ID: 518058
Sample Name: wsVomvavHj
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 23:15:38
Date: 08/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

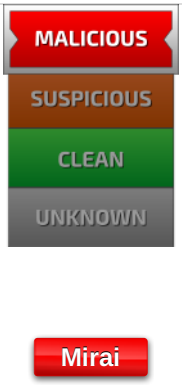
Linux Analysis Report wsVomvavHj

Overview

General Information

Sample Name:	wsVomvavHj
Analysis ID:	518058
MD5:	298cb9165abc05..
SHA1:	c168f1467498ad0.
SHA256:	1676dd00e2747f4.
Tags:	32 elf mirai motorola
Infos:	

Detection

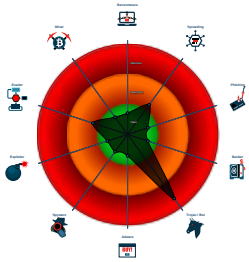


Score:	88
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Malicious sample detected (through ...
- Connects to many ports of the same...
- Uses known network protocols on no...
- Yara signature match
- Uses the "uname" system call to qu...
- Enumerates processes within the "p...
- Detected TCP or UDP traffic on non...
- Sample listens on a socket
- Sample tries to kill a process (SIGK...

Classification



Analysis Advice

Some HTTP requests failed (404). It is likely the sample will exhibit less behavior

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:	518058
Start date:	08.11.2021
Start time:	23:15:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wsVomvavHj
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:	mal88.troj.lin@0/2@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- wsVomvavHj (PID: 5240, Parent: 5117, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/wsVomvavHj
  - wsVomvavHj New Fork (PID: 5242, Parent: 5240)
    - wsVomvavHj New Fork (PID: 5384, Parent: 5242)
    - wsVomvavHj New Fork (PID: 5386, Parent: 5242)
      - wsVomvavHj New Fork (PID: 5388, Parent: 5386)
        - wsVomvavHj New Fork (PID: 5421, Parent: 5388)
        - wsVomvavHj New Fork (PID: 5422, Parent: 5388)
        - wsVomvavHj New Fork (PID: 5424, Parent: 5388)
      - wsVomvavHj New Fork (PID: 5389, Parent: 5386)
      - wsVomvavHj New Fork (PID: 5392, Parent: 5386)
      - wsVomvavHj New Fork (PID: 5393, Parent: 5386)
      - wsVomvavHj New Fork (PID: 5394, Parent: 5386)
      - wsVomvavHj New Fork (PID: 5397, Parent: 5386)
      - wsVomvavHj New Fork (PID: 5399, Parent: 5386)
      - wsVomvavHj New Fork (PID: 5400, Parent: 5386)
    - wsVomvavHj New Fork (PID: 5243, Parent: 5240)
    - wsVomvavHj New Fork (PID: 5244, Parent: 5240)
      - wsVomvavHj New Fork (PID: 5248, Parent: 5244)
        - wsVomvavHj New Fork (PID: 5405, Parent: 5248)
        - wsVomvavHj New Fork (PID: 5406, Parent: 5248)
        - wsVomvavHj New Fork (PID: 5408, Parent: 5248)
        - wsVomvavHj New Fork (PID: 5409, Parent: 5248)
        - wsVomvavHj New Fork (PID: 5412, Parent: 5248)
        - wsVomvavHj New Fork (PID: 5413, Parent: 5248)
        - wsVomvavHj New Fork (PID: 5414, Parent: 5248)
      - wsVomvavHj New Fork (PID: 5249, Parent: 5244)
      - wsVomvavHj New Fork (PID: 5254, Parent: 5244)
      - wsVomvavHj New Fork (PID: 5255, Parent: 5244)
- systemd New Fork (PID: 5280, Parent: 1)
- sshd (PID: 5280, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5281, Parent: 1)
- sshd (PID: 5281, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
wsVomvavHj	MAL_ELF_LNX_Mirai_Oct10_1	Detects ELF Mirai variant	Florian Roth	• 0x1d26b:$x2: /bin/busybox chmod 777 * /tmp/ • 0x1cfd4:$s1: POST /ctrlt/DeviceUpgrade_1 HTTP/1.1
wsVomvavHj	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

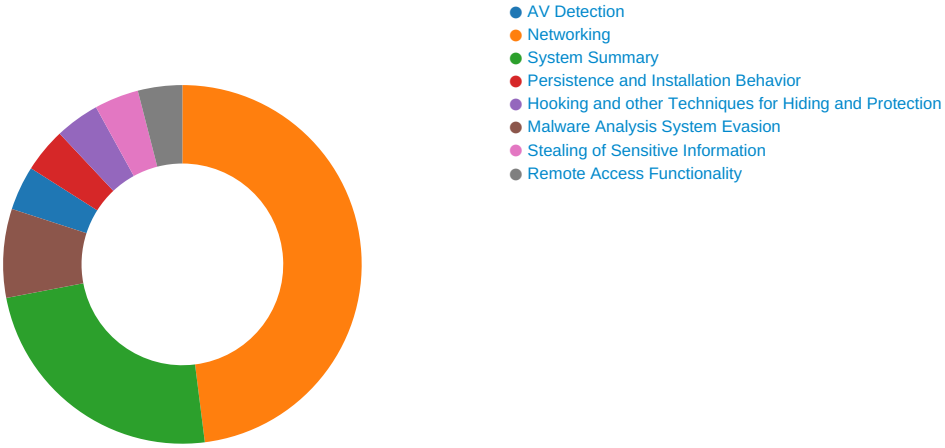
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5240.1.00000000f463d34a.00000000206d7a94.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_1	Detects ELF Mirai variant	Florian Roth	• 0x1d26b:$x2: /bin/busybox chmod 777 * /tmp/ • 0x1cfd4:$s1: POST /ctrlt/DeviceUpgrade_1 HTTP/1.1
5240.1.00000000f463d34a.00000000206d7a94.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5243.1.00000000f463d34a.00000000206d7a94.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_1	Detects ELF Mirai variant	Florian Roth	• 0x1d26b:$x2: /bin/busybox chmod 777 * /tmp/ • 0x1cfd4:$s1: POST /ctrlt/DeviceUpgrade_1 HTTP/1.1
5243.1.00000000f463d34a.00000000206d7a94.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5242.1.00000000f463d34a.00000000206d7a94.r-x.sdmp	MAL_ELF_LNX_Mirai_Oct10_1	Detects ELF Mirai variant	Florian Roth	• 0x1d26b:$x2: /bin/busybox chmod 777 * /tmp/ • 0x1cfd4:$s1: POST /ctrlt/DeviceUpgrade_1 HTTP/1.1
Click to see the 3 entries				

Jbx Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

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

Connects to many ports of the same IP (likely port scanning)

Uses known network protocols on non-standard ports

System Summary:

Malicious sample detected (through community Yara rule)

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

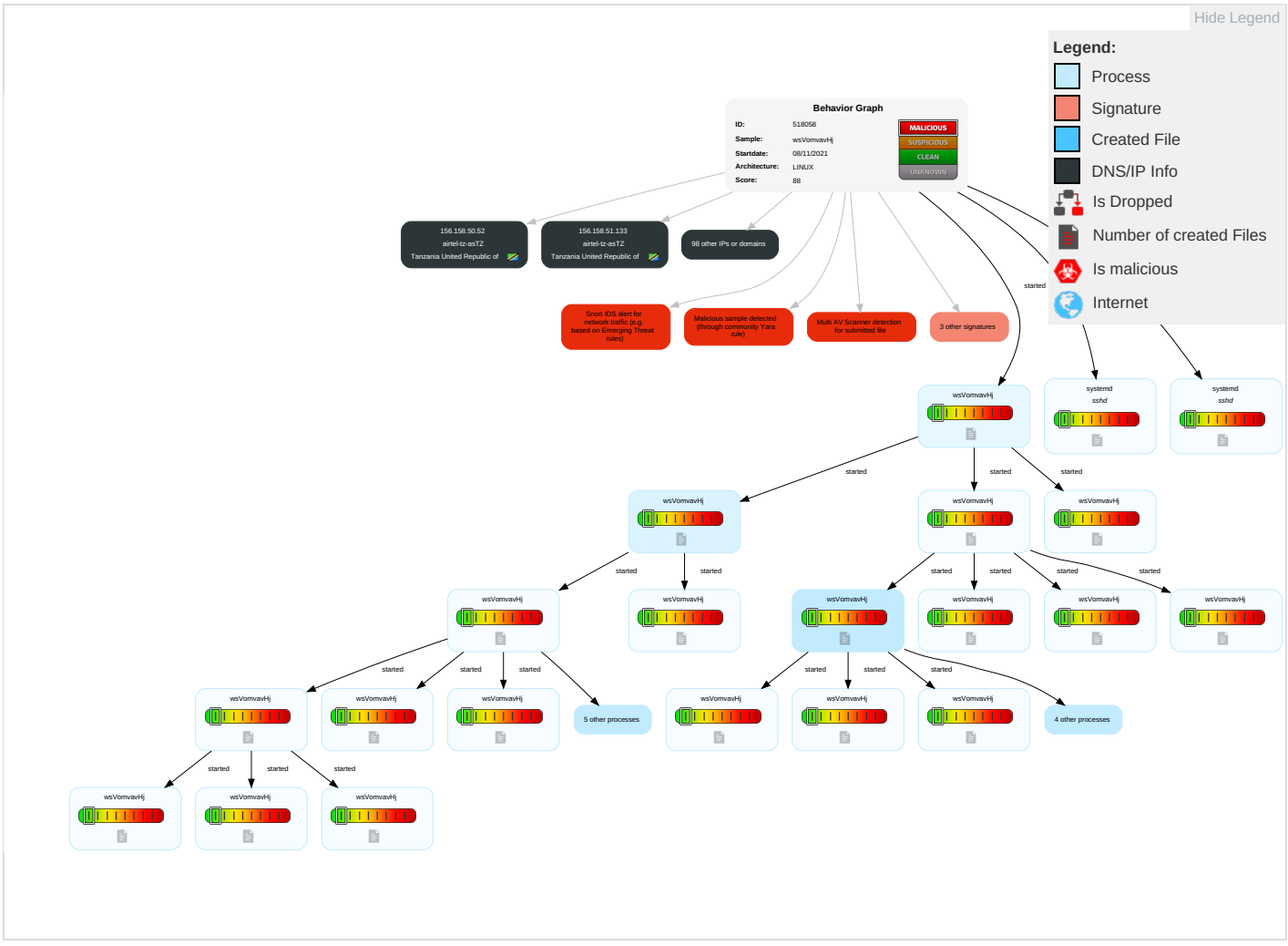
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct 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 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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 4	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Ingress Tool Transfer 3	Manipulate Device Communication		Manipu App Sto Rankin or Ratir

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
wsVomvavHj	48%	Virustotal		Browse
wsVomvavHj	42%	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://209.141.42.149/bins/os.x86	15%	Virustotal		Browse
http://209.141.42.149/bins/os.x86	100%	Avira URL Cloud	malware	
http://209.141.42.149/bins/os.arm7;chmod	0%	Avira URL Cloud	safe	
http://209.141.42.149/bins/sora.x86	17%	Virustotal		Browse
http://209.141.42.149/bins/sora.x86	100%	Avira URL Cloud	malware	
http://127.0.0.1/cgi-bin/ViewLog.asp	0%	Avira URL Cloud	safe	
http://127.0.0.1:52869/wanipcn.xml	0%	Avira URL Cloud	safe	
http://209.141.42.149/sh%20-O%20-%3E%20/tmp/kh;sh%20/tmp/kh%27$	0%	Avira URL Cloud	safe	
http://purenetworks.com/HNAP1/	0%	URL Reputation	safe	
http://209.141.42.149/bins/os.mips	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:52869/picdesc.xml	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://127.0.0.1/cgi-bin/ViewLog.asp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:52869/wanipcn.xml	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
78.54.40.243	unknown	Germany		6805	TDDE-ASN1DE	false
207.141.211.147	unknown	United States		2386	INS-ASUS	false
149.197.143.228	unknown	Finland		1759	TSF-IP-CORETeliaFinlandOyjEU	false
39.180.65.71	unknown	China		56041	CMNET-ZHEJIANG-APChinaMobilecommunicationscorporationC	false
206.134.246.45	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
134.45.110.33	unknown	United States		395226	SACRAMENTO-COEUS	false
37.124.245.227	unknown	Saudi Arabia		35819	MOBILY-ASEtihadEtisalatCompanyMobilySA	false
41.102.161.61	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.237.248.167	unknown	Kenya		15399	WANANCHI-KE	false
156.5.232.58	unknown	United States		29975	VODACOM-ZA	false
79.21.13.227	unknown	Italy		3269	ASN-IBSNAZIT	false
192.184.132.99	unknown	United States		7065	SONOMAUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
86.179.34.195	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
112.13.87.15	unknown	China		56041	CMNET-ZHEJIANG-APChinaMobilecommunicationscorporationC	false
58.112.88.160	unknown	Japan		9595	XEPHIONNTT-MECorporationJP	false
37.35.168.88	unknown	Spain		12479	UNI2-ASES	false
197.118.32.216	unknown	Algeria		36947	ALGTEL-ASDZ	false
156.5.207.96	unknown	United States		29975	VODACOM-ZA	false
206.246.191.214	unknown	United States		7332	LIGHTBOUND-ASUS	false
181.175.18.85	unknown	Ecuador		14522	SatnetEC	false
200.194.14.170	unknown	Mexico		6503	AxtelSABdeCVMX	false
212.182.231.71	unknown	Finland		1759	TSF-IP-CORETeliaFinlandOyjEU	false
181.74.231.14	unknown	Chile		6535	TelmexServiciosEmpresarialesSACL	false
200.209.218.212	unknown	Brazil		4230	CLAROSABR	false
197.200.123.7	unknown	Algeria		36947	ALGTEL-ASDZ	false
156.130.158.133	unknown	United States		29975	VODACOM-ZA	false
206.18.18.133	unknown	United States		4265	CERNET-ASN-BLOCKUS	false
197.211.66.47	unknown	South Africa		29918	IMPOL-ASNZA	false
156.79.67.34	unknown	United States		11363	FUJITSU-USAUS	false
76.137.238.137	unknown	United States		7922	COMCAST-7922US	false
178.129.91.30	unknown	Russian Federation		28812	JSCBIS-ASRU	false
217.213.219.141	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
101.242.68.60	unknown	China		17429	BGCTVNETBEIJINGGEHUACATVNETWORKCOLTDCN	false
60.38.65.61	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
94.227.194.72	unknown	Belgium		6848	TELENET-ASBE	false
200.48.112.85	unknown	Peru		6147	TelefonicadelPeruSAAPE	false
82.177.144.70	unknown	Poland		206093	SILICON_SOFTWARE-ASPL	false
206.163.104.138	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
95.28.117.13	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
103.172.4.110	unknown	unknown		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
42.5.237.3	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
82.74.56.170	unknown	Netherlands		33915	TNF-ASNL	false
87.208.121.103	unknown	Netherlands		13127	VERSATELASfortheTrans-EuropeanTele2IPTransportbackbo	false
114.39.195.73	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
193.213.89.103	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
206.22.75.125	unknown	United States		7270	NET2PHONEUS	false
66.163.125.139	unknown	United States		29877	STS-TELECOM-AS-1US	false
112.70.224.21	unknown	Japan		17511	OPTAGEOPTAGEIncJP	false
197.60.107.91	unknown	Egypt		8452	TE-ASTE-ASEG	false
23.239.26.116	unknown	United States		63949	LINODE-APLinodeLLCUS	false
69.63.229.4	unknown	United States		14103	ACDNET-ASN1US	false
95.239.15.24	unknown	Italy		3269	ASN-IBSNAZIT	false
82.247.213.171	unknown	France		12322	PROXADFR	false
123.142.108.104	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
197.3.15.250	unknown	Tunisia		37705	TOPNETTN	false
156.43.68.63	unknown	United Kingdom		4211	ASN-MARICOPA1US	false
210.47.182.175	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
95.145.60.40	unknown	United Kingdom		12576	EELtdGB	false
156.158.51.133	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
181.81.244.11	unknown	Argentina		7303	TelecomArgentinaSAAR	false
156.164.16.3	unknown	Egypt		36992	ETISALAT-MISREG	false
44.179.130.197	unknown	United States		7377	UCSDUS	false
197.12.31.207	unknown	Tunisia		37703	ATLAXTN	false
203.153.200.75	unknown	Australia		38790	SPIRIT-TELECOMSpiritTelecomAustraliaPtyLtdAU	false
156.33.207.15	unknown	United States		3495	SENATE-ASUS	false
243.26.61.235	unknown	Reserved		unknown	unknown	false
189.151.224.69	unknown	Mexico		8151	UninetSAdeCVMX	false
80.55.180.249	unknown	Poland		5617	TPNETPL	false
168.4.133.156	unknown	United States		8	RICE-ASUS	false
172.36.187.102	unknown	United States		21928	T-MOBILE-AS21928US	false
122.140.177.239	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
90.69.108.105	unknown	France		12479	UNI2-ASES	false
246.112.160.176	unknown	Reserved		unknown	unknown	false
208.35.186.106	unknown	United States		10333	DIGITALINSIGHTUS	false
65.63.38.165	unknown	United States		32475	SINGLEHOP-LLCUS	false
181.31.213.37	unknown	Argentina		10318	TelecomArgentinaSAAR	false
197.163.185.209	unknown	Egypt		24863	LINKdotNET-ASEG	false
169.108.151.42	unknown	United States		37611	AfrihostZA	false
178.10.231.77	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
197.164.175.165	unknown	Egypt		24863	LINKdotNET-ASEG	false
206.124.141.215	unknown	United States		18530	ISOMEDIA-1US	false
197.12.117.170	unknown	Tunisia		37703	ATLAXTN	false
86.111.25.11	unknown	Russian Federation		6863	ROSNET-ASRU	false
213.249.241.144	unknown	United Kingdom		12390	KINGSTON-UK-ASGB	false
156.158.50.52	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
44.59.10.142	unknown	United States		7377	UCSDUS	false
142.30.156.245	unknown	Canada		3633	PROVINCE-OF-BRITISH-COLUMBIACA	false
213.136.10.210	unknown	Netherlands		12859	NL-BITBITBVNL	false
213.41.59.49	unknown	United Kingdom		8220	COLTCOLTTechnologyServicesGroupLimitedGB	false
169.11.83.210	unknown	United States		203	CENTURYLINK-LEGACY-LVLT-203US	false
163.246.206.184	unknown	United States		3512	EUSHCUS	false
148.237.106.189	unknown	Mexico		7325	UniversidadAutonomaDeTamaulipasMX	false
133.150.124.115	unknown	Japan		10021	KVHKVHCoLtdJP	false
54.56.4.159	unknown	United States		14618	AMAZON-AESUS	false
157.161.177.111	unknown	Switzerland		6772	IMPNET-ASCH	false
169.108.151.34	unknown	United States		37611	AfrihostZA	false
169.75.134.88	unknown	United States		37611	AfrihostZA	false
178.103.83.133	unknown	United Kingdom		12576	EELtdGB	false
5.167.132.112	unknown	Russian Federation		52207	TULA-ASRU	false
125.76.82.22	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false

Runtime Messages

Command:	/tmp/wsVomvavHj
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
156.130.158.133	1ahsk4RbWN	Get hash	malicious	Browse	
37.35.168.88	ieoZF9F4TX	Get hash	malicious	Browse	
197.118.32.216	1M4azHIecM	Get hash	malicious	Browse	
197.211.66.47	b3astmode.x86	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
INS-ASUS	FAuA0G2obM	Get hash	malicious	Browse	• 199.106.169.184
	cpnO27Hi5Q	Get hash	malicious	Browse	• 70.235.78.46
	rXFu2DZdQq	Get hash	malicious	Browse	• 12.150.44.16
	b3astmode.x86	Get hash	malicious	Browse	• 12.150.19.43
	sora.arm7	Get hash	malicious	Browse	• 148.66.241.179
	sora.arm7	Get hash	malicious	Browse	• 70.235.2.45
	mRQwOz6Oit	Get hash	malicious	Browse	• 12.203.209.102
	Antisocial.arm	Get hash	malicious	Browse	• 207.141.211.138
	OhUy3woBmb	Get hash	malicious	Browse	• 156.89.9.174
	heHfsavwfJ	Get hash	malicious	Browse	• 12.167.196.223
	5odXR1ZmTd	Get hash	malicious	Browse	• 207.141.211.180
	x86	Get hash	malicious	Browse	• 148.128.197.31
	JUZVpUSH0W	Get hash	malicious	Browse	• 70.235.30.87
	bKHI9UT0D1	Get hash	malicious	Browse	• 168.185.112.79
	IcwrPqGkXP	Get hash	malicious	Browse	• 155.2.116.79
	sora.arm	Get hash	malicious	Browse	• 168.184.223.154
	UZ4YNXCyrA	Get hash	malicious	Browse	• 155.2.141.19
	gSqIRpsggd	Get hash	malicious	Browse	• 12.183.21.131
	Z1JWqe0tZn	Get hash	malicious	Browse	• 70.235.2.30
	BXQb7BRQx7	Get hash	malicious	Browse	• 155.2.116.46
TDDE-ASN1DE	zF8n7qO4Uw	Get hash	malicious	Browse	• 77.188.86.243
	fCca2FJVXG	Get hash	malicious	Browse	• 85.182.12.252
	DDgJHmrtcG	Get hash	malicious	Browse	• 46.115.53.10
	zJqtqFt8jv	Get hash	malicious	Browse	• 188.46.136.222
	rXFu2DZdQq	Get hash	malicious	Browse	• 93.128.152.101
	IYcCOLfGT7	Get hash	malicious	Browse	• 62.54.189.154
	AjNJHZfSOB	Get hash	malicious	Browse	• 2.245.92.232
	F0ihkIMDf2	Get hash	malicious	Browse	• 2.240.233.152
	YYcy9gLbBC	Get hash	malicious	Browse	• 2.210.162.98
	rMwxCtXmuJ	Get hash	malicious	Browse	• 217.191.218.253
	uV1rj8v43F	Get hash	malicious	Browse	• 46.115.207.229
	xd.arm7	Get hash	malicious	Browse	• 89.15.98.110
	HdZIgkO5be	Get hash	malicious	Browse	• 77.179.253.44
	ApuXjs7iJm	Get hash	malicious	Browse	• 85.181.173.179
	sora.arm	Get hash	malicious	Browse	• 62.52.62.60
	sora.x86	Get hash	malicious	Browse	• 77.0.151.251
	MkyxPXGeTq	Get hash	malicious	Browse	• 95.115.114.33
	JVHk2b1Yd5	Get hash	malicious	Browse	• 95.113.123.130
	o6aMoZKsIK	Get hash	malicious	Browse	• 62.52.13.72
	oiHTZaiKnI	Get hash	malicious	Browse	• 78.51.163.147

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5281/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:Co:Co
MD5:	1C6FED73033E83DA4459F2B85AD247AF
SHA1:	1D5EAD879734D1A4D955D5D5757F174066A8338A
SHA-256:	E7FEBA5833BED3FD6D9DFA3BB41A893A6860BCFC4EF933CF0B6242BD23DCD586
SHA-512:	08864AD9F6AF98209C5CD159384EB87BDF2F1320F2E36CD554A31FBB58D23F553D8CCA537C1A5A61DE71383BA34A141BB9867A9F950B27F1BC08DAC18ADF197
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	5281.

Static File Info

General	
File type:	ELF 32-bit MSB executable, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.39992195099751
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	wsVomvavHj
File size:	128312
MD5:	298cb9165abc05a5b2652163b7f6b9c3
SHA1:	c168f1467498ad0d5be13813d9c58c651c633aab
SHA256:	1676dd00e2747f47313ffc8dc3da211534784b184f382e75399541fec0956da5
SHA512:	3a53c30e9f2aad61afef3636e7013f60fea53861444aabf9f347c8db302087bd587e7d3562267d463e6bfb7057820cd7b51322f892d5b522aba4f0b6884469c
SSDEEP:	1536:IpPZmsLVUwLMZLNMAsDHeWmc3eVMDJFwFKkwvy8tPixSBrTRRgzjXdJvVdXpAwU8:IbmsL1MZhMAFm3eVzFHwvx5rlRGlpfdf

General

File Content Preview:	.ELF.....D...4.....4. ...(..... .....l..f..... .dt.Q.....NV..a....da....t N^NuNV..J9...hf>"y.... QJ.g.X.#.....N."y.... QJ.f.A.....J.g. Hy....N.X.....hN^NuNV..N^NuN

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MC68000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x80000144
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	127912
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	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0x1c29e	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x8001c346	0x1c346	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x8001c354	0x1c354	0x2ca4	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x80020ffc	0x1effc	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x80021004	0x1f004	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x80021010	0x1f010	0x358	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x80021368	0x1f368	0x637c	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x1f368	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	0x80000000	0x80000000	0x1eff8	0x1eff8	4.5382	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0x1effc	0x80020ffc	0x80020ffc	0x36c	0x66e8	1.7844	0x6	RW	0x2000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

TCP Packets

HTTP Request Dependency Graph

- 127.0.0.1
- 127.0.0.1:52869

System Behavior

Analysis Process: wsVomvavHj PID: 5240 Parent PID: 5117

General

Start time:	23:16:20
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	/tmp/wsVomvavHj
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: wsVomvavHj PID: 5242 Parent PID: 5240

General

Start time:	23:16:20
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: wsVomvavHj PID: 5384 Parent PID: 5242

General

Start time:	23:19:22
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5386 Parent PID: 5242

General

Start time:	23:19:22
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj

Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5388 Parent PID: 5386

General

Start time:	23:19:22
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5421 Parent PID: 5388

General

Start time:	23:19:27
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5422 Parent PID: 5388

General

Start time:	23:19:27
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5424 Parent PID: 5388

General

Start time:	23:19:27
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5389 Parent PID: 5386

General

Start time:	23:19:22

Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5392 Parent PID: 5386

General

Start time:	23:19:23
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5393 Parent PID: 5386

General

Start time:	23:19:23
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5394 Parent PID: 5386

General

Start time:	23:19:23
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5397 Parent PID: 5386

General

Start time:	23:19:23
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5399 Parent PID: 5386

General

Start time:	23:19:23
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5400 Parent PID: 5386

General

Start time:	23:19:23
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5243 Parent PID: 5240

General

Start time:	23:16:20
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5244 Parent PID: 5240

General

Start time:	23:16:20
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5248 Parent PID: 5244

General

Start time:	23:16:20
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: wsVomvavHj PID: 5405 Parent PID: 5248

General

Start time:	23:19:23
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5406 Parent PID: 5248

General

Start time:	23:19:23
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5408 Parent PID: 5248

General

Start time:	23:19:23
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5409 Parent PID: 5248

General

Start time:	23:19:23
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5412 Parent PID: 5248

General

Start time:	23:19:23
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj

Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5413 Parent PID: 5248

General

Start time:	23:19:23
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5414 Parent PID: 5248

General

Start time:	23:19:23
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5249 Parent PID: 5244

General

Start time:	23:16:20
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5254 Parent PID: 5244

General

Start time:	23:16:20
Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: wsVomvavHj PID: 5255 Parent PID: 5244

General

Start time:	23:16:20

Start date:	08/11/2021
Path:	/tmp/wsVomvavHj
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: systemd PID: 5280 Parent PID: 1

General

Start time:	23:16:31
Start date:	08/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5280 Parent PID: 1

General

Start time:	23:16:31
Start date:	08/11/2021
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: 5281 Parent PID: 1

General

Start time:	23:16:31
Start date:	08/11/2021
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:	23:16:31
Start date:	08/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated