ID: 513296
Sample Name: KHSQ48GkGn
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 01:50:54
Date: 02/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

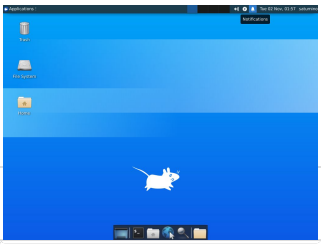
Linux Analysis Report KHSQ48GkGn

Overview

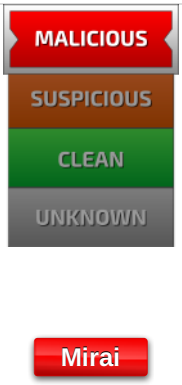
General Information

Sample Name:	KHSQ48GkGn
Analysis ID:	513296
MD5:	905f7222e4cc699..
SHA1:	84210b6c2c580b..
SHA256:	cd091f9f91f7483…
Tags:	32 elf mips mirai
Infos:	

Most interesting Screenshot:



Detection

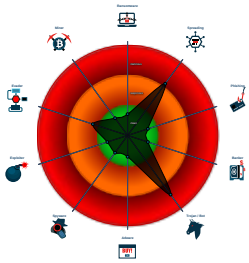


Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e.…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Uses known network protocols on no…
- Sample tries to kill many processes…
- 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…
- Enumerates processes within the "p…
- 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:	513296
Start date:	02.11.2021
Start time:	01:50:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KHSQ48GkGn
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.lin@0/2@0/0
Warnings:	Show All

Process Tree

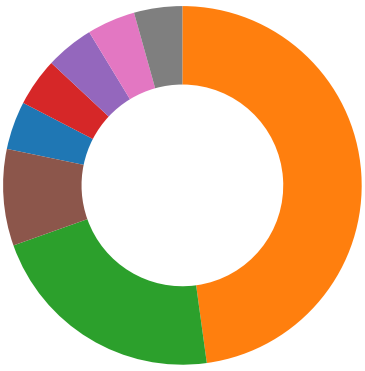
- **system is lnxubuntu20**
- KHSQ48GkGn (PID: 5238, Parent: 5121, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/KHSQ48GkGn
  - KHSQ48GkGn New Fork (PID: 5240, Parent: 5238)
  - KHSQ48GkGn New Fork (PID: 5241, Parent: 5238)
  - KHSQ48GkGn New Fork (PID: 5242, Parent: 5238)
    - KHSQ48GkGn New Fork (PID: 5246, Parent: 5242)
    - KHSQ48GkGn New Fork (PID: 5247, Parent: 5242)
    - KHSQ48GkGn New Fork (PID: 5248, Parent: 5242)
    - KHSQ48GkGn New Fork (PID: 5249, Parent: 5242)
    - KHSQ48GkGn New Fork (PID: 5255, Parent: 5242)
- systemd New Fork (PID: 5281, Parent: 1)
  - sshd (PID: 5281, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5282, Parent: 1)
  - sshd (PID: 5282, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- **cleanup**

Yara Overview

PCAP (Network Traffic)

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

Jbx Signature Overview



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)

System Summary:

Sample tries to kill many processes (SIGKILL)

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

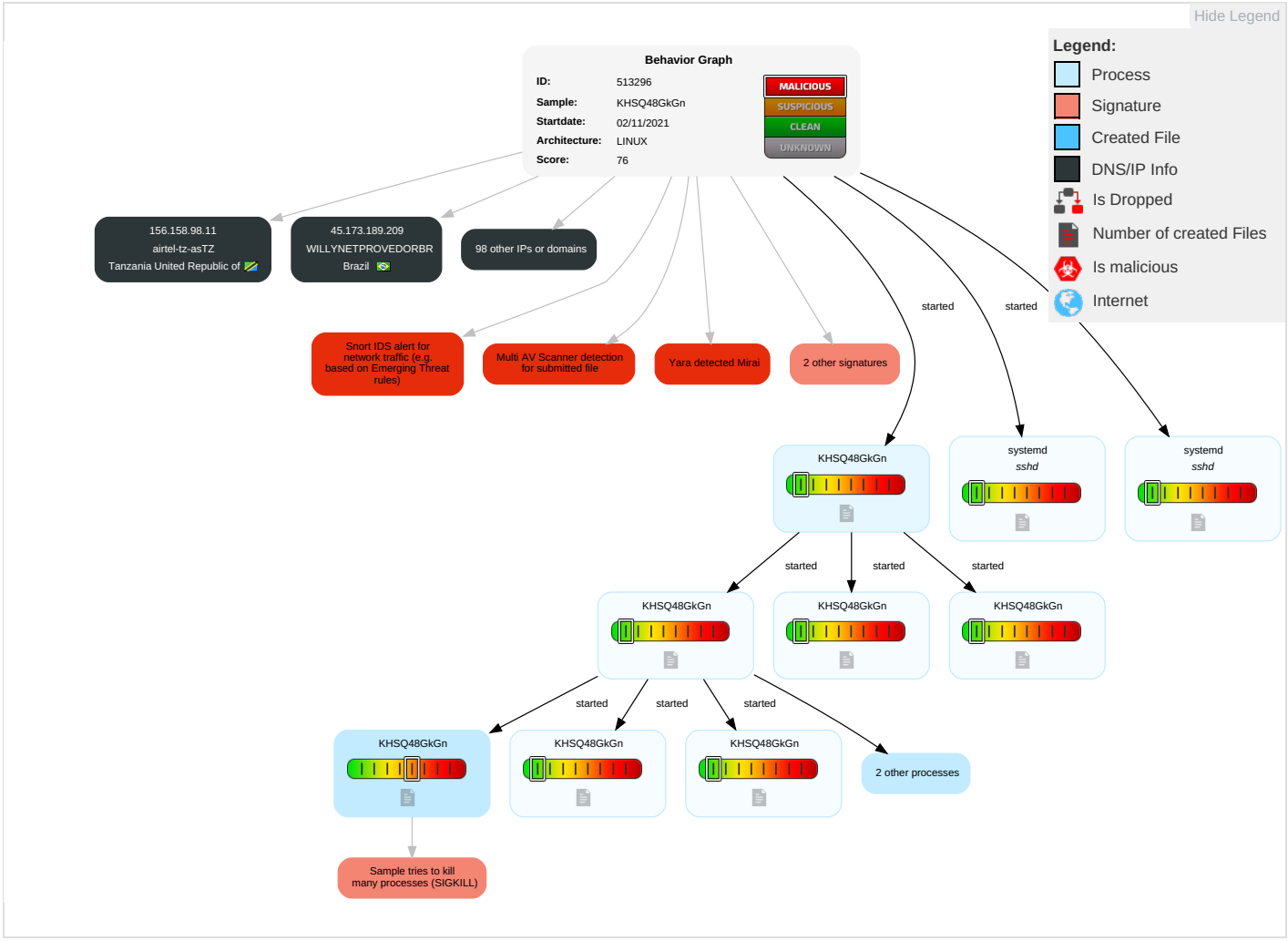
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockou
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	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

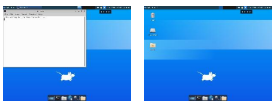
Behavior Graph

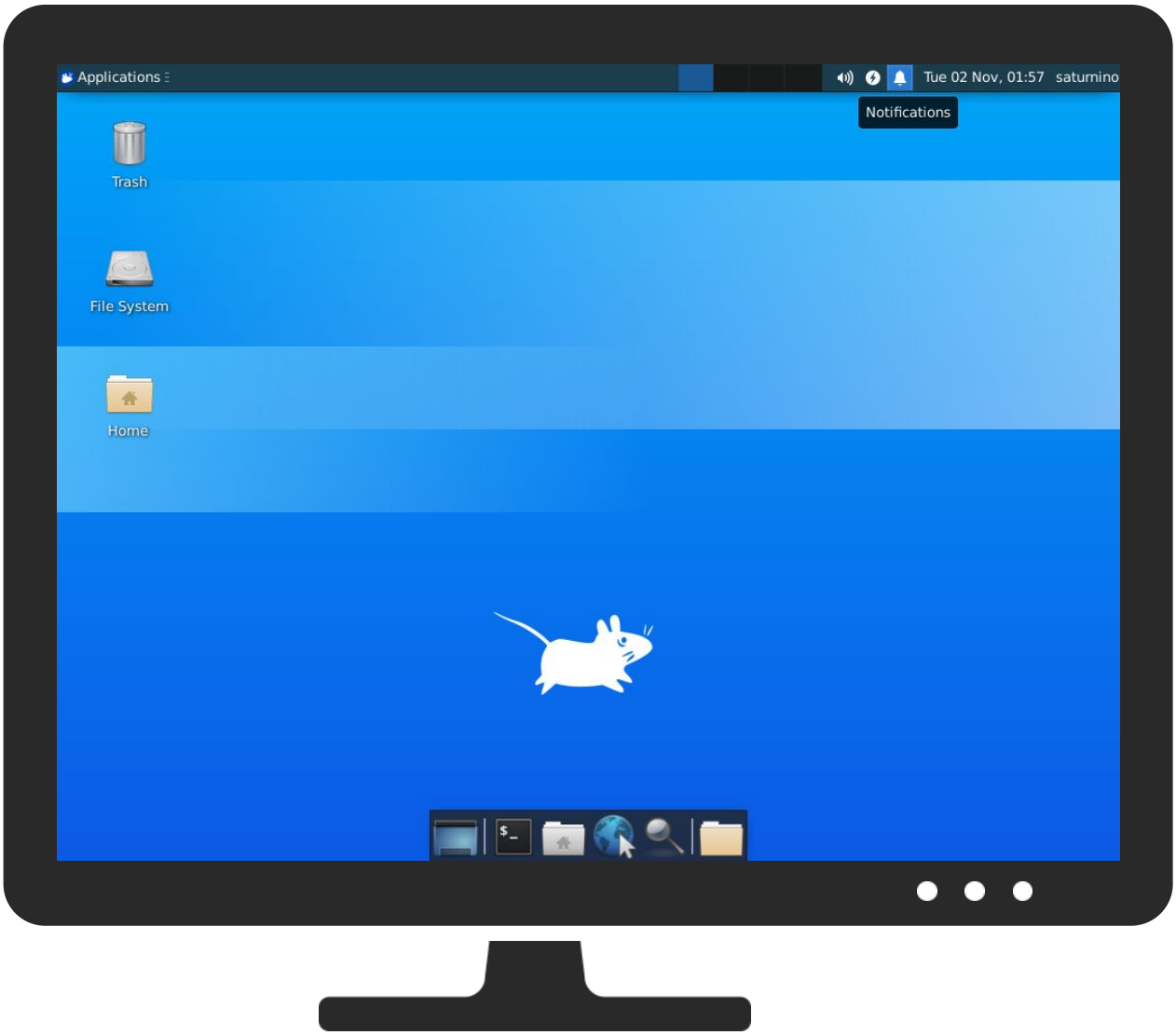


Screenshots

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
KHSQ48GkGn	62%	Virustotal		Browse
KHSQ48GkGn	64%	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://37.0.9.202/bins/Hilix.mips	9%	Virustotal		Browse
http://37.0.9.202/bins/Hilix.mips	100%	Avira URL Cloud	malware	
http://127.0.0.1:52869/wanipcn.xml	0%	Virustotal		Browse
http://127.0.0.1:52869/wanipcn.xml	0%	Avira URL Cloud	safe	

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
85.5.0.31	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
91.140.176.176	unknown	Kuwait		3225	GULFNET-KUWAITKW	false
156.158.98.11	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
45.131.150.244	unknown	Hungary		47169	HPC-MVM-ASHU	false
107.112.85.166	unknown	United States		7018	ATT-INTERNET4US	false
132.31.235.152	unknown	United States		386	AFCONC-BLOCK1-ASUS	false
45.196.195.162	unknown	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	false
185.149.136.56	unknown	Luxembourg		2602	RESTENAReseauTeleinformatiquedelEducationNationaleLU	false
185.249.62.132	unknown	United Kingdom		55933	CLOUDIE-AS-APCloudieLimitedHK	false
170.38.145.59	unknown	Malaysia		139776	PETRONAS-BHD-AS-APPetroliamNasionalBerhadMY	false
185.169.213.25	unknown	Germany		13012	GENIAS-ASDE	false
91.205.183.109	unknown	Russian Federation		51811	LOKOBANK-ASRU	false
185.142.235.90	unknown	Iran (ISLAMIC Republic Of)		206065	FDIIR	false
156.114.82.8	unknown	Netherlands		59630	NN_INSURANCE_EURASIA_NV_ITH-ASNL	false
156.144.112.175	unknown	United States		3743	ARCEL-2US	false
91.242.75.160	unknown	Moldova Republic of		202960	DONTU-PRIM-ASMD	false
91.181.131.206	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
185.96.90.189	unknown	Denmark		24800	BORNFIBERDK	false
91.53.180.247	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
41.37.180.38	unknown	Egypt		8452	TE-ASTE-ASEG	false
45.96.249.240	unknown	Egypt		37069	MOBINILEG	false
99.73.84.185	unknown	United States		7018	ATT-INTERNET4US	false
191.109.65.152	unknown	Colombia		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
45.172.252.178	unknown	Brazil		268834	CARRAROTELECOMLTDAMEBR	false
45.118.249.131	unknown	Hong Kong		134705	ITACE-AS-APItaceInternationalLimitedHK	false
187.230.235.180	unknown	Mexico		8151	UninetSAdeCVMX	false
45.255.85.14	unknown	China		132116	ANINETWORK-INAniNetworkPvtLtdIN	false
85.126.133.227	unknown	Austria		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
185.35.202.49	unknown	Norway		50304	BLIXNO	false
45.172.252.173	unknown	Brazil		268834	CARRAROTELECOMLTDAMEBR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.173.189.209	unknown	Brazil		268886	WILLYNETPROVEDORBR	false
185.53.235.150	unknown	Russian Federation		57571	TELEKONIKA_RUZA-ASRU	false
207.24.250.131	unknown	United States		701	UUNETUS	false
91.198.46.44	unknown	Russian Federation		206012	AXIOSTV-AS---UpStreams---RU	false
23.224.58.148	unknown	United States		40065	CNSERVERSUS	false
185.167.210.139	unknown	Czech Republic		199657	TOUSKOVNETCZ	false
45.196.195.141	unknown	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	false
199.212.31.185	unknown	Canada		19350	CENTENNIALCOLLEGECA	false
185.122.183.95	unknown	Germany		51862	PROFITBRICKS-ASDE	false
45.242.108.18	unknown	Egypt		24863	LINKdotNET-ASEG	false
59.253.101.44	unknown	China		37937	CNNIC-EGOVNET-APChinaeGovNetInformationCenterCN	false
185.231.215.241	unknown	Germany		204965	MED360GRADDE	false
45.79.143.153	unknown	United States		63949	LINODE-APLinodeLLCUS	false
91.11.116.160	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
45.224.65.249	unknown	Brazil		266916	MARCIOCARDOSOFAGUNDESMEBR	false
185.234.46.239	unknown	Germany		204975	BERTIN-IT-ASFR	false
185.246.165.84	unknown	Greece		204932	FRIKTORIANETGR	false
197.39.177.21	unknown	Egypt		8452	TE-ASTE-ASEG	false
185.58.180.30	unknown	Slovenia		5603	SIOL-NETTelekomSlovenijeddSI	false
154.181.133.50	unknown	Egypt		8452	TE-ASTE-ASEG	false
45.7.164.141	unknown	Brazil		266592	REALLIFEINTERNETBR	false
185.51.254.84	unknown	United Kingdom		26178	ATKINS-NORTH-AMERICAUS	false
220.94.246.139	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
91.142.10.20	unknown	Latvia		20910	BALTKOM-ASLV	false
79.69.90.139	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	false
91.108.31.247	unknown	United Kingdom		42065	ETELECOM-ASRU	false
45.221.254.36	unknown	Benin		328092	SUD-TELCOM-ASBJ	false
91.228.141.143	unknown	Romania		49074	TECHNOLOGICALRO	false
91.74.182.160	unknown	United Arab Emirates		15802	DU-AS1AE	false
91.196.209.249	unknown	Spain		205295	ACCESSCABLEES	false
45.181.208.42	unknown	Brazil		269201	UPFOURNETTELECOMLTDABR	false
185.188.24.204	unknown	Italy		206380	ONECLOUDIT	false
54.87.50.158	unknown	United States		14618	AMAZON-AESUS	false
185.91.208.160	unknown	Azerbaijan		198193	ASN-TCABLEES	false
185.169.47.106	unknown	Italy		33986	ASN-REDDERIT	false
115.164.29.141	unknown	Malaysia		4818	DIGIIX-APDiGiTelecommunicationsSdnBhdMY	false
166.255.95.155	unknown	United States		22394	CELLCOUS	false
45.187.4.115	unknown	unknown		269846	TVZAMORACAVE	false
185.41.197.151	unknown	Russian Federation		62293	URALCHEM-ASRU	false
91.140.204.28	unknown	Kuwait		3225	GULFNET-KUWAITKW	false
41.140.123.128	unknown	Morocco		36903	MT-MPLSMA	false
4.210.184.215	unknown	United States		3356	LEVEL3US	false
20.193.115.4	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.139.130.131	unknown	Canada		11998	GNB-ORGCA	false
45.9.143.88	unknown	Russian Federation		209038	ALEXGEINERMSKRU	false
152.53.40.69	unknown	United States		81	NCRENUS	false
91.201.104.36	unknown	Russian Federation		201141	JSCINSURANCEALDAGGE	false
45.181.208.55	unknown	Brazil		269201	UPFOURNETTELECOMLTDABR	false
185.187.222.179	unknown	Italy		31543	MYNET-ASmyNETgmbhAT	false
61.141.69.229	unknown	China		4813	BACKBONE-GUANGDONG-APChinaTelecomGroupCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.120.116.253	unknown	Hungary		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
188.103.181.60	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
91.100.152.122	unknown	Denmark		15516	DK-DANSKKABELTVDK	false
185.25.208.132	unknown	United Kingdom		60804	SWISS-NETWORKCH	false
91.119.249.18	unknown	Austria		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
45.144.98.124	unknown	United Kingdom		50113	SUPERSERVERSDATACENTERRU	false
143.50.98.191	unknown	Austria		1114	UniversitaetGrazAT	false
45.253.148.4	unknown	China		45062	NETEASE-ASGuangzhouNetEaseComputerSystemCoLtdCN	false
45.227.105.111	unknown	Brazil		267019	AHPROVEDORTELECOMBR	false
91.5.46.33	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
41.6.4.185	unknown	South Africa		29975	VODACOM-ZA	false
185.222.2.230	unknown	Austria		206091	PLANET-DIGITALAT	false
185.113.156.34	unknown	Portugal		12926	ARTELECOMPTArTelecomAutonomousSystemPT	false
45.104.92.39	unknown	Egypt		37069	MOBINILEG	false
41.176.104.145	unknown	Egypt		36992	ETISALAT-MISREG	false
197.160.66.227	unknown	Egypt		24863	LINKdotNET-ASEG	false
73.60.156.200	unknown	United States		7922	COMCAST-7922US	false
185.203.74.221	unknown	Switzerland		42240	VARITI-INT-ASCH	false
161.111.188.83	unknown	Spain		766	REDIRISRedIRISAutonomousSystemES	false
131.239.204.208	unknown	United States		14985	VEROXITYUS	false

Runtime Messages

Command:	/tmp/KHSQ48GkGn
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.181.131.206	dTmYFku6X8	Get hash	malicious	Browse	
107.112.85.166	hWT9RJDotD	Get hash	malicious	Browse	
41.37.180.38	Hilix.arm7	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GULFNET-KUWAITKW	Hilix.x86	Get hash	malicious	Browse	• 91.140.204.23
	Antisocial.arm	Get hash	malicious	Browse	• 91.140.204.32
	OhUy3woBmb	Get hash	malicious	Browse	• 91.140.204.13
	tW62PMv9cz	Get hash	malicious	Browse	• 185.75.59.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ndx4U5fTTa	Get hash	malicious	Browse	• 91.140.253.18
	dTmYFku6X8	Get hash	malicious	Browse	• 91.140.204.27
	lu8Qn68jzj	Get hash	malicious	Browse	• 91.140.204.28
	Hilix.arm7	Get hash	malicious	Browse	• 91.140.204.17
	Hilix.arm	Get hash	malicious	Browse	• 91.140.176.165
	dark.x86	Get hash	malicious	Browse	• 91.140.204.30
	soYc0hhOqy	Get hash	malicious	Browse	• 91.140.128.247
	UguI8hPCWh	Get hash	malicious	Browse	• 91.140.204.21
	Yx8iF6YZtN	Get hash	malicious	Browse	• 91.140.204.10
	QIJ16axero	Get hash	malicious	Browse	• 91.140.204.26
	8BzsRiOWfD	Get hash	malicious	Browse	• 91.140.204.31
	BuJw0YL8x3	Get hash	malicious	Browse	• 91.140.216.235
	rCr0tVxmK3	Get hash	malicious	Browse	• 91.140.128.225
	og3IM7rP72	Get hash	malicious	Browse	• 185.75.59.214
	nomn0m.x86	Get hash	malicious	Browse	• 91.140.204.39
SWISSCOMSwisscomSwitzerlandLtdCH	L831wSjET5	Get hash	malicious	Browse	• 164.195.19 5.131
	WhFNix8BoE	Get hash	malicious	Browse	• 80.75.208.151
	wt5i2fAcF0	Get hash	malicious	Browse	• 212.243.180.23
	dUW6YG1Tdv	Get hash	malicious	Browse	• 85.4.205.13
	RPov9E0iot	Get hash	malicious	Browse	• 164.227.243.19
	1Y2rsDBP9s	Get hash	malicious	Browse	• 213.200.200.68
	P8AVd483d7	Get hash	malicious	Browse	• 194.209.21 3.213
	mips	Get hash	malicious	Browse	• 178.197.62.170
	swOGb2sZYt	Get hash	malicious	Browse	• 199.58.40.60
	yxD7DmfG2j	Get hash	malicious	Browse	• 164.194.83.85
	z0x3n.arm	Get hash	malicious	Browse	• 85.5.212.96
	QtNnZoNz75	Get hash	malicious	Browse	• 85.3.66.122
	S13B4aCa4E	Get hash	malicious	Browse	• 85.4.81.68
	8MPbeDAwwZ	Get hash	malicious	Browse	• 85.4.81.66
	Tsunami.arm7	Get hash	malicious	Browse	• 184.86.82.9
	Tsunami.arm	Get hash	malicious	Browse	• 85.4.129.124
	Z7QqCH0bak	Get hash	malicious	Browse	• 178.197.15 9.198
	nUDLlJvoP4	Get hash	malicious	Browse	• 85.4.56.29
	9QPGr9LMaq	Get hash	malicious	Browse	• 199.58.40.41
	32UX3eB2m0	Get hash	malicious	Browse	• 85.0.181.75

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5282/oom_score_adj	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	6
Entropy (8bit):	1.7924812503605778
Encrypted:	false
SSDEEP:	3:ptn:Dn
MD5:	CBF282CC55ED0792C33D10003D1F760A
SHA1:	007DD8BD75468E6B7ABA4285E9B267202C7EAEED
SHA-256:	FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22
SHA-512:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC0
Malicious:	false

/proc/5282/oom_score_adj	
Reputation:	high, very likely benign file
Preview:	-1000.

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:CF:CF
MD5:	77E31130E90E9883A9065686679D54C0
SHA1:	9EB2EFEC6EC51EAA639F2D599C5EC6DBEC86364A
SHA-256:	EBCC6D4C0E3D89DCD951179B37A6B54CE9B4BB2F26A4E8EF448BAE0C67B074B2
SHA-512:	B92DC2F240498F724A465012B966B0E71911714970CFC01D244F01B9C39DF182C362E24FE3A8A8B2571342A81E185369095326FB7B8AA6A1D4A79B75B95A8162
Malicious:	false
Reputation:	low
Preview:	5282.

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.532720047701684
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	KHSQ48GkGn
File size:	77284
MD5:	905f7222e4cc69941935cdef4fa16246
SHA1:	84210b6c2c580b67c433e56c0d41831ce17bdd74
SHA256:	cd091f9f91f748395e30fa49ed2c4fc9e68247d5e9ae08982d5a2fb3ed074280
SHA512:	248640416fb1fe7276cd1f1d05c3fc444e5aff292103ebb95032abf5af1fe012a49756a36406f00d6dc5c10f01fcc7134cea28f266ac0af9581d489c1f7b7d6c
SSDEEP:	1536:aVNzbOfVDFKxJrilJTlzE0eGT2oBjnknutbjopj/Mf8bI3mC:aVdbS8rivlzE0eGT2oB4KjopzM0LC
File Content Preview:	.ELF.....@.`...4..+.....4. ...(.....@...@....%0..%0.....%4.E%4.E%4.....\.....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:	76724
Section Header Size:	40

ELF header

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	0x11230	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x411350	0x11350	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x4113b0	0x113b0	0x1180	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x452534	0x12534	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x45253c	0x1253c	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x452548	0x12548	0x4	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x452550	0x12550	0x250	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x4527a0	0x127a0	0x3b0	0x4	0x10000003	WA	0	0	16
.sbss	NOBITS	0x452b50	0x12b50	0x24	0x0	0x10000003	WA	0	0	4
.bss	NOBITS	0x452b80	0x12b50	0x310	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x6d2	0x12b50	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x12b50	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	0x12530	0x12530	3.5366	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x12534	0x452534	0x452534	0x61c	0x95c	2.4528	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: KHSQ48GkGn PID: 5238 Parent PID: 5121

General

Start time:	01:55:28
Start date:	02/11/2021
Path:	/tmp/KHSQ48GkGn
Arguments:	/tmp/KHSQ48GkGn
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: KHSQ48GkGn PID: 5240 Parent PID: 5238

General

Start time:	01:55:28
Start date:	02/11/2021
Path:	/tmp/KHSQ48GkGn
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: KHSQ48GkGn PID: 5241 Parent PID: 5238

General

Start time:	01:55:28
Start date:	02/11/2021
Path:	/tmp/KHSQ48GkGn
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: KHSQ48GkGn PID: 5242 Parent PID: 5238

General

Start time:	01:55:28
Start date:	02/11/2021
Path:	/tmp/KHSQ48GkGn
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: KHSQ48GkGn PID: 5246 Parent PID: 5242

General

Start time:	01:55:28
Start date:	02/11/2021
Path:	/tmp/KHSQ48GkGn
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: KHSQ48GkGn PID: 5247 Parent PID: 5242

General

Start time:	01:55:28
Start date:	02/11/2021
Path:	/tmp/KHSQ48GkGn
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: KHSQ48GkGn PID: 5248 Parent PID: 5242

General

Start time:	01:55:28
Start date:	02/11/2021
Path:	/tmp/KHSQ48GkGn
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: KHSQ48GkGn PID: 5249 Parent PID: 5242

General

Start time:	01:55:28
Start date:	02/11/2021
Path:	/tmp/KHSQ48GkGn
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: KHSQ48GkGn PID: 5255 Parent PID: 5242

General

Start time:	01:55:29
Start date:	02/11/2021
Path:	/tmp/KHSQ48GkGn
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: systemd PID: 5281 Parent PID: 1

General

Start time:	01:55:40
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd

Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5281 Parent PID: 1

General

Start time:	01:55:40
Start date:	02/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5282 Parent PID: 1

General

Start time:	01:55:40
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5282 Parent PID: 1

General

Start time:	01:55:40
Start date:	02/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated