ID: 680649
Sample Name: YbuW0MHZo0
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 23:22:33
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

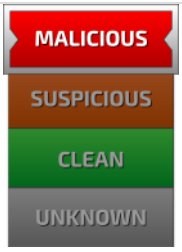
YbuW0MHZo0

Overview

General Information

Sample Name:	YbuW0MHZo0
Analysis ID:	680649
MD5:	dcdd462eaf7676..
SHA1:	df86c4b2b98e4f5..
SHA256:	12bcdc291270a3..
Tags:	32 elf mirai motorola
Infos:	

Detection



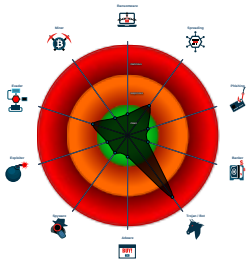
Mirai

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:	680649
Start date and time: 08/08/202223:22:33	2022-08-08 23:22:33 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	YbuW0MHZo0
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/YbuW0MHZo0
PID:	6225
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- YbuW0MHZo0 (PID: 6225, Parent: 6125, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/YbuW0MHZo0
  - YbuW0MHZo0 New Fork (PID: 6227, Parent: 6225)
    - YbuW0MHZo0 New Fork (PID: 6328, Parent: 6227)
    - YbuW0MHZo0 New Fork (PID: 6331, Parent: 6227)
      - YbuW0MHZo0 New Fork (PID: 6335, Parent: 6331)
        - YbuW0MHZo0 New Fork (PID: 6345, Parent: 6335)
        - YbuW0MHZo0 New Fork (PID: 6346, Parent: 6335)
      - YbuW0MHZo0 New Fork (PID: 6338, Parent: 6331)
      - YbuW0MHZo0 New Fork (PID: 6339, Parent: 6331)
    - YbuW0MHZo0 New Fork (PID: 6228, Parent: 6225)
    - YbuW0MHZo0 New Fork (PID: 6230, Parent: 6225)
      - YbuW0MHZo0 New Fork (PID: 6233, Parent: 6230)
        - YbuW0MHZo0 New Fork (PID: 6327, Parent: 6233)
        - YbuW0MHZo0 New Fork (PID: 6330, Parent: 6233)
      - YbuW0MHZo0 New Fork (PID: 6234, Parent: 6230)
      - YbuW0MHZo0 New Fork (PID: 6235, Parent: 6230)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
YbuW0MHZo0	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
YbuW0MHZo0	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xe858:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe86c:$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 • 0xe880:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe894:$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 • 0xe8a8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe8bc:$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 • 0xe8d0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe8e4:$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 • 0xe8f8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe90c:$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 • 0xe920:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe934:$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 • 0xe948:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe95c:$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 • 0xe970:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe984:$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 • 0xe998:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe9ac:$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 • 0xe9c0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe9d4:$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 • 0xe9e8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
YbuW0MHZo0	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0xeda9:$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
6338.1.00007fc900001000.00007fc900011000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6338.1.00007fc900001000.00007fc900011000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xe858:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe86c:$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 • 0xe880:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe894:$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 • 0xe8a8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe8bc:$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 • 0xe8d0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe8e4:$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 • 0xe8f8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe90c:$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 • 0xe920:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe934:$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 • 0xe948:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe95c:$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 • 0xe970:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe984:$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 • 0xe998:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe9ac:$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 • 0xe9c0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe9d4:$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 • 0xe9e8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6338.1.00007fc900001000.00007fc900011000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0xeda9:$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
6228.1.00007fc900001000.00007fc900011000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6228.1.00007fc900001000.00007fc900011000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xe858:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe86c:$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 • 0xe880:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe894:$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 • 0xe8a8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe8bc:$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 • 0xe8d0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe8e4:$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 • 0xe8f8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe90c:$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 • 0xe920:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe934:$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 • 0xe948:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe95c:$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 • 0xe970:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe984:$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 • 0xe998:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe9ac:$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 • 0xe9c0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xe9d4:$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 • 0xe9e8:$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 32 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

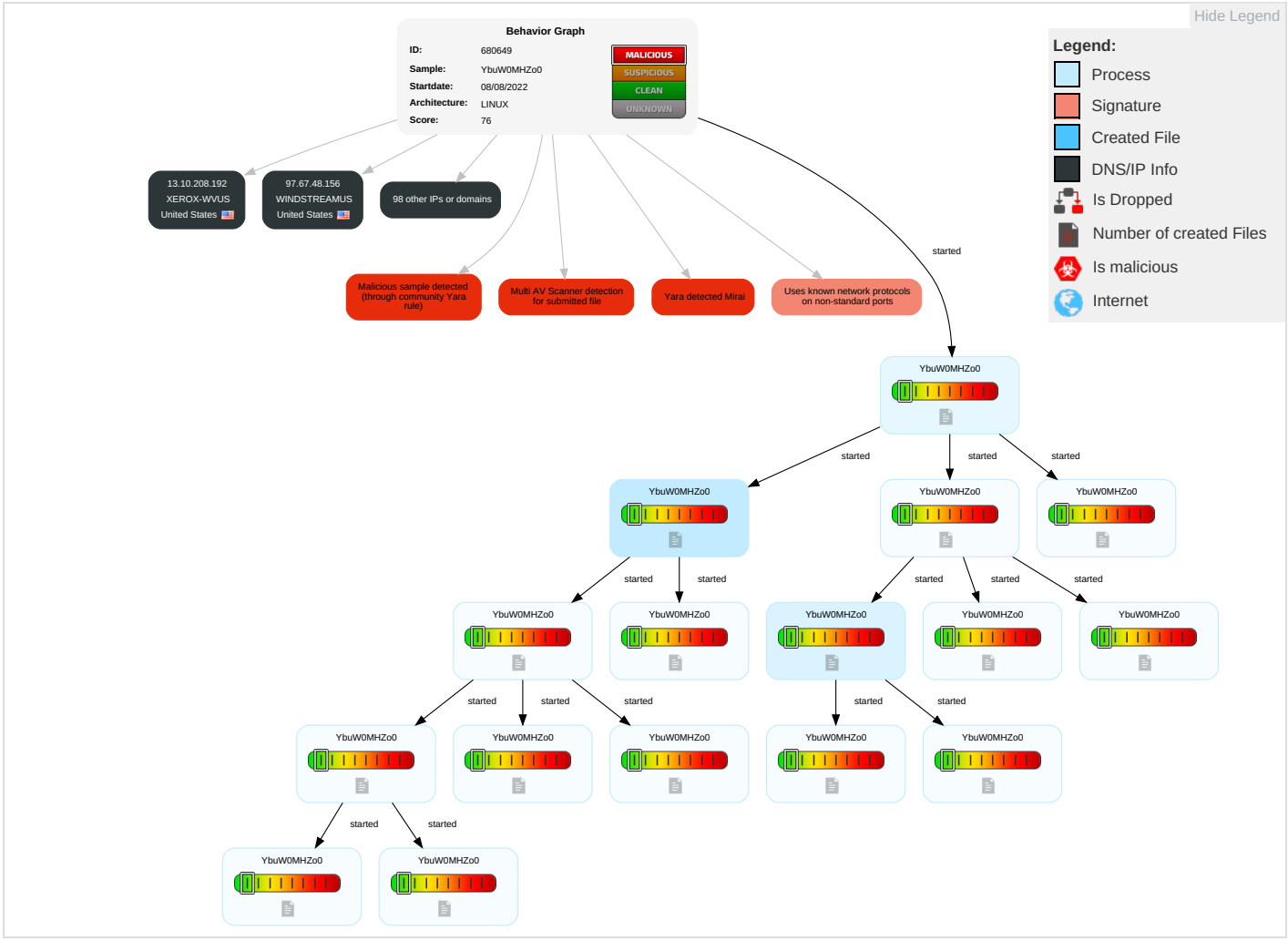
Mitre Att&ck Matrix

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
YbuW0MHZo0	59%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

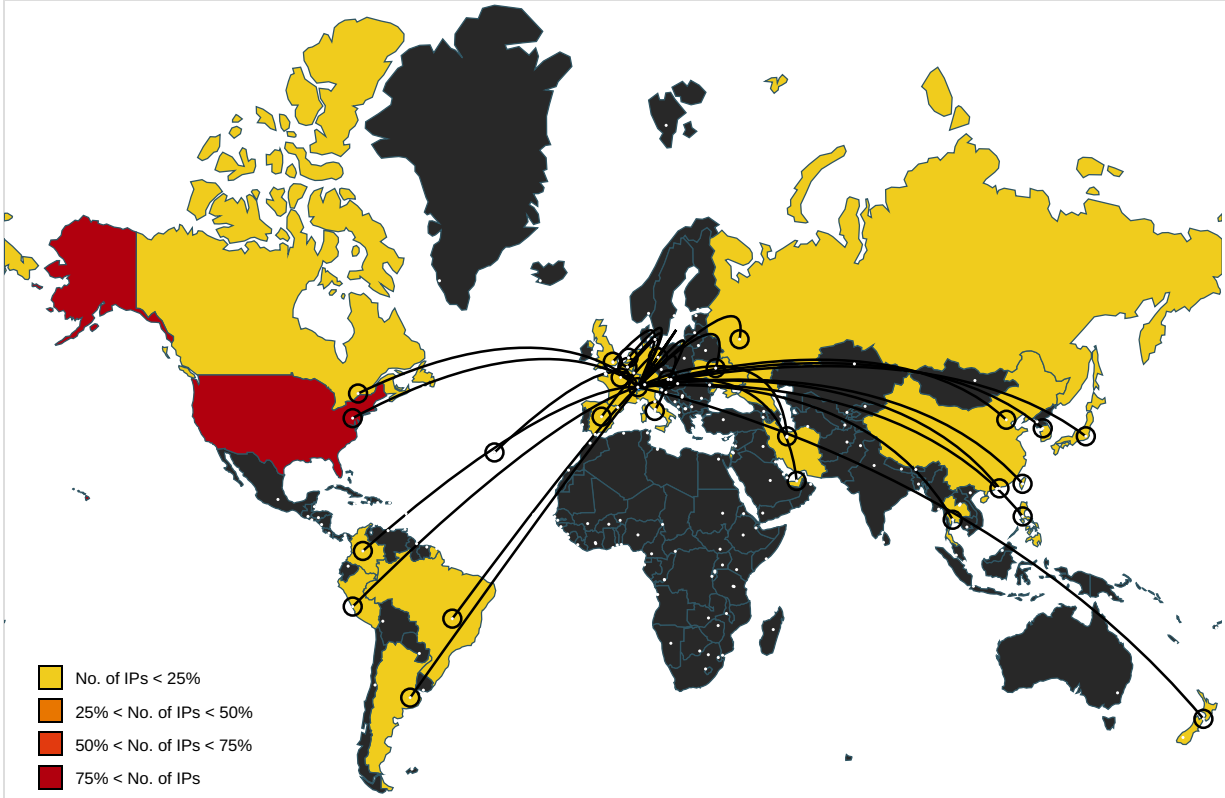
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
139.169.35.31	unknown	United States		270	AS270US	false
218.191.217.214	unknown	Hong Kong		9304	HUTCHISON-AS-APHGCGlobalCommunicationsLimitedHK	false
91.103.53.121	unknown	Spain		31262	EDICOMES	false
246.132.183.69	unknown	Reserved		unknown	unknown	false
115.143.117.94	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
221.157.77.15	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
69.44.220.229	unknown	United States		13767	DATABANK-DFWUS	false
219.191.176.119	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
66.186.44.1	unknown	United States		40891	SDI-MEDIA-GROUPUS	false
191.149.218.193	unknown	Colombia		26611	COMCELSACO	false
178.228.58.237	unknown	Netherlands		31615	TMO-NL-ASNL	false
248.133.158.76	unknown	Reserved		unknown	unknown	false
180.23.142.196	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
162.52.78.41	unknown	United States		35893	ACPCA	false
69.37.49.65	unknown	United States		7018	ATT-INTERNET4US	false
58.137.134.246	unknown	Thailand		18408	MITSUBISHIFA-CSLOXINFO-THCSLOXINFOTH	false
210.145.102.97	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
9.94.32.203	unknown	United States		3356	LEVEL3US	false
47.136.192.234	unknown	United States		5650	FRONTIER-FRTRUS	false
89.233.66.133	unknown	Germany		9145	EWETELCloppenburgerStrasse310DE	false
4.150.249.64	unknown	United States		3356	LEVEL3US	false
248.111.220.143	unknown	Reserved		unknown	unknown	false
66.139.105.234	unknown	United States		7018	ATT-INTERNET4US	false
212.58.250.97	unknown	United Kingdom		2818	BBCBBCInternetServicesUKGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.191.89.31	unknown	Spain		205512	WIFILAVALLES	false
89.109.12.129	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
43.152.14.154	unknown	Japan		4249	LILLY-ASUS	false
4.54.18.92	unknown	United States		3356	LEVEL3US	false
187.59.106.55	unknown	Brazil		18881	TELEFONICABRASILSABR	false
156.41.209.244	unknown	United States		1226	CTA-42-AS1226US	false
166.127.141.57	unknown	United States		4604	HOUSTON-ISDUS	false
181.230.242.157	unknown	Argentina		10481	TelecomArgentinaSAAR	false
61.9.25.51	unknown	Philippines		17970	SKYBB-AS-APSKYBroadbandSKYCableCorporationPH	false
211.175.131.86	unknown	Korea Republic of		9457	DREAMX-ASDREAMLINECOKR	false
62.0.77.79	unknown	Israel		1680	NV-ASNCELLCOMltdIL	false
168.189.78.57	unknown	United States		53526	THECLO-ASNUS	false
168.92.42.22	unknown	United States		16399	FIRSTCOMM-AS2US	false
200.121.65.160	unknown	Peru		6147	TelefonicadelPeruSAAPE	false
108.23.239.123	unknown	United States		5650	FRONTIER-FRTRUS	false
193.107.224.153	unknown	Ukraine		44041	UNICOMLAB-ASRU	false
32.41.122.209	unknown	United States		2686	ATGS-MMD-ASUS	false
42.207.180.116	unknown	China		7641	CHINABTNChinaBroadcastingTVNetCN	false
255.74.31.12	unknown	Reserved		unknown	unknown	false
121.9.180.68	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
17.42.161.130	unknown	United States		714	APPLE-ENGINEERINGUS	false
45.149.76.249	unknown	Iran (ISLAMIC Republic Of)		60631	PARVASYSTEMIR	false
61.202.226.226	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
57.64.2.157	unknown	Belgium		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
76.91.218.114	unknown	United States		20001	TWC-20001-PACWESTUS	false
67.80.199.42	unknown	United States		6128	CABLE-NET-1US	false
85.21.130.23	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
221.205.8.113	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
12.125.39.68	unknown	United States		7018	ATT-INTERNET4US	false
206.121.134.66	unknown	United States		7018	ATT-INTERNET4US	false
244.39.195.2	unknown	Reserved		unknown	unknown	false
252.194.182.128	unknown	Reserved		unknown	unknown	false
220.147.154.54	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	false
200.98.155.81	unknown	Brazil		7162	UniversoOnlineSABR	false
202.126.194.6	unknown	New Zealand		17492	VECTOR-COMMUNICATIONS-ASVectorCommunicationsLTDNZ	false
209.114.155.235	unknown	United States		17054	AS17054US	false
247.188.164.180	unknown	Reserved		unknown	unknown	false
179.10.161.252	unknown	Brazil		26615	TIMSABR	false
165.77.133.145	unknown	United States		4725	ODNSoftBankMobileCorpJP	false
73.236.36.102	unknown	United States		7922	COMCAST-7922US	false
216.135.68.192	unknown	United States		4261	BLUEGRASSNETUS	false
207.147.233.222	unknown	United States		2711	SPIRITTEL-ASUS	false
13.10.208.192	unknown	United States		26662	XEROX-WVUS	false
54.56.255.200	unknown	United States		14618	AMAZON-AESUS	false
150.145.85.46	unknown	Italy		137	ASGARRConsortiumGARREU	false
47.33.229.16	unknown	United States		20115	CHARTER-20115US	false
48.156.130.0	unknown	United States		2686	ATGS-MMD-ASUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
14.86.131.117	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
4.15.188.253	unknown	United States		3356	LEVEL3US	false
191.196.232.124	unknown	Brazil		26599	TELEFONICABRASILSABR	false
17.98.106.237	unknown	United States		714	APPLE-ENGINEERINGUS	false
111.214.188.218	unknown	China		9812	CNNIC-CN-COLNETOrientalCableNetworkCoLtdCN	false
177.8.210.235	unknown	Brazil		262819	LINKMAISPROVEDORDEACESSOASREDESDECOMLTDABR	false
195.248.34.203	unknown	Austria		8437	UTA-ASAT	false
136.140.138.103	unknown	United States		60311	ONEFMCH	false
62.210.152.239	unknown	France		12876	OnlineSASFR	false
47.114.18.29	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
104.1.204.81	unknown	United States		7018	ATT-INTERNET4US	false
223.113.238.121	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
141.135.42.36	unknown	Belgium		6848	TELENET-ASBE	false
207.68.157.241	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
180.156.74.127	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
187.51.205.116	unknown	Brazil		10429	TELEFONICABRASILSABR	false
118.242.64.239	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
93.231.80.206	unknown	Germany		3320	DTAGInternetserviceproviderоperationsDE	false
149.99.65.7	unknown	Canada		3602	AS3602-ROGERS-COMCA	false
155.197.111.86	unknown	United States		37197	SUDRENSD	false
84.56.216.101	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
122.121.155.169	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
104.170.219.173	unknown	United States		36352	AS-COLOCROSSINGUS	false
159.62.185.241	unknown	United States		7834	L3HARRIS-TECHNOLOGIESUS	false
1.19.209.35	unknown	Korea Republic of		45996	GNJ-AS-KRDAOUTECHNOLOGYKR	false
86.99.44.125	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
99.210.200.183	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
97.67.48.156	unknown	United States		7029	WINDSTREAMUS	false
209.148.121.224	unknown	United States		7065	SONOMAUS	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):	6.290380807981935
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	YbuW0MHZo0
File size:	65100
MD5:	dcdd462eaf76769b9a0b79640b98065b
SHA1:	df86c4b2b98e4f540d31ff8bba0c2d5beda8b9e6
SHA256:	12bcdc291270a3506825c13eaa2efb0f6f4a4304a504db2ed3a427414adca191
SHA512:	e5736231dc5c0d552c9437827830a509b02a3cc9de4d948acca5f98dcc6c4fd34073bb4a585cc51537299f32e84f0f5e66b49dcf77b05c9c1248ee0eecb2fe07
SSDEEP:	768:me4gpsM204GEkRbjveXl/nQi122EQtBSv3gFHn1eu48B8vB6J7EzNfXQuJpozfyE:mo3EkRbDSoiz6IFn1X48B2SEzNfAuJ3E
TLSH:	DE533B99F4029E3DF88FE9BA84160E05B93023D112931B2767ABFDE37D331659D12E45
File Content Preview:	.ELF.....D...4.....4. ...(.....R...R..... .....X...X...X...$...`..... .dt.Q.....NV..a....da....xN^NuNV..J9...|f>"y...p QJ.g.X.#....pN."y...p QJ.f.A.....J.g.Hy...TN.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:	64700
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

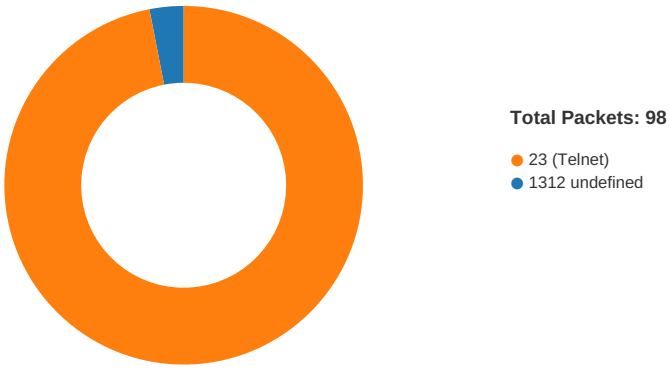
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0xe7a2	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x8000e84a	0xe84a	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x8000e858	0xe858	0x11fa	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x80011a58	0xfa58	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x80011a60	0xfa60	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x80011a6c	0xfa6c	0x210	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x80011c7c	0xfc7c	0x23c	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xfc7c	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	0xfa52	0xfa52	6.3209	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0xfa58	0x80011a58	0x80011a58	0x224	0x460	3.0327	0x6	RW	0x2000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: YbuW0MHZo0 PID: 6225, Parent PID: 6125

General

Start time:	23:23:19
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	/tmp/YbuW0MHZo0
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: YbuW0MHZo0 PID: **6227**, Parent PID: **6225**

General

Start time:	23:23:19
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: YbuW0MHZo0 PID: **6328**, Parent PID: **6227**

General

Start time:	23:26:12
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: YbuW0MHZo0 PID: **6331**, Parent PID: **6227**

General

Start time:	23:26:12
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: YbuW0MHZo0 PID: **6335**, Parent PID: **6331**

General

Start time:	23:26:12
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: YbuW0MHZo0 PID: **6345**, Parent PID: **6335**

General

Start time:	23:26:17
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: YbuW0MHZo0 PID: **6346**, Parent PID: **6335**

General

Start time:	23:26:17
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0

Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: YbuW0MHZo0 PID: **6338**, Parent PID: **6331**

General

Start time:	23:26:12
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: YbuW0MHZo0 PID: **6339**, Parent PID: **6331**

General

Start time:	23:26:12
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: YbuW0MHZo0 PID: **6228**, Parent PID: **6225**

General

Start time:	23:23:19
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: YbuW0MHZo0 PID: **6230**, Parent PID: **6225**

General

Start time:	23:23:19
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: YbuW0MHZo0 PID: **6233**, Parent PID: **6230**

General

Start time:	23:23:19
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: YbuW0MHZo0 PID: **6327**, Parent PID: **6233**

General	
Start time:	23:26:12
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: YbuW0MHZo0 PID: **6330**, Parent PID: **6233**

General	
Start time:	23:26:12
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: YbuW0MHZo0 PID: **6234**, Parent PID: **6230**

General	
Start time:	23:23:19
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: YbuW0MHZo0 PID: **6235**, Parent PID: **6230**

General	
Start time:	23:23:19
Start date:	08/08/2022
Path:	/tmp/YbuW0MHZo0
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc