ID: 507447
Sample Name: IcwrPqGkXP
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 09:08:35
Date: 22/10/2021
Version: 33.0.0 White Diamond

Table of Contents

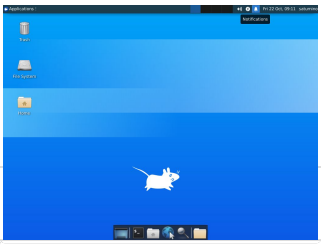
Linux Analysis Report IcwrPqGkXP

Overview

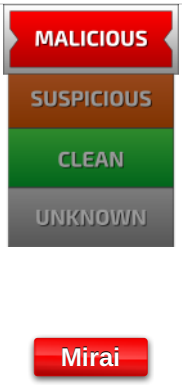
General Information

Sample Name:	IcwrPqGkXP
Analysis ID:	507447
MD5:	18fe913ce8856fc..
SHA1:	ff1494dd42dcda4..
SHA256:	dea614c4a0a319..
Tags:	32 elf mips mirai
Infos:	

Most interesting Screenshot:



Detection

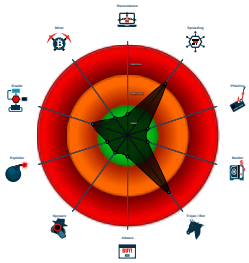


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Sample tries to kill many processes...
- 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

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

All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work

Static ELF header machine description suggests that the sample might not execute correctly on this machine

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	507447
Start date:	22.10.2021
Start time:	09:08:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IcwrPqGkXP
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.spre.troj.lin@0/6@0/0
Warnings:	Show All

Process Tree

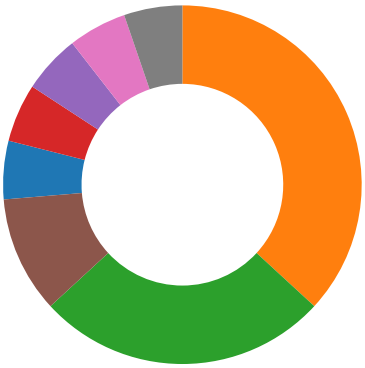
- **system is lnxubuntu20**
- IcwrPqGkXP (PID: 5250, Parent: 5121, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/IcwrPqGkXP
  - IcwrPqGkXP New Fork (PID: 5253, Parent: 5250)
  - IcwrPqGkXP New Fork (PID: 5254, Parent: 5250)
  - IcwrPqGkXP New Fork (PID: 5255, Parent: 5250)
    - IcwrPqGkXP New Fork (PID: 5259, Parent: 5255)
    - IcwrPqGkXP New Fork (PID: 5261, Parent: 5255)
    - IcwrPqGkXP New Fork (PID: 5263, Parent: 5255)
- systemd New Fork (PID: 5287, Parent: 1)
  - sshd (PID: 5287, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5290, Parent: 1)
  - sshd (PID: 5290, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 5404, Parent: 1)
  - sshd (PID: 5404, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5405, Parent: 1)
  - sshd (PID: 5405, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 5406, Parent: 1)
  - sshd (PID: 5406, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5407, Parent: 1)
  - sshd (PID: 5407, 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

System Summary:

Sample tries to kill many processes (SIGKILL)

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

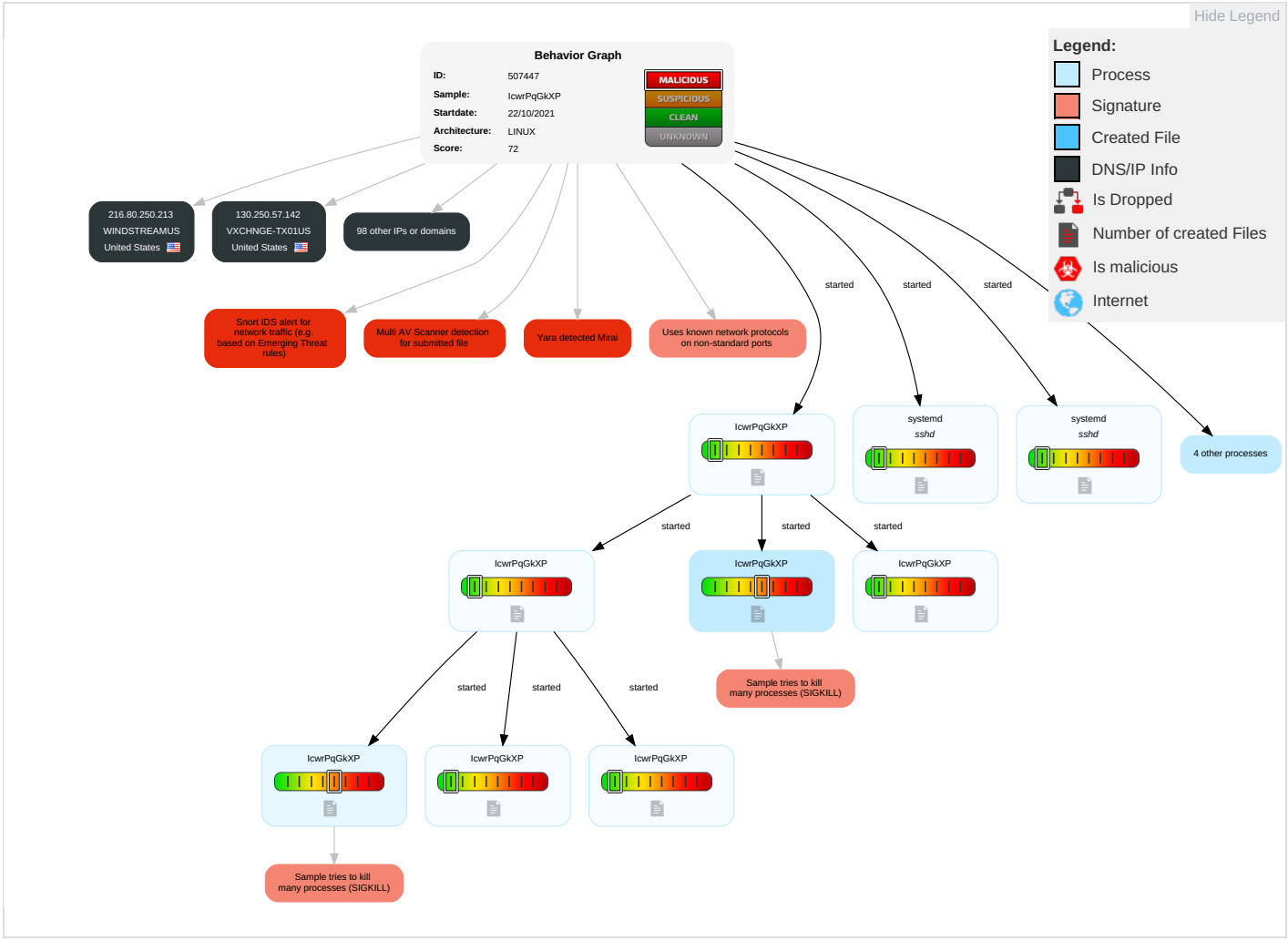
Mitre Att&ck Matrix

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

Malware Configuration

No configs have been found

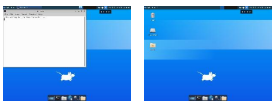
Behavior Graph

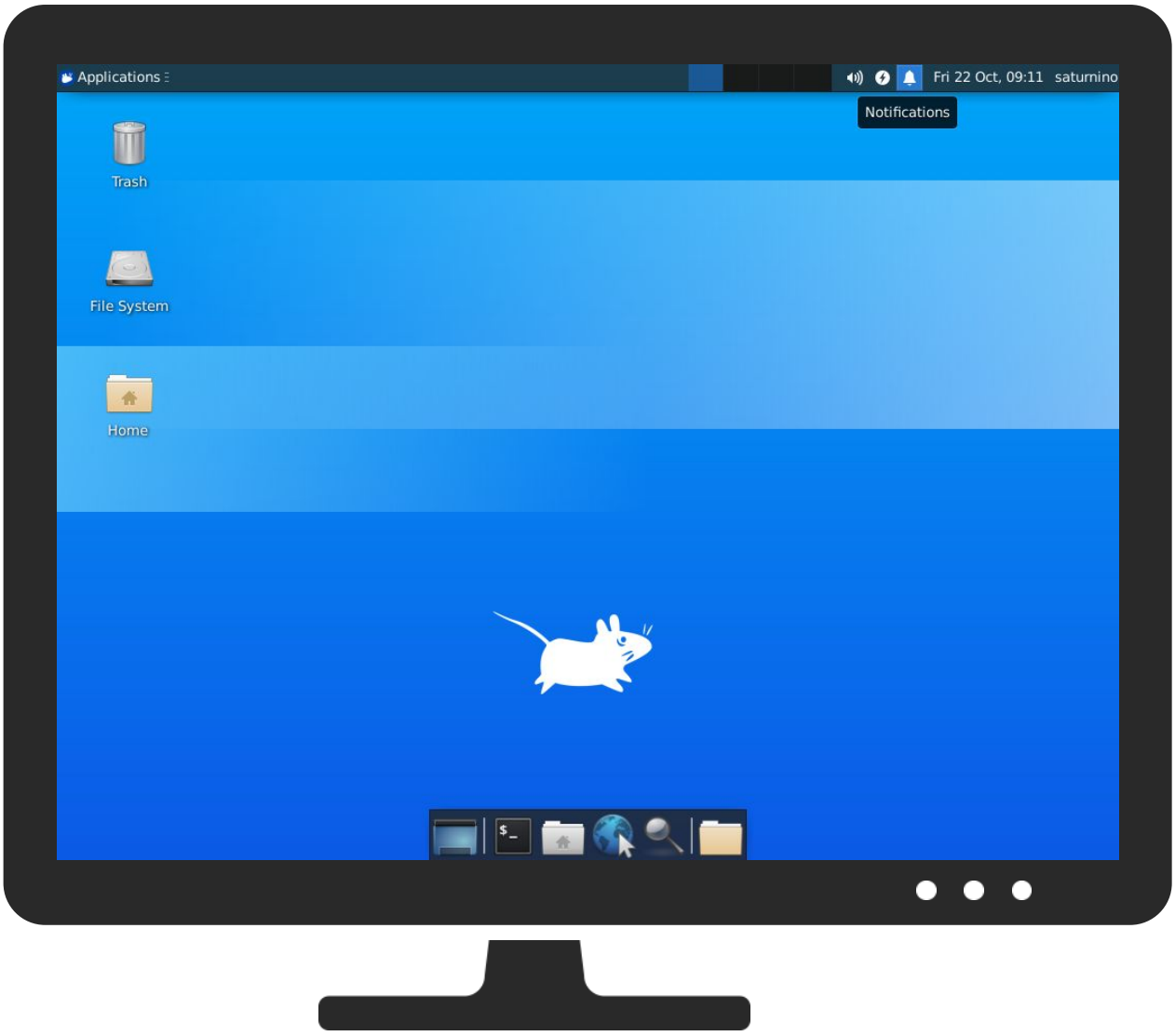


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
IcwrPqGkXP	50%	Virustotal		Browse
IcwrPqGkXP	55%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.142.57.149	unknown	United States		10967	HOMEDEPOTNETUS	false
186.246.4.65	unknown	Brazil		7738	TelemarNorteLesteSABR	false
136.244.180.180	unknown	United States		3606	CONNCOLL-ASUS	false
114.246.134.99	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
87.99.160.241	unknown	Sweden		12501	NORRNODITSSE	false
220.10.138.154	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
111.98.122.40	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
168.245.234.50	unknown	United States		393706	NELSONCABLEUS	false
191.169.131.225	unknown	Brazil		26615	TIMSABR	false
201.21.20.15	unknown	Brazil		28573	CLAROSABR	false
115.191.0.168	unknown	China		7497	CSTNET-AS-APComputerNetworkInformationCenterCN	false
182.67.0.254	unknown	India		45609	BHARTI-MOBILITY-AS-APBhartiAirtelLtdASforGPRSService	false
184.254.1.5	unknown	United States		10507	SPCSUS	false
149.12.44.6	unknown	United States		48945	IFNL-ASGB	false
240.193.66.243	unknown	Reserved		unknown	unknown	false
216.221.62.137	unknown	Canada		6280	SYNAPSECA	false
130.250.57.142	unknown	United States		394901	VXCHNGE-TX01US	false
92.210.255.138	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
175.244.101.81	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
109.226.128.16	unknown	Germany		21032	TELTA-ASDE	false
133.120.23.87	unknown	Japan		2522	PPP-EXPJapanNetworkInformationCenterJP	false
148.70.47.116	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
42.203.248.247	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
60.158.0.171	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
151.112.119.144	unknown	United States		32480	LLUMCUS	false
110.111.113.82	unknown	China		38341	CNNIC-HCENET-APHEXIEInformationtechnologyCoLtdCN	false
113.180.223.7	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
61.185.194.127	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
67.206.151.115	unknown	United States		26857	TRUSTCOMM-ASUS	false
158.126.37.100	unknown	Sweden		31756	COLORADOSPRINGS-GOVUS	false
213.146.201.54	unknown	Portugal		5626	ONIInternetServiceProviderPT	false
59.19.24.218	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
155.2.116.79	unknown	United States		2386	INS-ASUS	false
85.45.125.184	unknown	Italy		3269	ASN-IBSNAZIT	false
5.160.167.152	unknown	Iran (ISLAMIC Republic Of)		42337	RESPINA-ASIR	false
31.121.69.183	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
159.7.220.25	unknown	Sweden		1906	NORTHROP-GRUMMANUS	false
83.44.49.14	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
84.247.123.155	unknown	Romania		60509	TELEPERFORMANCE-ASRO	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.80.250.213	unknown	United States		7029	WINDSTREAMUS	false
61.111.143.75	unknown	Korea Republic of		4670	HYUNDAI-KRShinbiroKR	false
93.169.65.140	unknown	Saudi Arabia		39891	ALJAWWALSTC-ASSA	false
195.223.249.170	unknown	Italy		3269	ASN-IBSNAZIT	false
8.135.206.253	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
192.244.191.206	unknown	Japan		11363	FUJITSU-USAUS	false
138.236.115.201	unknown	United States		17234	GACUS	false
94.42.249.41	unknown	Poland		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
199.3.5.110	unknown	United States		1239	SPRINTLINKUS	false
149.115.226.181	unknown	United States		174	COGENT-174US	false
96.66.178.36	unknown	United States		7922	COMCAST-7922US	false
195.66.5.176	unknown	Germany		9063	SAARGATE-ASVSENETGmbHDE	false
121.201.230.87	unknown	China		17623	CNCGROUP-SZChinaUnicomShenzennetworkCN	false
188.13.148.235	unknown	Italy		3269	ASN-IBSNAZIT	false
246.179.47.128	unknown	Reserved		unknown	unknown	false
246.9.73.167	unknown	Reserved		unknown	unknown	false
164.113.178.223	unknown	United States		2495	KANRENUS	false
44.26.197.42	unknown	United States		63069	SURELINEUS	false
197.2.84.140	unknown	Tunisia		37705	TOPNETTN	false
78.50.41.178	unknown	Germany		6805	TDDE-ASN1DE	false
38.217.98.240	unknown	United States		174	COGENT-174US	false
115.247.124.243	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
184.11.40.157	unknown	United States		7011	FRONTIER-AND-CITIZENSUS	false
16.142.65.134	unknown	United States		unknown	unknown	false
204.8.204.13	unknown	Angola		328165	Banco-de-Investimento-RuralAO	false
223.221.104.203	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
45.145.30.173	unknown	Turkey		197328	INETLTDTR	false
82.141.139.16	unknown	Hungary		12301	INVITECHHU	false
219.21.25.139	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
185.70.34.116	unknown	United Kingdom		201353	NSUKGB	false
35.84.199.85	unknown	United States		237	MERIT-AS-14US	false
48.233.101.228	unknown	United States		2686	ATGS-MMD-ASUS	false
175.219.69.250	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
76.145.199.51	unknown	United States		7922	COMCAST-7922US	false
123.73.29.199	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
221.163.247.179	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
183.3.52.187	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
17.109.252.29	unknown	United States		714	APPLE-ENGINEERINGUS	false
99.48.195.62	unknown	United States		7018	ATT-INTERNET4US	false
102.112.147.46	unknown	Mauritius		23889	MauritiusTelecomMU	false
222.43.48.173	unknown	China		45069	CNNIC-CTTSDNET-APchinatietongShandongnetCN	false
117.186.4.82	unknown	China		24400	CMNET-V4SHANGHAI-AS-APShanghaiMobileCommunicationsCoLt	false
96.1.87.79	unknown	Canada		852	ASN852CA	false
157.10.154.106	unknown	unknown		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
247.78.135.221	unknown	Reserved		unknown	unknown	false
71.161.252.154	unknown	United States		701	UUNETUS	false
72.113.124.144	unknown	United States		22394	CELLCOUS	false
115.30.102.59	unknown	Taiwan; Republic of China (ROC)		133747	TRIUMPH-AS-APTRIUMPHDYNASTYLimitedHK	false
121.231.7.49	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
254.5.211.44	unknown	Reserved		unknown	unknown	false
97.250.16.26	unknown	United States		6167	CELLCO-PARTUS	false
85.136.14.63	unknown	Spain		12357	COMUNITELSPAINES	false
211.91.48.146	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
48.171.221.80	unknown	United States		2686	ATGS-MMD-ASUS	false
9.172.67.125	unknown	United States		3356	LEVEL3US	false
255.56.145.124	unknown	Reserved		unknown	unknown	false
203.27.10.136	unknown	China		2764	AAPTAAPTLimitedAU	false
106.34.174.230	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
210.226.36.155	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
32.1.117.241	unknown	United States		2686	ATGS-MMD-ASUS	false
212.249.81.39	unknown	Switzerland		702	UUNETUS	false

Runtime Messages

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

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TelemarNorteLesteSABR	MPnFvIsvJp	Get hash	malicious	Browse	• 201.19.52.194
	g22kPe2LIc	Get hash	malicious	Browse	• 186.246.215.95
	cosvgegE1S	Get hash	malicious	Browse	• 191.2.105.255
	gKCq4VLpjL	Get hash	malicious	Browse	• 191.45.41.196
	uK570ZEpyQ	Get hash	malicious	Browse	• 191.214.237.61
	F3br85KuNX	Get hash	malicious	Browse	• 201.18.7.193
	jvilYCvWBc	Get hash	malicious	Browse	• 191.42.56.200
	pLpqV3XZ76	Get hash	malicious	Browse	• 189.105.44.62
	ggtS1fKIqX	Get hash	malicious	Browse	• 191.0.212.55
	sora.arm	Get hash	malicious	Browse	• 187.43.203.27
	buiodawbdawbuiopdw.x86	Get hash	malicious	Browse	• 187.43.170.12

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Kot3UfQMDm	Get hash	malicious	Browse	• 191.214.114.207
	arm7	Get hash	malicious	Browse	• 201.58.44.232
	arm7	Get hash	malicious	Browse	• 191.2.153.111
	JuofJwjQMT	Get hash	malicious	Browse	• 189.104.65.237
	x86	Get hash	malicious	Browse	• 189.105.20.47
	Z1JWqe0tZn	Get hash	malicious	Browse	• 179.67.232.124
	raCyB7pYpd	Get hash	malicious	Browse	• 152.237.114.166
	il32XbklZm	Get hash	malicious	Browse	• 201.32.125.192
	7SerHvEAjE	Get hash	malicious	Browse	• 179.68.219.97
HOMEDEPOTNETUS	il32XbklZm	Get hash	malicious	Browse	• 151.140.99.116
	8A5Aub0x7r	Get hash	malicious	Browse	• 151.140.70.186
	h8RVQktJXr	Get hash	malicious	Browse	• 165.131.82.191
	KG7X7nyxQ4	Get hash	malicious	Browse	• 165.130.201.189
	b3astmode.arm7	Get hash	malicious	Browse	• 151.140.99.100
	3DAMhv0DFI	Get hash	malicious	Browse	• 151.140.52.118
	jFQ6SEAt26	Get hash	malicious	Browse	• 165.130.6.234
	2YrqtABAvt	Get hash	malicious	Browse	• 165.131.138.205
	i64RJ7IpMW	Get hash	malicious	Browse	• 207.11.39.140
	b3astmode.arm7	Get hash	malicious	Browse	• 151.142.57.178
	l9Ix5r5wGZ	Get hash	malicious	Browse	• 165.130.248.172
	e5q6xjMRES	Get hash	malicious	Browse	• 151.140.146.198
	DLGXmh48ND	Get hash	malicious	Browse	• 151.142.57.102
	bwuBy0kegz	Get hash	malicious	Browse	• 151.140.128.106
	x86_unpacked	Get hash	malicious	Browse	• 151.142.57.160
	fil1	Get hash	malicious	Browse	• 151.142.57.173

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5290/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.

/proc/5405/oom_score_adj	
Process:	/usr/sbin/sshd
File Type:	ASCII text

/proc/5405/oom_score_adj	
Category:	dropped
Size (bytes):	6
Entropy (8bit):	1.7924812503605778
Encrypted:	false
SSDEEP:	3:ptn:Dn
MD5:	CBF282CC55ED0792C33D10003D1F760A
SHA1:	007DD8BD75468E6B7ABA4285E9B267202C7EAEED
SHA-256:	FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22
SHA-512:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC 0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	 -1000.

/proc/5407/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:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC 0
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:E4v:Ei
MD5:	C1CD8B3D865DA678B4D32DDFFA91B683
SHA1:	DBD80617342B88805FEC6EFEC7A720E751598798
SHA-256:	11D1C64BB9D6C776EF791C61A88BB582C6AD4C816754E5BF48C9327DDBF39BDF
SHA-512:	3B0D361F3DD594CFA593C98E571C58A3D86FB9A1F1E8F8C78F505BE5231C312E63AB5DD724BF3D8DEDE78DF740C5D0BAB5DB0DA1916EAAAB6A4BCA289A56 313
Malicious:	false
Reputation:	low
Preview:	 5407.

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.296758508714272
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	IcwrPqGkXP
File size:	71764
MD5:	18fe913ce8856fc1ea6ebc0412e09da7
SHA1:	ff1494dd42dcda452120a9af38a1f5550bd29c55

General

SHA256:	dea614c4a0a319bb53e0d5d9b77d360e23d79e43e4c7a5 179c9c3f6b66c26e74
SHA512:	487221c1701546a05d979979ff75ceaf3600c504da5b658 1ea90e627a81b07869442431a4d1b157cb9620c60d92d9 d3ddee7d8de37249b7b402bc419eb4da617
SSDEEP:	1536:WkvDSnAd6mYoPdd8TVs1o0vB1tA0iLuYw2+O/8 2:WkLSA3vGko0pTAmYw2+OE2
File Content Preview:	.ELF.....@.`...4...L....4. ...(.....@...@..... .....E...E.....dt.Q.....<...'.... ..I'.....<...'.....I.. ....'9... .....<...'.....! .....'9.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	71244
Section Header Size:	40
Number of Section Headers:	13
Header String Table Index:	12

Sections

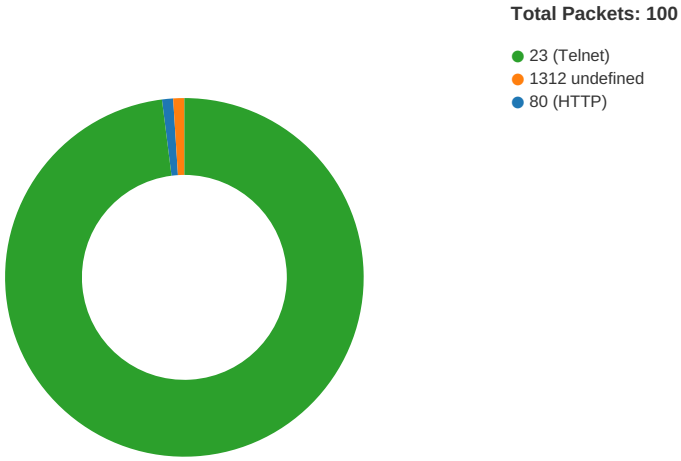
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0xffe0	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x410100	0x10100	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x410160	0x10160	0x660	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x451000	0x11000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x451008	0x11008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x451020	0x11020	0x190	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x4511b0	0x111b0	0x444	0x4	0x10000003	WA	0	0	16
.sbss	NOBITS	0x4515f4	0x115f4	0x24	0x0	0x10000003	WA	0	0	4
.bss	NOBITS	0x451620	0x115f4	0x2a0	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x72c	0x115f4	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x115f4	0x57	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x107c0	0x107c0	3.3492	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x11000	0x451000	0x451000	0x5f4	0x8c0	1.8117	0x6	RW	0x10000		.ctors .dtors .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: IcwrPqGkXP PID: 5250 Parent PID: 5121

General

Start time:	09:09:20
Start date:	22/10/2021
Path:	/tmp/IcwrPqGkXP
Arguments:	/tmp/IcwrPqGkXP
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: IcwrPqGkXP PID: 5253 Parent PID: 5250

General

Start time:	09:09:20
Start date:	22/10/2021
Path:	/tmp/IcwrPqGkXP
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: IcwrPqGkXP PID: 5254 Parent PID: 5250

General

Start time:	09:09:20
Start date:	22/10/2021
Path:	/tmp/IcwrPqGkXP
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: IcwrPqGkXP PID: 5255 Parent PID: 5250

General

Start time:	09:09:20
Start date:	22/10/2021
Path:	/tmp/IcwrPqGkXP
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: IcwrPqGkXP PID: 5259 Parent PID: 5255

General

Start time:	09:09:20
Start date:	22/10/2021
Path:	/tmp/IcwrPqGkXP
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: IcwrPqGkXP PID: 5261 Parent PID: 5255

General

Start time:	09:09:20
Start date:	22/10/2021
Path:	/tmp/IcwrPqGkXP
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: IcwrPqGkXP PID: 5263 Parent PID: 5255

General

Start time:	09:09:20

Start date:	22/10/2021
Path:	/tmp/IcwrPqGkXP
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: systemd PID: 5287 Parent PID: 1

General

Start time:	09:09:33
Start date:	22/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5287 Parent PID: 1

General

Start time:	09:09:33
Start date:	22/10/2021
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: 5290 Parent PID: 1

General

Start time:	09:09:34
Start date:	22/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5290 Parent PID: 1

General

Start time:	09:09:34
Start date:	22/10/2021
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: systemd PID: 5404 Parent PID: 1

General

Start time:	09:12:19
Start date:	22/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5404 Parent PID: 1

General

Start time:	09:12:19
Start date:	22/10/2021
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: 5405 Parent PID: 1

General

Start time:	09:12:19
Start date:	22/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5405 Parent PID: 1

General

Start time:	09:12:19
Start date:	22/10/2021

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: systemd PID: 5406 Parent PID: 1

General

Start time:	09:12:21
Start date:	22/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5406 Parent PID: 1

General

Start time:	09:12:21
Start date:	22/10/2021
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: 5407 Parent PID: 1

General

Start time:	09:12:21
Start date:	22/10/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5407 Parent PID: 1

General

Start time:	09:12:21
Start date:	22/10/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated