ID: 680657
Sample Name: 2DbzKHhgOH
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 23:35:59
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

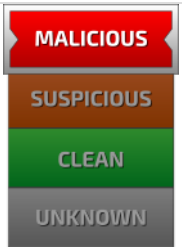
2DbzKHhgOH

Overview

General Information

Sample Name:	2DbzKHhgOH
Analysis ID:	680657
MD5:	91e1ba2317dac6..
SHA1:	314ac7afbe482e..
SHA256:	7610f435e009a5..
Tags:	32 elf mirai sparc
Infos:	

Detection



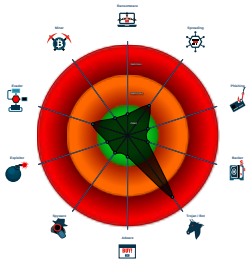
Mirai

Score:	76
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…
- 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…
- Sample listens on a socket

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:	680657
Start date and time: 08/08/202223:35:59	2022-08-08 23:35:59 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2DbzKHhgOH
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:	mal76.troj.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/2DbzKHhgOH
PID:	6223
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- 2DbzKHhgOH (PID: 6223, Parent: 6120, MD5: 7dc1c0e23cd5e102bb12e5c29403410e) Arguments: /tmp/2DbzKHhgOH
  - 2DbzKHhgOH New Fork (PID: 6226, Parent: 6223)
    - 2DbzKHhgOH New Fork (PID: 6242, Parent: 6226)
    - 2DbzKHhgOH New Fork (PID: 6244, Parent: 6226)
      - 2DbzKHhgOH New Fork (PID: 6246, Parent: 6244)
        - 2DbzKHhgOH New Fork (PID: 6256, Parent: 6246)
        - 2DbzKHhgOH New Fork (PID: 6257, Parent: 6246)
      - 2DbzKHhgOH New Fork (PID: 6251, Parent: 6244)
      - 2DbzKHhgOH New Fork (PID: 6253, Parent: 6244)
    - 2DbzKHhgOH New Fork (PID: 6227, Parent: 6223)
    - 2DbzKHhgOH New Fork (PID: 6229, Parent: 6223)
      - 2DbzKHhgOH New Fork (PID: 6232, Parent: 6229)
        - 2DbzKHhgOH New Fork (PID: 6260, Parent: 6232)
        - 2DbzKHhgOH New Fork (PID: 6262, Parent: 6232)
      - 2DbzKHhgOH New Fork (PID: 6234, Parent: 6229)
      - 2DbzKHhgOH New Fork (PID: 6236, Parent: 6229)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
2DbzKHhgOH	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
2DbzKHhgOH	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	0x10310:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x10324:$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 0x10338:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x1034c:$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 0x10360:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x10374:$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 0x10388:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x1039c:$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 0x103b0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x103c4:$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 0x103d8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x103ec:$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 0x10400:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x10414:$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 0x10428:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x1043c:$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 0x10450:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x10464:$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 0x10478:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0x1048c:$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 0x104a0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
2DbzKHhgOH	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	0x10870:$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
6223.1.00007f4910011000.00007f4910023000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6223.1.00007f4910011000.00007f4910023000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x10310:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10324:$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 • 0x10338:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1034c:$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 • 0x10360:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10374:$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 • 0x10388:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1039c:$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 • 0x103b0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x103c4:$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 • 0x103d8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x103ec:$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 • 0x10400:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10414:$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 • 0x10428:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1043c:$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 • 0x10450:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10464:$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 • 0x10478:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1048c:$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 • 0x104a0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6223.1.00007f4910011000.00007f4910023000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0x10870:$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
6242.1.00007f4910011000.00007f4910023000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6242.1.00007f4910011000.00007f4910023000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x10310:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10324:$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 • 0x10338:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1034c:$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 • 0x10360:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10374:$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 • 0x10388:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1039c:$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 • 0x103b0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x103c4:$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 • 0x103d8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x103ec:$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 • 0x10400:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10414:$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 • 0x10428:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1043c:$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 • 0x10450:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10464:$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 • 0x10478:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1048c:$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 • 0x104a0:$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 33 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)

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

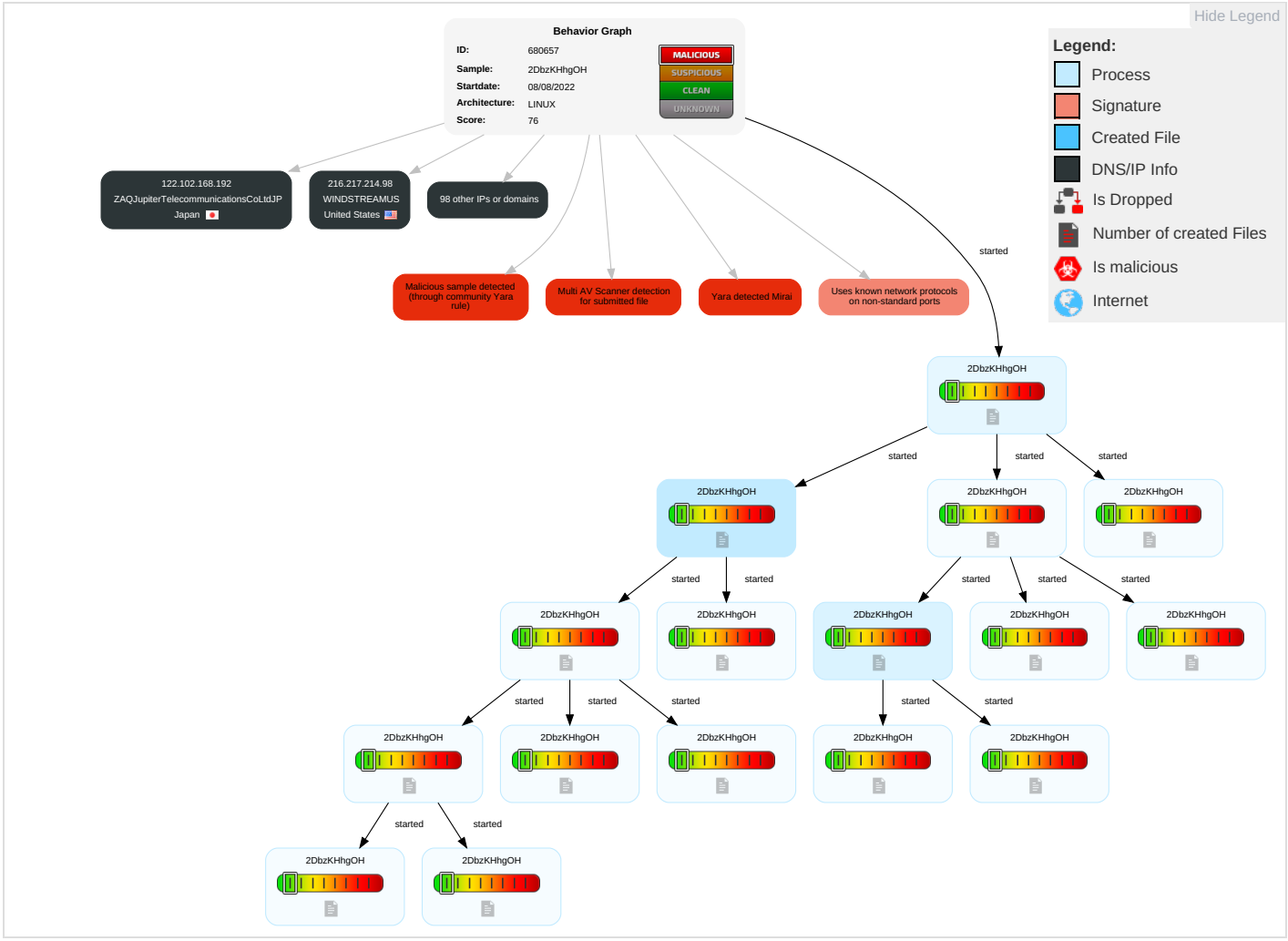
Mitre Att&ck Matrix

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	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
2DbzKHhgOH	56%	Virustotal		Browse
2DbzKHhgOH	54%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

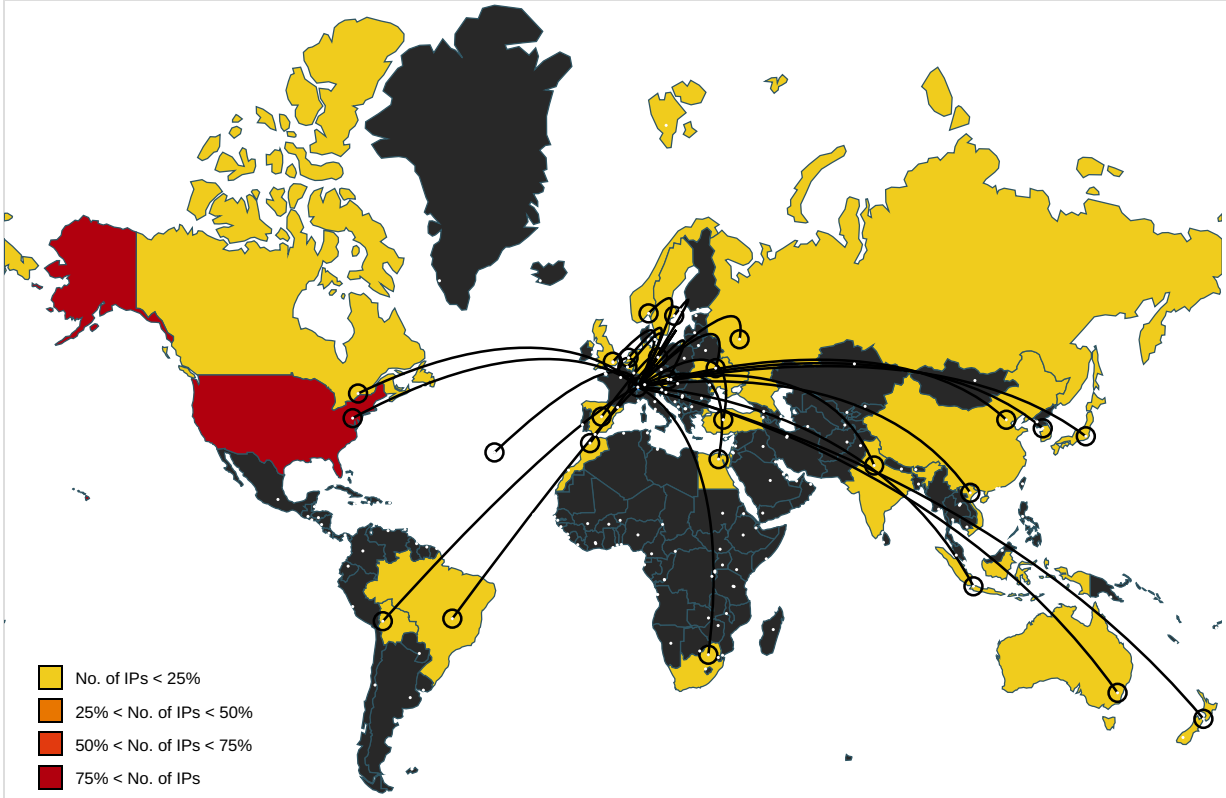
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
168.232.195.12	unknown	Brazil		264947	LUIZLIMAECIALTDA-MEBR	false
172.242.149.102	unknown	United States		7155	VIASAT-SP-BACKBONEUS	false
244.20.66.52	unknown	Reserved		unknown	unknown	false
171.113.147.143	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
19.169.88.87	unknown	United States		3	MIT-GATEWAYSUS	false
63.89.37.172	unknown	United States		701	UUNETUS	false
57.250.79.115	unknown	Belgium		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
17.187.225.236	unknown	United States		714	APPLE-ENGINEERINGUS	false
179.178.200.39	unknown	Brazil		18881	TELEFONICABRASILSAB R	false
212.236.166.35	unknown	Austria		8245	VIDEOBROADCAST-ASAT	false
156.111.211.80	unknown	United States		395139	NYP-INTERNETUS	false
172.249.237.250	unknown	United States		20001	TWC-20001-PACWESTUS	false
154.141.21.12	unknown	Egypt		37069	MOBINILEG	false
172.78.20.231	unknown	United States		5650	FRONTIER-FRTRUS	false
242.114.167.34	unknown	Reserved		unknown	unknown	false
250.72.175.183	unknown	Reserved		unknown	unknown	false
12.33.245.124	unknown	United States		7018	ATT-INTERNET4US	false
92.100.198.12	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
148.183.118.63	unknown	United States		11529	NGUS-ASUS	false
74.164.154.157	unknown	United States		6389	BELLSOUTH-NET-BLKUS	false
187.0.44.224	unknown	unknown		270589	MarcioHenriqueMalaquiasJuniorBR	false
101.91.3.194	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
162.41.243.8	unknown	United States		53984	AS-WELLSTARUS	false
76.251.40.142	unknown	United States		7018	ATT-INTERNET4US	false
9.234.214.193	unknown	United States		3356	LEVEL3US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
210.55.200.75	unknown	New Zealand		4648	SPARK-NZGlobal-GatewayInternetNZ	false
210.151.57.163	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
146.35.171.49	unknown	United States		197938	TRAVIANGAMESDE	false
130.1.17.5	unknown	United States		6908	DATAHOPDatahop-SixDegreesGB	false
242.60.251.65	unknown	Reserved		unknown	unknown	false
193.215.94.85	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
69.241.251.91	unknown	United States		7922	COMCAST-7922US	false
5.248.220.111	unknown	Ukraine		15895	KSNET-ASUA	false
53.70.141.206	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
145.161.131.179	unknown	Netherlands		59524	KPN-IAASNL	false
255.235.153.74	unknown	Reserved		unknown	unknown	false
124.168.11.239	unknown	Australia		7545	TPG-INTERNET-APTPGTelecomLimitedAU	false
12.238.112.74	unknown	United States		11085	PDI-HQ-INETUS	false
81.156.178.92	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
112.58.214.171	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
16.122.9.243	unknown	United States		unknown	unknown	false
142.148.79.137	unknown	Canada		808	GONET-ASN-1CA	false
171.117.63.31	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
105.237.204.73	unknown	South Africa		16637	MTNNS-ASZA	false
84.228.172.237	unknown	Israel		9116	GOLDENLINES-ASNPartnerCommunicationsMainAutonomousSyste	false
41.143.104.16	unknown	Morocco		36903	MT-MPLSMA	false
255.108.118.255	unknown	Reserved		unknown	unknown	false
91.220.198.112	unknown	Ukraine		50304	BLIXNO	false
57.184.201.154	unknown	Belgium		2686	ATGS-MMD-ASUS	false
212.225.90.64	unknown	United Kingdom		2529	DEMON-INTERNETNowmaintainedbyCableWirelessWorldwide	false
14.251.158.152	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
167.185.27.193	unknown	United States		15071	BAX-BGPUS	false
70.46.78.210	unknown	United States		7029	WINDSTREAMUS	false
188.201.177.170	unknown	Netherlands		1136	KPNKPNNationalEU	false
129.6.93.246	unknown	United States		49	US-NATIONAL-INSTITUTE-OF-STANDARDS-AND-TECHNOLOGYUS	false
44.80.25.38	unknown	United States		7377	UCSDUS	false
190.14.82.129	unknown	Bolivia		22541	MegaLinkBO	false
91.118.21.149	unknown	Austria		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
246.114.251.206	unknown	Reserved		unknown	unknown	false
98.33.199.221	unknown	United States		7922	COMCAST-7922US	false
76.240.155.100	unknown	United States		7018	ATT-INTERNET4US	false
175.227.77.55	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
216.217.214.98	unknown	United States		7029	WINDSTREAMUS	false
154.40.28.102	unknown	United States		174	COGENT-174US	false
210.77.15.166	unknown	China		7497	CSTNET-AS-APComputerNetworkInformationCenterCN	false
207.218.72.98	unknown	United States		3549	LVLT-3549US	false
244.239.113.71	unknown	Reserved		unknown	unknown	false
199.55.108.184	unknown	United States		398192	ARDOT-NET-01US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
219.111.80.29	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
109.35.142.232	unknown	Netherlands		15480	VFNL-ASVodafoneNLAutonomousSystemNL	false
240.58.79.8	unknown	Reserved		unknown	unknown	false
218.19.201.2	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
161.210.39.255	unknown	United States		14513	DMACCUS	false
223.30.216.212	unknown	India		9583	SIFY-AS-INSifyLimitedIN	false
14.88.182.111	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
177.67.65.0	unknown	Brazil		53011	KARCHERINDECOMLTDABR	false
85.144.20.7	unknown	Netherlands		50266	TMOBILE-THUISNL	false
220.53.144.208	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
2.64.113.156	unknown	Sweden		44034	HI3GSE	false
202.153.150.34	unknown	Indonesia		10208	THENET-AS-ID-APPTMilleniumInternetindoID	false
42.42.63.189	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
65.195.47.35	unknown	United States		701	UUNETUS	false
57.62.64.150	unknown	Belgium		2686	ATGS-MMD-ASUS	false
165.176.234.90	unknown	United States		7046	RFC2270-UUNET-CUSTOMERUS	false
184.178.190.91	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
91.19.165.16	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
122.102.168.192	unknown	Japan		9617	ZAQJupiterTelecommunicationsCoLtdJP	false
174.92.228.99	unknown	Canada		577	BACOMCA	false
79.156.170.130	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
204.151.108.241	unknown	United States		11303	DATARETURNUS	false
246.235.249.98	unknown	Reserved		unknown	unknown	false
212.127.114.0	unknown	Turkey		12729	HSBC_TR_BANK_INTERNETTR	false
176.28.39.79	unknown	Germany		35329	GD-EMEA-DC-CGN3DE	false
254.151.225.92	unknown	Reserved		unknown	unknown	false
182.133.200.190	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
216.60.3.85	unknown	United States		7018	ATT-INTERNET4US	false
173.207.5.161	unknown	United States		6407	PRIMUS-AS6407CA	false
12.15.64.253	unknown	United States		32328	ALASCOM-IP-MANAGED-NETWORKUS	false
198.119.252.109	unknown	United States		297	AS297US	false
253.179.129.161	unknown	Reserved		unknown	unknown	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, SPARC, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.008811747351218
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	2DbzKHhgOH
File size:	74752
MD5:	91e1ba2317dac69005bd8f5494297730
SHA1:	314ac7afbe482e1a412632950bc03f5d00bd6e0a
SHA256:	7610f435e009a531631ad480f342b21b87e56c05ac55d66ad99a1a3e5523fad2
SHA512:	526e6ae27f06027083d7d0eb5c1b02bd0c5d3aae35769ba19fd15371a5c6b7bc1ce047c071c2b112cd9d0069094f29ca323cd1929ca6510723a7345babc27bec
SSDEEP:	1536:hD/B6f6UD5hAS7mo0DCCAXESKV6v3G78nN9WV:927jqCe8v3GI/W
TLSH:	82732A26B97A1E26C0D4B57E60FB8B11F5E1278E26B4C50A7D720E5EEF147006502EF7
File Content Preview:	.ELF.....4.."p.....4. ...(.....0...0..... ... ...0.....dt.Q.....@..(....@.@.....#.....b0..`.....!..... ...@....."........`.....$ ... ...@.....`....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	Sparc
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x101a4
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	74352
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

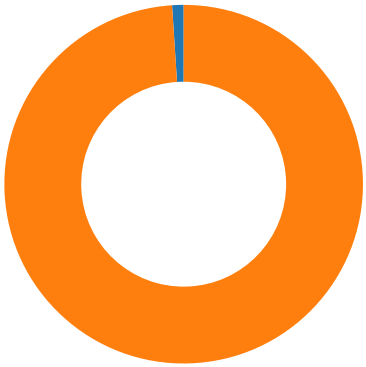
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10094	0x94	0x1c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100b0	0xb0	0x10248	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x202f8	0x102f8	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x20310	0x10310	0x1920	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x32000	0x12000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x32008	0x12008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x32018	0x12018	0x218	0x0	0x3	WA	0	0	8
.bss	NOBITS	0x32230	0x12230	0x288	0x0	0x3	WA	0	0	8
.shstrtab	STRTAB	0x0	0x12230	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	0x10000	0x10000	0x11c30	0x11c30	6.0760	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x12000	0x32000	0x32000	0x230	0x4b8	2.9317	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



Total Packets: 97

- 23 (Telnet)
- 1312 undefined

TCP Packets

System Behavior

Analysis Process: 2DbzKHhgOH PID: 6223, Parent PID: 6120

General

Start time:	23:36:44
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	/tmp/2DbzKHhgOH
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Analysis Process: 2DbzKHhgOH PID: **6226**, Parent PID: **6223**

General

Start time:	23:36:44
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Directory Enumerated

Analysis Process: 2DbzKHhgOH PID: **6242**, Parent PID: **6226**

General

Start time:	23:36:53
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 2DbzKHhgOH PID: **6244**, Parent PID: **6226**

General

Start time:	23:36:53
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 2DbzKHhgOH PID: **6246**, Parent PID: **6244**

General

Start time:	23:36:53
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 2DbzKHhgOH PID: **6256**, Parent PID: **6246**

General

Start time:	23:36:53
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 2DbzKHhgOH PID: **6257**, Parent PID: **6246**

General

Start time:	23:36:53
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 2DbzKHhgOH PID: **6251**, Parent PID: **6244**

General

Start time:	23:36:53
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 2DbzKHhgOH PID: **6253**, Parent PID: **6244**

General

Start time:	23:36:53
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 2DbzKHhgOH PID: **6227**, Parent PID: **6223**

General

Start time:	23:36:44
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 2DbzKHhgOH PID: **6229**, Parent PID: **6223**

General

Start time:	23:36:44
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 2DbzKHhgOH PID: **6232**, Parent PID: **6229**

General

Start time:	23:36:44
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Directory Enumerated

Analysis Process: 2DbzKHhgOH PID: **6260**, Parent PID: **6232**

General

Start time:	23:36:53
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 2DbzKHhgOH PID: **6262**, Parent PID: **6232**

General

Start time:	23:36:53
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 2DbzKHhgOH PID: **6234**, Parent PID: **6229**

General

Start time:	23:36:45
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: 2DbzKHhgOH PID: **6236**, Parent PID: **6229**

General

Start time:	23:36:45
Start date:	08/08/2022
Path:	/tmp/2DbzKHhgOH
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e