ID: 756120
Sample Name:
robinbot_sample2
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 16:51:40
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2022

Linux Analysis Report

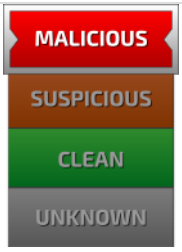
robinbot_sample2

Overview

General Information

Sample Name:	robinbot_sample2
Analysis ID:	756120
MD5:	d65bd6175517e0.
SHA1:	f1a6dc5a7b2678..
SHA256:	345e9c1b6ce0f3...
Infos:	

Detection



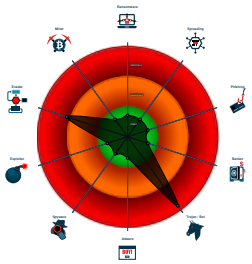
Mirai

Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample deletes itself
- Yara signature match
- Sample contains strings that are po…
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…

Classification



Analysis Advice

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

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

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756120
Start date and time:	2022-11-29 16:51:40 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	robinbot_sample2
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 16.04 x64 (Kernel 4.4.0-116, Firefox 88.0, Document Viewer 3.18.2, LibreOffice 5.1.6.2, OpenJDK 1.8.0_171)
Analysis Mode:	default
Detection:	MAL
Classification:	mal100.troj.evad.lin@0/2@0/0

Warnings

Runtime Messages

Command:	/tmp/robinbot_sample2
PID:	9446
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Hei
Standard Error:	

Copyright Joe Security LLC 2022

Process Tree

- **system is lnxubuntu1**
- robinbot_sample2 (PID: 9446, Parent: 9378, MD5: unknown) Arguments: /usr/bin/qemu-ppc /tmp/robinbot_sample2
  - robinbot_sample2 New Fork (PID: 9454, Parent: 9446)
    - robinbot_sample2 New Fork (PID: 9457, Parent: 9454)
    - robinbot_sample2 New Fork (PID: 9458, Parent: 9454)
    - robinbot_sample2 New Fork (PID: 9459, Parent: 9454)
    - robinbot_sample2 New Fork (PID: 9460, Parent: 9454)
- upstart New Fork (PID: 9467, Parent: 3310)
- sh (PID: 9467, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
  - sh New Fork (PID: 9468, Parent: 9467)
  - date (PID: 9468, Parent: 9467, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
  - sh New Fork (PID: 9485, Parent: 9467)
  - apport-checkreports (PID: 9485, Parent: 9467, MD5: 1a7d84ebc34df04e55ca3723541f48c9) Arguments: /usr/bin/python3 /usr/share/apport/apport-checkreports --system
- upstart New Fork (PID: 9494, Parent: 3310)
- sh (PID: 9494, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
  - sh New Fork (PID: 9495, Parent: 9494)
  - date (PID: 9495, Parent: 9494, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
  - sh New Fork (PID: 9501, Parent: 9494)
  - apport-gtk (PID: 9501, Parent: 9494, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- upstart New Fork (PID: 9521, Parent: 3310)
- sh (PID: 9521, Parent: 3310, MD5: e02ea3c3450d44126c46d658fa9e654c) Arguments: /bin/sh -e /proc/self/fd/9
  - sh New Fork (PID: 9526, Parent: 9521)
  - date (PID: 9526, Parent: 9521, MD5: 54903b613f9019bfca9f5d28a4fff34e) Arguments: date
  - sh New Fork (PID: 9533, Parent: 9521)
  - apport-gtk (PID: 9533, Parent: 9521, MD5: ec58a49a30ef6a29406a204f28cc7d87) Arguments: /usr/bin/python3 /usr/share/apport/apport-gtk
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
robinbot_sample2	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x1b9b8:$x2: /dev/misc/watchdog • 0x1b9a8:$x3: /dev/watchdog • 0x1dec0:$s1: LCOGQGPTGP • 0x1db94:$s3: CFOKLKQVPCVMP • 0x1db78:$s4: QWRGPTKQMP • 0x1dad4:$s5: HWCLVGAJ • 0x1dd44:$s6: NKQVGLKLE
robinbot_sample2	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
robinbot_sample2	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
robinbot_sample2	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
robinbot_sample2	JoeSecurity_Mirai_4	Yara detected Mirai	Joe Security	

Click to see the 1 entries

Memory Dumps

Source	Rule	Description	Author	Strings
9457.1.00007fddd7163000.00007fddd7183000.r-x.sdmp	Mirai_Botnet_Malware	Detects Mirai Botnet Malware	Florian Roth	• 0x1b9b8:$x2: /dev/misc/watchdog • 0x1b9a8:$x3: /dev/watchdog • 0x1dec0:$s1: LCOGQGPTGP • 0x1db94:$s3: CFOKLKQVPCVMP • 0x1db78:$s4: QWRGPTKQMP • 0x1dad4:$s5: HWCLVGAJ • 0x1dd44:$s6: NKQVGLKLE
9457.1.00007fddd7163000.00007fddd7183000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
9457.1.00007fddd7163000.00007fddd7183000.r-x.sdmp	JoeSecurity_Mirai_9	Yara detected Mirai	Joe Security	
9457.1.00007fddd7163000.00007fddd7183000.r-x.sdmp	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
9457.1.00007fddd7163000.00007fddd7183000.r-x.sdmp	JoeSecurity_Mirai_4	Yara detected Mirai	Joe Security	

Click to see the 19 entries

Copyright Joe Security LLC 2022

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Sample deletes itself

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

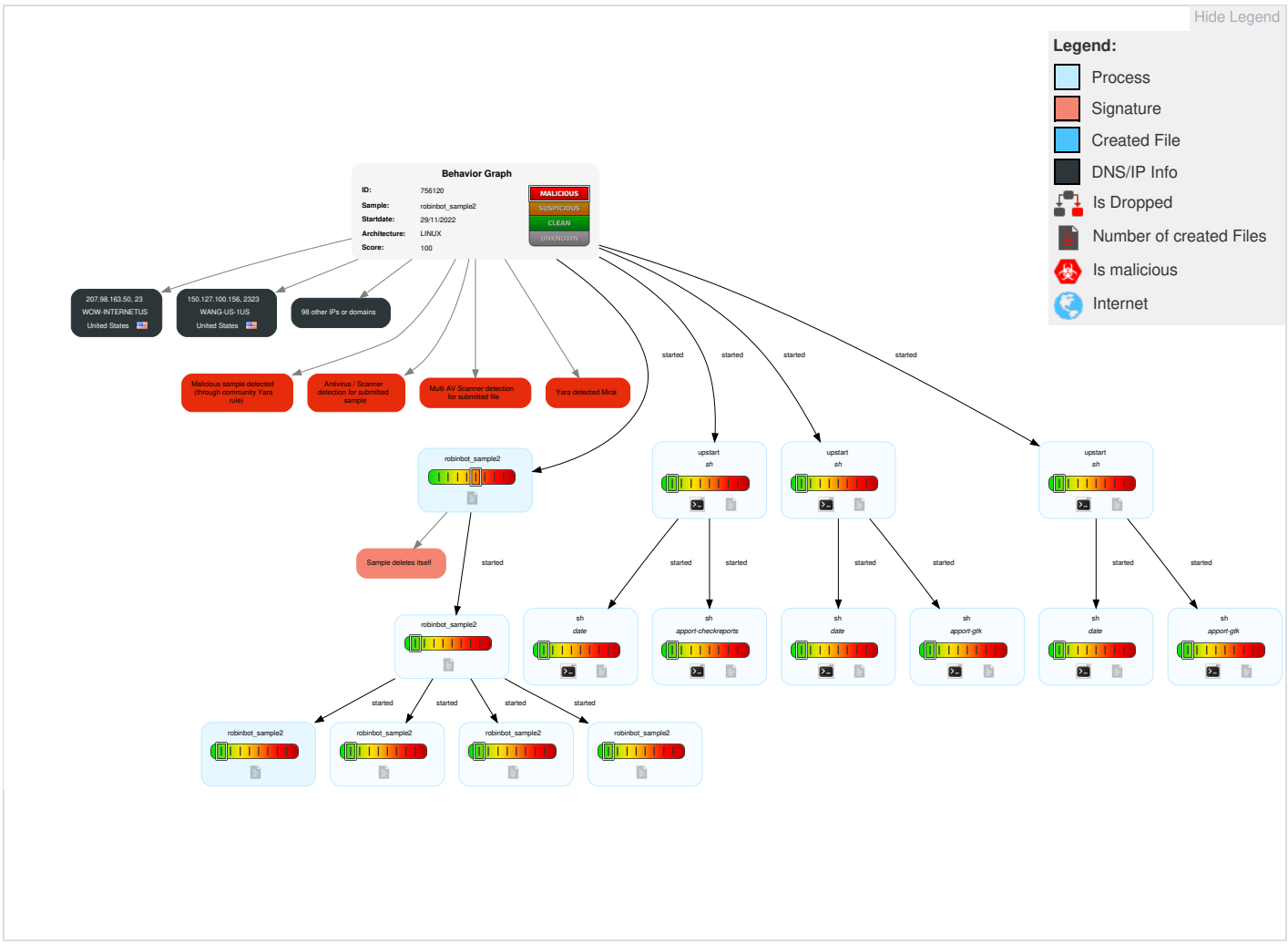
Mitre Att&ck Matrix

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	1 Command and Scripting Interpreter	Path Interception	Path Interception	1 File Deletion	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Non-Standard Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
robinbot_sample2	73%	ReversingLabs	Linux.Trojan.Mirai	
robinbot_sample2	100%	Avira	LINUX/Mirai.bonb	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://purenetworks.com/HNAP1/	0%	URL Reputation	safe	
http://176.97.210.195/mips	100%	Avira URL Cloud	malware	
http://176.97.210.195/bins.sh	100%	Avira URL Cloud	malware	
http://176.97.210.195/bins.sh;sh	100%	Avira URL Cloud	malware	
http://176.97.210.195/bin.sh;chmod	100%	Avira URL Cloud	malware	
http://176.97.210.195/bins.sh;	100%	Avira URL Cloud	malware	
http://176.97.210.195/bins.sh;chmod	100%	Avira URL Cloud	malware	
http://176.97.210.195/mipsel	100%	Avira URL Cloud	malware	
http://176.97.210.195/bins.sh;$	100%	Avira URL Cloud	malware	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://176.97.210.195/bins.sh;sh$	100%	Avira URL Cloud	malware	

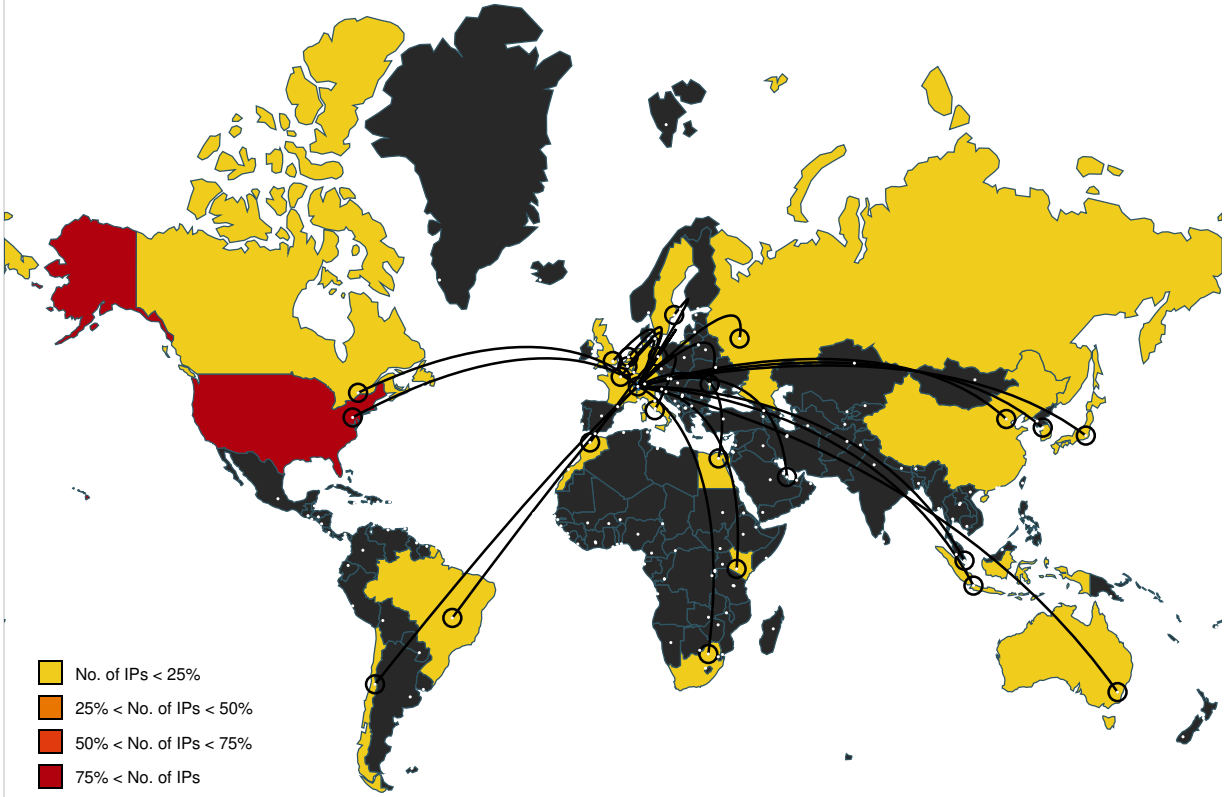
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.27.234.3	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
31.28.234.66	unknown	Russian Federation		35816	SEVSTARSevastopolRussiaRU	false
49.236.141.120	unknown	Korea Republic of		135354	NBPAP-AS-APNAVERBUSINESSPLATFORMASIAPACIFICPTELTD	false
201.86.197.70	unknown	Brazil		18881	TELEFONICABRASILSAB R	false
158.86.146.164	unknown	United States		20379	NET-BAKERUS	false
3.188.190.144	unknown	United States		16509	AMAZON-02US	false
57.27.53.12	unknown	Belgium		2686	ATGS-MMD-ASUS	false
44.83.193.57	unknown	United States		7377	UCSDUS	false
121.224.51.208	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
93.226.153.134	unknown	Germany		3320	DTAGInternetserviceproviderоperationsDE	false
204.191.7.105	unknown	Canada		7861	TELUS-7861CA	false
32.133.75.25	unknown	United States		2686	ATGS-MMD-ASUS	false
170.201.185.125	unknown	United States		10995	PNCBANKUS	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
6.194.255.36	unknown	United States		3356	LEVEL3US	false
103.184.187.32	unknown	unknown		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
84.74.191.135	unknown	Switzerland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
135.170.12.253	unknown	United States		14962	NCR-252US	false
175.60.169.1	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
53.116.197.151	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
150.29.125.60	unknown	Japan		23793	AISTNationalInstituteofAdvancedIndustrialScienceandT	false
196.69.167.121	unknown	Morocco		6713	IAM-ASMA	false
95.211.14.126	unknown	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
80.146.226.49	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
55.31.53.144	unknown	United States		350	DNIC-ASBLK-00306-00371US	false
160.94.227.81	unknown	United States		217	UMN-SYSTEMUS	false
4.171.111.142	unknown	United States		3356	LEVEL3US	false
3.84.38.38	unknown	United States		14618	AMAZON-AESUS	false
119.126.143.108	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
24.69.97.20	unknown	Canada		6327	SHAWCA	false
12.106.15.114	unknown	United States		7018	ATT-INTERNET4US	false
158.148.46.199	unknown	Italy		16232	ASN-TIMServiceProviderIT	false
159.199.123.51	unknown	United States		11363	FUJITSU-USAUS	false
19.160.34.92	unknown	United States		3	MIT-GATEWAYSUS	false
148.162.240.74	unknown	United States		6400	CompaniaDominicanadeTelefonosSADO	false
7.121.88.120	unknown	United States		3356	LEVEL3US	false
154.143.62.165	unknown	Egypt		37069	MOBINILEG	false
45.45.235.228	unknown	Reserved		5769	VIDEOTRONCA	false
47.41.11.60	unknown	United States		20115	CHARTER-20115US	false
16.230.224.193	unknown	United States		unknown	unknown	false
223.124.73.165	unknown	China		58453	CMI-INT-HKLevel30Tower1HK	false
3.40.199.201	unknown	United States		8987	AMAZONEXPANSIONGB	false
194.94.180.179	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
93.185.22.188	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
210.0.21.93	unknown	Australia		7474	OPTUSCOM-AS01-AUSingTelOptusPtyLtdAU	false
190.164.183.143	unknown	Chile		22047	VTRBANDAANCHASACL	false
6.213.11.12	unknown	United States		3356	LEVEL3US	false
24.230.110.223	unknown	United States		11232	MIDCO-NETUS	false
193.182.56.79	unknown	Sweden		9201	SWAFSwedishArmedForcesSE	false
108.19.232.183	unknown	United States		701	UUNETUS	false
125.103.51.240	unknown	Japan		17506	UCOMARTERIANetworksCorporationJP	false
207.98.163.50	unknown	United States		12083	WOW-INTERNETUS	false
128.229.125.156	unknown	United States		7281	BOOZ-ASUS	false
51.82.147.120	unknown	United States		2686	ATGS-MMD-ASUS	false
51.160.118.144	unknown	United States		2686	ATGS-MMD-ASUS	false
220.157.237.187	unknown	Japan		4685	ASAHI-NETAsahiNetJP	false
129.126.63.202	unknown	Singapore		17547	M1NET-SG-APM1NETLTDSG	false
145.113.110.141	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
219.246.105.254	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
153.201.81.145	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
30.127.22.132	unknown	United States		7922	COMCAST-7922US	false
48.21.211.75	unknown	United States		2686	ATGS-MMD-ASUS	false
22.102.182.225	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
39.177.207.101	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
49.19.218.103	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
163.200.71.205	unknown	South Africa		2018	TENET-1ZA	false
33.67.184.91	unknown	United States		2686	ATGS-MMD-ASUS	false
164.187.43.136	unknown	United States		37717	EL-KhawarizmiTN	false
196.97.30.53	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
178.153.100.6	unknown	Qatar		42298	GCC-MPLS-PEERINGGCCMPLSpeeringQA	false
29.249.249.192	unknown	United States		7922	COMCAST-7922US	false
108.235.89.235	unknown	United States		7018	ATT-INTERNET4US	false
75.227.38.99	unknown	United States		22394	CELLCOUS	false
108.87.62.138	unknown	United States		7018	ATT-INTERNET4US	false
15.16.33.196	unknown	United States		13979	ATT-IPFRUS	false
99.97.134.67	unknown	United States		7018	ATT-INTERNET4US	false
210.231.72.134	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
176.26.210.248	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
72.203.90.128	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
20.41.197.165	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
153.92.194.105	unknown	Germany		15817	MITTWALD-ASMittwaldCMServiceGmbHundCoKGDE	false
65.165.31.207	unknown	United States		1239	SPRINTLINKUS	false
70.247.33.149	unknown	United States		7018	ATT-INTERNET4US	false
192.21.78.209	unknown	United States		14153	EDGECAST-IRUS	false
91.174.124.138	unknown	France		12322	PROXADFR	false
93.113.82.42	unknown	Moldova Republic of		8926	MOLDTELECOM-ASMoldtelecomAutonomousSystemMD	false
170.92.154.205	unknown	United States		16595	TOROUS	false
20.8.210.112	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
173.139.249.160	unknown	United States		10507	SPCSUS	false
149.252.162.80	unknown	United States		20473	AS-CHOOPAUS	false
182.147.76.82	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
150.127.100.156	unknown	United States		3955	WANG-US-1US	false
193.175.87.171	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
182.7.149.218	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
96.106.36.210	unknown	United States		7922	COMCAST-7922US	false
123.230.133.241	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
51.110.98.238	unknown	United Kingdom		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
129.1.20.212	unknown	United States		55194	BGSUUS	false
70.214.149.19	unknown	United States		6167	CELLCO-PARTUS	false
203.125.36.165	unknown	Singapore		3758	SINGNETSingNetSG	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
135.0.33.192	unknown	Canada		54614	CIKTELECOM-CABLECA	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/var/crash/_usr_share_apport_apport-checkreports.1000.crash

/var/crash/_usr_share_apport_apport-gtk.1000.crash

Static File Info

General

File type:	ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.3249574223453475
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	robinbot_sample2
File size:	133568
MD5:	d65bd6175517e0bcb6a6fc077cdcb655
SHA1:	f1a6dc5a7b2678f6e499e44de99beb0c0936d626
SHA256:	345e9c1b6ce0f34a6be63e5411348f4c1588654f61fcbc4d667cab4c8aef1ae3
SHA512:	555dd3c9f17cc000d0cea50e68bca3c9c0070bb9d0c418ef7fb75340c531d69f5c4b40efe5921e9974912ff29124c82dafc62915ff0add44ebe7245b7b0bc753
SSDEEP:	3072:qy/2cCus/af/ASX47hHLTTZBZ6JdeJPMqv:7apG/ASodTZCJdG0qv
TLSH:	32D308CB5F263E97C0CB93FA7937A3ED07D9AD2113E401442856DD8207731B9E6A4A78
File Content Preview:	.ELF.....4...h.....4. ...(..... ... .).....dt.Q.....!..|.....$H...H.....$8!. |...N.. .!..|.....?...../...@..\?..... <.+../...A..$8...}).....<N..

Static ELF Info

ELF header

Class:	
Data:	
Version:	

ELF header	
Machine:	
Version Number:	
Type:	
OS/ABI:	
ABI Version:	
Entry Point Address:	
Flags:	
ELF Header Size:	
Program Header Offset:	
Program Header Size:	
Number of Program Headers:	
Section Header Offset:	
Section Header Size:	
Number of Section Headers:	
Header String Table Index:	

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10000094	0x94	0x24	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100000b8	0xb8	0x19044	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x100190fc	0x190fc	0x20	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x10019120	0x19120	0x64fc	0x0	0x2	A	0	0	8
.eh_frame	PROGBITS	0x1001f61c	0x1f61c	0x4	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x1002f620	0x1f620	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x1002f628	0x1f628	0x8	0x0	0x3	WA	0	0	4
.jcr	PROGBITS	0x1002f630	0x1f630	0x4	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x1002f638	0x1f638	0x3b8	0x0	0x3	WA	0	0	8
.sdata	PROGBITS	0x1002f9f0	0x1f9f0	0x48	0x0	0x3	WA	0	0	4
.sbss	NOBITS	0x1002fa38	0x1fa38	0xcc	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x1002fb04	0x1fa38	0x24e0	0x0	0x3	WA	0	0	4
.comment	PROGBITS	0x0	0x1fa38	0xccc	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x20704	0x63	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	0x10000000	0x10000000	0x1f620	0x1f620	6.3427	0x5	R E	0x10000		.init .text .fini .rodata .eh_frame
LOAD	0x1f620	0x1002f620	0x1002f620	0x418	0x29c4	2.8381	0x6	RW	0x10000		.ctors .dtors .jcr .data .sdata .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

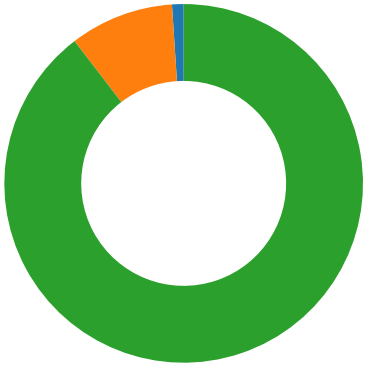
Network Behavior

Network Port Distribution

Total Packets: 96

- 23 (Telnet)
- 2323 undefined
- 8080 undefined

Copyright Joe Security LLC 2022



TCP Packets

System Behavior

Analysis Process: robinbot_sample2 PID: 9446, Parent PID: 9378

General

Start time:	16:52:25
Start date:	29/11/2022
Path:	/tmp/robinbot_sample2
Arguments:	/usr/bin/qemu-ppc /tmp/robinbot_sample2
File size:	0 bytes
MD5 hash:	unknown

File Activities

File Deleted

File Read

Analysis Process: robinbot_sample2 PID: 9454, Parent PID: 9446

General

Start time:	16:52:25
Start date:	29/11/2022
Path:	/tmp/robinbot_sample2
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: robinbot_sample2 PID: 9457, Parent PID: 9454

General

Start time:	16:52:25
Start date:	29/11/2022
Path:	/tmp/robinbot_sample2
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

File Activities

File Read

Copyright Joe Security LLC 2022

Analysis Process: robinbot_sample2 PID: **9458**, Parent PID: **9454**

General

Start time:	16:52:25
Start date:	29/11/2022
Path:	/tmp/robinbot_sample2
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: robinbot_sample2 PID: **9459**, Parent PID: **9454**

General

Start time:	16:52:25
Start date:	29/11/2022
Path:	/tmp/robinbot_sample2
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

File Activities

File Read

Analysis Process: robinbot_sample2 PID: **9460**, Parent PID: **9454**

General

Start time:	16:52:25
Start date:	29/11/2022
Path:	/tmp/robinbot_sample2
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: upstart PID: **9467**, Parent PID: **3310**

General

Start time:	16:52:32
Start date:	29/11/2022
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: sh PID: **9467**, Parent PID: **3310**

General

Start time:	16:52:32
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: **9468**, Parent PID: **9467**

General

Start time:	16:52:32

Copyright Joe Security LLC 2022

Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: **9468**, Parent PID: **9467**

General

Start time:	16:52:32
Start date:	29/11/2022
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: **9485**, Parent PID: **9467**

General

Start time:	16:52:32
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-checkreports PID: **9485**, Parent PID: **9467**

General

Start time:	16:52:32
Start date:	29/11/2022
Path:	/usr/share/apport/apport-checkreports
Arguments:	/usr/bin/python3 /usr/share/apport/apport-checkreports --system
File size:	1269 bytes
MD5 hash:	1a7d84ebc34df04e55ca3723541f48c9

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: upstart PID: **9494**, Parent PID: **3310**

General

Start time:	16:52:32
Start date:	29/11/2022
Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: sh PID: **9494**, Parent PID: **3310**

General

Start time:	16:52:32
Start date:	29/11/2022
Path:	/bin/sh

Copyright Joe Security LLC 2022

Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: **9495**, Parent PID: **9494**

General

Start time:	16:52:32
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: **9495**, Parent PID: **9494**

General

Start time:	16:52:32
Start date:	29/11/2022
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: **9501**, Parent PID: **9494**

General

Start time:	16:52:32
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: **9501**, Parent PID: **9494**

General

Start time:	16:52:32
Start date:	29/11/2022
Path:	/usr/share/apport/apport-gtk
Arguments:	/usr/bin/python3 /usr/share/apport/apport-gtk
File size:	23806 bytes
MD5 hash:	ec58a49a30ef6a29406a204f28cc7d87

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: upstart PID: **9521**, Parent PID: **3310**

General

Start time:	16:52:33
Start date:	29/11/2022

Path:	/sbin/upstart
Arguments:	n/a
File size:	0 bytes
MD5 hash:	unknown

Analysis Process: sh PID: **9521**, Parent PID: **3310**

General

Start time:	16:52:33
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	/bin/sh -e /proc/self/fd/9
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

File Activities

File Read

Analysis Process: sh PID: **9526**, Parent PID: **9521**

General

Start time:	16:52:33
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: date PID: **9526**, Parent PID: **9521**

General

Start time:	16:52:33
Start date:	29/11/2022
Path:	/bin/date
Arguments:	date
File size:	68464 bytes
MD5 hash:	54903b613f9019bfca9f5d28a4fff34e

File Activities

File Read

Analysis Process: sh PID: **9533**, Parent PID: **9521**

General

Start time:	16:52:33
Start date:	29/11/2022
Path:	/bin/sh
Arguments:	n/a
File size:	4 bytes
MD5 hash:	e02ea3c3450d44126c46d658fa9e654c

Analysis Process: apport-gtk PID: **9533**, Parent PID: **9521**

General

Start time:	16:52:33
Start date:	29/11/2022
Path:	/usr/share/apport/apport-gtk
Arguments:	/usr/bin/python3 /usr/share/apport/apport-gtk
File size:	23806 bytes
MD5 hash:	ec58a49a30ef6a29406a204f28cc7d87

Copyright Joe Security LLC 2022

File Activities

File Read

Directory Enumerated