ID: 533998
Sample Name: 61KiF94nKN
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 22:44:53
Date: 04/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

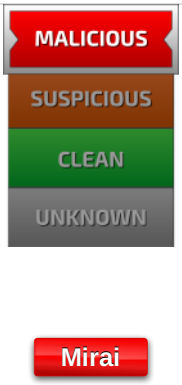
Linux Analysis Report 61KiF94nKN

Overview

General Information

Sample Name:	61KiF94nKN
Analysis ID:	533998
MD5:	06d58f655cb40ee.
SHA1:	84a92f7b7855ef9..
SHA256:	e0f8643b2d10593.
Tags:	32 elf mirai sparc
Infos:	

Detection

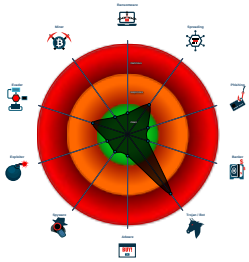


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Connects to many ports of the same...
- Sample has stripped symbol table
- 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...
- Sample listens on a socket
- Sample tries to kill a process (SIGK...

Classification



Analysis Advice

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:	533998
Start date:	04.12.2021
Start time:	22:44:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	61KiF94nKN
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.lin@0/2@13/0
Warnings:	Show All

Process Tree

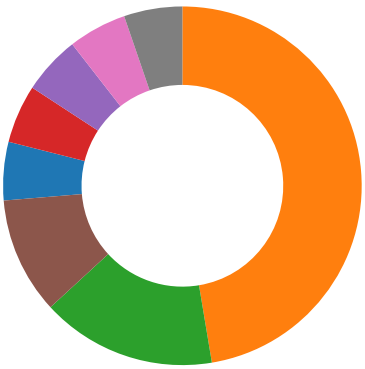
- **system is lnxubuntu20**
- 61KiF94nKN (PID: 5224, Parent: 5117, MD5: 7dc1c0e23cd5e102bb12e5c29403410e) Arguments: /tmp/61KiF94nKN
  - 61KiF94nKN New Fork (PID: 5226, Parent: 5224)
    - 61KiF94nKN New Fork (PID: 5265, Parent: 5226)
    - 61KiF94nKN New Fork (PID: 5266, Parent: 5226)
      - 61KiF94nKN New Fork (PID: 5269, Parent: 5266)
        - 61KiF94nKN New Fork (PID: 5276, Parent: 5269)
        - 61KiF94nKN New Fork (PID: 5278, Parent: 5269)
          - 61KiF94nKN New Fork (PID: 5300, Parent: 5278)
      - 61KiF94nKN New Fork (PID: 5272, Parent: 5266)
      - 61KiF94nKN New Fork (PID: 5274, Parent: 5266)
        - 61KiF94nKN New Fork (PID: 5315, Parent: 5274)
        - 61KiF94nKN New Fork (PID: 5358, Parent: 5274)
    - 61KiF94nKN New Fork (PID: 5227, Parent: 5224)
    - 61KiF94nKN New Fork (PID: 5228, Parent: 5224)
      - 61KiF94nKN New Fork (PID: 5232, Parent: 5228)
      - 61KiF94nKN New Fork (PID: 5233, Parent: 5228)
      - 61KiF94nKN New Fork (PID: 5235, Parent: 5228)
        - 61KiF94nKN New Fork (PID: 5288, Parent: 5235)
          - 61KiF94nKN New Fork (PID: 5296, Parent: 5288)
        - 61KiF94nKN New Fork (PID: 5294, Parent: 5235)
          - 61KiF94nKN New Fork (PID: 5326, Parent: 5294)
            - 61KiF94nKN New Fork (PID: 5332, Parent: 5326)
              - 61KiF94nKN New Fork (PID: 5336, Parent: 5332)
            - 61KiF94nKN New Fork (PID: 5334, Parent: 5326)
- systemd New Fork (PID: 5263, Parent: 1)
  - sshd (PID: 5263, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5264, Parent: 1)
  - sshd (PID: 5264, 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



- AV Detection
- Networking
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

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

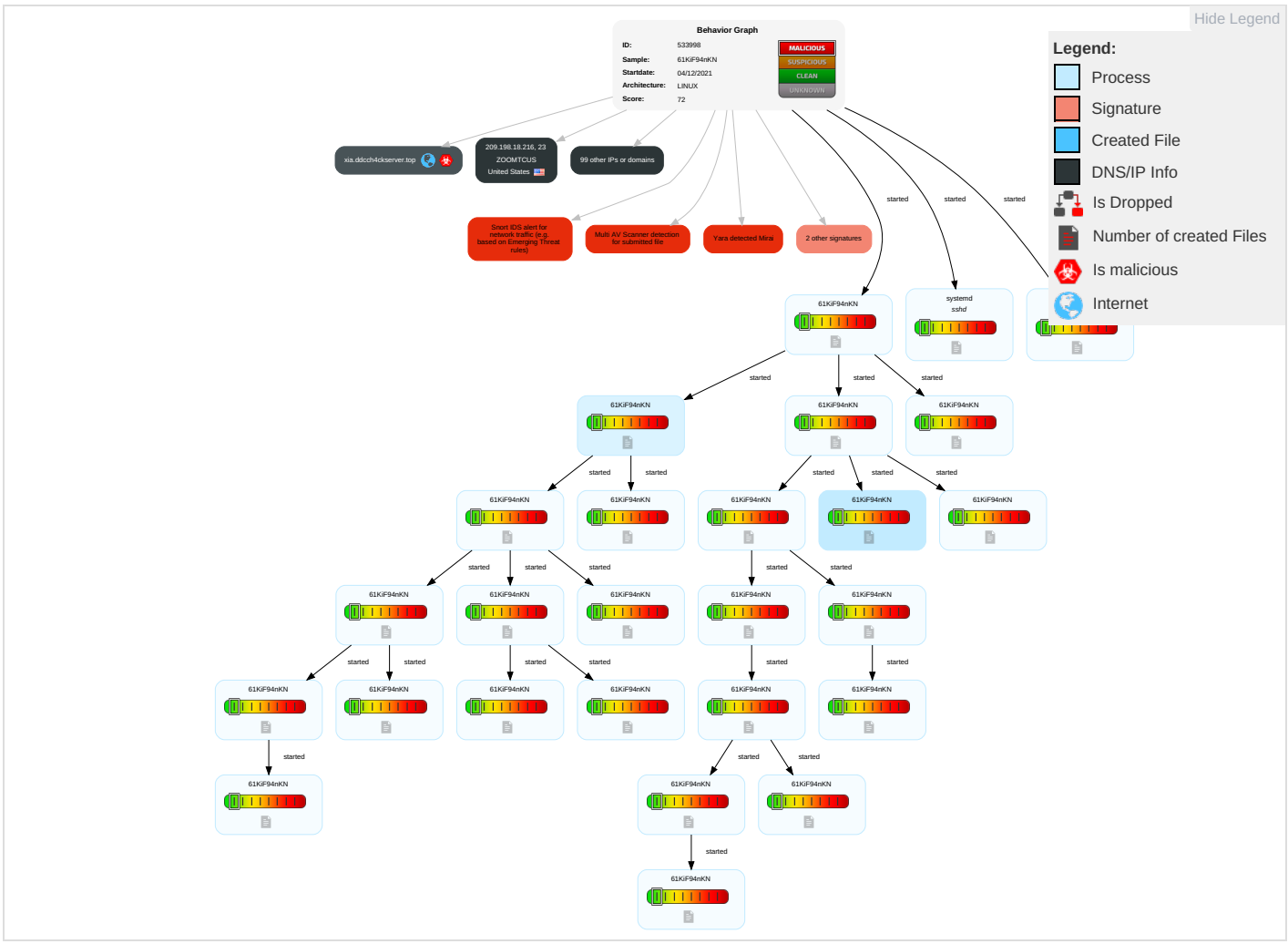
Mitre Att&ck Matrix

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 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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
61KiF94nKN	37%	Virustotal		Browse
61KiF94nKN	40%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
xia.ddcch4ckserver.top	13%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
xia.ddcch4ckserver.top	107.189.5.196	true	true	• 13%, Virustotal, Browse	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
246.249.140.98	unknown	Reserved		unknown	unknown	false
170.45.110.90	unknown	United States		264957	CoopercitrusCooperativadeProdutoresRuraisBR	false
47.252.160.8	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
60.98.164.176	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
243.254.229.225	unknown	Reserved		unknown	unknown	false
5.218.173.229	unknown	Iran (ISLAMIC Republic Of)		197207	MCCI-ASIR	false
185.65.70.223	unknown	Turkey		201735	PROPHASE-ASES	false
168.71.172.254	unknown	United States		7018	ATT-INTERNET4US	false
163.112.118.125	unknown	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
68.151.112.93	unknown	Canada		6327	SHAWCA	false
133.89.64.217	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
244.197.160.238	unknown	Reserved		unknown	unknown	false
211.188.243.31	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
80.124.79.187	unknown	France		15557	LDCOMNETFR	false
73.10.41.195	unknown	United States		7922	COMCAST-7922US	false
9.246.160.133	unknown	United States		3356	LEVEL3US	false
193.1.217.2	unknown	Ireland		1213	HEANETIE	false
89.82.198.141	unknown	France		5410	BOUYGTEL-ISPFR	false
191.82.108.49	unknown	Argentina		22927	TelefonicadeArgentinaAR	false
221.171.214.240	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
83.173.196.243	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
157.213.248.246	unknown	United States		4704	SANNETRakutenMobileIncJP	false
81.132.68.181	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
23.224.58.144	unknown	United States		40065	CNSERVERSUS	false
68.131.63.99	unknown	United States		701	UUNETUS	false
185.167.210.138	unknown	Czech Republic		199657	TOUSKOVNETCZ	false
74.112.219.16	unknown	United States		46132	VENTYX-AN-ABB-COMPANYUS	false
158.220.98.141	unknown	Switzerland		8556	LEVANTISCH	false
90.216.180.27	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
38.89.204.151	unknown	United States		174	COGENT-174US	false
254.94.23.229	unknown	Reserved		unknown	unknown	false
62.200.46.62	unknown	European Union		2686	ATGS-MMD-ASUS	false
59.51.33.190	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
143.28.20.34	unknown	United States		264008	LANCAMANTOANISERVICOSDEINFORMATICALTDA-MEBR	false
241.155.183.174	unknown	Reserved		unknown	unknown	false
45.234.130.236	unknown	Brazil		267365	GigaTecnologiaemRedeseInternetEIRELIBR	false
165.193.73.81	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
48.185.159.34	unknown	United States		2686	ATGS-MMD-ASUS	false
135.93.177.171	unknown	United States		10455	LUCENT-CIOUS	false
41.228.193.93	unknown	Tunisia		37693	TUNISIANATN	false
142.5.110.19	unknown	Canada		46606	UNIFIEDLAYER-AS-1US	false
163.61.118.81	unknown	unknown		2516	KDDIKDDICORPORATIONJP	false
62.191.178.99	unknown	United Kingdom		5586	MCI-INTGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
125.175.21.204	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
120.113.153.90	unknown	Taiwan; Republic of China (ROC)		17716	NTU-TWNationalTaiwanUniversityTW	false
171.113.147.123	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
135.46.199.217	unknown	United States		54614	CIKTELECOM-CABLECA	false
166.149.86.237	unknown	United States		22394	CELLCOUS	false
8.138.12.41	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
243.192.141.18	unknown	Reserved		unknown	unknown	false
192.237.118.230	unknown	United States		393238	IMONCUS	false
189.227.127.163	unknown	Mexico		8151	UninetSAdeCVMX	false
138.238.166.203	unknown	United States		33084	DC-NETUS	false
2.134.183.227	unknown	Kazakhstan		9198	KAZTELECOM-ASKZ	false
161.2.40.141	unknown	United Kingdom		15914	BritishAirwaysGB	false
173.154.95.216	unknown	United States		10507	SPCSUS	false
173.118.241.83	unknown	United States		10507	SPCSUS	false
115.234.54.210	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
222.124.195.220	unknown	Indonesia		17974	TELKOMNET-AS2-APPTTelekomunikasiIndonesiaID	false
105.16.125.186	unknown	Mauritius		37100	SEACOM-ASMU	false
255.1.14.8	unknown	Reserved		unknown	unknown	false
147.59.82.120	unknown	United States		1533	DNIC-AS-01533US	false
160.176.253.216	unknown	Morocco		36903	MT-MPLSMA	false
141.228.157.156	unknown	United Kingdom		12701	BARCAPLondonGB	false
109.146.97.99	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
77.229.193.246	unknown	Spain		12430	VODAFONE_ESES	false
205.213.14.73	unknown	United States		2381	WISCNET1-ASUS	false
85.33.215.213	unknown	Italy		3269	ASN-IBSNAZIT	false
84.116.116.153	unknown	Netherlands		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
161.252.120.236	unknown	Kuwait		42781	ZNETAS-KW	false
123.179.22.94	unknown	China		4809	CHINATELECOM-CORE-WAN-CN2ChinaTelecomNextGenerationCarr	false
194.215.184.123	unknown	Finland		1759	TSF-IP-CORETeliaFinlandOyjEU	false
146.24.187.201	unknown	United States		197938	TRAVIANGAMESDE	false
44.79.138.141	unknown	United States		7377	UCSDUS	false
99.190.186.31	unknown	United States		7018	ATT-INTERNET4US	false
119.47.10.35	unknown	Japan		55385	DADigitalAllianceCoLtdJP	false
145.25.161.151	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
177.185.203.216	unknown	Brazil		28299	IPV6InternetLtdaBR	false
110.62.148.219	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
213.198.183.239	unknown	Italy		15589	ASN-CLOUDITALIAIT	false
97.82.62.213	unknown	United States		20115	CHARTER-20115US	false
14.45.175.64	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
95.194.248.76	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
209.198.18.216	unknown	United States		31996	ZOOMTCUS	false
85.40.82.1	unknown	Italy		3269	ASN-IBSNAZIT	false
70.37.55.85	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
98.155.194.88	unknown	United States		20001	TWC-20001-PACWESTUS	false
18.125.179.241	unknown	United States		3	MIT-GATEWAYSUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
148.43.100.233	unknown	United States		6400	CompaniaDominicanadeTelefonosSADO	false
19.44.33.247	unknown	United States		3	MIT-GATEWAYSUS	false
219.181.80.241	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
89.207.8.195	unknown	Switzerland		31662	KNSURSELVAKommunikationsNetzSurselvaCH	false
35.198.202.160	unknown	United States		15169	GOOGLEUS	false
43.133.6.103	unknown	Japan		4249	LILLY-ASUS	false
53.71.21.3	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
113.19.180.129	unknown	India		23772	ORTELNET-ASMsOrtelCommunicationsLtdIN	false
194.12.240.1	unknown	Bulgaria		8262	EVOLINK-ASBG	false
253.82.17.118	unknown	Reserved		unknown	unknown	false
218.124.198.24	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
92.98.39.146	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false

Runtime Messages

Command:	/tmp/61KiF94nKN
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infected By Akiru
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
254.94.23.229	Darknet.x86	Get hash	malicious	Browse	
211.188.243.31	3DAMhv0DFI	Get hash	malicious	Browse	
193.1.217.2	X5bKvoLX1E	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
xia.ddcch4ckserver.top	GuSrMsLH0y	Get hash	malicious	Browse	• 107.189.5.196
	e8cvIYg1a3	Get hash	malicious	Browse	• 107.189.5.196
	wCEe6Y5TGI	Get hash	malicious	Browse	• 107.189.5.196
	Xp9AXIBaBp	Get hash	malicious	Browse	• 107.189.5.196

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CoopercitrusCooperativadeProdutoresRuraisBR	sora.x86	Get hash	malicious	Browse	• 170.37.47.60
	l8np4x8FGL	Get hash	malicious	Browse	• 170.40.43.249
	ZOi52gHoIY	Get hash	malicious	Browse	• 170.40.43.244
	M0ek1k58Q3	Get hash	malicious	Browse	• 170.41.140.221
	KKveTTgaAAsecNNaaaa.x86-20211122-0650	Get hash	malicious	Browse	• 170.1.225.236
	6L1AGNUMgk	Get hash	malicious	Browse	• 170.45.183.59
	mfFr814Hup	Get hash	malicious	Browse	• 170.40.43.210
	4i9Yl7vp8B	Get hash	malicious	Browse	• 170.40.43.243
	8cpsKRnU4r	Get hash	malicious	Browse	• 170.45.183.54
	K1kUt3MxkS	Get hash	malicious	Browse	• 170.0.2.234

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	bRQTHkekvv	Get hash	malicious	Browse	• 170.43.8.208
	RJHE1O7ZBF	Get hash	malicious	Browse	• 170.45.183.15
	HT7gBWexDX	Get hash	malicious	Browse	• 170.45.183.36
	DGxCnji49S	Get hash	malicious	Browse	• 170.45.134.66
	iQGF9sgxaB	Get hash	malicious	Browse	• 170.44.221.217
	z0x3n.x86-20211110-2150	Get hash	malicious	Browse	• 170.36.107.18
	pt7DJSPfna	Get hash	malicious	Browse	• 170.37.13.129
	QsSD7q2BRO	Get hash	malicious	Browse	• 170.45.109.60
	sora.arm	Get hash	malicious	Browse	• 170.40.43.246
	wRmHCEnowl	Get hash	malicious	Browse	• 170.40.43.214
GIGAINFRASoftbankBBCorpJP	GuSrMsLH0y	Get hash	malicious	Browse	• 221.75.228.134
	wCEe6Y5TGI	Get hash	malicious	Browse	• 220.0.129.221
	arm7	Get hash	malicious	Browse	• 218.121.111.189
	x86	Get hash	malicious	Browse	• 221.87.19.65
	arm	Get hash	malicious	Browse	• 126.22.226.224
	rELGr0VELq	Get hash	malicious	Browse	• 126.165.234.100
	ThhBCrYJCm	Get hash	malicious	Browse	• 221.73.91.128
	R5UqytMpoF	Get hash	malicious	Browse	• 126.25.240.2
	sora.x86	Get hash	malicious	Browse	• 220.19.206.59
	sora.arm7	Get hash	malicious	Browse	• 221.87.68.14
	sora.arm	Get hash	malicious	Browse	• 126.180.101.68
	OhDPOb1tfB	Get hash	malicious	Browse	• 126.215.126.182
	b3astmode.arm7	Get hash	malicious	Browse	• 221.17.155.132
	b3astmode.arm	Get hash	malicious	Browse	• 221.28.251.112
	tPC6yuAhsc	Get hash	malicious	Browse	• 126.98.144.148
	sora.x86	Get hash	malicious	Browse	• 126.195.188.132
	0VIoO2ovmF	Get hash	malicious	Browse	• 220.1.225.135
	6Zcc7k2JZy	Get hash	malicious	Browse	• 60.86.254.14
	nKv4cxjlx6	Get hash	malicious	Browse	• 219.18.123.200
	apep.arm7	Get hash	malicious	Browse	• 160.24.170.153
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	780426DE24AE46F300FDAF9CBF597C8F2164F7B6C525C.exe	Get hash	malicious	Browse	• 47.251.42.216
	Kq8hjfiv87.exe	Get hash	malicious	Browse	• 47.251.42.216
	C7304FF0966068D305DA031F9DA60C5B0EBE32AC43533.exe	Get hash	malicious	Browse	• 47.251.42.216
	arm	Get hash	malicious	Browse	• 8.208.25.42
	f2Y03RRaRe.exe	Get hash	malicious	Browse	• 8.209.79.122
	DrC7J6YQnm.exe	Get hash	malicious	Browse	• 8.209.71.17
	tips-5067550674.xls	Get hash	malicious	Browse	• 149.129.254.152
	tips920293137.xls	Get hash	malicious	Browse	• 149.129.254.152
	tips920293137.xls	Get hash	malicious	Browse	• 149.129.254.152
	156219029342206-107-0_attach.1.payment 264494490.xls	Get hash	malicious	Browse	• 149.129.254.152
	NVTNgwAjOK	Get hash	malicious	Browse	• 8.212.11.154
	RFQ-CIF DT22.doc	Get hash	malicious	Browse	• 47.241.96.113
	order 4544471372.xls	Get hash	malicious	Browse	• 149.129.254.152
	order 4544471372.xls	Get hash	malicious	Browse	• 149.129.254.152
	SecuriteInfo.com.Heur.31616.xls	Get hash	malicious	Browse	• 149.129.254.152
	SecuriteInfo.com.Heur.26641.xls	Get hash	malicious	Browse	• 149.129.254.152
	SecuriteInfo.com.Heur.5035.doc	Get hash	malicious	Browse	• 8.209.79.68
	SecuriteInfo.com.Heur.6074.doc	Get hash	malicious	Browse	• 8.209.79.68
	plans_48055147646.xls	Get hash	malicious	Browse	• 149.129.254.152
	plans_48055147646.xls	Get hash	malicious	Browse	• 149.129.254.152

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5264/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
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):	2.321928094887362
Encrypted:	false
SSDEEP:	3:Ct:Ct
MD5:	ED62F87F4EC9699FDAD6BAFEFC371E3D
SHA1:	F14CB0851A26C184C7614A62326934CBFDA85155
SHA-256:	EB4EE1B62A4108FE56E980DC18F22FA746F5060A5265EA1E101CB5CBA1F6F43E
SHA-512:	C3111F12F3B9DF49EBC63F082C6B267AE6DB6AC567E258584F5C8883B17DC683CE947F9BBF8E99F706C31ECB1B74EA7D6BCEA9F8F2D0BC668DF14123EF6B246B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	5264.

Static File Info

General

File type:	ELF 32-bit MSB executable, SPARC, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.009298823803464
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	61KiF94nKN
File size:	66380
MD5:	06d58f655cb40ee644bd74e19483ba8b
SHA1:	84a92f7b7855ef9f1ec12e10ef38b3bc7045d903
SHA256:	e0f8643b2d10593678b16fdaab7bc4a070cdbe4a8a617b0a37bda328f4002235
SHA512:	c1f7006c3f4a845df1b582b2fb6fcdfe83a033b8dd7cb9c7cde7afbcbce3ac57a467feda72f1c77d44843f05ca725ce50d6db93edf61f7680d247ca3258a4bc4
SSDEEP:	1536:0dn1Jb3SdNySlmbWfuPA+CbsyGjoycpbY+WJ:suv1sbWfu4Tsffcp0+WJ

General

File Content Preview:	.ELF.....4.....4. ...(..... ... .|.....dt.Q.....@..(....@.<. .....#.....a...`.....!..... ...@....."..... `.....$ ... ...@..... .....`....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	Sparc
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x101a4
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	65980
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10094	0x94	0x1c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100b0	0xb0	0xf3e8	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x1f498	0xf498	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1f4b0	0xf4b0	0x870	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x20000	0x10000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x20008	0x10008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x20018	0x10018	0x164	0x0	0x3	WA	0	0	8
.bss	NOBITS	0x20180	0x1017c	0x310	0x0	0x3	WA	0	0	8
.shstrtab	STRTAB	0x0	0x1017c	0x3e	0x0	0x0		0	0	1

Program Segments

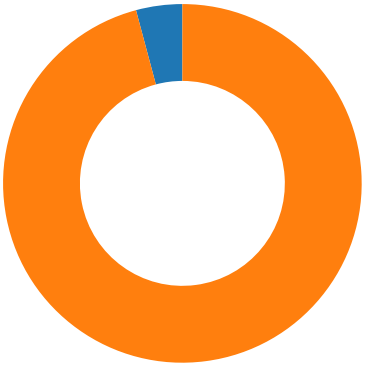
Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x10000	0x10000	0xfd20	0xfd20	3.3193	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x10000	0x20000	0x20000	0x17c	0x490	0.4307	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution

Total Packets: 96

- 23 (Telnet)
- 3175 undefined



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 4, 2021 22:45:34.386389017 CET	192.168.2.23	8.8.8.8	0xba5a	Standard query (0)	xia.ddcch4 ckserver.top	A (IP address)	IN (0x0001)
Dec 4, 2021 22:45:42.784358025 CET	192.168.2.23	8.8.8.8	0xba5a	Standard query (0)	xia.ddcch4 ckserver.top	A (IP address)	IN (0x0001)
Dec 4, 2021 22:45:42.874461889 CET	192.168.2.23	8.8.8.8	0xba5a	Standard query (0)	xia.ddcch4 ckserver.top	A (IP address)	IN (0x0001)
Dec 4, 2021 22:45:56.854185104 CET	192.168.2.23	8.8.8.8	0x6ef4	Standard query (0)	xia.ddcch4 ckserver.top	A (IP address)	IN (0x0001)
Dec 4, 2021 22:46:03.318275928 CET	192.168.2.23	8.8.8.8	0xd2d4	Standard query (0)	xia.ddcch4 ckserver.top	A (IP address)	IN (0x0001)
Dec 4, 2021 22:46:03.596966982 CET	192.168.2.23	8.8.8.8	0x2b86	Standard query (0)	xia.ddcch4 ckserver.top	A (IP address)	IN (0x0001)
Dec 4, 2021 22:46:09.163847923 CET	192.168.2.23	8.8.8.8	0xb537	Standard query (0)	xia.ddcch4 ckserver.top	A (IP address)	IN (0x0001)
Dec 4, 2021 22:46:33.807394981 CET	192.168.2.23	8.8.8.8	0x477c	Standard query (0)	xia.ddcch4 ckserver.top	A (IP address)	IN (0x0001)
Dec 4, 2021 22:46:55.184551001 CET	192.168.2.23	8.8.8.8	0x57bd	Standard query (0)	xia.ddcch4 ckserver.top	A (IP address)	IN (0x0001)
Dec 4, 2021 22:47:03.980705023 CET	192.168.2.23	8.8.8.8	0xd143	Standard query (0)	xia.ddcch4 ckserver.top	A (IP address)	IN (0x0001)
Dec 4, 2021 22:47:04.723417997 CET	192.168.2.23	8.8.8.8	0xf816	Standard query (0)	xia.ddcch4 ckserver.top	A (IP address)	IN (0x0001)
Dec 4, 2021 22:47:05.338871956 CET	192.168.2.23	8.8.8.8	0x1c2c	Standard query (0)	xia.ddcch4 ckserver.top	A (IP address)	IN (0x0001)
Dec 4, 2021 22:47:45.619473934 CET	192.168.2.23	8.8.8.8	0x203b	Standard query (0)	xia.ddcch4 ckserver.top	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 4, 2021 22:45:34.409746885 CET	8.8.8.8	192.168.2.23	0xba5a	No error (0)	xia.ddcch4 ckserver.top		107.189.5.196	A (IP address)	IN (0x0001)
Dec 4, 2021 22:45:42.890985012 CET	8.8.8.8	192.168.2.23	0xba5a	No error (0)	xia.ddcch4 ckserver.top		107.189.5.196	A (IP address)	IN (0x0001)
Dec 4, 2021 22:45:42.895654917 CET	8.8.8.8	192.168.2.23	0xba5a	No error (0)	xia.ddcch4 ckserver.top		107.189.5.196	A (IP address)	IN (0x0001)
Dec 4, 2021 22:45:56.872252941 CET	8.8.8.8	192.168.2.23	0x6ef4	No error (0)	xia.ddcch4 ckserver.top		107.189.5.196	A (IP address)	IN (0x0001)
Dec 4, 2021 22:46:03.609237909 CET	8.8.8.8	192.168.2.23	0xd2d4	No error (0)	xia.ddcch4 ckserver.top		107.189.5.196	A (IP address)	IN (0x0001)
Dec 4, 2021 22:46:03.615993023 CET	8.8.8.8	192.168.2.23	0x2b86	No error (0)	xia.ddcch4 ckserver.top		107.189.5.196	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 4, 2021 22:46:09.183428049 CET	8.8.8.8	192.168.2.23	0xb537	No error (0)	xia.ddcch4 ckserver.top		107.189.5.196	A (IP address)	IN (0x0001)
Dec 4, 2021 22:46:34.152484894 CET	8.8.8.8	192.168.2.23	0x477c	No error (0)	xia.ddcch4 ckserver.top		107.189.5.196	A (IP address)	IN (0x0001)
Dec 4, 2021 22:46:55.204437017 CET	8.8.8.8	192.168.2.23	0x57bd	No error (0)	xia.ddcch4 ckserver.top		107.189.5.196	A (IP address)	IN (0x0001)
Dec 4, 2021 22:47:04.003648996 CET	8.8.8.8	192.168.2.23	0xd143	No error (0)	xia.ddcch4 ckserver.top		107.189.5.196	A (IP address)	IN (0x0001)
Dec 4, 2021 22:47:04.741116047 CET	8.8.8.8	192.168.2.23	0xf816	No error (0)	xia.ddcch4 ckserver.top		107.189.5.196	A (IP address)	IN (0x0001)
Dec 4, 2021 22:47:05.358477116 CET	8.8.8.8	192.168.2.23	0x1c2c	No error (0)	xia.ddcch4 ckserver.top		107.189.5.196	A (IP address)	IN (0x0001)
Dec 4, 2021 22:47:45.642565966 CET	8.8.8.8	192.168.2.23	0x203b	No error (0)	xia.ddcch4 ckserver.top		107.189.5.196	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: 61KiF94nKN PID: 5224 Parent PID: 5117

General

Start time:	22:45:33
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	/tmp/61KiF94nKN
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Analysis Process: 61KiF94nKN PID: 5226 Parent PID: 5224

General

Start time:	22:45:33
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Directory Enumerated

Analysis Process: 61KiF94nKN PID: 5265 Parent PID: 5226

General

Start time:	22:45:40
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5266 Parent PID: 5226

General

Start time:	22:45:41
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5269 Parent PID: 5266

General

Start time:	22:45:41
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5276 Parent PID: 5269

General

Start time:	22:45:42
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5278 Parent PID: 5269

General

Start time:	22:45:42
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5300 Parent PID: 5278

General

Start time:	22:46:08
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5272 Parent PID: 5266

General

Start time:	22:45:41
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5274 Parent PID: 5266

General

Start time:	22:45:41
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5315 Parent PID: 5274

General

Start time:	22:46:33
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5358 Parent PID: 5274

General

Start time:	22:47:44
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5227 Parent PID: 5224

General

Start time:	22:45:33
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5228 Parent PID: 5224

General

Start time:	22:45:33
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5232 Parent PID: 5228

General

Start time:	22:45:33
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Directory Enumerated

Analysis Process: 61KiF94nKN PID: 5233 Parent PID: 5228

General

Start time:	22:45:33
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5235 Parent PID: 5228

General

Start time:	22:45:33
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5288 Parent PID: 5235

General

Start time:	22:45:56
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5296 Parent PID: 5288

General

Start time:	22:46:02
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5294 Parent PID: 5235

General

Start time:	22:46:02
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5326 Parent PID: 5294

General

Start time:	22:46:54
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5332 Parent PID: 5326

General

Start time:	22:47:03
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5336 Parent PID: 5332

General

Start time:	22:47:04
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 61KiF94nKN PID: 5334 Parent PID: 5326

General

Start time:	22:47:03
Start date:	04/12/2021
Path:	/tmp/61KiF94nKN
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: systemd PID: 5263 Parent PID: 1

General

Start time:	22:45:40
Start date:	04/12/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5263 Parent PID: 1

General

Start time:	22:45:40
Start date:	04/12/2021
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: 5264 Parent PID: 1

General

Start time:	22:45:40
Start date:	04/12/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5264 Parent PID: 1

General

Start time:	22:45:40
Start date:	04/12/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated