ID: 830765
Sample Name: VeTv7e9Dcz.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 17:11:42
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

Linux Analysis Report

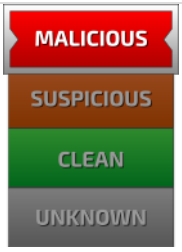
VeTv7e9Dcz.elf

Overview

General Information

Sample Name:	VeTv7e9Dcz.elf
Original Sample Name:	63ecd0078f4fa…
Analysis ID:	830765
MD5:	63ecd0078f4fa…
SHA1:	45784cb48d37…
SHA256:	363ff4d711108…
Tags:	32 elf mirai powerpc
Infos:	

Detection



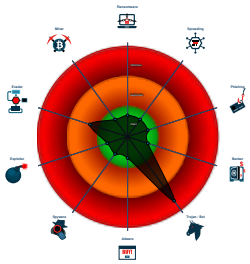
Mirai, Moobot

Score:	92
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Moobot
- Snort IDS alert for network traffic
- Connects to many ports of the same…
- Uses known network protocols on n…
- Sets full permissions to files and/or …
- Yara signature match
- Executes the "mkdir" command use…
- Uses the "uname" system call to qu…

Classification



Analysis Advice

All domains contacted by the sample do not resolve. The sample is likely an old dropper which does no longer work.

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:	37.0.0 Beryl
Analysis ID:	830765
Start date and time:	2023-03-20 17:11:42 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
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
Sample file name:	VeTv7e9Dcz.elf
Original Sample Name:	63ecd0078f4faaf6905fbbc25d6d2d64.elf
Detection:	MAL
Classification:	mal92.troj.linELF@0/0@100/0

Warnings

Runtime Messages

Command:	/tmp/VeTv7e9Dcz.elf
PID:	6226
Exit Code:	0
Exit Code Info:	

Killed:	False
Standard Output:	^p
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- VeTv7e9Dcz.elf (PID: 6226, Parent: 6121, MD5: ae65271c943d3451b7f026d1fadccea6) Arguments: /tmp/VeTv7e9Dcz.elf
  - VeTv7e9Dcz.elf New Fork (PID: 6228, Parent: 6226)
  - sh (PID: 6228, Parent: 6226, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf bin/systemd && mkdir bin; >bin/systemd && mv /tmp/VeTv7e9Dcz.elf bin/systemd; chmod 777 bin/systemd"
    - sh New Fork (PID: 6230, Parent: 6228)
    - rm (PID: 6230, Parent: 6228, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf bin/systemd
    - sh New Fork (PID: 6231, Parent: 6228)
    - mkdir (PID: 6231, Parent: 6228, MD5: 088c9d1df5a28ed16c726eca15964cb7) Arguments: mkdir bin
    - sh New Fork (PID: 6232, Parent: 6228)
    - mv (PID: 6232, Parent: 6228, MD5: 504f0590fa482d4da070a702260e3716) Arguments: mv /tmp/VeTv7e9Dcz.elf bin/systemd
    - sh New Fork (PID: 6233, Parent: 6228)
    - chmod (PID: 6233, Parent: 6228, MD5: 739483b900c045ae1374d6f53a86a279) Arguments: chmod 777 bin/systemd
  - VeTv7e9Dcz.elf New Fork (PID: 6234, Parent: 6226)
    - VeTv7e9Dcz.elf New Fork (PID: 6236, Parent: 6234)
    - VeTv7e9Dcz.elf New Fork (PID: 6237, Parent: 6234)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Mirai	Mirai is one of the first significant botnets targeting exposed networking devices running Linux. Found in August 2016 by MalwareMustDie, its name means "future" in Japanese. Nowadays it targets a wide range of networked embedded devices such as IP cameras, home routers (many vendors involved), and other IoT devices. Since the source code was published on "Hack Forums" many variants of the Mirai family appeared, infecting mostly home networks all around the world.	No Attribution	**http://** osint.bambenekconsulting.com/feeds/http://www.simonroses.com/2016/10/mirai-ddos-botnet-source-code-binary-analysis/https://blog.malwaremustdie.org/2020/02/mmd-0065-2021-linuxmirai-fbot-re.htmlhttps://blog.netlab.360.com/another-lilin-dvr-0-day-being-used-to-spread-mirai-en/https://blog.netlab.360.com/mirai_ptea-botnet-is-exploiting-undisclosed-kguard-dvr-vulnerability-en/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai

Name	Description	Attribution	Blogpost URLs	Link
MooBot		No Attribution	**http://** https://blog.netlab.360.com/ddos-botnet-moobot-en/https://blog.netlab.360.com/moobot-0day-unixcctv-dvr-en/https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/https://otx.alienvault.com/pulse/6075b645942d5adf9bb8949bhttps://unit42.paloaltonetworks.com/moobot-d-link-devices/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/elf.moobot

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
VeTv7e9Dcz.elf	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
VeTv7e9Dcz.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
VeTv7e9Dcz.elf	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xd33c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd350:$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 • 0xd364:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd378:$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 • 0xd38c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3a0:$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 • 0xd3b4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3c8:$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 • 0xd3dc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3f0:$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 • 0xd404:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd418:$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 • 0xd42c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd440:$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 • 0xd454:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd468:$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 • 0xd47c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd490:$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 • 0xd4a4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd4b8:$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 • 0xd4cc:$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

Memory Dumps

Source	Rule	Description	Author	Strings
6236.1.00007fa060001000.00007fa060011000.r-x.sdmp	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
6236.1.00007fa060001000.00007fa060011000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6236.1.00007fa060001000.00007fa060011000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xd33c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd350:$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 • 0xd364:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd378:$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 • 0xd38c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3a0:$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 • 0xd3b4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3c8:$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 • 0xd3dc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd3f0:$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 • 0xd404:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd418:$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 • 0xd42c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd440:$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 • 0xd454:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd468:$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 • 0xd47c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd490:$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 • 0xd4a4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xd4b8:$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 • 0xd4cc:$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
6226.1.00007fa060001000.00007fa060011000.r-x.sdmp	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
6226.1.00007fa060001000.00007fa060011000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Click to see the 5 entries				

Snort Signatures

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 41.232.168.144

Timestamp:	192.168.2.2341.232.168.14444248372152835222 03/20/23-17:12:55.092526
SID:	2835222
Source Port:	44248
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.246.213.142

Timestamp:	192.168.2.23197.246.213.14260578372152835222 03/20/23-17:13:02.227474
SID:	2835222
Source Port:	60578
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 84.7.168.241

Timestamp:	192.168.2.2384.7.168.241337783721528352222 03/20/23-17:12:38.593270
SID:	2835222
Source Port:	33778

Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

Connects to many ports of the same IP (likely port scanning)

Uses known network protocols on non-standard ports

System Summary

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior

Sets full permissions to files and/or directories

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Yara detected Moobot

Remote Access Functionality

Yara detected Mirai

Yara detected Moobot

Mitre Att&ck Matrix

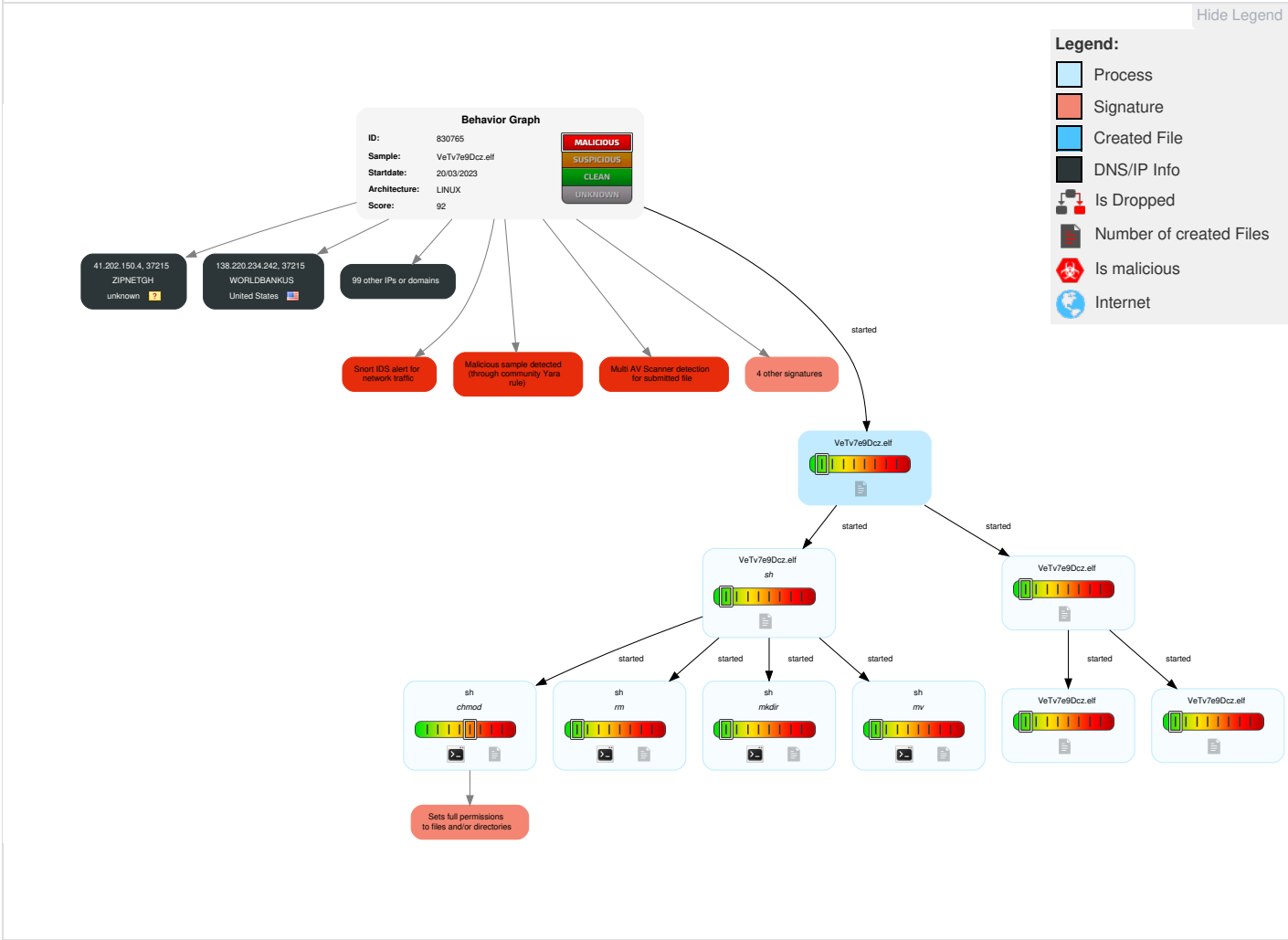
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	Path Interception	Path Interception	2 File and Directory Permissions Modification	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	1 Scripting	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)	1 File Deletion	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
VeTv7e9Dcz.elf	59%	ReversingLabs	Linux.Trojan.Mirai	

Source	Detection	Scanner	Label	Link
VeTv7e9Dcz.elf	61%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

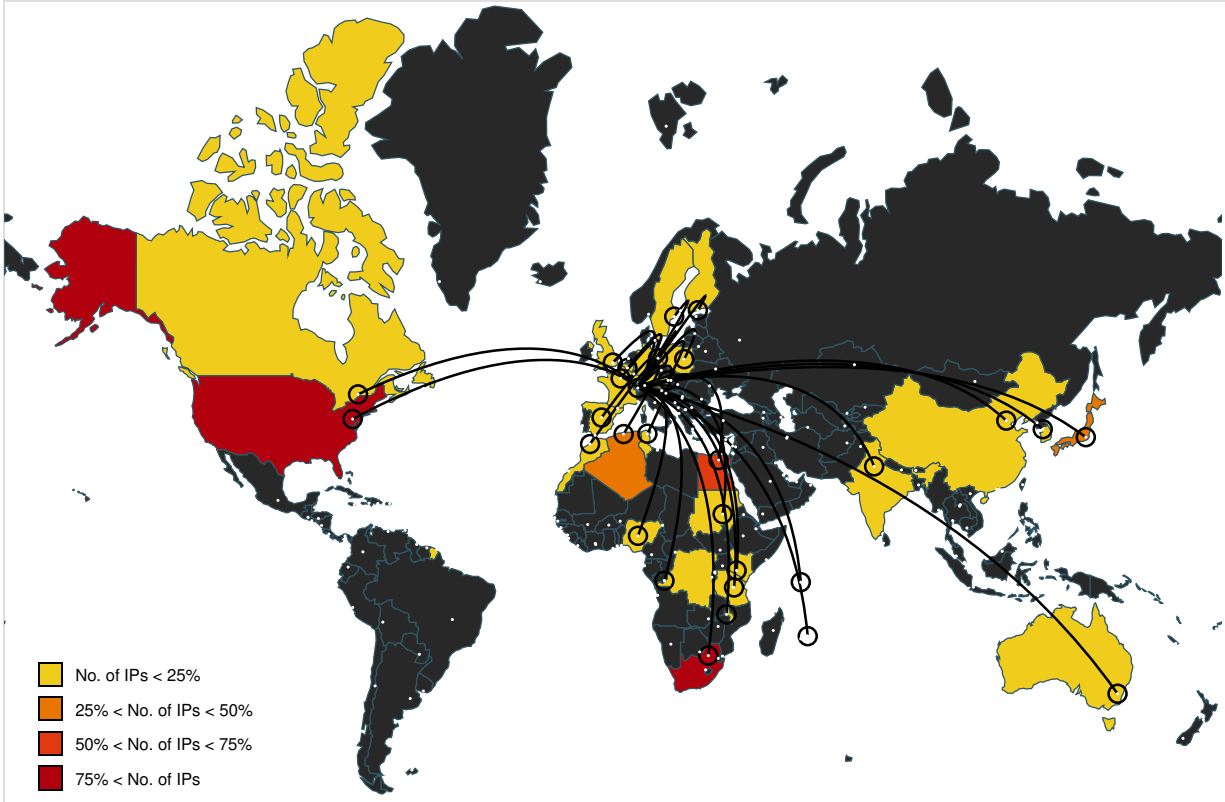
Domains and IPs

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
197.247.118.54	unknown	Morocco		36925	ASMediMA	false
57.27.35.138	unknown	Belgium		2686	ATGS-MMD-ASUS	false
197.234.167.185	unknown	South Africa		37315	CipherWaveZA	false
111.150.82.125	unknown	China		38370	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
197.87.221.134	unknown	South Africa		10474	OPTINETZA	false
41.42.229.210	unknown	Egypt		8452	TE-ASTE-ASEG	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.36.131.164	unknown	Egypt		8452	TE-ASTE-ASEG	false
157.201.251.216	unknown	United States		33281	BRIGHAM-YOUNG-UNIVERSITY-IDAHOUS	false
197.49.112.231	unknown	Egypt		8452	TE-ASTE-ASEG	false
62.161.162.146	unknown	France		3215	FranceTelecom-OrangeFR	false
41.203.250.186	unknown	Seychelles		36902	ASINTELVISIONSC	false
223.192.185.45	unknown	China		7497	CSTNET-AS-APComputerNetworkInformationCenterCN	false
41.251.165.149	unknown	Morocco		36903	MT-MPLSMA	false
81.156.178.88	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
41.3.250.50	unknown	South Africa		29975	VODACOM-ZA	false
157.97.64.139	unknown	Germany		25259	MDCLOUD-ES	false
157.48.186.148	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
197.46.166.28	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.21.215.59	unknown	South Africa		36994	Vodacom-VBZA	false
157.211.157.176	unknown	Australia		7573	UTASTheUniversityofTasmaniaAU	false
51.118.119.200	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
41.116.238.222	unknown	South Africa		16637	MTNNS-ASZA	false
197.118.80.100	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.77.77.97	unknown	South Africa		16637	MTNNS-ASZA	false
41.222.196.127	unknown	Congo The Democratic Republic of The		37020	CELTEL-DRCCD	false
197.59.205.50	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.145.166.81	unknown	South Africa		5713	SAIX-NETZA	false
157.124.146.107	unknown	Finland		1738	OKOBANK-ASEU	false
197.33.73.10	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.59.48.77	unknown	Tanzania United Republic of		33765	TTCLDATATZ	false
41.169.25.75	unknown	South Africa		36937	Neotel-ASZA	false
138.220.234.242	unknown	United States		10497	WORLDBANKUS	false
197.17.202.164	unknown	Tunisia		37693	TUNISIANATN	false
197.206.175.78	unknown	Algeria		36947	ALGTEL-ASDZ	false
157.25.46.232	unknown	Poland		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
41.135.57.100	unknown	South Africa		10474	OPTINETZA	false
157.34.57.103	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
197.165.44.53	unknown	Egypt		24863	LINKdotNET-ASEG	false
157.127.227.102	unknown	United States		1906	NORTHROP-GRUMMANUS	false
41.156.40.150	unknown	South Africa		37168	CELL-CZA	false
197.8.107.192	unknown	Tunisia		5438	ATI-TN	false
197.132.129.168	unknown	Egypt		24835	RAYA-ASEG	false
109.244.173.151	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
157.9.162.55	unknown	Japan		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
157.64.206.81	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
197.227.174.9	unknown	Mauritius		23889	MauritiusTelecomMU	false
41.96.36.205	unknown	Algeria		36947	ALGTEL-ASDZ	false
41.233.119.53	unknown	Egypt		8452	TE-ASTE-ASEG	false
66.113.21.21	unknown	United States		15221	STRATUSIQUS	false
135.253.41.199	unknown	United States		10455	LUCENT-CIOUS	false
41.49.24.129	unknown	South Africa		37168	CELL-CZA	false
157.20.207.5	unknown	unknown		24297	FCNUniversityPublicCorporationOsakaJP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
161.237.38.240	unknown	United States		396269	BPL-ASNUS	false
197.60.70.229	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.113.54.117	unknown	Algeria		36947	ALGTEL-ASDZ	false
157.23.1.231	unknown	France		7091	VIANET-ASNUS	false
41.67.115.101	unknown	unknown		36974	AFNET-ASCI	false
41.141.24.246	unknown	Morocco		36903	MT-MPLSMA	false
197.114.109.14	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.176.125.149	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
49.23.179.75	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
157.194.40.10	unknown	United States		4704	SANNETRakutenMobileIncJP	false
41.177.165.217	unknown	South Africa		36874	CybersmartZA	false
23.87.97.28	unknown	United States		395954	LEASEWEB-USA-LAX-11US	false
41.105.143.107	unknown	Algeria		36947	ALGTEL-ASDZ	false
157.247.33.248	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
197.178.176.162	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
197.180.107.68	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
41.202.150.4	unknown	unknown		36961	ZIPNETGH	false
157.40.148.205	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
169.92.64.135	unknown	United States		37611	AfrihostZA	false
41.224.199.208	unknown	Tunisia		37492	ORANGE-TN	false
157.245.169.42	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
8.42.101.221	unknown	United States		63168	TRP-COLORADO-SPRINGSUS	false
69.201.229.5	unknown	United States		12271	TWC-12271-NYCUS	false
41.112.57.241	unknown	South Africa		16637	MTNNS-ASZA	false
157.17.51.11	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
157.70.65.174	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
157.23.253.239	unknown	France		11251	DSTL-2-11251US	false
45.2.81.57	unknown	Canada		7311	FRONTIERCA	false
157.61.238.107	unknown	China		17622	CNCGROUP-GZChinaUnicomGuangzhounetworkCN	false
41.37.131.65	unknown	Egypt		8452	TE-ASTE-ASEG	false
102.70.113.12	unknown	Malawi		37294	TNMMW	false
157.105.123.94	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
44.126.188.18	unknown	United States		7377	UCSDUS	false
157.215.57.38	unknown	United States		4704	SANNETRakutenMobileIncJP	false
67.102.93.113	unknown	United States		18566	MEGAPATH5-US	false
197.90.25.91	unknown	South Africa		10474	OPTINETZA	false
147.220.248.115	unknown	Sweden		34576	REGIONSKANE-SEREGIONSKANESE	false
197.254.220.116	unknown	Sudan		33788	KANARTELSD	false
41.171.231.133	unknown	South Africa		36937	Neotel-ASZA	false
197.237.196.234	unknown	Kenya		15399	WANANCHI-KE	false
157.88.4.108	unknown	Spain		766	REDIRISRedIRISAutonomousSystemES	false
157.158.112.143	unknown	Poland		8508	SILWEB-AS-EDUSILWEBAutonomousSystem-AcademicPL	false
157.141.252.39	unknown	United States		27064	DNIC-ASBLK-27032-27159US	false
41.184.75.133	unknown	Nigeria		29091	IPNXngNG	false
41.133.51.96	unknown	South Africa		10474	OPTINETZA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.145.10.107	unknown	United States		719	ELISA-ASHelsinkiFinlandEU	false
41.225.189.122	unknown	Tunisia		37671	GLOBALNET-ASTN	false
157.42.204.199	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	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 (SYSV), statically linked, stripped
Entropy (8bit):	6.271541719812631
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	VeTv7e9Dcz.elf
File size:	62996
MD5:	63ecd0078f4faaf6905fbbc25d6d2d64
SHA1:	45784cb48d376fda8480e009405fc6f383e9d209
SHA256:	363ff4d7111088d2f670a7d4da8a3427ca5af8a8459b39366ae279e835977747
SHA512:	b44287de6279299d0f84ee7f23efcd0c7d806fa50902b0a4a6b845eb85d0e1ac449fbb44c1394c863a425b4419fe00cdca9430396fac2d457ee56fc832d93859
SSDEEP:	768:SEE5hjcoCkhVRGfRnbmX7/mG1nhG5UmtTy5EMwu/p9OyDQvSFRMNYL6FV+tg6wWA:+5HAdOmGyNtTAdpOyUaFRMNae+aTWp+
TLSH:	7A534B02B31C0E07D0A31AB0253F5BD197BEEAD022F4F684656F9B9A9675E361181FCD
File Content Preview:	.ELF.....4...4.....4. ...(.....x...x.....|...|...|..%t.....dt.Q.....!..|.....$H...H..-...$8!. |...N.. .!..|.....?.....\.../...@..\?.....+../...A..$8...}).....N..

Static ELF Info

ELF header

Class:	

ELF header	
Data:	
Version:	
Machine:	
Version Number:	
Type:	
OS/ABI:	
ABI Version:	
Entry Point Address:	
Flags:	
ELF Header Size:	
Program Header Offset:	
Program Header Size:	
Number of Program Headers:	
Section Header Offset:	
Section Header Size:	
Number of Section Headers:	
Header String Table Index:	

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10000094	0x94	0x24	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100000b8	0xb8	0xd184	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x1000d23c	0xd23c	0x20	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1000d260	0xd260	0x1e18	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x1001f07c	0xf07c	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x1001f084	0xf084	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x1001f090	0xf090	0x314	0x0	0x3	WA	0	0	8
.sdata	PROGBITS	0x1001f3a4	0xf3a4	0x44	0x0	0x3	WA	0	0	4
.sbss	NOBITS	0x1001f3e8	0xf3e8	0x74	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x1001f45c	0xf3e8	0x2194	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xf3e8	0x4b	0x0	0x0		0	0	1

Program Segments

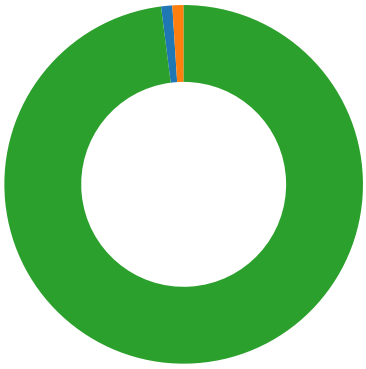
Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x10000000	0x10000000	0xf078	0xf078	6.3210	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xf07c	0x1001f07c	0x1001f07c	0x36c	0x2574	2.8558	0x6	RW	0x10000		.ctors .dtors .data .sdata .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2341.232.168.144442483721528352220 3/20/23-17:12:55.092526	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	44248	37215	192.168.2.23	41.232.168.144
192.168.2.23197.246.213.1426057837215283522203/20/23-17:13:02.227474	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	60578	37215	192.168.2.23	197.246.213.142
192.168.2.2384.7.168.24133778372152835222 03/20/23-17:12:38.593270	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	33778	37215	192.168.2.23	84.7.168.241

Network Port Distribution



Total Packets: 99

- 37215 undefined
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 17:12:32.492122889 CET	192.168.2.23	8.8.8.8	0x6162	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:32.517299891 CET	192.168.2.23	8.8.8.8	0x6162	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:32.537633896 CET	192.168.2.23	8.8.8.8	0x6162	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:32.557524920 CET	192.168.2.23	8.8.8.8	0x6162	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:32.575745106 CET	192.168.2.23	8.8.8.8	0x6162	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:39.600483894 CET	192.168.2.23	8.8.8.8	0xc1f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:39.622463942 CET	192.168.2.23	8.8.8.8	0xc1f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:39.641073942 CET	192.168.2.23	8.8.8.8	0xc1f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:39.662622929 CET	192.168.2.23	8.8.8.8	0xc1f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:39.683422089 CET	192.168.2.23	8.8.8.8	0xc1f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:49.704005957 CET	192.168.2.23	8.8.8.8	0x554d	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:49.722170115 CET	192.168.2.23	8.8.8.8	0x554d	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:49.742053986 CET	192.168.2.23	8.8.8.8	0x554d	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:49.762362003 CET	192.168.2.23	8.8.8.8	0x554d	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:49.780390024 CET	192.168.2.23	8.8.8.8	0x554d	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:58.800568104 CET	192.168.2.23	8.8.8.8	0xf9e6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:58.820017099 CET	192.168.2.23	8.8.8.8	0xf9e6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:58.840202093 CET	192.168.2.23	8.8.8.8	0xf9e6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:58.860093117 CET	192.168.2.23	8.8.8.8	0xf9e6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:58.886013031 CET	192.168.2.23	8.8.8.8	0xf9e6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:00.904612064 CET	192.168.2.23	8.8.8.8	0xdd9a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:00.924596071 CET	192.168.2.23	8.8.8.8	0xdd9a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 17:13:00.944766045 CET	192.168.2.23	8.8.8.8	0xdd9a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:00.964998960 CET	192.168.2.23	8.8.8.8	0xdd9a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:00.984601021 CET	192.168.2.23	8.8.8.8	0xdd9a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:11.004483938 CET	192.168.2.23	8.8.8.8	0x52b	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:11.027167082 CET	192.168.2.23	8.8.8.8	0x52b	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:11.045247078 CET	192.168.2.23	8.8.8.8	0x52b	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:11.063252926 CET	192.168.2.23	8.8.8.8	0x52b	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:11.081378937 CET	192.168.2.23	8.8.8.8	0x52b	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:16.099610090 CET	192.168.2.23	8.8.8.8	0xb14a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:16.119885921 CET	192.168.2.23	8.8.8.8	0xb14a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:16.138309002 CET	192.168.2.23	8.8.8.8	0xb14a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:16.155997992 CET	192.168.2.23	8.8.8.8	0xb14a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:16.174251080 CET	192.168.2.23	8.8.8.8	0xb14a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:22.192508936 CET	192.168.2.23	8.8.8.8	0x6156	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:22.210782051 CET	192.168.2.23	8.8.8.8	0x6156	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:22.230757952 CET	192.168.2.23	8.8.8.8	0x6156	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:22.249365091 CET	192.168.2.23	8.8.8.8	0x6156	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:22.269886017 CET	192.168.2.23	8.8.8.8	0x6156	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:24.288551092 CET	192.168.2.23	8.8.8.8	0x3ad3	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:24.306853056 CET	192.168.2.23	8.8.8.8	0x3ad3	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:24.327182055 CET	192.168.2.23	8.8.8.8	0x3ad3	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:24.346571922 CET	192.168.2.23	8.8.8.8	0x3ad3	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:24.365061998 CET	192.168.2.23	8.8.8.8	0x3ad3	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:26.385014057 CET	192.168.2.23	8.8.8.8	0xf22c	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:26.403367996 CET	192.168.2.23	8.8.8.8	0xf22c	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:26.423146009 CET	192.168.2.23	8.8.8.8	0xf22c	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:26.441109896 CET	192.168.2.23	8.8.8.8	0xf22c	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:26.461011887 CET	192.168.2.23	8.8.8.8	0xf22c	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:32.480617046 CET	192.168.2.23	8.8.8.8	0x9199	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:32.500961065 CET	192.168.2.23	8.8.8.8	0x9199	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:32.520802021 CET	192.168.2.23	8.8.8.8	0x9199	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:32.539278030 CET	192.168.2.23	8.8.8.8	0x9199	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:32.559184074 CET	192.168.2.23	8.8.8.8	0x9199	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:37.577591896 CET	192.168.2.23	8.8.8.8	0x5ff	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:37.598490000 CET	192.168.2.23	8.8.8.8	0x5ff	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 17:13:37.619050026 CET	192.168.2.23	8.8.8.8	0x5ff	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:37.642474890 CET	192.168.2.23	8.8.8.8	0x5ff	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:37.662600994 CET	192.168.2.23	8.8.8.8	0x5ff	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:42.680840015 CET	192.168.2.23	8.8.8.8	0x4f3d	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:42.700831890 CET	192.168.2.23	8.8.8.8	0x4f3d	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:42.718713999 CET	192.168.2.23	8.8.8.8	0x4f3d	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:42.738929987 CET	192.168.2.23	8.8.8.8	0x4f3d	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:42.756850958 CET	192.168.2.23	8.8.8.8	0x4f3d	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:52.776473999 CET	192.168.2.23	8.8.8.8	0x3963	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:52.796468973 CET	192.168.2.23	8.8.8.8	0x3963	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:52.814531088 CET	192.168.2.23	8.8.8.8	0x3963	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:52.832792044 CET	192.168.2.23	8.8.8.8	0x3963	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:52.851162910 CET	192.168.2.23	8.8.8.8	0x3963	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:01.871340036 CET	192.168.2.23	8.8.8.8	0x8cc2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:01.892065048 CET	192.168.2.23	8.8.8.8	0x8cc2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:01.910787106 CET	192.168.2.23	8.8.8.8	0x8cc2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:01.931792021 CET	192.168.2.23	8.8.8.8	0x8cc2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:01.952481031 CET	192.168.2.23	8.8.8.8	0x8cc2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:08.972430944 CET	192.168.2.23	8.8.8.8	0x643f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:08.990817070 CET	192.168.2.23	8.8.8.8	0x643f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:09.009038925 CET	192.168.2.23	8.8.8.8	0x643f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:09.030524969 CET	192.168.2.23	8.8.8.8	0x643f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:09.051043034 CET	192.168.2.23	8.8.8.8	0x643f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:18.069339037 CET	192.168.2.23	8.8.8.8	0xa1d0	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:18.090115070 CET	192.168.2.23	8.8.8.8	0xa1d0	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:18.108059883 CET	192.168.2.23	8.8.8.8	0xa1d0	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:18.128057003 CET	192.168.2.23	8.8.8.8	0xa1d0	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:18.145721912 CET	192.168.2.23	8.8.8.8	0xa1d0	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:27.165184021 CET	192.168.2.23	8.8.8.8	0x186f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:27.183620930 CET	192.168.2.23	8.8.8.8	0x186f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:27.203716040 CET	192.168.2.23	8.8.8.8	0x186f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:27.221940041 CET	192.168.2.23	8.8.8.8	0x186f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:27.240173101 CET	192.168.2.23	8.8.8.8	0x186f	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:29.260246038 CET	192.168.2.23	8.8.8.8	0x8d17	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:29.279043913 CET	192.168.2.23	8.8.8.8	0x8d17	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 17:14:29.299376011 CET	192.168.2.23	8.8.8.8	0x8d17	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:29.319619894 CET	192.168.2.23	8.8.8.8	0x8d17	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:29.339847088 CET	192.168.2.23	8.8.8.8	0x8d17	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:30.358474016 CET	192.168.2.23	8.8.8.8	0x7a2e	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:30.376990080 CET	192.168.2.23	8.8.8.8	0x7a2e	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:30.395179987 CET	192.168.2.23	8.8.8.8	0x7a2e	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:30.413711071 CET	192.168.2.23	8.8.8.8	0x7a2e	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:30.432341099 CET	192.168.2.23	8.8.8.8	0x7a2e	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 17:12:32.516231060 CET	8.8.8.8	192.168.2.23	0x6162	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:32.537130117 CET	8.8.8.8	192.168.2.23	0x6162	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:32.557233095 CET	8.8.8.8	192.168.2.23	0x6162	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:32.575474024 CET	8.8.8.8	192.168.2.23	0x6162	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:32.599232912 CET	8.8.8.8	192.168.2.23	0x6162	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:39.622071028 CET	8.8.8.8	192.168.2.23	0xc1f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:39.640789032 CET	8.8.8.8	192.168.2.23	0xc1f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:39.662328005 CET	8.8.8.8	192.168.2.23	0xc1f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:39.682928085 CET	8.8.8.8	192.168.2.23	0xc1f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:39.703553915 CET	8.8.8.8	192.168.2.23	0xc1f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:49.721863985 CET	8.8.8.8	192.168.2.23	0x554d	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:49.741826057 CET	8.8.8.8	192.168.2.23	0x554d	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:49.762021065 CET	8.8.8.8	192.168.2.23	0x554d	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:49.780055046 CET	8.8.8.8	192.168.2.23	0x554d	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:49.800240993 CET	8.8.8.8	192.168.2.23	0x554d	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:58.819556952 CET	8.8.8.8	192.168.2.23	0xf9e6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:58.839855909 CET	8.8.8.8	192.168.2.23	0xf9e6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 17:12:58.859692097 CET	8.8.8.8	192.168.2.23	0xf9e6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:58.885704994 CET	8.8.8.8	192.168.2.23	0xf9e6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:12:58.904095888 CET	8.8.8.8	192.168.2.23	0xf9e6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:00.924227953 CET	8.8.8.8	192.168.2.23	0xdd9a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:00.944436073 CET	8.8.8.8	192.168.2.23	0xdd9a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:00.964705944 CET	8.8.8.8	192.168.2.23	0xdd9a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:00.984287977 CET	8.8.8.8	192.168.2.23	0xdd9a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:01.004405022 CET	8.8.8.8	192.168.2.23	0xdd9a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:11.026776075 CET	8.8.8.8	192.168.2.23	0x52b	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:11.044946909 CET	8.8.8.8	192.168.2.23	0x52b	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:11.062887907 CET	8.8.8.8	192.168.2.23	0x52b	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:11.081073046 CET	8.8.8.8	192.168.2.23	0x52b	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:11.099245071 CET	8.8.8.8	192.168.2.23	0x52b	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:16.119565964 CET	8.8.8.8	192.168.2.23	0xb14a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:16.138021946 CET	8.8.8.8	192.168.2.23	0xb14a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:16.155735970 CET	8.8.8.8	192.168.2.23	0xb14a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:16.173990011 CET	8.8.8.8	192.168.2.23	0xb14a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:16.192210913 CET	8.8.8.8	192.168.2.23	0xb14a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:22.210215092 CET	8.8.8.8	192.168.2.23	0x6156	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:22.230431080 CET	8.8.8.8	192.168.2.23	0x6156	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:22.248961926 CET	8.8.8.8	192.168.2.23	0x6156	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:22.269521952 CET	8.8.8.8	192.168.2.23	0x6156	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:22.287919044 CET	8.8.8.8	192.168.2.23	0x6156	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:24.306523085 CET	8.8.8.8	192.168.2.23	0x3ad3	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:24.326883078 CET	8.8.8.8	192.168.2.23	0x3ad3	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 17:13:24.346240044 CET	8.8.8.8	192.168.2.23	0x3ad3	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:24.364700079 CET	8.8.8.8	192.168.2.23	0x3ad3	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:24.384423971 CET	8.8.8.8	192.168.2.23	0x3ad3	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:26.403085947 CET	8.8.8.8	192.168.2.23	0xf22c	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:26.422889948 CET	8.8.8.8	192.168.2.23	0xf22c	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:26.440850973 CET	8.8.8.8	192.168.2.23	0xf22c	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:26.460712910 CET	8.8.8.8	192.168.2.23	0xf22c	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:26.480361938 CET	8.8.8.8	192.168.2.23	0xf22c	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:32.500587940 CET	8.8.8.8	192.168.2.23	0x9199	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:32.520541906 CET	8.8.8.8	192.168.2.23	0x9199	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:32.538984060 CET	8.8.8.8	192.168.2.23	0x9199	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:32.558924913 CET	8.8.8.8	192.168.2.23	0x9199	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:32.577260017 CET	8.8.8.8	192.168.2.23	0x9199	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:37.598125935 CET	8.8.8.8	192.168.2.23	0x5ff	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:37.618659973 CET	8.8.8.8	192.168.2.23	0x5ff	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:37.642180920 CET	8.8.8.8	192.168.2.23	0x5ff	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:37.662312031 CET	8.8.8.8	192.168.2.23	0x5ff	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:37.680573940 CET	8.8.8.8	192.168.2.23	0x5ff	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:42.700556040 CET	8.8.8.8	192.168.2.23	0x4f3d	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:42.718492985 CET	8.8.8.8	192.168.2.23	0x4f3d	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:42.738679886 CET	8.8.8.8	192.168.2.23	0x4f3d	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:42.756644964 CET	8.8.8.8	192.168.2.23	0x4f3d	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:42.776458025 CET	8.8.8.8	192.168.2.23	0x4f3d	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:52.796152115 CET	8.8.8.8	192.168.2.23	0x3963	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:52.814260960 CET	8.8.8.8	192.168.2.23	0x3963	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 17:13:52.832432985 CET	8.8.8.8	192.168.2.23	0x3963	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:52.850893974 CET	8.8.8.8	192.168.2.23	0x3963	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:13:52.871275902 CET	8.8.8.8	192.168.2.23	0x3963	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:01.891750097 CET	8.8.8.8	192.168.2.23	0x8cc2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:01.910582066 CET	8.8.8.8	192.168.2.23	0x8cc2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:01.931508064 CET	8.8.8.8	192.168.2.23	0x8cc2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:01.952198982 CET	8.8.8.8	192.168.2.23	0x8cc2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:01.972140074 CET	8.8.8.8	192.168.2.23	0x8cc2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:08.990540981 CET	8.8.8.8	192.168.2.23	0x643f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:09.008733988 CET	8.8.8.8	192.168.2.23	0x643f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:09.030216932 CET	8.8.8.8	192.168.2.23	0x643f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:09.050682068 CET	8.8.8.8	192.168.2.23	0x643f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:09.069377899 CET	8.8.8.8	192.168.2.23	0x643f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:18.089854956 CET	8.8.8.8	192.168.2.23	0xa1d0	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:18.107858896 CET	8.8.8.8	192.168.2.23	0xa1d0	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:18.127896070 CET	8.8.8.8	192.168.2.23	0xa1d0	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:18.145593882 CET	8.8.8.8	192.168.2.23	0xa1d0	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:18.165282011 CET	8.8.8.8	192.168.2.23	0xa1d0	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:27.183267117 CET	8.8.8.8	192.168.2.23	0x186f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:27.203397989 CET	8.8.8.8	192.168.2.23	0x186f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:27.221693039 CET	8.8.8.8	192.168.2.23	0x186f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:27.239876032 CET	8.8.8.8	192.168.2.23	0x186f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:27.259748936 CET	8.8.8.8	192.168.2.23	0x186f	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:29.278733015 CET	8.8.8.8	192.168.2.23	0x8d17	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:29.298923969 CET	8.8.8.8	192.168.2.23	0x8d17	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 17:14:29.319319010 CET	8.8.8.8	192.168.2.23	0x8d17	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:29.339601040 CET	8.8.8.8	192.168.2.23	0x8d17	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:29.357830048 CET	8.8.8.8	192.168.2.23	0x8d17	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:30.376674891 CET	8.8.8.8	192.168.2.23	0x7a2e	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:30.394891024 CET	8.8.8.8	192.168.2.23	0x7a2e	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:30.413374901 CET	8.8.8.8	192.168.2.23	0x7a2e	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:30.432030916 CET	8.8.8.8	192.168.2.23	0x7a2e	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:14:30.450268984 CET	8.8.8.8	192.168.2.23	0x7a2e	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: VeTv7e9Dcz.elf PID: **6226**, Parent PID: **6121**

General

Start time:	17:12:31
Start date:	20/03/2023
Path:	/tmp/VeTv7e9Dcz.elf
Arguments:	/tmp/VeTv7e9Dcz.elf
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Analysis Process: VeTv7e9Dcz.elf PID: **6228**, Parent PID: **6226**

General

Start time:	17:12:31
Start date:	20/03/2023
Path:	/tmp/VeTv7e9Dcz.elf
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

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

General

Start time:	17:12:31
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	sh -c "rm -rf bin/systemd && mkdir bin; >bin/systemd && mv /tmp/VeTv7e9Dcz.elf bin/systemd; chmod 777 bin/systemd"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **6230**, Parent PID: **6228**

General

Start time:	17:12:31
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **6230**, Parent PID: **6228**

General

Start time:	17:12:31
Start date:	20/03/2023
Path:	/usr/bin/rm
Arguments:	rm -rf bin/systemd
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

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

General

Start time:	17:12:31
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	17:12:31
Start date:	20/03/2023
Path:	/usr/bin/mkdir
Arguments:	mkdir bin
File size:	88408 bytes
MD5 hash:	088c9d1df5a28ed16c726eca15964cb7

File Activities

File Read

Directory Created

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

General

Start time:	17:12:31
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

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

General

Start time:	17:12:31
Start date:	20/03/2023
Path:	/usr/bin/mv
Arguments:	mv /tmp/VeTv7e9Dcz.elf bin/systemd
File size:	149888 bytes
MD5 hash:	504f0590fa482d4da070a702260e3716

File Activities

File Read

File Moved

Analysis Process: sh PID: **6233**, Parent PID: **6228**

General

Start time:	17:12:31
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: chmod PID: **6233**, Parent PID: **6228**

General

Start time:	17:12:31
Start date:	20/03/2023
Path:	/usr/bin/chmod
Arguments:	chmod 777 bin/systemd
File size:	63864 bytes
MD5 hash:	739483b900c045ae1374d6f53a86a279

File Activities

File Read

Permission Modified

Analysis Process: VeTv7e9Dcz.elf PID: **6234**, Parent PID: **6226**

General

Start time:	17:12:31
Start date:	20/03/2023
Path:	/tmp/VeTv7e9Dcz.elf
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: VeTv7e9Dcz.elf PID: **6236**, Parent PID: **6234**

General

Start time:	17:12:31
Start date:	20/03/2023
Path:	/tmp/VeTv7e9Dcz.elf
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: VeTv7e9Dcz.elf PID: **6237**, Parent PID: **6234**

General	
Start time:	17:12:31
Start date:	20/03/2023
Path:	/tmp/VeTv7e9Dcz.elf
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6