

ID: 626461
Sample Name: peYe24ayqp
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 03:49:31
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Linux Analysis Report peYe24ayqp 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Analysis Advice 4
General Information 4
Warnings 4
Runtime Messages 4
Process Tree 5
Yara Signatures 5
PCAP (Network Traffic) 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
Data Obfuscation 5
Hooking and other Techniques for Hiding and Protection 5
Stealing of Sensitive Information 5
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Malware Configuration 6
Behavior Graph 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Domains 7
URLs 7
Domains and IPs 7
Contacted Domains 7
URLs from Memory and Binaries 8
World Map of Contacted IPs 8
Public IPs 8
Joe Sandbox View / Context 10
IPs 10
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 11
General 11
Static ELF Info 11
ELF header 11
Program Segments 12
Network Behavior 12
Network Port Distribution 12
TCP Packets 12
System Behavior 12
Analysis Process: peYe24ayqp PID: 6228, Parent PID: 6125 12
General 12
File Activities 12
File Read 12
Analysis Process: peYe24ayqp PID: 6230, Parent PID: 6228 12
General 12
File Activities 13
File Read 13
Directory Enumerated 13
Analysis Process: peYe24ayqp PID: 6326, Parent PID: 6230 13
General 13
Analysis Process: peYe24ayqp PID: 6329, Parent PID: 6230 13
General 13
Analysis Process: peYe24ayqp PID: 6334, Parent PID: 6329 13
General 13
Analysis Process: peYe24ayqp PID: 6344, Parent PID: 6334 13
General 13
Analysis Process: peYe24ayqp PID: 6345, Parent PID: 6334 13
General 13
Analysis Process: peYe24ayqp PID: 6336, Parent PID: 6329 14
General 14
Analysis Process: peYe24ayqp PID: 6338, Parent PID: 6329 14
General 14
Analysis Process: peYe24ayqp PID: 6231, Parent PID: 6228 14
General 14

Copyright Joe Security LLC 2022

Analysis Process: peYe24ayqp PID: 6232, Parent PID: 6228 14
General 14
Analysis Process: peYe24ayqp PID: 6236, Parent PID: 6232 14
General 14
File Activities 14
File Read 14
Directory Enumerated 14
Analysis Process: peYe24ayqp PID: 6327, Parent PID: 6236 14
General 14
Analysis Process: peYe24ayqp PID: 6331, Parent PID: 6236 15
General 15
Analysis Process: peYe24ayqp PID: 6238, Parent PID: 6232 15
General 15
Analysis Process: peYe24ayqp PID: 6239, Parent PID: 6232 15
General 15

Copyright Joe Security LLC 2022

Linux Analysis Report

peYe24ayqp

Overview

General Information

Sample Name:	peYe24ayqp
Analysis ID:	626461
MD5:	9bfc4e323b0925..
SHA1:	9a6e06578d0f9e..
SHA256:	1e85e1f64e03c6..
Tags:	32 elf mips mirai
Infos:	

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

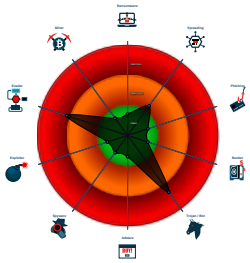
Mirai

Score:	64
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Uses known network protocols on n…
- Sample contains only a LOAD segm…
- 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.

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626461
Start date and time: 14/05/202203:49:31	2022-05-14 03:49:31 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	peYe24ayqp
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:	mal64.troj.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/peYe24ayqp
PID:	6228
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC

Copyright Joe Security LLC 2022

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- peYe24ayqp (PID: 6228, Parent: 6125, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/peYe24ayqp
  - peYe24ayqp New Fork (PID: 6230, Parent: 6228)
    - peYe24ayqp New Fork (PID: 6326, Parent: 6230)
    - peYe24ayqp New Fork (PID: 6329, Parent: 6230)
      - peYe24ayqp New Fork (PID: 6334, Parent: 6329)
        - peYe24ayqp New Fork (PID: 6344, Parent: 6334)
        - peYe24ayqp New Fork (PID: 6345, Parent: 6334)
      - peYe24ayqp New Fork (PID: 6336, Parent: 6329)
      - peYe24ayqp New Fork (PID: 6338, Parent: 6329)
    - peYe24ayqp New Fork (PID: 6231, Parent: 6228)
    - peYe24ayqp New Fork (PID: 6232, Parent: 6228)
      - peYe24ayqp New Fork (PID: 6236, Parent: 6232)
        - peYe24ayqp New Fork (PID: 6327, Parent: 6236)
        - peYe24ayqp New Fork (PID: 6331, Parent: 6236)
      - peYe24ayqp New Fork (PID: 6238, Parent: 6232)
      - peYe24ayqp New Fork (PID: 6239, Parent: 6232)
- **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



Multi AV Scanner detection for submitted file

Networking



Uses known network protocols on non-standard ports

Data Obfuscation



Sample is packed with UPX

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

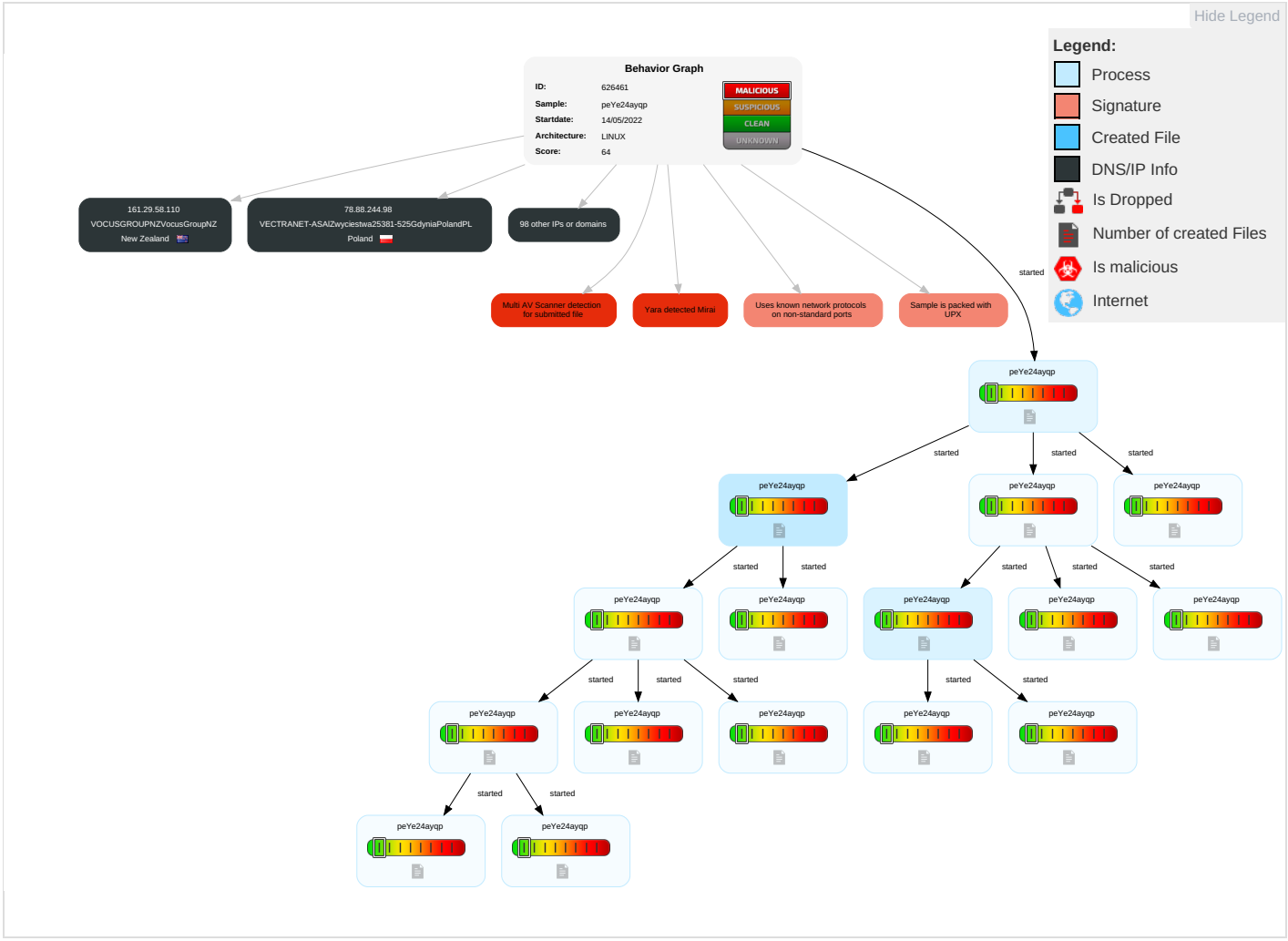
Mitre Att&ck Matrix

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	1 Obfuscated Files or Information	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 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
peYe24ayqp	39%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

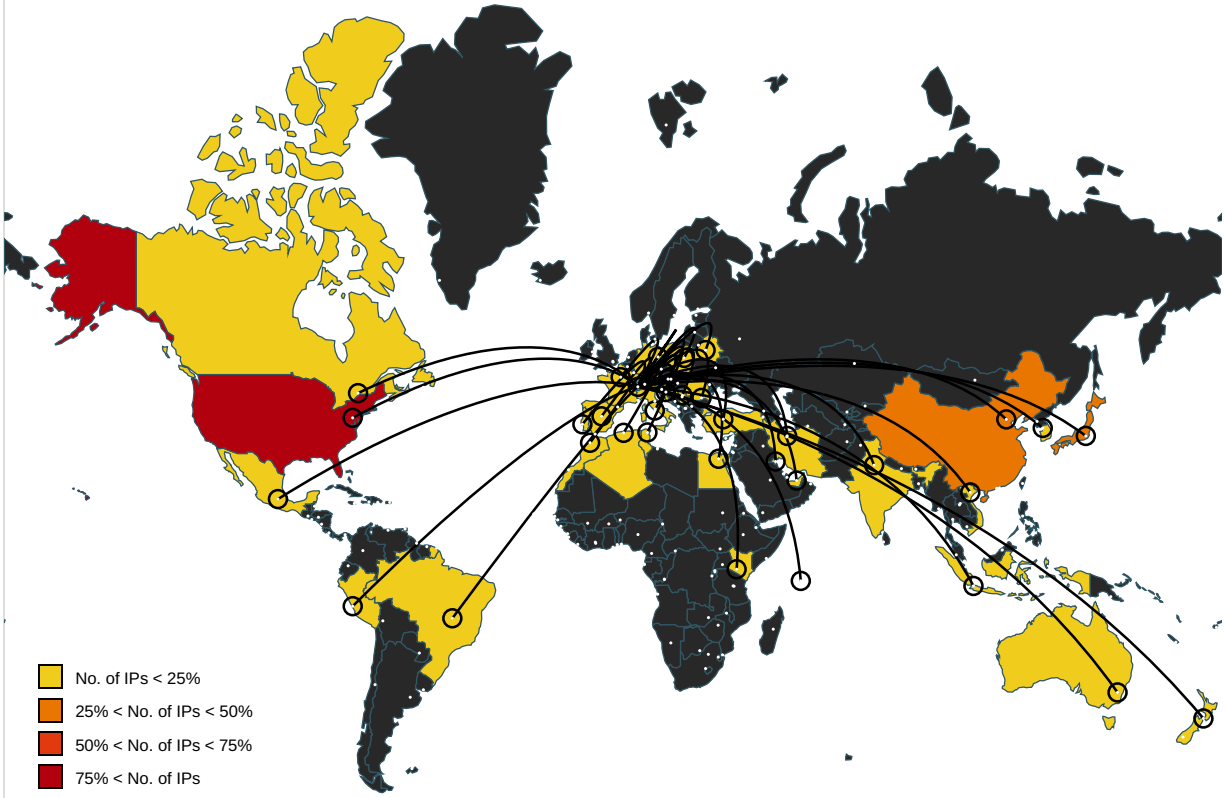
Domains and IPs

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
14.29.123.26	unknown	China		58466	CT-GUANGZHOU-IDCCHINANETGuangdongprovincenetworkCN	false
68.146.32.212	unknown	Canada		6327	SHAWCA	false
102.55.12.135	unknown	Morocco		6713	IAM-ASMA	false
119.135.93.16	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
4.126.218.135	unknown	United States		3356	LEVEL3US	false
161.29.58.110	unknown	New Zealand		9790	VOCUSGROUPNZVocusGroupNZ	false
190.41.237.126	unknown	Peru		6147	TelefonicadelPeruSAAPE	false
157.199.114.232	unknown	United States		3356	LEVEL3US	false
133.84.240.180	unknown	Japan		55904	KOGAKUIN-ASKOGAKUINUniversityJP	false
32.129.235.55	unknown	United States		2686	ATGS-MMD-ASUS	false
24.210.193.128	unknown	United States		10796	TWC-10796-MIDWESTUS	false
177.35.57.101	unknown	Brazil		28573	CLAROSABR	false
253.161.145.216	unknown	Reserved		unknown	unknown	false
58.208.50.191	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
160.27.251.134	unknown	Japan		9371	SAKURA-CSAKURAInternetIncJP	false
14.222.189.102	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
240.152.191.178	unknown	Reserved		unknown	unknown	false
60.181.164.23	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
42.116.150.25	unknown	Viet Nam		18403	FPT-AS-APTheCorporationforFinancingPromotingTechnolo	false
95.229.249.242	unknown	Italy		3269	ASN-IBSNAZIT	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
68.232.101.62	unknown	United States		21570	ACI-1CA	false
252.212.204.102	unknown	Reserved		unknown	unknown	false
240.245.1.2	unknown	Reserved		unknown	unknown	false
161.93.54.151	unknown	Japan		14298	EPA-NETUS	false
46.56.82.245	unknown	Belarus		25106	MTSBY-ASBY	false
41.215.59.21	unknown	Kenya		15808	ACCESSKENYA-KEACCESSKENYAGROUPLTDisanISPservingKE	false
59.84.94.186	unknown	Japan		10010	TOKAITOKAICommunicationsCorporationJP	false
207.123.91.124	unknown	United States		3356	LEVEL3US	false
45.2.242.94	unknown	Canada		7311	FRONTIERCA	false
78.166.82.213	unknown	Turkey		9121	TTNETTR	false
187.218.161.255	unknown	Mexico		8151	UninetSAdeCVMX	false
12.175.157.173	unknown	United States		7018	ATT-INTERNET4US	false
194.175.56.102	unknown	Germany		702	UUNETUS	false
43.110.126.185	unknown	Japan		4249	LILLY-ASUS	false
74.205.21.243	unknown	United States		27357	RACKSPACEUS	false
113.155.242.51	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
39.205.48.21	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
93.143.119.222	unknown	Croatia (LOCAL Name: Hrvatska)		5391	T-HTCroatianTelecomIncHR	false
14.49.183.189	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
105.108.43.204	unknown	Algeria		36947	ALGTEL-ASDZ	false
32.66.61.204	unknown	United States		2686	ATGS-MMD-ASUS	false
81.223.241.91	unknown	Austria		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
142.124.141.1	unknown	Canada		577	BACOMCA	false
169.209.98.56	unknown	Korea Republic of		37611	AfrihostZA	false
209.101.91.219	unknown	United States		4565	MEGAPATH2-US	false
210.212.47.131	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
86.55.160.151	unknown	Iran (ISLAMIC Republic Of)		197207	MCCI-ASIR	false
210.212.47.132	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
89.45.44.194	unknown	Romania		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
156.146.203.249	unknown	United States		1448	UNITED-BROADBANDUS	false
35.21.235.111	unknown	United States		36375	UMICH-AS-5US	false
62.215.172.89	unknown	Kuwait		21050	FAST-TELCOKW	false
110.42.146.95	unknown	China		136188	CHINATELECOM-ZHEJIANG-NINGBO-IDCNINGBOZHEJIANGProvince	false
252.12.195.243	unknown	Reserved		unknown	unknown	false
78.88.244.98	unknown	Poland		29314	VECTRANET-ASAlZwyciestwa25381-525GdyniaPolandPL	false
213.13.73.149	unknown	Portugal		3243	MEO-RESIDENCIALPT	false
39.29.179.34	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
37.165.124.192	unknown	France		51207	FREEMFR	false
69.174.188.24	unknown	United States		54373	MESSAGEEXPRESSINTERNETUS	false
107.232.142.23	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
172.141.183.80	unknown	United States		7018	ATT-INTERNET4US	false
89.62.186.148	unknown	Germany		5430	FREENETDEfreenetDatenkommunikationsGmbHDE	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.228.181.104	unknown	United States		7018	ATT-INTERNET4US	false
254.126.128.144	unknown	Reserved		unknown	unknown	false
31.193.145.83	unknown	Iran (ISLAMIC Republic Of)		58224	TCIIR	false
100.167.204.98	unknown	United States		21928	T-MOBILE-AS21928US	false
121.65.193.191	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
203.23.189.104	unknown	unknown		17914	MULTIBASETECH-AS-APMultibaseTechnologiesPtyLtdAU	false
142.121.109.61	unknown	Canada		577	BACOMCA	false
182.251.40.205	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
249.7.138.185	unknown	Reserved		unknown	unknown	false
58.44.27.66	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
102.40.44.183	unknown	Egypt		8452	TE-ASTE-ASEG	false
165.170.160.55	unknown	United States		5647	ASN-KODAKUS	false
196.177.152.107	unknown	Tunisia		37693	TUNISIANATN	false
187.206.32.243	unknown	Mexico		8151	UninetSAdeCVMX	false
172.255.161.128	unknown	United States		395954	LEASEWEB-USA-LAX-11US	false
31.215.25.216	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
189.218.211.162	unknown	Mexico		11888	TelevisionInternacionalSAdeCVMX	false
196.17.109.119	unknown	Seychelles		9009	M247GB	false
74.66.112.106	unknown	United States		12271	TWC-12271-NYCUS	false
195.176.251.214	unknown	Switzerland		559	SWITCHPeeringrequestspeeringswitchchEU	false
98.60.86.32	unknown	United States		7922	COMCAST-7922US	false
121.44.190.55	unknown	Australia		4739	INTERNODE-ASInternodePtyLtdAU	false
202.218.0.120	unknown	Japan		4694	IDCFIDCFrontierIncJP	false
117.58.42.55	unknown	China		4782	GSNETDataCommunicationBusinessGroupTW	false
117.69.181.50	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
109.93.37.75	unknown	Serbia		8400	TELEKOM-ASRS	false
83.54.6.155	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
147.195.9.104	unknown	United States		15128	COMWAVE-BGP-01CA	false
8.90.239.74	unknown	United States		3356	LEVEL3US	false
153.158.25.137	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
71.19.80.21	unknown	Canada		14366	MNTNCA	false
92.184.7.87	unknown	France		12479	UNI2-ASES	false
85.136.26.187	unknown	Spain		12357	COMUNITELSPAINES	false
35.149.133.149	unknown	United States		394141	ROCKET-FIBERUS	false
18.81.216.181	unknown	United States		3	MIT-GATEWAYSUS	false
68.219.64.2	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
61.242.114.67	unknown	China		17622	CNCGROUP-GZChinaUnicomGuangzhounetworkCN	false
104.94.61.209	unknown	United States		16625	AKAMAI-ASUS	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, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	7.871636882566792
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	peYe24ayqp
File size:	26184
MD5:	9bfc4e323b0925534fea18588b776a79
SHA1:	9a6e06578d0f9ebfc65c39c513b4c6ee9015a6b0
SHA256:	1e85e1f64e03c60ea0cdf08ef7227e6153fad2810dff6a58a0c49da88fce3c9b
SHA512:	90e59d30018fafdad426a28fd1cd8e9c8453b34753b8d93233910171c7b8ecdaeec215f60e1b305a414447ef4e86f60ee55b55e7ad13400f62c74c596f2f9d45
SSDEEP:	768:I2G214DFyosXqgvV9o1ndB08FJgGlzDpbuR1JK:I2GdDgosaaO1ndVVJu8
TLSH:	B6C2D088274919E9C2F9C13843B81B6919B40FAAF80ADC8578F8F7529D8E4753057ED9
File Content Preview:	.ELF.....Q....4.....4. ...(.....e...e.....E...E.....UPX!.h.....T...T.....T.....?.E.h4...@b..) ..]....E...GS.U....e5.T3z".J{..m...|0.L.!Q.....j...].....Yt.//..@...,..N.....

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:	0x1051d8
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	2

Copyright Joe Security LLC 2022

ELF header

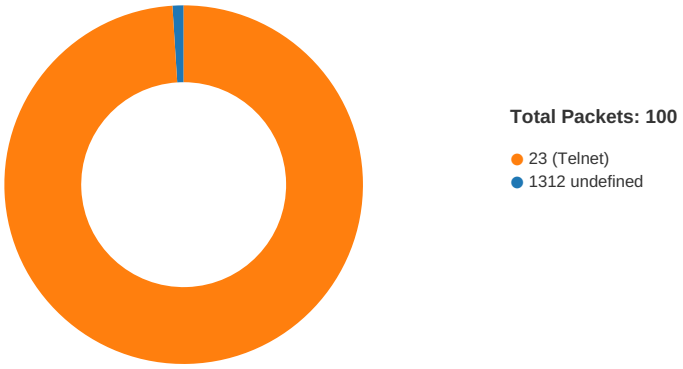
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x100000	0x100000	0x651c	0x651c	4.1678	0x5	R E	0x10000		
LOAD	0x18c0	0x4518c0	0x4518c0	0x0	0x0	0.0000	0x6	RW	0x10000		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: peYe24ayqp PID: 6228, Parent PID: 6125

General

Start time:	03:50:16
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp
Arguments:	/tmp/peYe24ayqp
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: peYe24ayqp PID: 6230, Parent PID: 6228

General

Start time:	03:50:16
Start date:	14/05/2022

Copyright Joe Security LLC 2022

Path:	/tmp/peYe24ayqp
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: peYe24ayqp PID: **6326**, Parent PID: **6230**

General

Start time:	03:53:07
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: peYe24ayqp PID: **6329**, Parent PID: **6230**

General

Start time:	03:53:07
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: peYe24ayqp PID: **6334**, Parent PID: **6329**

General

Start time:	03:53:07
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: peYe24ayqp PID: **6344**, Parent PID: **6334**

General

Start time:	03:53:12
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: peYe24ayqp PID: **6345**, Parent PID: **6334**

General

Start time:	03:53:12
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Copyright Joe Security LLC 2022

Analysis Process: peYe24ayqp PID: **6336**, Parent PID: **6329**

General

Start time:	03:53:07
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: peYe24ayqp PID: **6338**, Parent PID: **6329**

General

Start time:	03:53:07
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: peYe24ayqp PID: **6231**, Parent PID: **6228**

General

Start time:	03:50:16
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: peYe24ayqp PID: **6232**, Parent PID: **6228**

General

Start time:	03:50:16
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: peYe24ayqp PID: **6236**, Parent PID: **6232**

General

Start time:	03:50:16
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: peYe24ayqp PID: **6327**, Parent PID: **6236**

General

Start time:	03:53:07
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp

Copyright Joe Security LLC 2022

Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: peYe24ayqp PID: **6331**, Parent PID: **6236**

General

Start time:	03:53:07
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: peYe24ayqp PID: **6238**, Parent PID: **6232**

General

Start time:	03:50:16
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: peYe24ayqp PID: **6239**, Parent PID: **6232**

General

Start time:	03:50:16
Start date:	14/05/2022
Path:	/tmp/peYe24ayqp
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Copyright Joe Security LLC 2022