ID: 512582
Sample Name: QtNnZoNz75
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 05:42:12
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

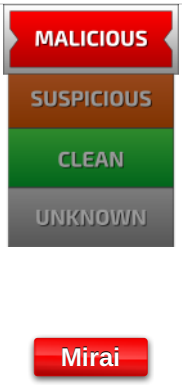
Linux Analysis Report QtNnZoNz75

Overview

General Information

Sample Name:	QtNnZoNz75
Analysis ID:	512582
MD5:	9afa6f4cec8bd12..
SHA1:	10efbc551846704.
SHA256:	0faa53c63781c3f..
Tags:	32 elf mirai sparc
Infos:	

Detection

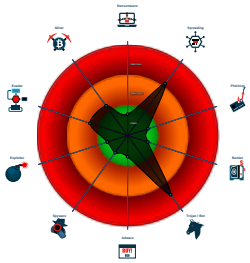


Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through …
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample tries to kill many processes…
- Reads CPU information from /sys in…
- Yara signature match
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Detected TCP or UDP traffic on non…
- Executes the "rm" command used to…
- Sample listens on a socket

Classification



Analysis Advice

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:	512582
Start date:	01.11.2021
Start time:	05:42:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QtNnZoNz75
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@0/9@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- QtNnZoNz75 (PID: 5235, Parent: 5113, MD5: 7dc1c0e23cd5e102bb12e5c29403410e) Arguments: /tmp/QtNnZoNz75
  - QtNnZoNz75 New Fork (PID: 5237, Parent: 5235)
    - QtNnZoNz75 New Fork (PID: 5239, Parent: 5237)
    - QtNnZoNz75 New Fork (PID: 5240, Parent: 5237)
    - QtNnZoNz75 New Fork (PID: 5242, Parent: 5237)
    - QtNnZoNz75 New Fork (PID: 5244, Parent: 5237)
    - QtNnZoNz75 New Fork (PID: 5246, Parent: 5237)
    - QtNnZoNz75 New Fork (PID: 5248, Parent: 5237)
    - QtNnZoNz75 New Fork (PID: 5249, Parent: 5237)
    - QtNnZoNz75 New Fork (PID: 5250, Parent: 5237)
- systemd New Fork (PID: 5276, Parent: 1)
- sshd (PID: 5276, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5277, Parent: 1)
- systemd-resolved (PID: 5277, Parent: 1, MD5: c93bbc5e20248114c56896451eab7a8b) Arguments: /lib/systemd/systemd-resolved
- systemd New Fork (PID: 5544, Parent: 1)
- systemd-logind (PID: 5544, Parent: 1, MD5: 8dd58a1b4c12f7a1d5fe3ce18b2aaeef) Arguments: /lib/systemd/systemd-logind
- systemd New Fork (PID: 5611, Parent: 1)
- sshd (PID: 5611, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- gdm3 New Fork (PID: 5633, Parent: 1320)
- Default (PID: 5633, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5649, Parent: 1320)
- Default (PID: 5649, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- xfce4-session New Fork (PID: 5666, Parent: 1900)
- rm (PID: 5666, Parent: 1900, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /home/saturnino/.cache/sessions/Thunar-2ec9153f1-6fa0-4067-96b1-e5fe875b1e51
- systemd New Fork (PID: 5791, Parent: 1)
- sshd (PID: 5791, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5894, Parent: 1)
- sshd (PID: 5894, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5967, Parent: 1)
- sshd (PID: 5967, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5968, Parent: 1)
- sshd (PID: 5968, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- gdm3 New Fork (PID: 5979, Parent: 1320)
- Default (PID: 5979, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- xfce4-session New Fork (PID: 5982, Parent: 1900)
- xfwm4 (PID: 5982, Parent: 1900, MD5: 59defa3c00cc30d85ed77b738d55e9da) Arguments: xfwm4 --display :1.0 --sm-client-id 2389ab8d9-421f-49fc-90ad-c6cc4c15ac4c
- xfce4-session New Fork (PID: 5983, Parent: 1900)
- xfce4-panel (PID: 5983, Parent: 1900, MD5: a15b657c7d54ac1385f1f15004ea6784) Arguments: xfce4-panel --display :1.0 --sm-client-id 2b4cc744e-8b9d-436f-9a4a-312b40faa2ec
- systemd New Fork (PID: 6006, Parent: 1860)
- pulseaudio (PID: 6006, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- **cleanup**

Yara Overview

Initial Sample

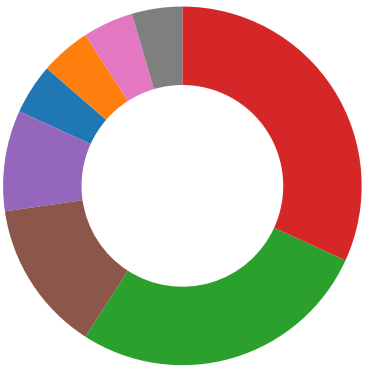
Source	Rule	Description	Author	Strings
QtNnZoNz75	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x11708:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x11768:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x11808:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3
QtNnZoNz75	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x10900:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
QtNnZoNz75	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
QtNnZoNz75	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5240.1.000000008f29600c.000000000adcf760.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x28c:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x2ec:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x390:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3
5242.1.000000001db6ec02.000000001ace8034.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x11708:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x11768:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3 • 0x11808:$xo1: \xCE\xEC\xF9\xEA\xEF\xEF\xE2\xAC\xB6\xAD\xB3

Source	Rule	Description	Author	Strings
5242.1.000000001db6ec02.000000001ace8034.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_2	Detects ELF malware Mirai related	Florian Roth	• 0x10900:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A
5242.1.000000001db6ec02.000000001ace8034.r-x.sdmp	JoeSecurity_Mirai_5	Yara detected Mirai	Joe Security	
5242.1.000000001db6ec02.000000001ace8034.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Click to see the 35 entries				

Jbx Signature Overview



- AV Detection
- Bitcoin Miner
- Networking
- System Summary
- Persistence and Installation Behavior
- 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

System Summary:

Malicious sample detected (through community Yara rule)

Sample tries to kill many processes (SIGKILL)

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

Mitre Att&ck Matrix

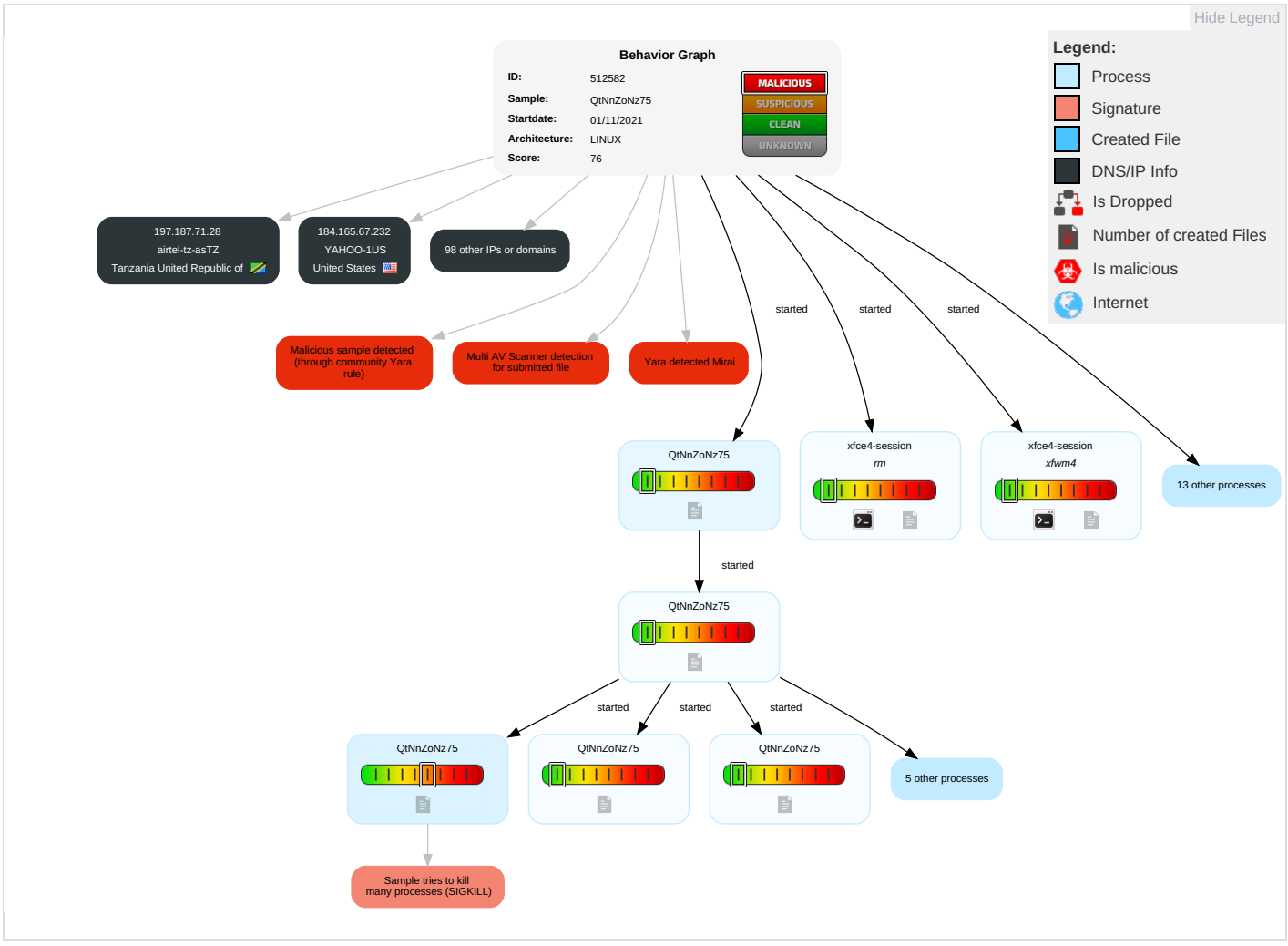
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	File Deletion 1	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	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockou

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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
QtNnZoNz75	48%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://23.94.37.59/bin	0%	Avira URL Cloud	safe	
http://23.94.37.59/bins/Tsunami.mips;	100%	Avira URL Cloud	malware	
http://23.94.37.59/bins/Tsunami.x86	15%	Virustotal		Browse
http://23.94.37.59/bins/Tsunami.x86	100%	Avira URL Cloud	malware	
http://23.94.37.59/zyxel.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
212.181.200.45	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
172.48.184.69	unknown	United States		21928	T-MOBILE-AS21928US	false
95.38.199.78	unknown	Iran (ISLAMIC Republic Of)		41881	FANAVA-ASFanavaGroupCommunicationCoIR	false
62.69.53.237	unknown	United Kingdom		5413	AS5413GB	false
85.11.217.242	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
95.182.199.211	unknown	Belgium		12392	ASBRUTELEVOOBE	false
62.105.232.171	unknown	Netherlands		4589	EASYNETEasynetGlobalServicesEU	false
79.132.155.90	unknown	Germany		29084	COMNET-ASBG	false
62.16.140.4	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
98.188.105.37	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
197.203.165.197	unknown	Algeria		36947	ALGTEL-ASDZ	false
184.165.67.232	unknown	United States		10310	YAHOO-1US	false
31.126.79.2	unknown	United Kingdom		12576	EELtdGB	false
109.24.240.206	unknown	France		15557	LDCOMNETFR	false
85.120.111.194	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
184.225.235.113	unknown	United States		10507	SPCSUS	false
210.147.65.78	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
41.187.177.10	unknown	Egypt		20928	NOOR-ASEG	false
31.25.124.180	unknown	Switzerland		61174	GLATTWERKUsterstrasse111CH	false
197.56.218.254	unknown	Egypt		8452	TE-ASTE-ASEG	false
31.211.232.97	unknown	Sweden		33885	OWNITKatarinavagen15SE	false
5.44.126.217	unknown	Switzerland		45031	PROVIDERBOXIPv4IPv6DUS1DE	false
31.251.56.63	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
95.116.116.148	unknown	Germany		6805	TDDE-ASN1DE	false
94.101.162.38	unknown	United Kingdom		47797	ESSEXCC-ASGB	false
98.250.124.94	unknown	United States		7922	COMCAST-7922US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.3.66.122	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
95.107.112.137	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
62.28.166.138	unknown	Portugal		15525	MEO-EMPRESASPT	false
2.134.216.76	unknown	Kazakhstan		9198	KAZTELECOM-ASKZ	false
5.170.86.3	unknown	Italy		16232	ASN-TIMServiceProviderIT	false
112.157.171.161	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
31.100.75.13	unknown	United Kingdom		12576	EELtdGB	false
98.247.137.234	unknown	United States		7922	COMCAST-7922US	false
172.203.238.149	unknown	United States		18747	IFX18747US	false
184.116.8.78	unknown	United States		7922	COMCAST-7922US	false
95.144.231.152	unknown	United Kingdom		12576	EELtdGB	false
98.95.4.45	unknown	United States		11351	TWC-11351-NORTHEASTUS	false
184.102.107.234	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
197.179.206.127	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
197.131.22.46	unknown	Morocco		6713	IAM-ASMA	false
172.176.216.186	unknown	United States		7018	ATT-INTERNET4US	false
95.18.93.133	unknown	Spain		12479	UNI2-ASES	false
2.209.223.77	unknown	Germany		6805	TDDE-ASN1DE	false
178.253.26.126	unknown	Iran (ISLAMIC Republic Of)		42337	RESPINA-ASIR	false
94.144.155.70	unknown	Denmark		9158	TELENOR_DANMARK_ASDK	false
95.193.205.56	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
172.239.185.221	unknown	United States		20940	AKAMAI-ASN1EU	false
184.110.63.159	unknown	United States		7922	COMCAST-7922US	false
79.47.183.43	unknown	Italy		3269	ASN-IBSNAZIT	false
197.70.244.246	unknown	South Africa		16637	MTNNS-ASZA	false
184.173.22.236	unknown	United States		36351	SOFTLAYERUS	false
5.66.172.125	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
85.144.200.240	unknown	Netherlands		50266	TMOBILE-THUISNL	false
184.207.33.128	unknown	United States		10507	SPCSUS	false
2.127.239.49	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
98.114.59.243	unknown	United States		701	UUNETUS	false
95.131.237.190	unknown	Malta		20521	ASN-BELLNETMT	false
98.60.253.119	unknown	United States		7922	COMCAST-7922US	false
94.146.57.77	unknown	Denmark		9158	TELENOR_DANMARK_ASDK	false
31.232.160.24	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
62.51.196.155	unknown	European Union		10310	YAHOO-1US	false
112.148.105.93	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
172.48.155.181	unknown	United States		21928	T-MOBILE-AS21928US	false
95.169.14.70	unknown	Canada		25820	IT7NETCA	false
62.24.111.82	unknown	Kenya		12455	JAMBONETKE	false
98.105.187.55	unknown	United States		6167	CELLCO-PARTUS	false
98.62.2.56	unknown	United States		7922	COMCAST-7922US	false
197.207.242.240	unknown	Algeria		36947	ALGTEL-ASDZ	false
62.184.167.195	unknown	European Union		34456	RIALCOM-ASRU	false
31.223.213.245	unknown	Bosnia and Herzegowina		21107	BLICNET-ASBLICNETASpeeringinfoBA	false
98.60.168.2	unknown	United States		7922	COMCAST-7922US	false
85.211.146.68	unknown	United Kingdom		9105	TISCALI-UKTalkTalkCommunicationsLimitedGB	false
95.58.131.8	unknown	Kazakhstan		9198	KAZTELECOM-ASKZ	false
62.1.27.147	unknown	Greece		1241	FORTHNET-GRForthnetEU	false
95.71.147.158	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
85.136.244.35	unknown	Spain		6739	ONO-ASCableuropa-ONOES	false
85.22.207.206	unknown	Germany		15763	ASDOKOMDE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
184.167.73.179	unknown	United States		33588	BRESNAN-33588US	false
197.187.71.28	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
172.36.83.93	unknown	United States		21928	T-MOBILE-AS21928US	false
94.3.251.65	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
172.211.100.124	unknown	United States		18747	IFX18747US	false
85.56.103.10	unknown	Spain		12479	UNI2-ASES	false
98.108.222.166	unknown	United States		6167	CELLCO-PARTUS	false
98.119.14.31	unknown	United States		5650	FRONTIER-FRTRUS	false
5.107.68.173	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
172.206.179.201	unknown	United States		18747	IFX18747US	false
184.82.217.184	unknown	Thailand		133481	AIS-FIBRE-AS-APAISFibreTH	false
94.252.43.143	unknown	Luxembourg		56665	TANGO-TELINDUSLU	false
85.130.194.40	unknown	Israel		8551	BEZEQ-INTERNATIONAL-ASBezeqintInternetBackboneIL	false
5.141.203.182	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
31.225.15.194	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
184.45.199.248	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
197.69.172.170	unknown	South Africa		16637	MTNNS-ASZA	false
112.161.236.248	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
94.25.27.81	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
41.22.234.51	unknown	South Africa		29975	VODACOM-ZA	false
184.118.189.159	unknown	United States		7922	COMCAST-7922US	false
31.24.164.137	unknown	Netherlands		200831	MIHOSNETNL	false

Runtime Messages

Command:	/tmp/QtNnZoNz75
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	kebabware installed
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
T-MOBILE-AS21928US	gbk4XWulUo	Get hash	malicious	Browse	• 172.51.68.68
	8MPbeDAwwZ	Get hash	malicious	Browse	• 172.48.74.209
	Xs0PMn85CN	Get hash	malicious	Browse	• 100.223.41.12
	Tsunami.x86	Get hash	malicious	Browse	• 172.50.129.160
	Tsunami.arm7	Get hash	malicious	Browse	• 172.32.220.75
	Tsunami.arm	Get hash	malicious	Browse	• 172.48.74.201
	x86	Get hash	malicious	Browse	• 208.55.26.159

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	zouBbQwUTb	Get hash	malicious	Browse	• 172.51.93.43
	0r73kbzSGC	Get hash	malicious	Browse	• 100.204.63.154
	PpZvxl4DJg	Get hash	malicious	Browse	• 100.218.62.91
	9QPGr9LMaq	Get hash	malicious	Browse	• 100.169.45.232
	dqnskKAmQq	Get hash	malicious	Browse	• 100.187.166.234
	jJ6GK5qbZt	Get hash	malicious	Browse	• 172.59.43.117
	st2AAeCXsR	Get hash	malicious	Browse	• 172.53.135.96
	arm7	Get hash	malicious	Browse	• 172.51.44.42
	mdyu2wtnR8	Get hash	malicious	Browse	• 172.59.61.178
	GQM8qzLfFs	Get hash	malicious	Browse	• 100.172.227.209
	6NzbU4oW61	Get hash	malicious	Browse	• 100.221.177.246
	GvPilhzmX1	Get hash	malicious	Browse	• 100.195.157.51
	sora.arm	Get hash	malicious	Browse	• 162.179.208.125
FANAVA-ASFanavaGroupCommunicationCoIR	Dy4UCGJRnG	Get hash	malicious	Browse	• 95.38.211.201
	5odXR1ZmTd	Get hash	malicious	Browse	• 95.38.211.211
	jew.arm7	Get hash	malicious	Browse	• 78.157.47.106
	jew.arm7	Get hash	malicious	Browse	• 95.38.171.194
	wL8CswnbUJ	Get hash	malicious	Browse	• 95.38.211.224
	Tsunami.arm7	Get hash	malicious	Browse	• 95.38.211.227
	mA7WUZVyyP	Get hash	malicious	Browse	• 95.38.211.222
	PTn4GPy1jh	Get hash	malicious	Browse	• 95.38.211.253
	qLadwVPkMz	Get hash	malicious	Browse	• 95.38.211.219
	CxPvMBx5Uj	Get hash	malicious	Browse	• 95.38.211.204
	RBXY9MffiU	Get hash	malicious	Browse	• 95.38.211.212
	aG1mulwSeH	Get hash	malicious	Browse	• 95.38.211.212
	yeeted.arm7	Get hash	malicious	Browse	• 87.107.232.244
	LDit8hIL8X	Get hash	malicious	Browse	• 95.38.211.214
	mjzvlwau	Get hash	malicious	Browse	• 87.107.232.213
	http://sjmm.2.vu/vv	Get hash	malicious	Browse	• 78.157.40.245
	http://https://surl.me/117k	Get hash	malicious	Browse	• 78.157.43.149
	mssecsvc.exe	Get hash	malicious	Browse	• 95.38.33.251
	http://iranfanavar.com/Copy_Invoice/zHkL-zO4_FLnSagoRP-Ke/	Get hash	malicious	Browse	• 164.215.130.74
TELIANET-SWEDENTeliaCompanySE	S13B4aCa4E	Get hash	malicious	Browse	• 95.204.92.3
	x86	Get hash	malicious	Browse	• 90.230.133.93
	arm7	Get hash	malicious	Browse	• 95.205.178.15
	WnhlYWJ5C5	Get hash	malicious	Browse	• 95.205.130.71
	nUDLlJvoP4	Get hash	malicious	Browse	• 95.205.130.34
	RVG73cR3DP	Get hash	malicious	Browse	• 95.192.7.112
	A0Pvsxsjf7	Get hash	malicious	Browse	• 95.205.130.98
	5odXR1ZmTd	Get hash	malicious	Browse	• 95.205.105.97
	hvYTLlrdRm	Get hash	malicious	Browse	• 90.233.95.70
	2pPPNW1XSo	Get hash	malicious	Browse	• 81.235.23.38
	st2AAeCXsR	Get hash	malicious	Browse	• 78.68.4.139
	egd7wSpaw2	Get hash	malicious	Browse	• 217.209.19.44
	txwaNf62fv	Get hash	malicious	Browse	• 157.180.240.240
	apep.arm7	Get hash	malicious	Browse	• 95.192.7.116
	db0fa4b8db0333367e9bda3ab68b8042.x86	Get hash	malicious	Browse	• 2.255.34.221
	MPnFvIsvJp	Get hash	malicious	Browse	• 81.235.47.61
	sora.arm	Get hash	malicious	Browse	• 78.66.23.17
	bqrHRKVNod	Get hash	malicious	Browse	• 213.65.26.65
	hWT9RJDotD	Get hash	malicious	Browse	• 2.253.167.75
	fzkfNBkz1C	Get hash	malicious	Browse	• 78.64.70.0

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	10
Entropy (8bit):	2.9219280948873623
Encrypted:	false
SSDEEP:	3:5bkPn:pkP
MD5:	FF001A15CE15CF062A3704CEA2991B5F
SHA1:	B06F6855F376C3245B82212AC73ADED55DFE5DEF
SHA-256:	C54830B41ECFA1B6FBDC30397188DDA86B7B200E62AEAC21AE694A6192DCC38A
SHA-512:	65EBF7C31F6F65713CE01B38A112E97D0AE64A6BD1DA40CE4C1B998F10CD3912EE1A48BB2B279B24493062118AAB3B8753742E2AF28E56A31A7AAB27DE80E7BF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	auto_null.

/home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	18
Entropy (8bit):	3.4613201402110088
Encrypted:	false
SSDEEP:	3:5bkrIZsXvn:pkckv
MD5:	28FE6435F34B3367707BB1C5D5F6B430
SHA1:	EB8FE2D16BD6BBCCE106C94E4D284543B2573CF6
SHA-256:	721A37C69E555799B41D308849E8F8125441883AB021B723FED90A9B744F36C0
SHA-512:	6B6AB7C0979629D0FEF6BE47C5C6BCC367EDD0AAE3FC973F4DE2FD5F0A819C89E7656DB65D453B1B5398E54012B27EDFE02894AD87A7E0AF3A9C5F2EB24A919
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	auto_null.monitor.

/proc/5611/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):	1.9219280948873623
Encrypted:	false

/run/sshd.pid

SSDEEP:	3:G9:G9
MD5:	9BDB73B4AB00EEB5150A78B758D8C6C2
SHA1:	755C5F5F5AF3196B5120CDCB4FE39C20A33037C1
SHA-256:	C05A5BCCB0FA554C3A9257002D8827119501E8B3FAAF2000970B0C4FB027C88C
SHA-512:	0971C873D34BD3A598F8E58BA9C588B653B62E1F689BC9C2FB933E0BCF62C726F1EEEABEE96FC6756E9F2A3838229A9330CA7BE2323B4FA93C9961B8EF057A6 1
Malicious:	false
Reputation:	low
Preview:	 5611.

/run/systemd/inhibit/.#4vGW7qo

Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	143
Entropy (8bit):	5.109910338925392
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMs/eWJAAVu9ifSU1IppTMXSHK72X8/SflY:SbFuFyL8OAApfZApLHK7wRS
MD5:	E374D3E418E44E444D586B8A667BA7B9
SHA1:	10E313EA3C86F242B0921AB80E794817F858DE3C
SHA-256:	E3C381103F615FE4A0F85F9F07DBD40A4E8DB91EAA187D48472C7EEC6772C23C
SHA-512:	42AD26F8C651EF390A526392C492526AA81919D09085D7DB9A6DE067AADEE06AA8E908638667AFAE1A79F2C632E430868E9D87D36BF45DE0E708BFE83993E99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	 # This is private data. Do not parse..WHAT=sleep.MODE=delay.UID=0.PID=1599.WHO=UPower.WHY=Pause device polling.FIFO=/run/systemd/inhibit/4.ref.

/run/systemd/resolve/.#resolv.confH13lrd

Process:	/lib/systemd/systemd-resolved
File Type:	ASCII text
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.60400988248083
Encrypted:	false
SSDEEP:	12:q4djH9R2vbcAS5wtRZ6F5j9oA/7gc5LcmnFQ1X6BCQ9OgXX2TcgvArHW:qmmIz07IuKD24CUB3Og2Tca
MD5:	DAC2BDC6F091CE9ED180809307F777AE
SHA1:	3A8F59FD68419F9C574C3A9D04E3AA76D6343EC1
SHA-256:	4EF31D415ECE44921919EFA070C04F3F43945336D75D4C1E7354637BCD20DCDD
SHA-512:	F23E4320950F84461552D438F264B17DEB2747061FD13F8A435DAF810E53CBCDAC77122A2B7382DE484931D469EDEF4A52C19EEDB01CEFD5A63D4AB7B6DB26 0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	 # This file is managed by man:systemd-resolved(8). Do not edit..#.# This is a dynamic resolv.conf file for connecting local clients directly to.# all known uplink DNS ser vers. This file lists all configured search domains..#.# Third party programs must not access this file directly, but only through the.# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,.# replace this symlink by a static file or a different symlink..#.# See man:systemd-resolved.service(8) for details about the supported modes of.# operation for /etc/resolv.conf...nameserver 1.1.1.1.nameserver 8.8.8.8.

/run/systemd/resolve/.#stub-resolv.confXxZgNf

Process:	/lib/systemd/systemd-resolved
File Type:	ASCII text
Category:	dropped
Size (bytes):	717
Entropy (8bit):	4.618141658133841
Encrypted:	false
SSDEEP:	12:q4djH9R2vbcAYEcWcXxRdxwlvj+ScH6F5j9oA/7gc5LcmnFQ1X6BCQ9OgXX2TcgF:qmmIREPcXxnxwIRcHIuKD24CUB3Og2TX
MD5:	FBFDE622AE28A4DCFBF73A397A10C6AE
SHA1:	E6B5915B590FC5A4FB484D2E456E76466DB7BD17
SHA-256:	DBEFE28051828B529E2299A83A76F268A8CF9FE686B1FA09DEC61F7AB1222658
SHA-512:	C966F0F8483378A55654A40B2ED05F1C4057D11BBB8C83D4BAA9921460C8028CF71FCA2E08DAFAB2C7C421FCDBDD7ABD78BF951DC2D9416547A5579E925CC F0
Malicious:	false
Reputation:	moderate, very likely benign file

/run/systemd/resolve/.#stub-resolv.confXxZgNf	
Preview:	# This file is managed by man:systemd-resolved(8). Do not edit..#.# This is a dynamic resolv.conf file for connecting local clients to the.# internal DNS stub resolver of systemd-resolved. This file lists all.# configured search domains..#.# Run "resolvectl status" to see details about the uplink DNS servers.# currently in use..#.# Third party programs must not access this file directly, but only through the.# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,.# replace this symlink by a static file or a different symlink..#.# See man:systemd-resolved.service(8) for details about the supported modes of.# operation for /etc/resolv.conf...nameserver 127.0.0.53.options edns0 trust-ad.

/run/systemd/seats/.#seat0U9R6fq	
Process:	/lib/systemd/systemd-logind
File Type:	ASCII text
Category:	dropped
Size (bytes):	95
Entropy (8bit):	4.921230646592726
Encrypted:	false
SSDEEP:	3:SbFVVmFyinKMsuH47rLg205vmLUbr+v:SbFuFyLwH47Pg20ggWv
MD5:	BE58CCABC942125F5E27AF6EB1BA2F88
SHA1:	07C20F55E36EE48869B223B8FC4DBC227C7353AC
SHA-256:	551B1D1C8E5953D5D0CF49C83C1568E2FBEF8BDDB69903B3DA82240B777B4629
SHA-512:	E5A270995FDE80530927E0BACD3BF76EE820C968AABD55D2E34579326F388AFD6DE7FB8C5D54F69D3F6AC30A5B587FD3B0456FC60326E7DF4F45789A900D046C
Malicious:	false
Preview:	# This is private data. Do not parse..IS_SEAT0=1.CAN_MULTI_SESSION=1.CAN_TTY=1.CAN_GRAPHICAL=0.

/run/user/1000/pulse/pid	
Process:	/usr/bin/pulseaudio
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.5219280948873621
Encrypted:	false
SSDEEP:	3:P:P
MD5:	E5551C7CEB360246793FEB483612E3F7
SHA1:	C63367AD165600AABDD1C574B992ADA67C56741C
SHA-256:	2C9F910541B11F5D89D7F8B9AF827D9017B9250944BFCF91BFB5AD4C028F332C
SHA-512:	DB97B1DD691B0A992DF510D6BD2D4DE6EFD277144B53C18FD8FB9D81578F4E5940B998FFE8886532907429894073OD83CF34BDBA18717875E56F6F7CC2DB2EA
Malicious:	false
Preview:	6006.

Static File Info

General

File type:	ELF 32-bit MSB executable, SPARC, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.189140212446064
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	QtNnZoNz75
File size:	74800
MD5:	9afa6f4cec8bd12babd83a6fb5211599
SHA1:	10efbc551846704ec95bd696b88da60d0ce3412a
SHA256:	0faa53c63781c3f54c5ac52fa4a454e7f6e5d92f7021b9577ef9617850630dab
SHA512:	62dfbadc14140208b17a6d1095a6f9150fd500e8023121013a8b3a760aad5c9676bc4bd504608d7629c137535746f7a8fdc54ffc360c4b14fb1c3175d14c2d77
SSDEEP:	1536:sJm8X/xO8cNJZtVydvpbLvGRB+oy+l8qVba:oPsY59rGRy+lG
File Content Preview:	.ELF.....4..".....4. ...(.....h...h.....@..(....@.B.....#.....b`..`.....!..... ...@....."........`.....$ ... ...@.. ..... `....

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:	74400
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	0x1083c	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x208ec	0x108ec	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x20900	0x10900	0x1668	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x32000	0x12000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x32008	0x12008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x32018	0x12018	0x248	0x0	0x3	WA	0	0	8
.bss	NOBITS	0x32260	0x12260	0x540	0x0	0x3	WA	0	0	8
.shstrtab	STRTAB	0x0	0x12260	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	0x11f68	0x11f68	3.6076	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x12000	0x32000	0x32000	0x260	0x7a0	1.7653	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

TCP Packets

System Behavior

Analysis Process: QtNnZoNz75 PID: 5235 Parent PID: 5113

General

Start time:	05:42:52
Start date:	01/11/2021
Path:	/tmp/QtNnZoNz75
Arguments:	/tmp/QtNnZoNz75
File size:	4379400 bytes

MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Analysis Process: QtNnZoNz75 PID: 5237 Parent PID: 5235

General

Start time:	05:42:52
Start date:	01/11/2021
Path:	/tmp/QtNnZoNz75
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QtNnZoNz75 PID: 5239 Parent PID: 5237

General

Start time:	05:42:52
Start date:	01/11/2021
Path:	/tmp/QtNnZoNz75
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QtNnZoNz75 PID: 5240 Parent PID: 5237

General

Start time:	05:42:52
Start date:	01/11/2021
Path:	/tmp/QtNnZoNz75
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QtNnZoNz75 PID: 5242 Parent PID: 5237

General

Start time:	05:42:53
Start date:	01/11/2021
Path:	/tmp/QtNnZoNz75
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QtNnZoNz75 PID: 5244 Parent PID: 5237

General

Start time:	05:42:53
Start date:	01/11/2021
Path:	/tmp/QtNnZoNz75
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QtNnZoNz75 PID: 5246 Parent PID: 5237

General

Start time:	05:42:53
Start date:	01/11/2021
Path:	/tmp/QtNnZoNz75
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QtNnZoNz75 PID: 5248 Parent PID: 5237

General

Start time:	05:42:53
Start date:	01/11/2021
Path:	/tmp/QtNnZoNz75
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QtNnZoNz75 PID: 5249 Parent PID: 5237

General

Start time:	05:42:53
Start date:	01/11/2021
Path:	/tmp/QtNnZoNz75
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: QtNnZoNz75 PID: 5250 Parent PID: 5237

General

Start time:	05:42:53
Start date:	01/11/2021
Path:	/tmp/QtNnZoNz75
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5276 Parent PID: 1

General

Start time:	05:42:57
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5276 Parent PID: 1

General

Start time:	05:42:57
Start date:	01/11/2021
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: 5277 Parent PID: 1

General

Start time:	05:42:58
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-resolved PID: 5277 Parent PID: 1

General

Start time:	05:42:58
Start date:	01/11/2021
Path:	/lib/systemd/systemd-resolved
Arguments:	/lib/systemd/systemd-resolved
File size:	415968 bytes
MD5 hash:	c93bbc5e20248114c56896451eab7a8b

File Activities

File Deleted

File Read

File Written

Permission Modified

Analysis Process: systemd PID: 5544 Parent PID: 1

General

Start time:	05:42:58
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-logind PID: 5544 Parent PID: 1

General

Start time:	05:42:58
Start date:	01/11/2021
Path:	/lib/systemd/systemd-logind
Arguments:	/lib/systemd/systemd-logind
File size:	268576 bytes
MD5 hash:	8dd58a1b4c12f7a1d5fe3ce18b2aaeef

File Activities

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: systemd PID: 5611 Parent PID: 1

General

Start time:	05:42:58
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5611 Parent PID: 1

General

Start time:	05:42:58
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: gdm3 PID: 5633 Parent PID: 1320

General

Start time:	05:42:58
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5633 Parent PID: 1320

General

Start time:	05:42:58
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gdm3 PID: 5649 Parent PID: 1320

General

Start time:	05:42:58
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5649 Parent PID: 1320

General

Start time:	05:42:58
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: xfce4-session PID: 5666 Parent PID: 1900

General

Start time:	05:42:59
Start date:	01/11/2021
Path:	/usr/bin/xfce4-session
Arguments:	n/a
File size:	264752 bytes
MD5 hash:	648919f03ad356720c8c27f5aaaf75d1

Analysis Process: rm PID: 5666 Parent PID: 1900

General

Start time:	05:42:59
Start date:	01/11/2021
Path:	/usr/bin/rm
Arguments:	rm -f /home/saturnino/.cache/sessions/Thunar-2ec9153f1-6fa0-4067-96b1-e5fe875b1e51
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: systemd PID: 5791 Parent PID: 1

General

Start time:	05:43:02
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5791 Parent PID: 1

General

Start time:	05:43:02
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Analysis Process: systemd PID: 5894 Parent PID: 1

General

Start time:	05:43:02
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5894 Parent PID: 1

General

Start time:	05:43:02
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Analysis Process: systemd PID: 5967 Parent PID: 1

General

Start time:	05:43:03
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5967 Parent PID: 1

General

Start time:	05:43:03
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Analysis Process: systemd PID: 5968 Parent PID: 1

General

Start time:	05:43:03
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5968 Parent PID: 1

General

Start time:	05:43:03
Start date:	01/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Analysis Process: gdm3 PID: 5979 Parent PID: 1320

General

Start time:	05:43:23
Start date:	01/11/2021
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5979 Parent PID: 1320

General

Start time:	05:43:23
Start date:	01/11/2021
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: xfce4-session PID: 5982 Parent PID: 1900

General

Start time:	05:43:23
Start date:	01/11/2021
Path:	/usr/bin/xfce4-session
Arguments:	n/a
File size:	264752 bytes
MD5 hash:	648919f03ad356720c8c27f5aaaf75d1

Analysis Process: xfwm4 PID: 5982 Parent PID: 1900

General

Start time:	05:43:23
Start date:	01/11/2021
Path:	/usr/bin/xfwm4
Arguments:	xfwm4 --display :1.0 --sm-client-id 2389ab8d9-421f-49fc-90ad-c6cc4c15ac4c
File size:	420424 bytes
MD5 hash:	59defa3c00cc30d85ed77b738d55e9da

File Activities

File Read

Analysis Process: xfce4-session PID: 5983 Parent PID: 1900

General

Start time:	05:43:23
Start date:	01/11/2021
Path:	/usr/bin/xfce4-session
Arguments:	n/a
File size:	264752 bytes
MD5 hash:	648919f03ad356720c8c27f5aaaf75d1

Analysis Process: xfce4-panel PID: 5983 Parent PID: 1900

General

Start time:	05:43:23
Start date:	01/11/2021
Path:	/usr/bin/xfce4-panel

Arguments:	xfce4-panel --display :1.0 --sm-client-id 2b4cc744e-8b9d-436f-9a4a-312b40faa2ec
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: systemd PID: 6006 Parent PID: 1860

General

Start time:	05:43:24
Start date:	01/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 6006 Parent PID: 1860

General

Start time:	05:43:24
Start date:	01/11/2021
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

File Activities

File Read

File Written

Directory Enumerated

Directory Created