ID: 680642
Sample Name: HUIHmcbfpW
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 23:06:11
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

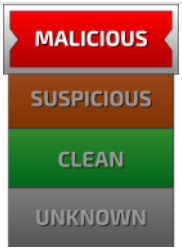
HUIHmcbfpW

Overview

General Information

Sample Name:	HUIHmcbfpW
Analysis ID:	680642
MD5:	7463d28ae705f2..
SHA1:	ca0836b4c352f1...
SHA256:	ed29224a554dd5.
Tags:	32 elf mirai powerpc
Infos:	

Detection



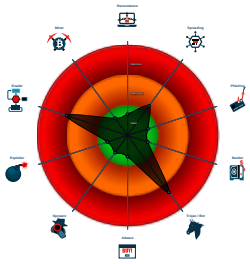
Mirai

Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through...
- 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...
- Yara signature match
- 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:	680642
Start date and time: 08/08/202223:06:11	2022-08-08 23:06:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HUIHmcbfpW
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:	mal72.troj.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/HUIHmcbfpW
PID:	6226
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- HUIHmcbfpW (PID: 6226, Parent: 6125, MD5: ae65271c943d3451b7f026d1fadccea6) Arguments: /tmp/HUIHmcbfpW
  - HUIHmcbfpW New Fork (PID: 6228, Parent: 6226)
    - HUIHmcbfpW New Fork (PID: 6325, Parent: 6228)
    - HUIHmcbfpW New Fork (PID: 6326, Parent: 6228)
      - HUIHmcbfpW New Fork (PID: 6329, Parent: 6326)
        - HUIHmcbfpW New Fork (PID: 6342, Parent: 6329)
        - HUIHmcbfpW New Fork (PID: 6344, Parent: 6329)
      - HUIHmcbfpW New Fork (PID: 6330, Parent: 6326)
      - HUIHmcbfpW New Fork (PID: 6332, Parent: 6326)
    - HUIHmcbfpW New Fork (PID: 6229, Parent: 6226)
    - HUIHmcbfpW New Fork (PID: 6230, Parent: 6226)
      - HUIHmcbfpW New Fork (PID: 6234, Parent: 6230)
        - HUIHmcbfpW New Fork (PID: 6336, Parent: 6234)
        - HUIHmcbfpW New Fork (PID: 6338, Parent: 6234)
      - HUIHmcbfpW New Fork (PID: 6235, Parent: 6230)
      - HUIHmcbfpW New Fork (PID: 6236, Parent: 6230)
- **cleanup**

Yara Signatures

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
6336.1.00007f8a6400b000.00007f8a64010000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x41d0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x41e4:$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 • 0x41f8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x420c:$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 • 0x4220:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4234:$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 • 0x4248:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x425c:$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 • 0x4270:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4284:$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 • 0x4298:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42ac:$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 • 0x42c0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42d4:$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 • 0x42e8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42fc:$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 • 0x4310:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4324:$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 • 0x4338:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x434c:$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 • 0x4360:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6336.1.00007f8a6400b000.00007f8a64010000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0x4728:$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
6229.1.00007f8a6400b000.00007f8a64010000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x41d0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x41e4:$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 • 0x41f8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x420c:$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 • 0x4220:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4234:$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 • 0x4248:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x425c:$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 • 0x4270:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4284:$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 • 0x4298:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42ac:$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 • 0x42c0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42d4:$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 • 0x42e8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42fc:$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 • 0x4310:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4324:$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 • 0x4338:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x434c:$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 • 0x4360:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6229.1.00007f8a6400b000.00007f8a64010000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0x4728:$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
6228.1.00007f8a6400b000.00007f8a64010000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x41d0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x41e4:$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 • 0x41f8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x420c:$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 • 0x4220:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4234:$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 • 0x4248:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x425c:$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 • 0x4270:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4284:$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 • 0x4298:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42ac:$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 • 0x42c0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42d4:$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 • 0x42e8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x42fc:$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 • 0x4310:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x4324:$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 • 0x4338:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x434c:$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 • 0x4360:$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

Source	Rule	Description	Author	Strings
Click to see the 22 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)

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

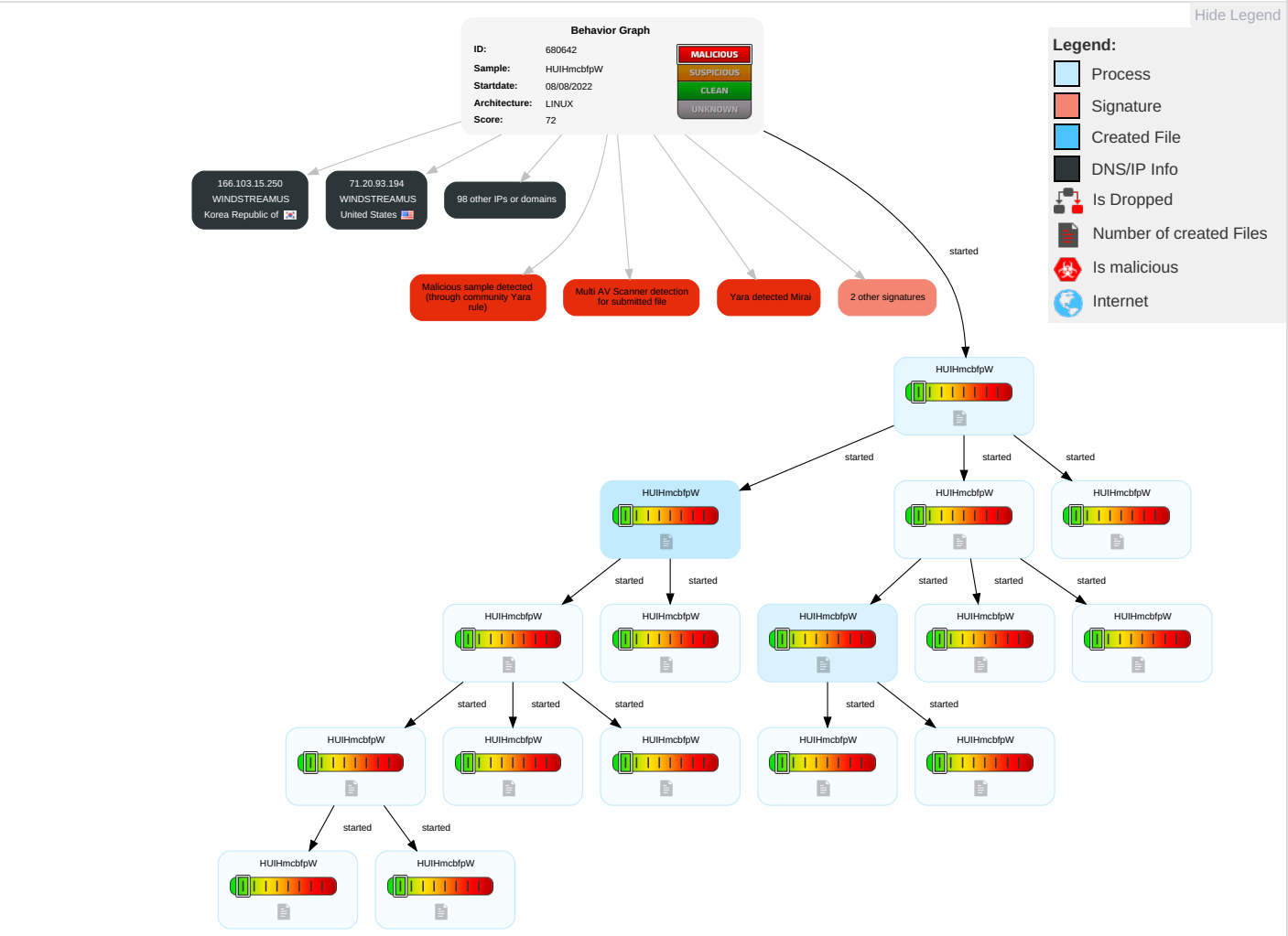
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 1 Obfuscated 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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
HUIHmcbfpW	42%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

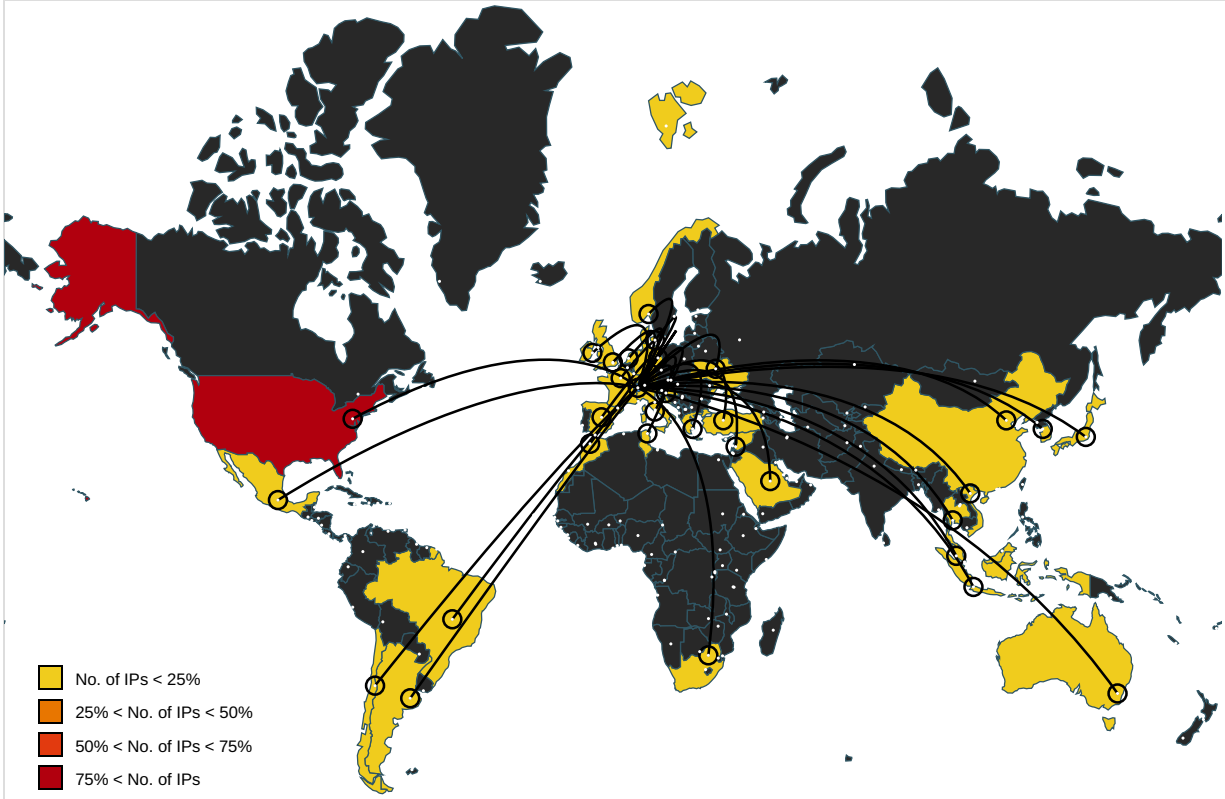
Domains and IPs

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
115.70.214.247	unknown	Australia		10143	EXETEL-AS-APExetelPtyLtdAU	false
75.108.75.216	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	false
93.195.229.176	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
34.133.78.216	unknown	United States		2686	ATGS-MMD-ASUS	false
114.199.124.68	unknown	Indonesia		24525	SAP-AS-IDPTSolusiAksesindoPratamaID	false
218.33.69.123	unknown	Indonesia		9919	NCIC-TWNewCenturyInfoCommTechCoLtdTW	false
155.195.109.15	unknown	United States		8698	NationwideBuildingSocietyGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
183.195.9.118	unknown	China		24400	CMNET-V4SHANGHAI-AS-APShanghaiMobileCommunicationsCoLt	false
218.131.175.97	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
75.123.52.91	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
213.153.202.31	unknown	Turkey		34984	TELLCOM-ASTR	false
34.81.60.26	unknown	United States		15169	GOOGLEUS	false
244.122.119.68	unknown	Reserved		unknown	unknown	false
207.16.235.134	unknown	United States		701	UUNETUS	false
35.1.148.43	unknown	United States		36375	UMICH-AS-5US	false
41.225.142.123	unknown	Tunisia		37671	GLOBALNET-ASTN	false
75.9.11.2	unknown	United States		7018	ATT-INTERNET4US	false
17.226.59.114	unknown	United States		714	APPLE-ENGINEERINGUS	false
18.8.247.30	unknown	United States		3	MIT-GATEWAYSUS	false
108.184.71.71	unknown	United States		20001	TWC-20001-PACWESTUS	false
80.94.206.63	unknown	United Kingdom		199335	TALKSTRAIGHTGB	false
17.11.240.42	unknown	United States		714	APPLE-ENGINEERINGUS	false
194.248.0.38	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
100.25.217.60	unknown	United States		14618	AMAZON-AESUS	false
150.57.210.52	unknown	Japan		17511	OPTAGEOPTAGEIncJP	false
17.45.206.26	unknown	United States		714	APPLE-ENGINEERINGUS	false
1.20.112.75	unknown	Thailand		23969	TOT-NETTOTPublicCompanyLimitedTH	false
169.25.164.54	unknown	United States		37611	AfrihostZA	false
106.17.155.36	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
123.140.76.147	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
40.29.213.216	unknown	United States		4249	LILLY-ASUS	false
27.66.85.154	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	false
178.255.242.149	unknown	Italy		13287	NIXVALIP-ASNIXVALDatacenterES	false
125.153.47.14	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
65.201.108.232	unknown	United States		701	UUNETUS	false
194.220.87.9	unknown	Spain		12430	VODAFONE_ESES	false
78.204.247.20	unknown	France		12322	PROXADFR	false
247.49.166.233	unknown	Reserved		unknown	unknown	false
70.139.248.245	unknown	United States		7018	ATT-INTERNET4US	false
147.136.11.53	unknown	United States		16753	UNASSIGNED	false
148.250.20.98	unknown	Mexico		6503	AxtelSABdeCVMX	false
161.45.98.33	unknown	United States		26335	MTSUUS	false
151.208.146.197	unknown	United States		11003	PANDGUS	false
240.48.3.48	unknown	Reserved		unknown	unknown	false
73.250.35.113	unknown	United States		7922	COMCAST-7922US	false
32.143.82.94	unknown	United States		7018	ATT-INTERNET4US	false
76.251.40.162	unknown	United States		7018	ATT-INTERNET4US	false
208.52.153.4	unknown	United States		22626	VCI-22626US	false
14.108.217.117	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
183.41.239.45	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
176.131.97.133	unknown	France		5410	BOUYGTEL-ISPFR	false
43.36.69.65	unknown	Japan		4249	LILLY-ASUS	false
73.33.179.23	unknown	United States		7922	COMCAST-7922US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
2.86.93.252	unknown	Greece		6799	OTENET-GRAthens-GreeceGR	false
164.171.204.251	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
115.13.47.220	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
130.180.210.162	unknown	Ukraine		31343	INTERTELECOMUA	false
177.112.198.189	unknown	Brazil		26599	TELEFONICABRASILSABR	false
166.103.15.250	unknown	Korea Republic of		7029	WINDSTREAMUS	false
156.14.91.235	unknown	Italy		137	ASGARRConsortiumGARREU	false
32.198.117.210	unknown	United States		2686	ATGS-MMD-ASUS	false
148.125.59.177	unknown	United States		2119	TELENOR-NEXTELTelenorNorgeASNO	false
40.93.122.158	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
108.127.33.16	unknown	United States		10507	SPCSUS	false
120.140.255.84	unknown	Malaysia		45177	DEVOLI-AS-APDevoliNZ	false
84.107.200.105	unknown	Netherlands		33915	TNF-ASNL	false
2.106.168.48	unknown	Denmark		3292	TDCTDCASDK	false
150.108.196.65	unknown	United States		32531	FORDHAM-UNIVERSITYUS	false
204.156.18.99	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
13.51.123.170	unknown	United States		16509	AMAZON-02US	false
71.20.93.194	unknown	United States		7029	WINDSTREAMUS	false
74.93.248.194	unknown	United States		7922	COMCAST-7922US	false
23.240.15.65	unknown	United States		20001	TWC-20001-PACWESTUS	false
130.34.207.192	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
190.162.40.247	unknown	Chile		22047	VTRBANDAANCHASACL	false
60.63.70.32	unknown	China		9812	CNNIC-CN-COLNETOrientalCableNetworkCoLtdCN	false
178.52.228.3	unknown	Syrian Arab Republic		29256	INT-PDN-STE-ASSTEPDNInternalASSY	false
9.62.229.54	unknown	United States		3356	LEVEL3US	false
197.146.254.207	unknown	Morocco		36884	MAROCCONNECTMA	false
13.207.127.225	unknown	United States		7018	ATT-INTERNET4US	false
184.38.86.44	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
2.15.132.102	unknown	France		3215	FranceTelecom-OrangeFR	false
95.187.223.59	unknown	Saudi Arabia		39891	ALJAWWALSTC-ASSA	false
149.53.234.146	unknown	United States		174	COGENT-174US	false
197.185.70.91	unknown	South Africa		37105	NEOLOGY-ASZA	false
118.123.103.248	unknown	China		38283	CHINANET-SCIDC-AS-APCHINANETSiChuanTelecomInternetData	false
87.44.156.228	unknown	Ireland		1213	HEANETIE	false
223.223.106.42	unknown	Japan		18144	AS-ENECOMEnergiaCommunicationsIncJP	false
78.180.81.253	unknown	Turkey		9121	TTNETTR	false
174.243.224.93	unknown	United States		22394	CELLCOUS	false
207.5.2.91	unknown	United States		22646	HARCOM1US	false
93.141.216.21	unknown	Croatia (LOCAL Name: Hrvatska)		5391	T-HTCroatianTelecomIncHR	false
16.107.72.161	unknown	United States		unknown	unknown	false
31.17.181.253	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
60.233.124.194	unknown	China		1221	ASN-TELSTRATelstraCorporationLtdAU	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.162.116.56	unknown	Denmark		210210	REGION-MIDTJYLLAND-DK	false
223.64.16.29	unknown	China		56046	CMNET-JIANGSU-APChinaMobilecommunicationscorporationCN	false
125.8.172.81	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
45.161.181.39	unknown	Argentina		266892	SEBECABLESRLAR	false
174.47.121.216	unknown	United States		32419	BALDWIN-LYONSUS	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, PowerPC or cisco 4500, version 1 (GNU/Linux), statically linked, stripped
Entropy (8bit):	7.927381241431452
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	HUIHmcbfpW
File size:	26224
MD5:	7463d28ae705f29277567f6888315855
SHA1:	ca0836b4c352f1dd91a77422b952987f466f40e3
SHA256:	ed29224a554dd58df35208de727e297679bcbe2101d877e67736986deecffa8f
SHA512:	c3bd88c2b4cc13b51abaecd73895e3f854195620d3a9e61e4d93cf3004e10954234070f2447a6ac49ecbdca778bb0468df00fd6521ceed7de3b1d9046ba4be77
SSDEEP:	768:JKnqLiChP7gI5KUwxw2iEc0fxzULa2XiR4uVcqgw09v:JKqL1hz+iuGLaoiR4u+qgw09v
TLSH:	9CC2E170F8415E5AEBECDEF5D661C0D463AA8F4FA276DCB66045AF5043280238F5C56C
File Content Preview:	.ELF.....S....4.....4. ... (.....ex..ex.....D...D...D.....dt.Q.....UPX!.....T.....?.E.h4...@b.....H...i.&...Us..S?....Q..u.....B....|4...5|}

Static ELF Info

ELF header

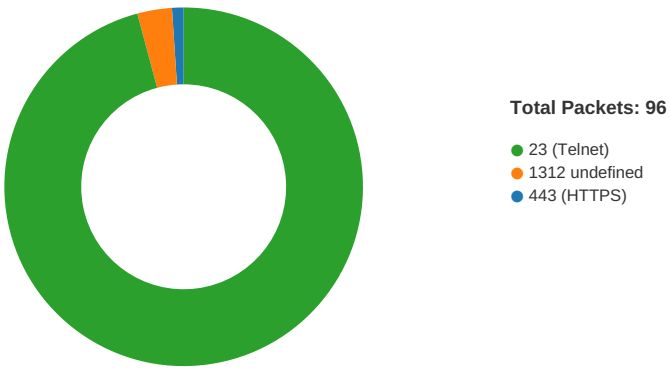
Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	PowerPC
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - Linux
ABI Version:	0
Entry Point Address:	0x105390
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
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	0x6578	0x6578	7.9313	0x5	R E	0x10000		
LOAD	0xfb44	0x1001fb44	0x1001fb44	0x0	0x0	0.0000	0x6	RW	0x10000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: HUIHmcbfpW PID: **6226**, Parent PID: **6125**

General

Start time:	23:06:57
Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	/tmp/HUIHmcbfpW
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Analysis Process: HUIHmcbfpW PID: **6228**, Parent PID: **6226**

General

Start time:	23:06:57
Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: HUIHmcbfpW PID: **6325**, Parent PID: **6228**

General

Start time:	23:09:48
Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: HUIHmcbfpW PID: **6326**, Parent PID: **6228**

General

Start time:	23:09:48
Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: HUIHmcbfpW PID: **6329**, Parent PID: **6326**

General

Start time:	23:09:48
Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: HUIHmcbfpW PID: **6342**, Parent PID: **6329**

General

Start time:	23:09:53

Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: HUIHmcbfpW PID: **6344**, Parent PID: **6329**

General

Start time:	23:09:53
Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: HUIHmcbfpW PID: **6330**, Parent PID: **6326**

General

Start time:	23:09:48
Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: HUIHmcbfpW PID: **6332**, Parent PID: **6326**

General

Start time:	23:09:48
Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: HUIHmcbfpW PID: **6229**, Parent PID: **6226**

General

Start time:	23:06:57
Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: HUIHmcbfpW PID: **6230**, Parent PID: **6226**

General

Start time:	23:06:57
Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

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

General

Start time:	23:06:57

Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: HUIHmcbfpW PID: **6336**, Parent PID: **6234**

General

Start time:	23:09:48
Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: HUIHmcbfpW PID: **6338**, Parent PID: **6234**

General

Start time:	23:09:48
Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

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

General

Start time:	23:06:57
Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: HUIHmcbfpW PID: **6236**, Parent PID: **6230**

General

Start time:	23:06:57
Start date:	08/08/2022
Path:	/tmp/HUIHmcbfpW
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6