544	IQPL-ASPL	false
91.11.116.155	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
41.77.181.127	unknown	Algeria		36974	AFNET-ASCI	false
45.221.254.20	unknown	Benin		328092	SUD-TELCOM-ASBJ	false
197.130.137.42	unknown	Morocco		6713	IAM-ASMA	false
156.89.9.174	unknown	United States		2386	INS-ASUS	false
45.104.148.40	unknown	Egypt		37069	MOBINILEG	false
45.150.101.139	unknown	Liechtenstein		47987	LOVESERVERSGB	false
45.21.146.156	unknown	United States		7018	ATT-INTERNET4US	false
45.242.108.19	unknown	Egypt		24863	LINKdotNET-ASEG	false
88.238.150.252	unknown	Turkey		9121	TTNETTR	false
91.49.236.103	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
73.114.184.204	unknown	United States		7922	COMCAST-7922US	false
185.75.12.215	unknown	Spain		201942	SOLTIAES	false
91.112.149.138	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
41.39.124.196	unknown	Egypt		8452	TE-ASTE-ASEG	false
185.70.34.136	unknown	United Kingdom		201353	NSUKGB	false
91.11.116.162	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
172.185.62.64	unknown	United States		7018	ATT-INTERNET4US	false
185.78.207.53	unknown	United Kingdom		8426	CLARANET-ASClaraNETLTDGB	false
185.138.105.205	unknown	France		39405	FULLSAVE-ASFR	false
41.89.178.176	unknown	Kenya		36914	KENET-ASKE	false
189.96.48.176	unknown	Brazil		27699	TELEFONICABRASILSABR	false
185.185.4.35	unknown	France		34659	KEYYOFR	false
27.213.223.43	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.202.220.134	unknown	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	false
41.35.82.90	unknown	Egypt		8452	TE-ASTE-ASEG	false
195.240.221.175	unknown	Netherlands		1136	KPNKPNNationalEU	false
45.199.228.221	unknown	Seychelles		8100	ASN-QUADRANET-GLOBALUS	false
91.186.75.29	unknown	Norway		56828	NORWEGIANHEALTHNETWORKNO	false
146.3.248.101	unknown	Luxembourg		200139	STATENS-VEGVESENNO	false
197.149.52.196	unknown	Madagascar		37054	Telecom-MalagasyMG	false
91.199.162.56	unknown	Germany		42652	DELUNETDE	false
185.38.220.173	unknown	Poland		56523	AMELEKTRONIKPL	false
45.50.203.116	unknown	United States		20001	TWC-20001-PACWESTUS	false
91.72.131.124	unknown	United Arab Emirates		15802	DU-AS1AE	false
91.198.173.188	unknown	Switzerland		43477	WIRBANK-ASSteinengraben12CH	false
185.146.72.16	unknown	Russian Federation		41639	INCOMSV-ASRU	false
91.198.173.189	unknown	Switzerland		43477	WIRBANK-ASSteinengraben12CH	false
115.240.160.182	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
45.250.127.6	unknown	China		23860	ALLIANCE-GATEWAY-AS-APAllianceBroadbandServicesPvtLtd	false
185.158.165.180	unknown	Netherlands		48635	ASTRALUSNL	false
45.63.53.220	unknown	United States		20473	AS-CHOOPAUS	false
185.106.143.10	unknown	Serbia		7979	SERVERS-COMUS	false
185.34.243.0	unknown	Russian Federation		44943	RAMNET-ASInternetServiceProviderRamNetRU	false
45.130.62.162	unknown	Israel		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
45.201.177.14	unknown	Seychelles		131178	KINGCORP-KHOpenNetISPCambodiaKH	false
197.67.29.136	unknown	South Africa		16637	MTNNS-ASZA	false
185.11.6.126	unknown	Russian Federation		15493	RUSCOMP-ASRussiancompanyLLCInternetServiceProviderT	false
91.140.204.13	unknown	Kuwait		3225	GULFNET-KUWAITKW	false
91.72.131.130	unknown	United Arab Emirates		15802	DU-AS1AE	false
91.54.23.53	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
91.167.86.188	unknown	France		12322	PROXADFR	false
17.70.140.211	unknown	United States		714	APPLE-ENGINEERINGUS	false
91.183.234.13	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
185.75.12.234	unknown	Spain		201942	SOLTIAES	false
45.199.228.216	unknown	Seychelles		8100	ASN-QUADRANET-GLOBALUS	false
68.170.200.125	unknown	United States		32327	ZAYOB-NEUS	false
205.199.62.96	unknown	United States		133847	ICT-AS-APAnppleTechEnterpriseMY	false
68.64.25.115	unknown	United States		16815	GOTO-PRIMARY-ASUS	false
73.108.225.187	unknown	United States		7922	COMCAST-7922US	false
98.198.78.68	unknown	United States		7922	COMCAST-7922US	false
91.11.116.127	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
185.185.4.51	unknown	France		34659	KEYYOFR	false
91.111.200.218	unknown	United Kingdom		12576	EELtdGB	false
185.203.160.98	unknown	Iran (ISLAMIC Republic Of)		205837	SADADPSP-ASSadadProcessingModernServicesCompanyPJS	false
197.222.170.109	unknown	Egypt		37069	MOBINILEG	false
185.86.223.117	unknown	Iceland		200868	KAPALVAEDINGIS	false
185.225.116.251	unknown	Palestinian Territory Occupied		205205	PS-BADAWIPS	false
185.37.230.226	unknown	Spain		60458	ASN-XTUDIONETES	false
151.27.221.102	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
130.89.21.100	unknown	Netherlands		1133	UTWENTE-ASUniversityTwenteNL	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.206.90.63	unknown	Seychelles		328608	Africa-on-Cloud-ASZA	false
17.78.52.251	unknown	United States		714	APPLE-ENGINEERINGUS	false
41.171.231.136	unknown	South Africa		36937	Neotel-ASZA	false
45.103.171.141	unknown	Egypt		37069	MOBINILEG	false
185.50.154.116	unknown	United Kingdom		50203	UK-REYNOLDS-ASNGB	false
185.126.207.148	unknown	Italy		208920	ROCKETWAY-ASIT	false
185.113.220.220	unknown	Turkey		42926	RADORETR	false
83.103.229.192	unknown	Romania		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
85.48.206.139	unknown	Spain		12479	UNI2-ASES	false
185.162.213.115	unknown	Germany		207210	SW-COTTBUS-ASDE	false
45.103.171.147	unknown	Egypt		37069	MOBINILEG	false
91.18.128.126	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
185.10.95.110	unknown	Germany		12676	NCORE-ASHochstadenstr5DE	false
197.82.246.65	unknown	South Africa		10474	OPTINETZA	false

Runtime Messages

Command:	/tmp/OhUy3woBmb
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
91.90.138.83	Antisocial.x86	Get hash	malicious	Browse	
45.221.254.20	17Rom1F3MY	Get hash	malicious	Browse	
91.19.189.236	93T511Z3h8	Get hash	malicious	Browse	
156.249.107.12	UnHAnaAW.arm7	Get hash	malicious	Browse	
41.39.124.196	2UFDZwqcvk	Get hash	malicious	Browse	
45.11.15.127	GEso3CniSk	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
STARNET-AS-IDPTCemerlangMultimediaID	yJOZ3EeESV	Get hash	malicious	Browse	• 45.127.206.109
	apep.arm7	Get hash	malicious	Browse	• 45.127.206.162
	x86_64	Get hash	malicious	Browse	• 103.57.39.81
	dTmYFku6X8	Get hash	malicious	Browse	• 45.127.206.139
	tI0W00k1vt	Get hash	malicious	Browse	• 45.127.206.129
	Hilix.x86	Get hash	malicious	Browse	• 45.127.206.142
	Hilix.arm7	Get hash	malicious	Browse	• 45.127.206.119
	Hilix.x86	Get hash	malicious	Browse	• 45.127.206.167
	xbx6bxavxK	Get hash	malicious	Browse	• 45.127.206.127
	arm	Get hash	malicious	Browse	• 103.57.39.17
	frosty.x86	Get hash	malicious	Browse	• 45.127.206.119
	QUqBgpQj3B	Get hash	malicious	Browse	• 45.127.206.136

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	eOtLRCQr22	Get hash	malicious	Browse	• 45.127.206.120
	7OAzOUL9cd	Get hash	malicious	Browse	• 103.57.39.22
BSKYB-BROADBAND-ASGB	S8G5z3pdHw	Get hash	malicious	Browse	• 2.221.89.134
	9o6Z1wEokT	Get hash	malicious	Browse	• 94.7.176.226
	pTF1ilCUEm	Get hash	malicious	Browse	• 78.86.242.253
	x86	Get hash	malicious	Browse	• 90.197.108.7
	arm7	Get hash	malicious	Browse	• 188.221.61.80
	z0x3n.arm7	Get hash	malicious	Browse	• 94.195.52.233
	z0x3n.x86	Get hash	malicious	Browse	• 151.226.142.75
	yJOZ3EeESV	Get hash	malicious	Browse	• 94.14.249.1
	apep.x86	Get hash	malicious	Browse	• 94.11.75.112
	QtNnZoNz75	Get hash	malicious	Browse	• 94.3.251.65
	S13B4aCa4E	Get hash	malicious	Browse	• 94.15.123.77
	gbk4XWulUo	Get hash	malicious	Browse	• 94.8.166.122
	QZ2CN6CUyv	Get hash	malicious	Browse	• 90.199.199.227
	8MPbeDAwwZ	Get hash	malicious	Browse	• 94.194.73.233
	Ceji2MdFHD	Get hash	malicious	Browse	• 94.0.122.104
	Xs0PMn85CN	Get hash	malicious	Browse	• 2.127.1.8
	INsMwWSMeh	Get hash	malicious	Browse	• 94.8.166.146
	Tsunami.arm	Get hash	malicious	Browse	• 94.194.150.89
	ivImhRZqGa	Get hash	malicious	Browse	• 176.251.137.208
	zouBbQwUTb	Get hash	malicious	Browse	• 94.194.198.37
TWC-20001-PACWESTUS	V2WzER53Tt	Get hash	malicious	Browse	• 107.185.34.158
	a5nulABeSk	Get hash	malicious	Browse	• 172.89.127.43
	032k4JmR0U	Get hash	malicious	Browse	• 98.149.242.241
	arm7	Get hash	malicious	Browse	• 172.248.96.0
	z0x3n.arm	Get hash	malicious	Browse	• 45.50.73.120
	yJOZ3EeESV	Get hash	malicious	Browse	• 45.48.194.37
	lYmYPlzghQ	Get hash	malicious	Browse	• 107.185.81.50
	T0uznhDXKw	Get hash	malicious	Browse	• 45.48.169.43
	S13B4aCa4E	Get hash	malicious	Browse	• 172.116.65.65
	gbk4XWulUo	Get hash	malicious	Browse	• 98.153.107.47
	HgTC70XRum	Get hash	malicious	Browse	• 98.155.194.67
	Xs0PMn85CN	Get hash	malicious	Browse	• 172.116.139.119
	INsMwWSMeh	Get hash	malicious	Browse	• 172.250.116.248
	Tsunami.arm7	Get hash	malicious	Browse	• 172.119.50.251
	Tsunami.arm	Get hash	malicious	Browse	• 172.114.72.150
	a37hI2I7yO	Get hash	malicious	Browse	• 98.153.107.17
	RVG73cR3DP	Get hash	malicious	Browse	• 75.83.35.22
	32UX3eB2m0	Get hash	malicious	Browse	• 45.48.169.73
	jJ6GK5qbZt	Get hash	malicious	Browse	• 66.74.99.64
	JUZVpUSH0W	Get hash	malicious	Browse	• 209.134.80.45

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.4488416358353815
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	OhUy3woBmb
File size:	85612
MD5:	213da876cd489b0813581d6dab558c28
SHA1:	2c155fc36dfcb27c5cf6b5b78e209e11d2683747
SHA256:	0a331e7b35913f9672c2608954ee521f1b58b2a6415303c a31a09c844590e5ae
SHA512:	f21701dcea20253905b0e6dffe1efe5fd14d17d4c706b768 104191fedcca9bc446cd6882d60c536e6fd11daa3806add 47b497ec7639f4cf879bafdd2ae4ba511
SSDEEP:	1536:Qat8EmQaBYT1MUFUVXwz8Mv1C2G9/NMusj60 NJAUhQ4HB:Qat8Em1cMU+Xwz8MvDKausj6077FB
File Content Preview:	.ELF.....@.`...4..L<.....4. ...(.....@...@....6. ..6.....@..E@..E@...../ .....dt.Q..... .<...'.....!'.....<...'.....!... ....'9... ....'.....!.....'9.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big 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	0x11b50	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x411c70	0x11c70	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x411cd0	0x11cd0	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	0x13690	0x13690	3.5737	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	2.9248	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

TCP Packets

HTTP Request Dependency Graph

- 127.0.0.1:52869

System Behavior

Analysis Process: OhUy3woBmb PID: 5254 Parent PID: 5137

General

Start time:	10:20:21
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	/tmp/OhUy3woBmb
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: OhUy3woBmb PID: 5256 Parent PID: 5254

General

Start time:	10:20:21
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5275 Parent PID: 5256

General

Start time:	10:20:26
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a

File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5277 Parent PID: 5256

General

Start time:	10:20:26
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5279 Parent PID: 5277

General

Start time:	10:20:26
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5301 Parent PID: 5279

General

Start time:	10:20:31
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5303 Parent PID: 5279

General

Start time:	10:20:31
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5305 Parent PID: 5279

General

Start time:	10:20:31
Start date:	01/11/2021

Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5306 Parent PID: 5279

General

Start time:	10:20:31
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5281 Parent PID: 5277

General

Start time:	10:20:26
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5284 Parent PID: 5277

General

Start time:	10:20:26
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5288 Parent PID: 5277

General

Start time:	10:20:26
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5294 Parent PID: 5277

General

Start time:	10:20:26
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5257 Parent PID: 5254

General

Start time:	10:20:21
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5259 Parent PID: 5254

General

Start time:	10:20:21
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5262 Parent PID: 5259

General

Start time:	10:20:21
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5282 Parent PID: 5262

General

Start time:	10:20:26
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5286 Parent PID: 5262

General

Start time:	10:20:26
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5292 Parent PID: 5262

General

Start time:	10:20:26
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5295 Parent PID: 5262

General

Start time:	10:20:26
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5263 Parent PID: 5259

General

Start time:	10:20:21
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5265 Parent PID: 5259

General

Start time:	10:20:21
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5267 Parent PID: 5259

General

Start time:	10:20:21
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: OhUy3woBmb PID: 5270 Parent PID: 5259

General

Start time:	10:20:21
Start date:	01/11/2021
Path:	/tmp/OhUy3woBmb
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c