ID: 679491
Sample Name: PPyJlaRy0K
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 21:53:08
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Linux Analysis Report PPyJlaRy0K 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Analysis Advice 3
General Information 3
Warnings 3
Runtime Messages 3
Process Tree 4
Yara Signatures 4
PCAP (Network Traffic) 4
Snort Signatures 4
Joe Sandbox Signatures 4
AV Detection 4
Hooking and other Techniques for Hiding and Protection 4
Stealing of Sensitive Information 4
Remote Access Functionality 4
Mitre Att&ck Matrix 4
Malware Configuration 5
Behavior Graph 5
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 6
Dropped Files 6
Domains 6
URLs 6
Domains and IPs 6
Contacted Domains 6
World Map of Contacted IPs 6
Public IPs 6
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
Static ELF Info 10
ELF header 10
Sections 10
Program Segments 10
Network Behavior 10
Network Port Distribution 10
TCP Packets 11
System Behavior 11
Analysis Process: PPyJlaRy0K PID: 6234, Parent PID: 6124 11
General 11
File Activities 11
File Deleted 11
File Read 11
Directory Deleted 11
Analysis Process: PPyJlaRy0K PID: 6236, Parent PID: 6234 11
General 11
File Activities 11
File Read 11
Directory Enumerated 11
Analysis Process: PPyJlaRy0K PID: 6238, Parent PID: 6234 11
General 11
Analysis Process: PPyJlaRy0K PID: 6239, Parent PID: 6234 12
General 12
Analysis Process: PPyJlaRy0K PID: 6243, Parent PID: 6234 12
General 12
File Activities 12
File Read 12
Analysis Process: PPyJlaRy0K PID: 6249, Parent PID: 6243 12
General 12
File Activities 12
File Read 12
Directory Enumerated 12
Analysis Process: PPyJlaRy0K PID: 6251, Parent PID: 6243 12
General 12
Analysis Process: PPyJlaRy0K PID: 6253, Parent PID: 6243 12
General 12

Copyright Joe Security LLC 2022

Linux Analysis Report

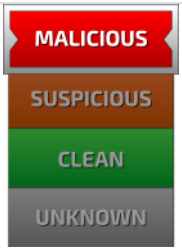
PPyJlaRy0K

Overview

General Information

Sample Name:	PPyJlaRy0K
Analysis ID:	679491
MD5:	6e38620768d8b3.
SHA1:	64a0eb90426549.
SHA256:	0d69d7b9183771.
Tags:	32 elf mirai motorola
Infos:	

Detection



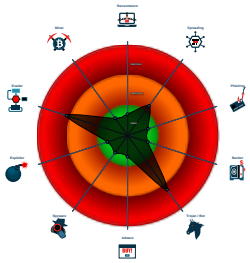
Mirai

Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample deletes itself
- 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 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:	35.0.0 Citrine
Analysis ID:	679491
Start date and time: 05/08/202221:53:08	2022-08-05 21:53:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PPyJlaRy0K
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:	mal68.troj.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/PPyJlaRy0K
PID:	6234
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	BEASTMODE-BITCHES@@"/proc
Standard Error:	

Copyright Joe Security LLC 2022

Process Tree

- **system is lnxubuntu20**
- PPyJlaRy0K (PID: 6234, Parent: 6124, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/PPyJlaRy0K
  - PPyJlaRy0K New Fork (PID: 6236, Parent: 6234)
  - PPyJlaRy0K New Fork (PID: 6238, Parent: 6234)
  - PPyJlaRy0K New Fork (PID: 6239, Parent: 6234)
  - PPyJlaRy0K New Fork (PID: 6243, Parent: 6234)
    - PPyJlaRy0K New Fork (PID: 6249, Parent: 6243)
    - PPyJlaRy0K New Fork (PID: 6251, Parent: 6243)
    - PPyJlaRy0K New Fork (PID: 6253, Parent: 6243)
- **cleanup**

Yara Signatures

PCAP (Network Traffic)

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

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

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

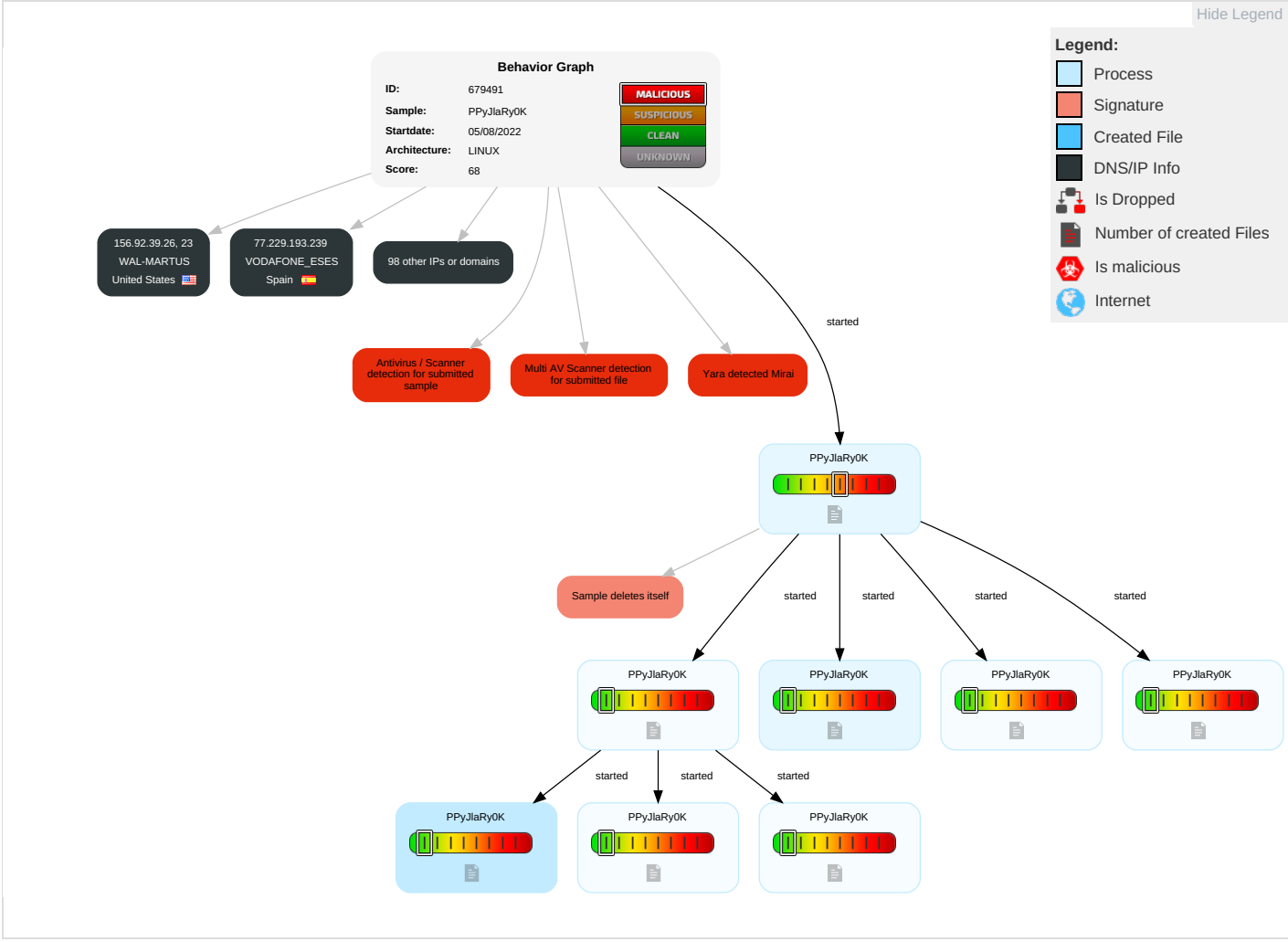
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

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	1 File Deletion	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
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	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
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	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PPyJlaRy0K	60%	Virustotal		Browse
PPyJlaRy0K	100%	Avira	LINUX/Mirai.bonb	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

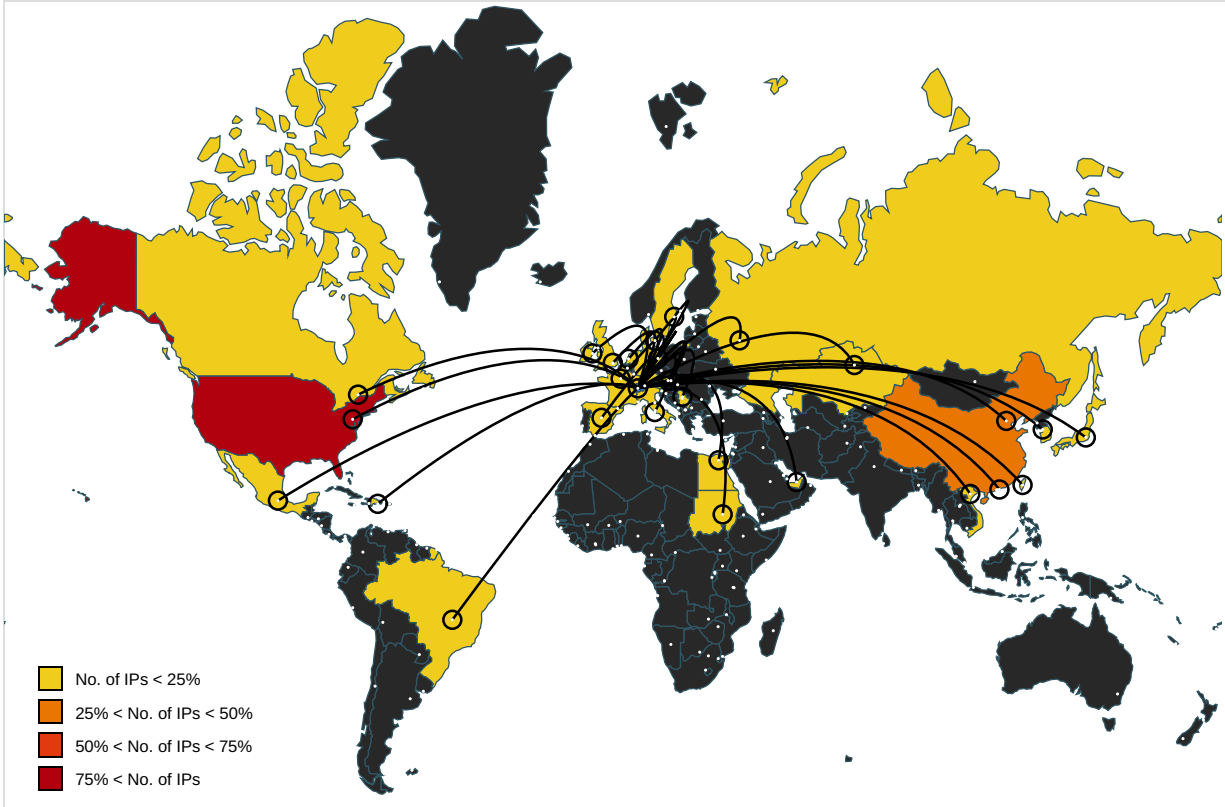
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
62.140.95.229	unknown	Egypt		36992	ETISALAT-MISREG	false
144.44.131.254	unknown	European Union		21286	KPN-CORPORATE-MARKETNL	false
48.239.135.196	unknown	United States		2686	ATGS-MMD-ASUS	false
63.140.123.191	unknown	United States		7782	ALSK-7782US	false
206.50.86.49	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
35.198.197.229	unknown	United States		15169	GOOGLEUS	false
206.49.61.98	unknown	United States		5511	OPENTRANSITFR	false
211.1.137.125	unknown	Japan		7670	CTNETEnergiaCommunicationsIncJP	false
77.229.193.239	unknown	Spain		12430	VODAFONE_ESES	false
110.167.255.14	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
85.36.243.95	unknown	Italy		3269	ASN-IBSNAZIT	false
38.198.245.85	unknown	United States		174	COGENT-174US	false
112.24.113.121	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
107.157.252.28	unknown	United States		7065	SONOMAUS	false
20.41.197.186	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
115.27.36.214	unknown	China		24349	CNGI-BJ-IX3-AS-APCERNET2IXatPekingUniversityCN	false
18.158.195.5	unknown	United States		16509	AMAZON-02US	false
164.179.118.105	unknown	United States		37717	EL-KhawarizmiTN	false
19.88.233.149	unknown	United States		3	MIT-GATEWAYSUS	false
53.95.225.43	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
156.92.39.26	unknown	United States		10695	WAL-MARTUS	false
108.69.103.251	unknown	United States		7018	ATT-INTERNET4US	false
48.188.11.242	unknown	United States		2686	ATGS-MMD-ASUS	false
141.61.172.159	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
249.224.32.81	unknown	Reserved		unknown	unknown	false
89.191.53.233	unknown	Ireland		34912	IFN-ASIE	false
203.175.15.185	unknown	Hong Kong		132422	TELECOM-HKHongKongTelecomGlobalDataCentreHK	false
70.53.164.81	unknown	Canada		577	BACOMCA	false
185.93.212.192	unknown	Austria		5405	CSO_NETAT	false
80.129.10.249	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
48.188.58.235	unknown	United States		2686	ATGS-MMD-ASUS	false
101.128.154.220	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
212.200.150.44	unknown	Serbia		8400	TELEKOM-ASRS	false
101.25.171.135	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
252.233.82.244	unknown	Reserved		unknown	unknown	false
195.240.221.173	unknown	Netherlands		1136	KPNKPNNationalEU	false
90.229.219.156	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
217.204.215.106	unknown	United Kingdom		4589	EASYNETEasynetGlobalServicesEU	false
53.175.161.109	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
109.145.152.50	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
192.197.244.49	unknown	Canada		40119	NAITCA	false
187.245.174.172	unknown	Mexico		13999	MegaCableSAdeCVMX	false
122.132.163.153	unknown	Japan		2518	BIGLOBEBIGLOBEIncJP	false
140.251.58.29	unknown	United States		20252	JSIWMCUS	false
93.2.49.28	unknown	France		15557	LDCOMNETFR	false
123.26.120.242	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
136.236.253.143	unknown	United States		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
105.34.73.29	unknown	Egypt		37069	MOBINILEG	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
117.124.229.145	unknown	China		7641	CHINABTNChinaBroadcastingTVNetCN	false
170.80.238.157	unknown	Brazil		264900	RJNETTelecomunicacoesLtdaMEBR	false
79.206.197.157	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
83.216.89.97	unknown	United Kingdom		29009	UKBROADBAND-ASGB	false
47.148.154.31	unknown	United States		5650	FRONTIER-FRTRUS	false
145.184.172.234	unknown	Netherlands		59524	KPN-IAASNL	false
202.39.18.22	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
9.58.225.2	unknown	United States		3356	LEVEL3US	false
118.140.192.89	unknown	Hong Kong		9304	HUTCHISON-AS-APHGCGlobalCommunicationsLimitedHK	false
58.249.118.249	unknown	China		17622	CNCGROUP-GZChinaUnicomGuangzhounetworkCN	false
80.157.211.142	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
157.176.156.215	unknown	United States		22192	SSHENETUS	false
34.139.83.202	unknown	United States		2686	ATGS-MMD-ASUS	false
106.83.177.81	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
38.89.199.238	unknown	United States		174	COGENT-174US	false
205.162.26.114	unknown	United States		1239	SPRINTLINKUS	false
85.135.185.167	unknown	Slovakia (SLOVAK Republic)		8257	SLOVANET-BROADBANDhttpwwwslovanetnetSK	false
5.195.158.253	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
70.177.73.27	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
183.9.56.234	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
245.20.165.139	unknown	Reserved		unknown	unknown	false
2.135.247.76	unknown	Kazakhstan		9198	KAZTELECOM-ASKZ	false
116.151.71.20	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
80.15.108.19	unknown	France		3215	FranceTelecom-OrangeFR	false
175.201.107.84	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
146.24.16.91	unknown	United States		197938	TRAVIANGAMESDE	false
16.229.63.233	unknown	United States		unknown	unknown	false
242.240.230.159	unknown	Reserved		unknown	unknown	false
141.1.99.63	unknown	Germany		1273	CWVodafoneGroupPLCEU	false
212.189.34.190	unknown	Netherlands		286	KPNNL	false
250.203.44.27	unknown	Reserved		unknown	unknown	false
87.135.183.102	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
98.103.113.20	unknown	United States		10796	TWC-10796-MIDWESTUS	false
135.1.189.43	unknown	United States		10455	LUCENT-CIOUS	false
175.252.70.19	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
73.252.98.90	unknown	United States		7922	COMCAST-7922US	false
12.155.145.176	unknown	United States		7018	ATT-INTERNET4US	false
151.193.122.24	unknown	United States		13945	PRISMTECHNOLOGIESABQUS	false
145.235.141.99	unknown	Sweden		1257	TELE2EU	false
250.6.231.16	unknown	Reserved		unknown	unknown	false
46.191.173.29	unknown	Russian Federation		24955	UBN-ASRU	false
197.251.50.171	unknown	Sudan		37197	SUDRENSD	false
161.211.117.223	unknown	United States		14513	DMACCUS	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
152.0.229.102	unknown	Dominican Republic		6400	CompaniaDominicanadeTelefonosSADO	false
66.43.252.243	unknown	United States		5056	AUREON-5056US	false
37.96.237.17	unknown	Denmark		9158	TELENOR_DANMARK_ASDK	false
23.1.146.48	unknown	United States		6762	SEABONE-NETTELECOMITALIASPARKLESpAIT	false
205.143.2.90	unknown	United States		30404	BSCL-11US	false
169.11.240.130	unknown	United States		203	CENTURYLINK-LEGACY-LVLT-203US	false
145.161.131.111	unknown	Netherlands		59524	KPN-IAASNL	false
115.120.47.40	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
18.247.1.132	unknown	United States		16509	AMAZON-02US	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

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit MSB executable, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.3139750011225555
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	PPyJlaRy0K
File size:	61576
MD5:	6e38620768d8b3cd84319f2ee3d4235d
SHA1:	64a0eb90426549c47177b6d3f927a6fa7cd19cba
SHA256:	0d69d7b91837715976e968862b79a944fe3d074713ce2d80f678af5993df75ed

Copyright Joe Security LLC 2022

SHA512:	aed43619bb54c0c9a61f25166820e0ea99756fb427faa96958af0a4ae26e7ee4d8af86eadf87441cd2d9c3649707329873262307d171577197cb26093687d38e
SSDEEP:	1536:soBAmWmHv11dPBEMURJA87HONbg1pr8QOEawj0GKLUKQf8V:s0wMqeuprJFjsVQG
TLSH:	DE535CD9B8019E7DF58BEABE40224E0BF532761154921B377733FD83BD32169A816D0A
File Content Preview:	.ELF.....D...4.....4. ...(..... .....(..... .dt.Q.....NV..a...da.....N^NuNV..J9....f>"y.... QJ.g.X.#.....N."y.... QJ.f.A.....J.g.Hy....N.X.....N^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:	61176
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	0xe22a	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x8000e2d2	0xe2d2	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x8000e2e0	0xe2e0	0x9aa	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x80010c90	0xec90	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x80010c98	0xec98	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x80010ca4	0xeca4	0x214	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x80010eb8	0xeeb8	0x474	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xeeb8	0x3e	0x0	0x0		0	0	1

Program Segments

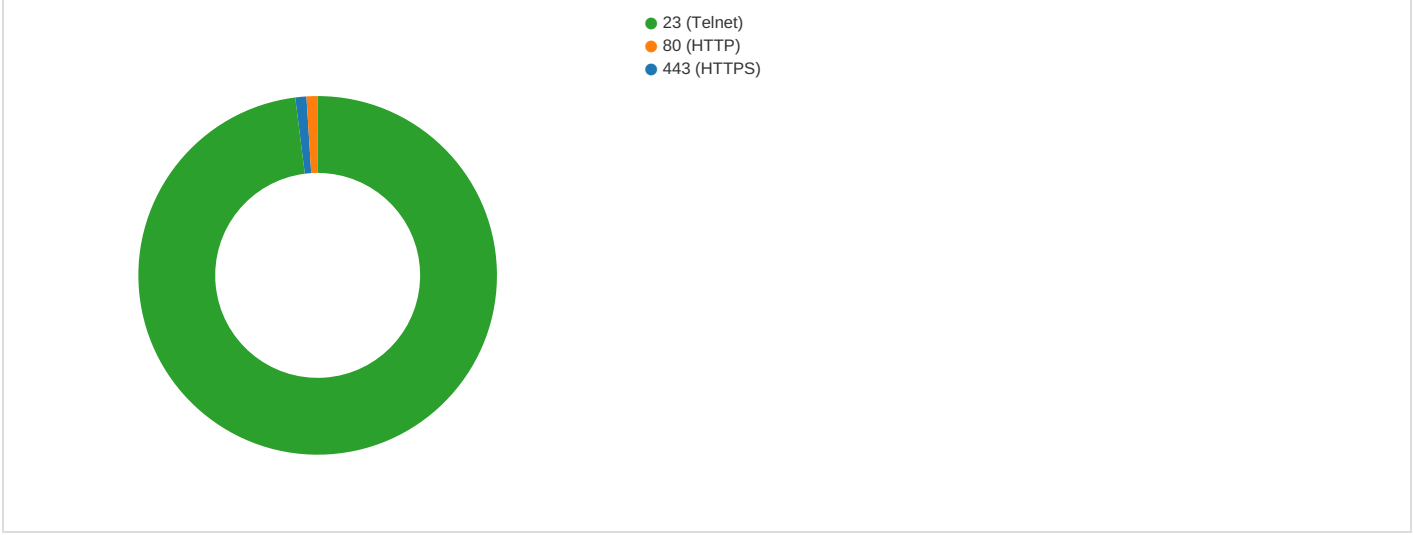
Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x80000000	0x80000000	0xec8a	0xec8a	6.3460	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0xec90	0x80010c90	0x80010c90	0x228	0x69c	3.0061	0x6	RW	0x2000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution

Total Packets: 100

Copyright Joe Security LLC 2022



TCP Packets

System Behavior

Analysis Process: PPyJlaRy0K PID: 6234, Parent PID: 6124

General

Start time:	21:53:52
Start date:	05/08/2022
Path:	/tmp/PPyJlaRy0K
Arguments:	/tmp/PPyJlaRy0K
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Deleted

File Read

Directory Deleted

Analysis Process: PPyJlaRy0K PID: 6236, Parent PID: 6234

General

Start time:	21:53:56
Start date:	05/08/2022
Path:	/tmp/PPyJlaRy0K
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: PPyJlaRy0K PID: 6238, Parent PID: 6234

General

Start time:	21:53:56
Start date:	05/08/2022
Path:	/tmp/PPyJlaRy0K
Arguments:	n/a
File size:	4463432 bytes

Copyright Joe Security LLC 2022

MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: PPyJlaRy0K PID: **6239**, Parent PID: **6234**

General

Start time:	21:53:56
Start date:	05/08/2022
Path:	/tmp/PPyJlaRy0K
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: PPyJlaRy0K PID: **6243**, Parent PID: **6234**

General

Start time:	21:53:56
Start date:	05/08/2022
Path:	/tmp/PPyJlaRy0K
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: PPyJlaRy0K PID: **6249**, Parent PID: **6243**

General

Start time:	21:54:02
Start date:	05/08/2022
Path:	/tmp/PPyJlaRy0K
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: PPyJlaRy0K PID: **6251**, Parent PID: **6243**

General

Start time:	21:54:02
Start date:	05/08/2022
Path:	/tmp/PPyJlaRy0K
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: PPyJlaRy0K PID: **6253**, Parent PID: **6243**

General

Start time:	21:54:02
Start date:	05/08/2022
Path:	/tmp/PPyJlaRy0K
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Copyright Joe Security LLC 2022