ID: 680645
Sample Name: 6e180puJTD
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 23:11:37
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

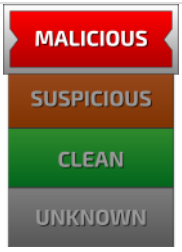
6e180puJTD

Overview

General Information

Sample Name:	6e180puJTD
Analysis ID:	680645
MD5:	b19338343c7925..
SHA1:	584b5f2f0dd993a.
SHA256:	091731e0f53b9f9.
Tags:	32 elf mirai renesas
Infos:	

Detection



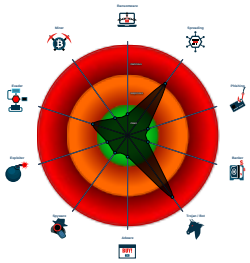
Mirai

Score:	80
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Uses known network protocols on n…
- Sample tries to kill multiple process…
- Yara signature match
- 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…

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:	680645
Start date and time: 08/08/202223:11:37	2022-08-08 23:11:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6e180puJTD
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:	mal80.spre.troj.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/6e180puJTD
PID:	6227
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- 6e180puJTD (PID: 6227, Parent: 6121, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/6e180puJTD
  - 6e180puJTD New Fork (PID: 6229, Parent: 6227)
  - 6e180puJTD New Fork (PID: 6230, Parent: 6227)
  - 6e180puJTD New Fork (PID: 6232, Parent: 6227)
    - 6e180puJTD New Fork (PID: 6235, Parent: 6232)
      - 6e180puJTD New Fork (PID: 6337, Parent: 6235)
      - 6e180puJTD New Fork (PID: 6339, Parent: 6235)
    - 6e180puJTD New Fork (PID: 6236, Parent: 6232)
    - 6e180puJTD New Fork (PID: 6237, Parent: 6232)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
6e180puJTD	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6e180puJTD	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xdf64:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdf78:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdf8c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdfa0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdfb4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdfc8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdfdc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdff0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe004:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe018:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe02c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe040:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe054:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe068:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe07c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe090:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0a4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0b8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0cc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0e0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0f4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6e180puJTD	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0xe4bc:$a: 53 65 6C 66 20 52 65 70 20 46 75 63 6B 69 6E 67 20 4E 65 54 69 53 20 61 6E 64

PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
6337.1.00007f87d0400000.00007f87d0410000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6237.1.00007f87d0400000.00007f87d0410000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6337.1.00007f87d0400000.00007f87d0410000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xdf64:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdf78:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdf8c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdfa0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdfb4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdfc8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdfdc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdff0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe004:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe018:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe02c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe040:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe054:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe068:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe07c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe090:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0a4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0b8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0cc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0e0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0f4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6337.1.00007f87d0400000.00007f87d0410000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0xe4bc:$a: 53 65 6C 66 20 52 65 70 20 46 75 63 6B 69 6E 67 20 4E 65 54 69 53 20 61 6E 64

Source	Rule	Description	Author	Strings
6237.1.00007f87d0400000.00007f87d0410000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xdf64:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdf78:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdf8c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdfa0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdfb4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdfc8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdfdc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xdff0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe004:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe018:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe02c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe040:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe054:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe068:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe07c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe090:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0a4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0b8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0cc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0e0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe0f4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
Click to see the 25 entries				

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

System Summary

Malicious sample detected (through community Yara rule)

Sample tries to kill multiple 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

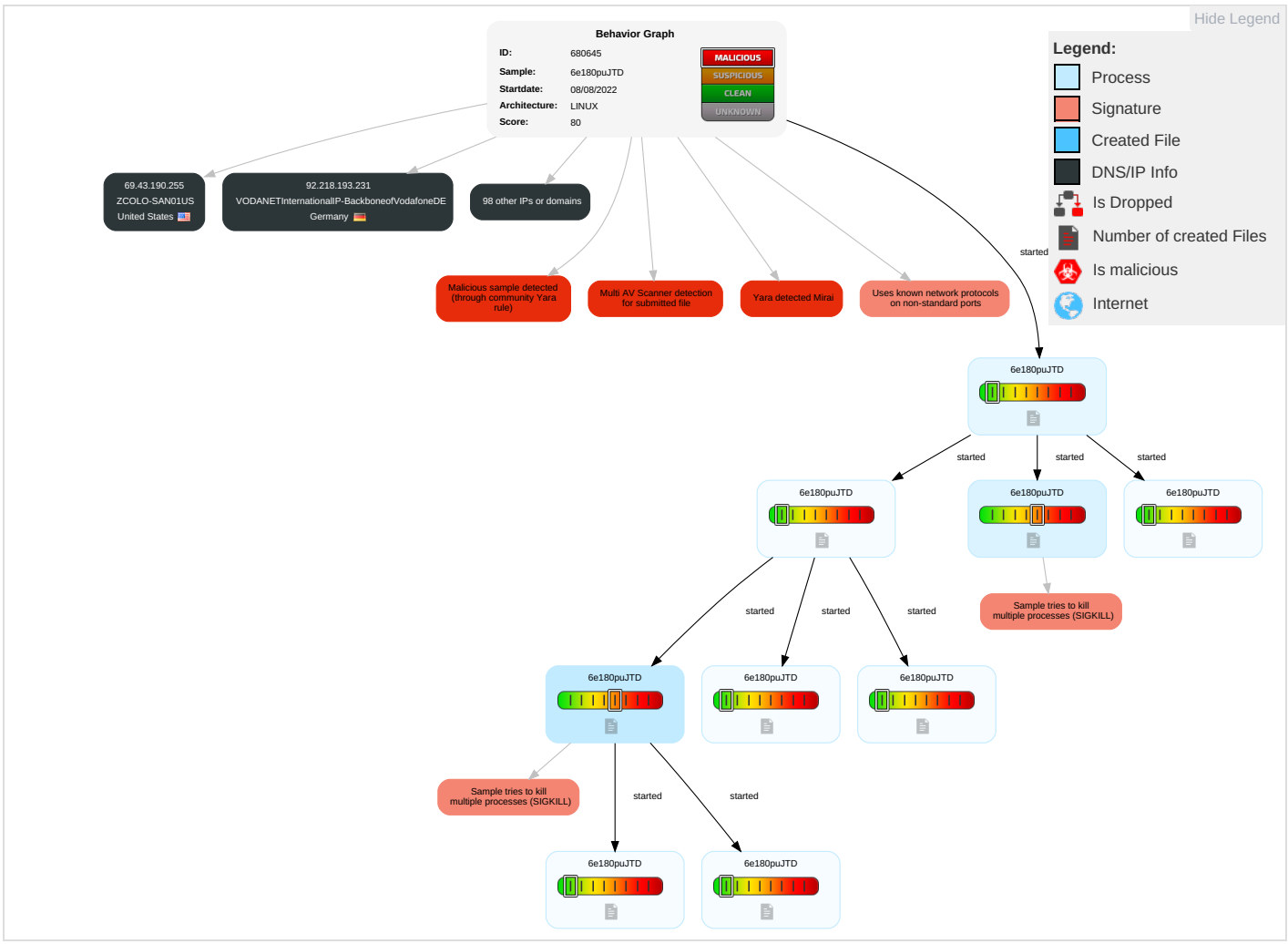
Mitre Att&ck Matrix

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	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	1 Service Stop
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
6e180puJTD	54%	Virustotal		Browse
6e180puJTD	54%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

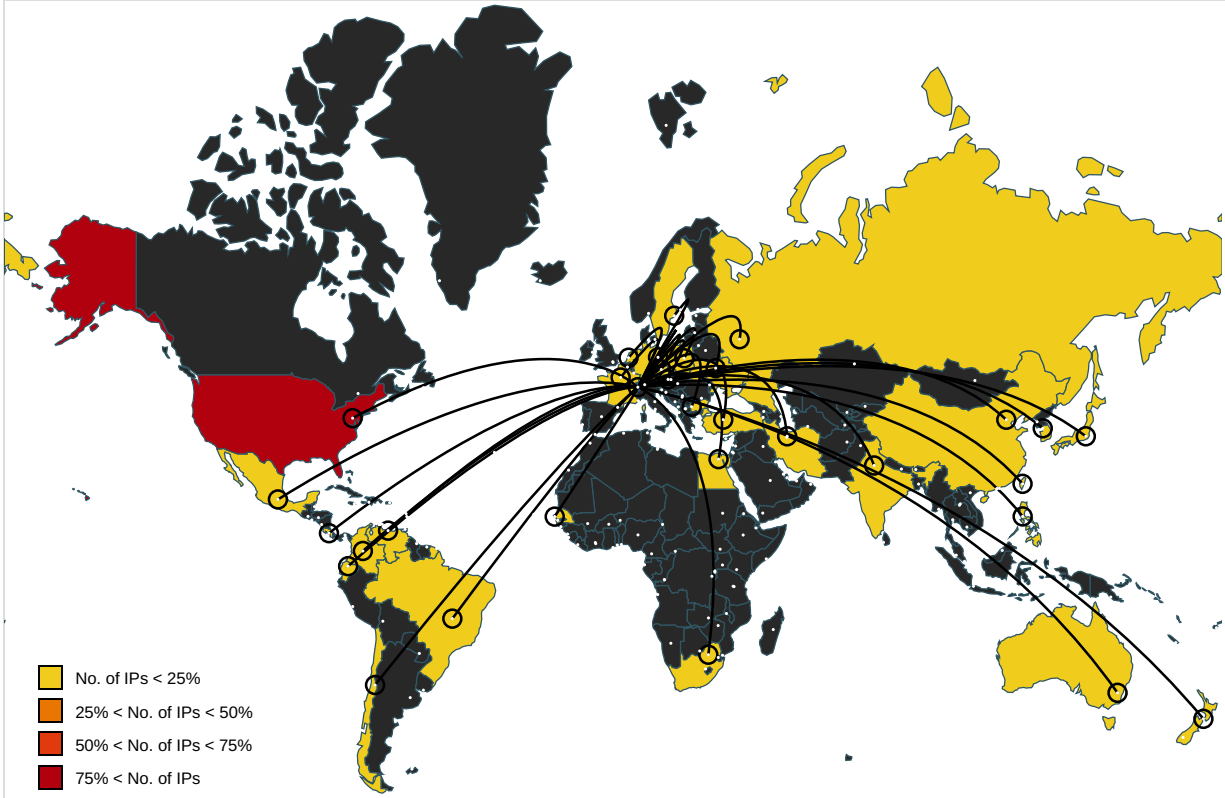
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
241.48.61.17	unknown	Reserved		unknown	unknown	false
202.4.16.34	unknown	New Zealand		7306	ASIANDEVBANKUS	false
92.218.193.231	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
111.45.222.204	unknown	China		56044	CMNET-AS-LIAONINGChinaMobilecommunicationscorporationC	false
213.154.66.80	unknown	Senegal		8346	SONATEL-ASAutonomousSystemEU	false
170.167.20.34	unknown	United States		19739	COUNTY-SANBERNARDINOUS	false
23.57.232.20	unknown	United States		16625	AKAMAI-ASUS	false
94.72.180.46	unknown	Bulgaria		42735	MAXTELECOM-ASBG	false
152.53.64.70	unknown	United States		81	NCRENUS	false
181.254.19.203	unknown	Colombia		26611	COMCELSACO	false
112.198.124.93	unknown	Philippines		132199	GLOBE-MOBILE-5TH-GEN-ASGlobeTelecomIncPH	false
42.32.216.135	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
216.253.193.160	unknown	United States		3549	LVLT-3549US	false
255.25.47.63	unknown	Reserved		unknown	unknown	false
116.75.187.136	unknown	India		17488	HATHWAY-NET-APHathwayIPOverCableInternetIN	false
152.140.145.146	unknown	United States		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
136.114.115.150	unknown	United States		15169	GOOGLEUS	false
61.199.87.85	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
121.243.246.239	unknown	India		17908	TCISLTataCommunicationsIN	false
201.236.67.216	unknown	Chile		15311	TelefonicaEmpresasCL	false
105.219.30.248	unknown	South Africa		16637	MTNNS-ASZA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
211.228.82.203	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
23.211.33.0	unknown	United States		20940	AKAMAI-ASN1EU	false
54.62.178.249	unknown	United States		14618	AMAZON-AESUS	false
106.8.250.67	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
245.43.211.188	unknown	Reserved		unknown	unknown	false
240.188.31.120	unknown	Reserved		unknown	unknown	false
53.84.230.224	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
89.166.205.104	unknown	Germany		9145	EWETELCloppenburgerStrasse310DE	false
211.238.83.67	unknown	Korea Republic of		9976	ICNDP-AS-KRNamincheonBrodcastingCoLtdKR	false
248.231.5.213	unknown	Reserved		unknown	unknown	false
181.199.34.216	unknown	Ecuador		27947	TelconetSAEC	false
212.182.0.33	unknown	Poland		12324	LUBMAN-EDU-ASPolandLublinPL	false
99.25.205.72	unknown	United States		7018	ATT-INTERNET4US	false
162.47.196.174	unknown	United States		3378	MCI-ASNUS	false
221.135.3.139	unknown	India		9583	SIFY-AS-INSifyLimitedIN	false
107.239.142.218	unknown	United States		20057	ATT-MOBILITY-LLC-AS20057US	false
148.171.245.152	unknown	United States		397879	LUMINATE-01US	false
194.6.220.151	unknown	Russian Federation		197498	VERBETA-ASRU	false
170.249.28.22	unknown	United States		46208	PFNL-ASNUS	false
161.87.168.161	unknown	Netherlands		14298	EPA-NETUS	false
182.223.152.232	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
149.166.36.96	unknown	United States		87	INDIANA-ASUS	false
160.248.62.68	unknown	Japan		2514	INFOSPHERENTTPCCommunicationsIncJP	false
69.43.190.255	unknown	United States		22489	ZCOLO-SAN01US	false
180.149.166.204	unknown	Japan		4721	JCNJupiterTelecommunicationsCoLtdJP	false
27.168.199.202	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
12.202.34.160	unknown	United States		22983	FISERV-INCUS	false
90.39.150.123	unknown	France		3215	FranceTelecom-OrangeFR	false
190.72.15.38	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	false
223.1.225.83	unknown	China		63555	CNBIDCCBeijingBeilongYunhaiNetworkDataTechnologyCorpo	false
154.50.90.162	unknown	United States		174	COGENT-174US	false
107.164.228.73	unknown	United States		18779	EGIHOSTINGUS	false
153.237.4.55	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
20.58.232.198	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
242.167.10.248	unknown	Reserved		unknown	unknown	false
198.154.232.182	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
80.119.148.81	unknown	France		15557	LDCOMNETFR	false
159.11.199.53	unknown	United States		16983	AS16983US	false
135.89.233.67	unknown	United States		10455	LUCENT-CIOUS	false
9.172.236.202	unknown	United States		3356	LEVEL3US	false
146.120.215.100	unknown	Czech Republic		61240	SKYNET2010-ASUA	false
178.245.89.170	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
123.46.180.186	unknown	Korea Republic of		6619	SAMSUNGSDS-AS-KRSamsungSDSIncKR	false
153.178.204.6	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
39.114.213.225	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
12.247.187.54	unknown	United States		7018	ATT-INTERNET4US	false
71.211.10.242	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
167.27.235.115	unknown	United States		7838	USAAUS	false
2.145.36.98	unknown	Iran (ISLAMIC Republic Of)		44244	IRANCELL-ASIR	false
210.194.84.73	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
246.109.35.156	unknown	Reserved		unknown	unknown	false
200.102.192.29	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
69.119.225.193	unknown	United States		6128	CABLE-NET-1US	false
58.107.214.72	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
141.201.90.37	unknown	Austria		1109	UNI-SALZBURGUniversityofSalzburgAT	false
66.157.86.21	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
141.95.237.110	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
201.166.226.252	unknown	Mexico		11888	TelevisionInternacionalSAdeCVMX	false
67.24.66.23	unknown	United States		202818	LEVEL3COMMUNICATIONSFR	false
37.55.245.82	unknown	Ukraine		6849	UKRTELNETUA	false
89.59.121.171	unknown	Germany		5430	FREENETDEfreenetDatenkommunikationsGmbHDE	false
175.183.201.54	unknown	Taiwan; Republic of China (ROC)		18049	TINP-TWTaiwanInfrastructureNetworkTechnologieTW	false
254.14.236.113	unknown	Reserved		unknown	unknown	false
184.85.6.114	unknown	United States		16625	AKAMAI-ASUS	false
184.209.135.95	unknown	United States		10507	SPCSUS	false
107.114.209.29	unknown	United States		7018	ATT-INTERNET4US	false
173.73.28.233	unknown	United States		701	UUNETUS	false
251.157.26.163	unknown	Reserved		unknown	unknown	false
73.108.225.174	unknown	United States		7922	COMCAST-7922US	false
92.33.148.109	unknown	Sweden		2119	TELENOR-NEXTELTelenorNorgeASNO	false
141.166.179.222	unknown	United States		20105	URICHMONDUS	false
46.118.113.132	unknown	Ukraine		15895	KSNET-ASUA	false
242.215.49.122	unknown	Reserved		unknown	unknown	false
163.178.130.139	unknown	Costa Rica		11830	InstitutoCostarricensedeElectricidadyTelecomCR	false
41.35.35.120	unknown	Egypt		8452	TE-ASTE-ASEG	false
152.253.191.168	unknown	Brazil		26599	TELEFONICABRASILSABR	false
75.203.185.46	unknown	United States		22394	CELLCOUS	false
199.52.203.174	unknown	United States		398192	ARDOT-NET-01US	false
12.189.115.9	unknown	United States		7018	ATT-INTERNET4US	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 LSB executable, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.776759926089661
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	6e180puJTD
File size:	63480
MD5:	b19338343c7925b9ee1683f1371171f4
SHA1:	584b5f2f0dd993ab0e12869ec59f286174e31b18
SHA256:	091731e0f53b9f9b1c7d7c84b037c197b839949988d47aed4c8e23d6f3edaed5
SHA512:	4366eae63878492ddbb82a20ab2a90eec1f2387efcc5fbee67512fa17748222b41ecf8e3430f4d7b82f9ef1ae8452a51d94008491fc647eb3a50ca26aabb1dfb
SSDEEP:	1536:ragXV1f1Fl/wtkniPQauiufs3li3O/qyD6EZeCc:r57f1b/0QHf+Iey6EZe
TLSH:	1D538D75D12DAEA8C0414AB4A9198E704F13E4C046733EF7EA9587A68443DBCF858FF8
File Content Preview:	.ELF.....*.....@.4...h.....4. ... (.....@...@.....A...A.$.....Q.td....././"O.n.....#.*@.....#.*@L....o&O.n...l....././.../.a"O.!...n...a.b("...q.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	<unknown>
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x4001a0
Flags:	0x9
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	63080
Section Header Size:	40
Number of Section Headers:	10

ELF header

Header String Table Index:	9

Sections

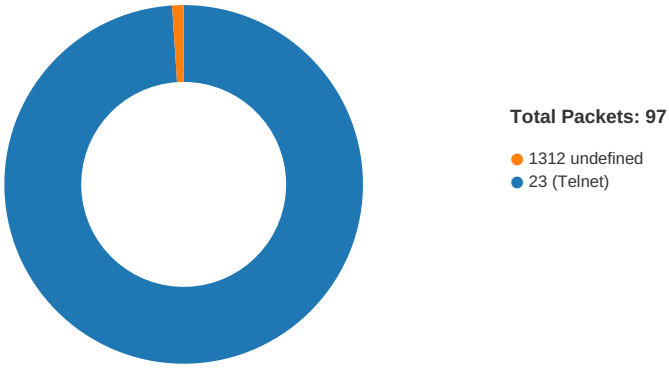
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x30	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x4000e0	0xe0	0xde60	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x40df40	0xdf40	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x40df64	0xdf64	0x149c	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x41f404	0xf404	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x41f40c	0xf40c	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x41f418	0xf418	0x210	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x41f628	0xf628	0x280	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xf628	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	0x400000	0x400000	0xf400	0xf400	6.8133	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xf404	0x41f404	0x41f404	0x224	0x4a4	2.9546	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: 6e180puJTD PID: 6227, Parent PID: 6121

General

Start time:	23:17:51
Start date:	08/08/2022
Path:	/tmp/6e180puJTD

Arguments:	/tmp/6e180puJTD
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Analysis Process: 6e180puJTD PID: **6229**, Parent PID: **6227**

General

Start time:	23:17:51
Start date:	08/08/2022
Path:	/tmp/6e180puJTD
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: 6e180puJTD PID: **6230**, Parent PID: **6227**

General

Start time:	23:17:51
Start date:	08/08/2022
Path:	/tmp/6e180puJTD
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: 6e180puJTD PID: **6232**, Parent PID: **6227**

General

Start time:	23:17:51
Start date:	08/08/2022
Path:	/tmp/6e180puJTD
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: 6e180puJTD PID: **6235**, Parent PID: **6232**

General

Start time:	23:17:51
Start date:	08/08/2022
Path:	/tmp/6e180puJTD
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Directory Enumerated

Analysis Process: 6e180puJTD PID: **6337**, Parent PID: **6235**

General

Start time:	23:21:01
Start date:	08/08/2022

Path:	/tmp/6e180puJTD
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: 6e180puJTD PID: **6339**, Parent PID: **6235**

General

Start time:	23:21:01
Start date:	08/08/2022
Path:	/tmp/6e180puJTD
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: 6e180puJTD PID: **6236**, Parent PID: **6232**

General

Start time:	23:17:51
Start date:	08/08/2022
Path:	/tmp/6e180puJTD
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: 6e180puJTD PID: **6237**, Parent PID: **6232**

General

Start time:	23:17:51
Start date:	08/08/2022
Path:	/tmp/6e180puJTD
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9