ID: 830809
Sample Name: 8oxYPvmeaT.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 17:52:57
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

Linux Analysis Report

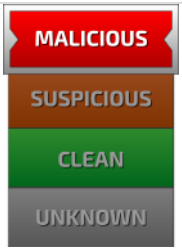
8oxYPvmeaT.elf

Overview

General Information

Sample Name:	8oxYPvmeaT.elf
Original Sample Name:	4b9afff9b19166..
Analysis ID:	830809
MD5:	4b9afff9b19166..
SHA1:	31d41fd14ab0b..
SHA256:	e3fde73a75a23..
Tags:	32 elf mirai renesas
Infos:	

Detection



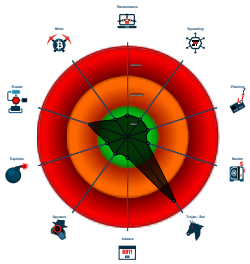
Mirai, Moobot

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:	830809
Start date and time:	2023-03-20 17:52:57 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 50s
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:	8oxYPvmeaT.elf
Original Sample Name:	4b9afff9b19166f6e9ee490e32e0fb15.elf
Detection:	MAL
Classification:	mal92.troj.linELF@0/0@105/0

Warnings

Runtime Messages

Command:	/tmp/8oxYPvmeaT.elf
PID:	6231
Exit Code:	0
Exit Code Info:	

Killed:	False
Standard Output:	^p
Standard Error:	chmod: cannot access "$'\377\177"bin/systemd'$'\177\030\374\377\177"8'$'\374\377\177"d'$'\374\377\177\230\221"@': No such file or directory

Process Tree

- **system is lnxubuntu20**
- 8oxYPvmeaT.elf (PID: 6231, Parent: 6132, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/8oxYPvmeaT.elf
  - 8oxYPvmeaT.elf New Fork (PID: 6233, Parent: 6231)
  - sh (PID: 6233, Parent: 6231, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf bin/systemd && mkdir bin; >bin/systemd && mv /tmp/8oxYPvmeaT.elf bin/systemd; chmod 777 \\xffbin/systemd\\xfc\\xff8\\xfc\\xffd\\xfc\\xff\\x98\\x91@"
    - sh New Fork (PID: 6235, Parent: 6233)
    - rm (PID: 6235, Parent: 6233, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf bin/systemd
    - sh New Fork (PID: 6236, Parent: 6233)
    - mkdir (PID: 6236, Parent: 6233, MD5: 088c9d1df5a28ed16c726eca15964cb7) Arguments: mkdir bin
    - sh New Fork (PID: 6237, Parent: 6233)
    - mv (PID: 6237, Parent: 6233, MD5: 504f0590fa482d4da070a702260e3716) Arguments: mv /tmp/8oxYPvmeaT.elf bin/systemd
    - sh New Fork (PID: 6238, Parent: 6233)
    - chmod (PID: 6238, Parent: 6233, MD5: 739483b900c045ae1374d6f53a86a279) Arguments: chmod 777 \\xffbin/systemd\\xfc\\xff8\\xfc\\xffd\\xfc\\xff\\x98\\x91@
  - 8oxYPvmeaT.elf New Fork (PID: 6239, Parent: 6231)
    - 8oxYPvmeaT.elf New Fork (PID: 6241, Parent: 6239)
    - 8oxYPvmeaT.elf New Fork (PID: 6243, Parent: 6239)
- **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
8oxYPvmeaT.elf	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
8oxYPvmeaT.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
8oxYPvmeaT.elf	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xbf60:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbf74:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbf88:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbf9c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbfb0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbfc4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbfd8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbfec:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc000:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc014:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc028:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc03c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc050:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc064:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc078:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc08c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc0a0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc0b4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc0c8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc0dc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc0f0:$a: 2F 78 33 38 2F 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
6231.1.00007fa678400000.00007fa67840e000.r-x.sdmp	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
6231.1.00007fa678400000.00007fa67840e000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6231.1.00007fa678400000.00007fa67840e000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xbf60:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbf74:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbf88:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbf9c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbfb0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbfc4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbfd8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xbfec:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc000:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc014:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc028:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc03c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc050:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc064:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc078:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc08c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc0a0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc0b4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc0c8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc0dc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc0f0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6241.1.00007fa678400000.00007fa67840e000.r-x.sdmp	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
6241.1.00007fa678400000.00007fa67840e000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Click to see the 4 entries				

Snort Signatures

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.3.233.174

Timestamp:	192.168.2.23197.3.233.174341263721528352222 03/20/23-17:55:45.971245
SID:	2835222
Source Port:	34126
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: 177.177.96.51

Timestamp:	192.168.2.23177.177.96.51451063721528352222 03/20/23-17:55:17.129201
SID:	2835222
Source Port:	45106
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: 41.236.128.171

Timestamp:	192.168.2.2341.236.128.171558003721528352222 03/20/23-17:55:01.346736
SID:	2835222
Source Port:	55800

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: 197.39.127.12

Timestamp:	192.168.2.23197.39.127.1246968372152835222 03/20/23-17:55:10.843812
SID:	2835222
Source Port:	46968
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: 41.236.89.237

Timestamp:	192.168.2.2341.236.89.237560783721528352222 03/20/23-17:55:31.621522
SID:	2835222
Source Port:	56078
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

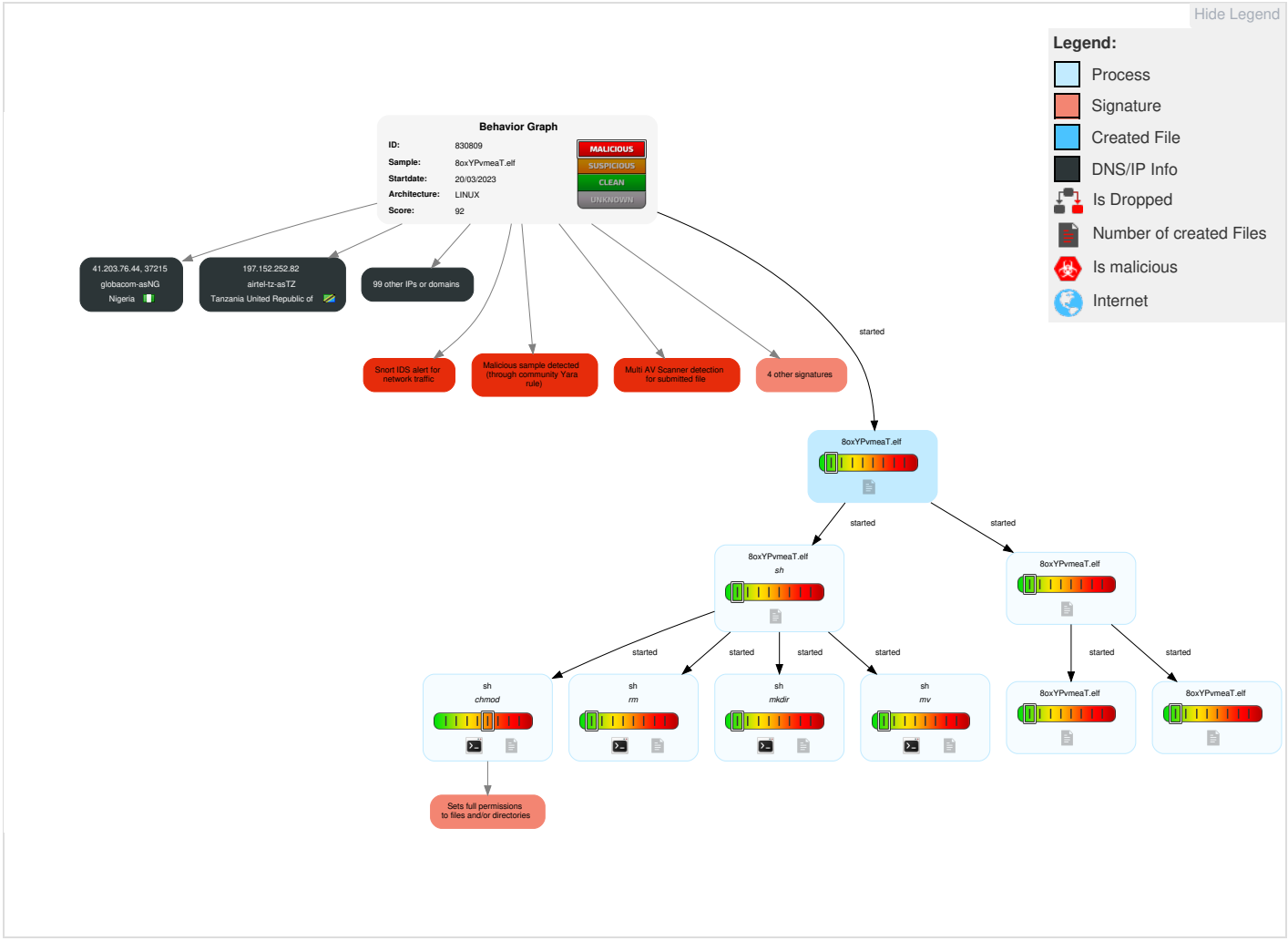
Mitre Att&ck Matrix

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	1 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
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
8oxYPvmeaT.elf	59%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

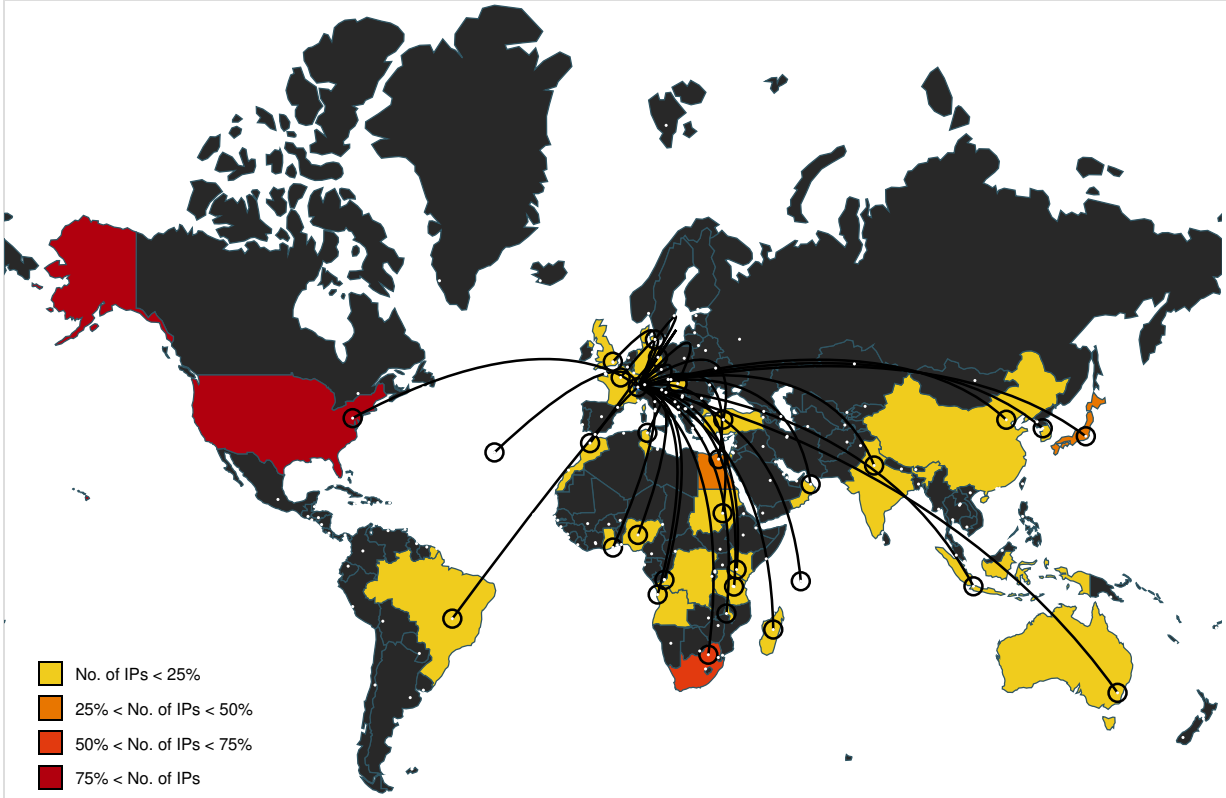
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.194.27.25	unknown	United States		4704	SANNETRakutenMobileIncJP	false
164.191.52.223	unknown	United States		668	DNIC-AS-00668US	false
12.149.18.17	unknown	United States		7018	ATT-INTERNET4US	false
157.112.136.32	unknown	Japan		9605	DOCOMONTTDOCOMOINCJP	false
197.14.36.251	unknown	Tunisia		37693	TUNISIANATN	false
157.161.130.142	unknown	Switzerland		6772	IMPNET-ASCH	false
34.39.73.212	unknown	United States		2686	ATGS-MMD-ASUS	false
197.6.201.4	unknown	Tunisia		5438	ATI-TN	false
41.30.144.223	unknown	South Africa		29975	VODACOM-ZA	false
157.227.30.118	unknown	Australia		4704	SANNETRakutenMobileIncJP	false
183.165.208.173	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
197.211.114.11	unknown	Malawi		37187	SKYBANDMW	false
157.46.135.120	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
43.61.37.90	unknown	Japan		4249	LILLY-ASUS	false
41.71.209.81	unknown	Nigeria		37053	RSAWEB-ASZA	false
197.222.169.246	unknown	Egypt		37069	MOBINILEG	false
157.12.245.236	unknown	Japan		24275	TOTOTOTOLTDJP	false
49.27.74.83	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
195.155.10.105	unknown	Turkey		33548	UNWIRED-NOCUS	false
157.49.72.74	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
197.78.0.1	unknown	South Africa		16637	MTNNS-ASZA	false
39.223.204.218	unknown	Indonesia		23693	TELKOMSEL-ASN-IDPTTelekomunikasiSelularID	false
157.198.38.197	unknown	United States		4704	SANNETRakutenMobileIncJP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.168.205.61	unknown	Switzerland		22192	SSHENETUS	false
19.78.174.40	unknown	United States		3	MIT-GATEWAYSUS	false
157.155.206.238	unknown	Australia		17983	COLESMYER-AS-APColesMyerAU	false
157.37.178.102	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
41.251.165.136	unknown	Morocco		36903	MT-MPLSMA	false
41.248.85.208	unknown	Morocco		36903	MT-MPLSMA	false
197.70.186.100	unknown	South Africa		16637	MTNNS-ASZA	false
82.178.96.254	unknown	Oman		28885	OMANTEL-NAP-ASOmanTelNAPOM	false
41.243.103.130	unknown	Congo The Democratic Republic of The		37684	ANGANI-ASKE	false
4.16.178.189	unknown	United States		3356	LEVEL3US	false
163.160.5.14	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
197.13.254.9	unknown	Tunisia		37504	MeninxTN	false
41.198.255.166	unknown	South Africa		328306	Avanti-ASZA	false
197.180.107.86	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
197.47.156.137	unknown	Egypt		8452	TE-ASTE-ASEG	false
113.20.31.99	unknown	Indonesia		45731	ARDH-AS-IDARDHGLOBALINDONESIAPTID	false
222.30.135.42	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
197.217.148.151	unknown	Angola		11259	ANGOLATELECOMAO	false
197.152.252.82	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
157.208.226.55	unknown	United States		12552	IPO-EUSE	false
52.248.235.152	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
150.34.187.3	unknown	Japan		9991	SHUDO-UHiroshimaShudoUniversityJP	false
197.251.97.136	unknown	Sudan		37197	SUDRENSD	false
157.83.166.153	unknown	United Kingdom		2501	UTNETTheUniversityofTokyoJP	false
197.46.254.206	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.203.76.44	unknown	Nigeria		37148	globacom-asNG	false
99.126.165.25	unknown	United States		7018	ATT-INTERNET4US	false
178.104.135.152	unknown	United Kingdom		12576	EELtdGB	false
157.198.196.23	unknown	United States		4704	SANNETRakutenMobileIncJP	false
197.41.45.220	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.69.11.67	unknown	South Africa		16637	MTNNS-ASZA	false
112.243.208.153	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
197.192.17.254	unknown	Egypt		36992	ETISALAT-MISREG	false
80.179.209.1	unknown	Israel		9116	GOLDENLINES-ASNPartnerCommunicationsMainAutonomousSyste	false
157.148.141.20	unknown	China		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
140.162.250.197	unknown	United States		19	LEIDOS-ASUS	false
17.3.75.80	unknown	United States		714	APPLE-ENGINEERINGUS	false
41.40.71.188	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.149.52.182	unknown	Madagascar		37054	Telecom-MalagasyMG	false
170.41.187.237	unknown	United States		26034	ASN-DELTA-OUTUS	false
157.181.65.107	unknown	Hungary		2012	ELTENETELTENETHU	false
157.35.127.105	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.235.142.169	unknown	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	false
157.245.170.67	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
41.57.232.93	unknown	Ghana		37103	BUSYINTERNETGH	false
157.105.195.243	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
43.57.106.108	unknown	Japan		4249	LILLY-ASUS	false
197.30.41.154	unknown	Tunisia		37492	ORANGE-TN	false
41.134.159.142	unknown	South Africa		10474	OPTINETZA	false
41.183.9.45	unknown	South Africa		37028	FNBCONNECTZA	false
157.181.106.8	unknown	Hungary		2012	ELTENETELTENETHU	false
185.78.207.38	unknown	United Kingdom		8426	CLARANET-ASClaraNETLTDGB	false
157.105.172.38	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
197.100.219.48	unknown	South Africa		3741	ISZA	false
197.65.82.70	unknown	South Africa		16637	MTNNS-ASZA	false
41.5.88.210	unknown	South Africa		29975	VODACOM-ZA	false
197.94.15.28	unknown	South Africa		10474	OPTINETZA	false
197.27.94.143	unknown	Tunisia		37492	ORANGE-TN	false
197.159.106.179	unknown	Kenya		37421	CellulantKE	false
157.90.191.238	unknown	United States		766	REDIRISRedIRISAutonomousSystemES	false
41.26.72.131	unknown	South Africa		29975	VODACOM-ZA	false
44.216.170.224	unknown	United States		14618	AMAZON-AESUS	false
201.35.92.211	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
157.254.215.181	unknown	United States		7768	TECHNICOLORUS	false
197.179.229.85	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
193.60.87.140	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
176.137.7.219	unknown	France		5410	BOUYGTEL-ISPFR	false
197.220.165.29	unknown	Ghana		37341	GLOMOBILEGH	false
197.99.16.216	unknown	South Africa		3741	ISZA	false
41.170.26.88	unknown	South Africa		36937	Neotel-ASZA	false
41.65.28.123	unknown	Egypt		36992	ETISALAT-MISREG	false
197.186.206.34	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
62.242.162.199	unknown	Denmark		3292	TDCTDCASDK	false
27.101.71.172	unknown	Korea Republic of		17841	NCIA-AS-KRNATIONALINFORMATIONRESOURCESSERVICEKR	false
19.216.213.107	unknown	United States		3	MIT-GATEWAYSUS	false
84.235.213.206	unknown	Germany		16360	SATLYNX_GMBHDE	false
63.5.159.46	unknown	United States		701	UUNETUS	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit LSB executable, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.782408732859346
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	8oxYPvmeaT.elf
File size:	58740
MD5:	4b9afff9b19166f6e9ee490e32e0fb15
SHA1:	31d41fd14ab0b236e2802e774c6f601f329d152e
SHA256:	e3fde73a75a23deb0a08b00b153097005ee62bca9969c37755557614efca9f80
SHA512:	46d3b5135db849d7a93c2fe314396c6668c8a5c96a23c2a8b393ed2bac2131c785ec44470e930314a984941554c76d6a72705287ddccc6912c3954263983f589
SSDEEP:	1536:Vaa0brW/Od9hlCR3KajKYXwKEpPDCMC2+WK:Vv0brWGd9X5aGYypPDL+v
TLSH:	A6438D37E96E1E74C04641B074748EB56F23B5C883972EB61AAAC2795483E9CF504FF8
File Content Preview:	.ELF.....*.....@.4.....4. ... (.....@...@.H...H.....A...A.x....%.....Q.td....././"O.n.....#.*@.....#.*@l....o&O.n...l....././.../.a"O.!...n...a.b("...q.

Static ELF Info

ELF header

Class:	
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

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x30	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x4000e0	0xe0	0xbd80	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x40be60	0xbe60	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x40be84	0xbe84	0x1dc4	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x41e000	0xe000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x41e008	0xe008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x41e014	0xe014	0x354	0x0	0x3	WA	0	0	4
.got	PROGBITS	0x41e368	0xe368	0x10	0x4	0x3	WA	0	0	4
.bss	NOBITS	0x41e378	0xe378	0x2214	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xe378	0x43	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0xdc48	0xdc48	6.9026	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xe000	0x41e000	0x41e000	0x378	0x258c	2.7313	0x6	RW	0x10000		.ctors .dtors .data .got .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

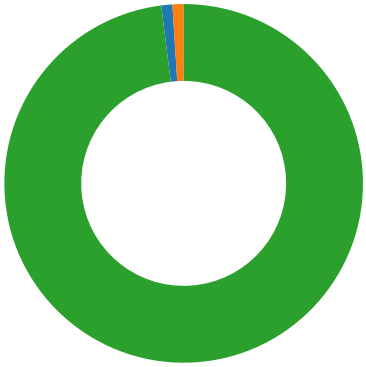
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.23197.3.233.174343126372152835222 03/20/23-17:55:45.971245	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	34126	37215	192.168.2.23	197.3.233.174
192.168.2.23177.177.96.514510637215283522203/20/23-17:55:17.129201	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45106	37215	192.168.2.23	177.177.96.51
192.168.2.2341.236.128.171558003721528352222 03/20/23-17:55:01.346736	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55800	37215	192.168.2.23	41.236.128.171
192.168.2.23197.39.127.124696837215283522203/20/23-17:55:10.843812	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46968	37215	192.168.2.23	197.39.127.12
192.168.2.2341.236.89.237560783721528352222 03/20/23-17:55:31.621522	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	56078	37215	192.168.2.23	41.236.89.237

Network Port Distribution

Total Packets: 100

- 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 17:53:48.765808105 CET	192.168.2.23	8.8.8.8	0x6bd4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:48.786621094 CET	192.168.2.23	8.8.8.8	0x6bd4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:48.805180073 CET	192.168.2.23	8.8.8.8	0x6bd4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:48.823740005 CET	192.168.2.23	8.8.8.8	0x6bd4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:48.841442108 CET	192.168.2.23	8.8.8.8	0x6bd4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:52.861957073 CET	192.168.2.23	8.8.8.8	0xd7fe	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:52.882245064 CET	192.168.2.23	8.8.8.8	0xd7fe	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:52.902170897 CET	192.168.2.23	8.8.8.8	0xd7fe	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:52.922446012 CET	192.168.2.23	8.8.8.8	0xd7fe	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:52.940380096 CET	192.168.2.23	8.8.8.8	0xd7fe	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:00.960326910 CET	192.168.2.23	8.8.8.8	0x29a5	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:00.980664968 CET	192.168.2.23	8.8.8.8	0x29a5	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:00.999131918 CET	192.168.2.23	8.8.8.8	0x29a5	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:01.019154072 CET	192.168.2.23	8.8.8.8	0x29a5	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:01.036737919 CET	192.168.2.23	8.8.8.8	0x29a5	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:08.057385921 CET	192.168.2.23	8.8.8.8	0xe94	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:08.077071905 CET	192.168.2.23	8.8.8.8	0xe94	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:08.097317934 CET	192.168.2.23	8.8.8.8	0xe94	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:08.117475986 CET	192.168.2.23	8.8.8.8	0xe94	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:08.137413025 CET	192.168.2.23	8.8.8.8	0xe94	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:13.159239054 CET	192.168.2.23	8.8.8.8	0xe218	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:13.179145098 CET	192.168.2.23	8.8.8.8	0xe218	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:13.199134111 CET	192.168.2.23	8.8.8.8	0xe218	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 17:54:13.217591047 CET	192.168.2.23	8.8.8.8	0xe218	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:13.236219883 CET	192.168.2.23	8.8.8.8	0xe218	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:16.254884958 CET	192.168.2.23	8.8.8.8	0xaba2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:16.273684025 CET	192.168.2.23	8.8.8.8	0xaba2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:16.294823885 CET	192.168.2.23	8.8.8.8	0xaba2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:16.313052893 CET	192.168.2.23	8.8.8.8	0xaba2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:16.337908983 CET	192.168.2.23	8.8.8.8	0xaba2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:18.359266996 CET	192.168.2.23	8.8.8.8	0x4b33	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:18.379901886 CET	192.168.2.23	8.8.8.8	0x4b33	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:18.400691986 CET	192.168.2.23	8.8.8.8	0x4b33	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:18.418754101 CET	192.168.2.23	8.8.8.8	0x4b33	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:18.439063072 CET	192.168.2.23	8.8.8.8	0x4b33	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:27.458336115 CET	192.168.2.23	8.8.8.8	0xab48	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:27.476732969 CET	192.168.2.23	8.8.8.8	0xab48	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:27.495090961 CET	192.168.2.23	8.8.8.8	0xab48	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:27.513151884 CET	192.168.2.23	8.8.8.8	0xab48	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:27.533427954 CET	192.168.2.23	8.8.8.8	0xab48	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:28.551873922 CET	192.168.2.23	8.8.8.8	0xe516	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:28.570219040 CET	192.168.2.23	8.8.8.8	0xe516	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:28.588200092 CET	192.168.2.23	8.8.8.8	0xe516	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:28.607949018 CET	192.168.2.23	8.8.8.8	0xe516	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:28.626174927 CET	192.168.2.23	8.8.8.8	0xe516	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:31.644567013 CET	192.168.2.23	8.8.8.8	0x6432	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:31.664761066 CET	192.168.2.23	8.8.8.8	0x6432	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:31.684782982 CET	192.168.2.23	8.8.8.8	0x6432	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:31.703013897 CET	192.168.2.23	8.8.8.8	0x6432	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:31.723485947 CET	192.168.2.23	8.8.8.8	0x6432	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:40.743345022 CET	192.168.2.23	8.8.8.8	0xe134	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:40.763360023 CET	192.168.2.23	8.8.8.8	0xe134	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:40.783502102 CET	192.168.2.23	8.8.8.8	0xe134	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:40.803735018 CET	192.168.2.23	8.8.8.8	0xe134	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:40.821953058 CET	192.168.2.23	8.8.8.8	0xe134	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:49.842055082 CET	192.168.2.23	8.8.8.8	0xcc36	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:49.862176895 CET	192.168.2.23	8.8.8.8	0xcc36	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:49.882498026 CET	192.168.2.23	8.8.8.8	0xcc36	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 17:54:49.902760983 CET	192.168.2.23	8.8.8.8	0xcc36	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:49.922875881 CET	192.168.2.23	8.8.8.8	0xcc36	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:51.943012953 CET	192.168.2.23	8.8.8.8	0xf168	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:51.962711096 CET	192.168.2.23	8.8.8.8	0xf168	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:51.980896950 CET	192.168.2.23	8.8.8.8	0xf168	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:51.999319077 CET	192.168.2.23	8.8.8.8	0xf168	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:52.016799927 CET	192.168.2.23	8.8.8.8	0xf168	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:00.034152985 CET	192.168.2.23	8.8.8.8	0x2cf6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:00.054399967 CET	192.168.2.23	8.8.8.8	0x2cf6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:00.074590921 CET	192.168.2.23	8.8.8.8	0x2cf6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:00.094912052 CET	192.168.2.23	8.8.8.8	0x2cf6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:00.115159035 CET	192.168.2.23	8.8.8.8	0x2cf6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:08.135184050 CET	192.168.2.23	8.8.8.8	0xaaf	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:08.153709888 CET	192.168.2.23	8.8.8.8	0xaaf	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:08.173207045 CET	192.168.2.23	8.8.8.8	0xaaf	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:08.191382885 CET	192.168.2.23	8.8.8.8	0xaaf	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:08.209104061 CET	192.168.2.23	8.8.8.8	0xaaf	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:14.229226112 CET	192.168.2.23	8.8.8.8	0x45cc	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:14.247893095 CET	192.168.2.23	8.8.8.8	0x45cc	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:14.266504049 CET	192.168.2.23	8.8.8.8	0x45cc	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:14.284995079 CET	192.168.2.23	8.8.8.8	0x45cc	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:14.305706024 CET	192.168.2.23	8.8.8.8	0x45cc	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:24.323476076 CET	192.168.2.23	8.8.8.8	0x3cf	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:24.345139027 CET	192.168.2.23	8.8.8.8	0x3cf	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:24.366708994 CET	192.168.2.23	8.8.8.8	0x3cf	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:24.384979010 CET	192.168.2.23	8.8.8.8	0x3cf	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:24.405069113 CET	192.168.2.23	8.8.8.8	0x3cf	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:30.423162937 CET	192.168.2.23	8.8.8.8	0x92f4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:30.443373919 CET	192.168.2.23	8.8.8.8	0x92f4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:30.463242054 CET	192.168.2.23	8.8.8.8	0x92f4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:30.483611107 CET	192.168.2.23	8.8.8.8	0x92f4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:30.501255035 CET	192.168.2.23	8.8.8.8	0x92f4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:36.519351006 CET	192.168.2.23	8.8.8.8	0xab28	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:36.539652109 CET	192.168.2.23	8.8.8.8	0xab28	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:36.559883118 CET	192.168.2.23	8.8.8.8	0xab28	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 17:55:36.577136993 CET	192.168.2.23	8.8.8.8	0xab28	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:36.595082045 CET	192.168.2.23	8.8.8.8	0xab28	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:43.614908934 CET	192.168.2.23	8.8.8.8	0x570a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:43.633196115 CET	192.168.2.23	8.8.8.8	0x570a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:43.651557922 CET	192.168.2.23	8.8.8.8	0x570a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:43.671310902 CET	192.168.2.23	8.8.8.8	0x570a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:43.689054966 CET	192.168.2.23	8.8.8.8	0x570a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:48.706892014 CET	192.168.2.23	8.8.8.8	0x6102	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:48.727046967 CET	192.168.2.23	8.8.8.8	0x6102	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:48.745249987 CET	192.168.2.23	8.8.8.8	0x6102	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:48.763377905 CET	192.168.2.23	8.8.8.8	0x6102	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:48.781891108 CET	192.168.2.23	8.8.8.8	0x6102	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 17:53:48.785645008 CET	8.8.8.8	192.168.2.23	0x6bd4	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:48.804846048 CET	8.8.8.8	192.168.2.23	0x6bd4	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:48.823394060 CET	8.8.8.8	192.168.2.23	0x6bd4	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:48.841208935 CET	8.8.8.8	192.168.2.23	0x6bd4	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:48.859812021 CET	8.8.8.8	192.168.2.23	0x6bd4	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:52.881905079 CET	8.8.8.8	192.168.2.23	0xd7fe	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:52.901875973 CET	8.8.8.8	192.168.2.23	0xd7fe	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:52.922226906 CET	8.8.8.8	192.168.2.23	0xd7fe	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:52.940161943 CET	8.8.8.8	192.168.2.23	0xd7fe	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:53:52.960112095 CET	8.8.8.8	192.168.2.23	0xd7fe	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:00.980245113 CET	8.8.8.8	192.168.2.23	0x29a5	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:00.998816013 CET	8.8.8.8	192.168.2.23	0x29a5	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:01.018902063 CET	8.8.8.8	192.168.2.23	0x29a5	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:01.036487103 CET	8.8.8.8	192.168.2.23	0x29a5	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 17:54:01.057027102 CET	8.8.8.8	192.168.2.23	0x29a5	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:08.076638937 CET	8.8.8.8	192.168.2.23	0xe94	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:08.096879959 CET	8.8.8.8	192.168.2.23	0xe94	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:08.117151022 CET	8.8.8.8	192.168.2.23	0xe94	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:08.137160063 CET	8.8.8.8	192.168.2.23	0xe94	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:08.158864975 CET	8.8.8.8	192.168.2.23	0xe94	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:13.178900003 CET	8.8.8.8	192.168.2.23	0xe218	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:13.198868036 CET	8.8.8.8	192.168.2.23	0xe218	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:13.217312098 CET	8.8.8.8	192.168.2.23	0xe218	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:13.235939980 CET	8.8.8.8	192.168.2.23	0xe218	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:13.254405975 CET	8.8.8.8	192.168.2.23	0xe218	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:16.273155928 CET	8.8.8.8	192.168.2.23	0xaba2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:16.294462919 CET	8.8.8.8	192.168.2.23	0xaba2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:16.312766075 CET	8.8.8.8	192.168.2.23	0xaba2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:16.337605953 CET	8.8.8.8	192.168.2.23	0xaba2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:16.358800888 CET	8.8.8.8	192.168.2.23	0xaba2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:18.379337072 CET	8.8.8.8	192.168.2.23	0x4b33	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:18.400316954 CET	8.8.8.8	192.168.2.23	0x4b33	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:18.418440104 CET	8.8.8.8	192.168.2.23	0x4b33	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:18.438781023 CET	8.8.8.8	192.168.2.23	0x4b33	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:18.458141088 CET	8.8.8.8	192.168.2.23	0x4b33	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:27.476335049 CET	8.8.8.8	192.168.2.23	0xab48	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:27.494751930 CET	8.8.8.8	192.168.2.23	0xab48	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:27.512846947 CET	8.8.8.8	192.168.2.23	0xab48	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:27.533068895 CET	8.8.8.8	192.168.2.23	0xab48	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 17:54:27.551265955 CET	8.8.8.8	192.168.2.23	0xab48	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:28.569852114 CET	8.8.8.8	192.168.2.23	0xe516	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:28.587887049 CET	8.8.8.8	192.168.2.23	0xe516	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:28.607677937 CET	8.8.8.8	192.168.2.23	0xe516	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:28.625890970 CET	8.8.8.8	192.168.2.23	0xe516	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:28.644021034 CET	8.8.8.8	192.168.2.23	0xe516	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:31.664563894 CET	8.8.8.8	192.168.2.23	0x6432	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:31.684451103 CET	8.8.8.8	192.168.2.23	0x6432	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:31.702680111 CET	8.8.8.8	192.168.2.23	0x6432	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:31.723128080 CET	8.8.8.8	192.168.2.23	0x6432	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:31.743057966 CET	8.8.8.8	192.168.2.23	0x6432	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:40.763046026 CET	8.8.8.8	192.168.2.23	0xe134	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:40.783210993 CET	8.8.8.8	192.168.2.23	0xe134	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:40.803396940 CET	8.8.8.8	192.168.2.23	0xe134	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:40.821602106 CET	8.8.8.8	192.168.2.23	0xe134	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:40.841882944 CET	8.8.8.8	192.168.2.23	0xe134	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:49.861897945 CET	8.8.8.8	192.168.2.23	0xcc36	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:49.882181883 CET	8.8.8.8	192.168.2.23	0xcc36	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:49.902401924 CET	8.8.8.8	192.168.2.23	0xcc36	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:49.922569036 CET	8.8.8.8	192.168.2.23	0xcc36	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:49.942471027 CET	8.8.8.8	192.168.2.23	0xcc36	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:51.962444067 CET	8.8.8.8	192.168.2.23	0xf168	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:51.980587959 CET	8.8.8.8	192.168.2.23	0xf168	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:51.999034882 CET	8.8.8.8	192.168.2.23	0xf168	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:54:52.016596079 CET	8.8.8.8	192.168.2.23	0xf168	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 17:54:52.033987045 CET	8.8.8.8	192.168.2.23	0xf168	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:00.054052114 CET	8.8.8.8	192.168.2.23	0x2cf6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:00.074170113 CET	8.8.8.8	192.168.2.23	0x2cf6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:00.094568968 CET	8.8.8.8	192.168.2.23	0x2cf6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:00.114831924 CET	8.8.8.8	192.168.2.23	0x2cf6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:00.134881020 CET	8.8.8.8	192.168.2.23	0x2cf6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:08.153223991 CET	8.8.8.8	192.168.2.23	0xaaf	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:08.172925949 CET	8.8.8.8	192.168.2.23	0xaaf	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:08.191107035 CET	8.8.8.8	192.168.2.23	0xaaf	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:08.208852053 CET	8.8.8.8	192.168.2.23	0xaaf	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:08.228847980 CET	8.8.8.8	192.168.2.23	0xaaf	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:14.247512102 CET	8.8.8.8	192.168.2.23	0x45cc	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:14.266140938 CET	8.8.8.8	192.168.2.23	0x45cc	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:14.284642935 CET	8.8.8.8	192.168.2.23	0x45cc	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:14.305341959 CET	8.8.8.8	192.168.2.23	0x45cc	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:14.323462009 CET	8.8.8.8	192.168.2.23	0x45cc	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:24.344758987 CET	8.8.8.8	192.168.2.23	0x3cf	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:24.366400003 CET	8.8.8.8	192.168.2.23	0x3cf	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:24.384679079 CET	8.8.8.8	192.168.2.23	0x3cf	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:24.404712915 CET	8.8.8.8	192.168.2.23	0x3cf	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:24.422852039 CET	8.8.8.8	192.168.2.23	0x3cf	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:30.443020105 CET	8.8.8.8	192.168.2.23	0x92f4	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:30.462937117 CET	8.8.8.8	192.168.2.23	0x92f4	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:30.483295918 CET	8.8.8.8	192.168.2.23	0x92f4	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:30.500965118 CET	8.8.8.8	192.168.2.23	0x92f4	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 17:55:30.518930912 CET	8.8.8.8	192.168.2.23	0x92f4	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:36.539282084 CET	8.8.8.8	192.168.2.23	0xab28	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:36.559565067 CET	8.8.8.8	192.168.2.23	0xab28	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:36.576880932 CET	8.8.8.8	192.168.2.23	0xab28	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:36.594791889 CET	8.8.8.8	192.168.2.23	0xab28	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:36.614631891 CET	8.8.8.8	192.168.2.23	0xab28	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:43.632838964 CET	8.8.8.8	192.168.2.23	0x570a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:43.651206970 CET	8.8.8.8	192.168.2.23	0x570a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:43.670981884 CET	8.8.8.8	192.168.2.23	0x570a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:43.688723087 CET	8.8.8.8	192.168.2.23	0x570a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:43.706509113 CET	8.8.8.8	192.168.2.23	0x570a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:48.726708889 CET	8.8.8.8	192.168.2.23	0x6102	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:48.744993925 CET	8.8.8.8	192.168.2.23	0x6102	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:48.763087988 CET	8.8.8.8	192.168.2.23	0x6102	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:48.781603098 CET	8.8.8.8	192.168.2.23	0x6102	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:55:48.799269915 CET	8.8.8.8	192.168.2.23	0x6102	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: 8oxYPvmeaT.elf PID: **6231**, Parent PID: **6132**

General

Start time:	17:53:47
Start date:	20/03/2023
Path:	/tmp/8oxYPvmeaT.elf
Arguments:	/tmp/8oxYPvmeaT.elf
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities

File Read

Analysis Process: 8oxYPvmeaT.elf PID: **6233**, Parent PID: **6231**

General

Start time:	17:53:47
Start date:	20/03/2023
Path:	/tmp/8oxYPvmeaT.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: sh PID: **6233**, Parent PID: **6231**

General

Start time:	17:53:47
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	sh -c "rm -rf bin/systemd && mkdir bin; >bin/systemd && mv /tmp/8oxYPvmeaT.elf bin/systemd; chmod 777 \\xffbin/systemd\\xfc\\xff8\\xfc\\xffd\\xfc\\xff\\x98\\x91@"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **6235**, Parent PID: **6233**

General

Start time:	17:53:47
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **6235**, Parent PID: **6233**

General

Start time:	17:53:47
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: **6236**, Parent PID: **6233**

General

Start time:	17:53:47
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mkdir PID: **6236**, Parent PID: **6233**

General

Start time:	17:53:47
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: **6237**, Parent PID: **6233**

General

Start time:	17:53:47
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mv PID: **6237**, Parent PID: **6233**

General

Start time:	17:53:47
Start date:	20/03/2023
Path:	/usr/bin/mv
Arguments:	mv /tmp/8oxYPvmeaT.elf bin/systemd
File size:	149888 bytes
MD5 hash:	504f0590fa482d4da070a702260e3716

File Activities

File Read

File Moved

Analysis Process: sh PID: **6238**, Parent PID: **6233**

General

Start time:	17:53:47
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: chmod PID: **6238**, Parent PID: **6233**

General

Start time:	17:53:47
Start date:	20/03/2023
Path:	/usr/bin/chmod
Arguments:	chmod 777 \\xffbin/systemd\\xfc\\xff8\\xfc\\xffd\\xfc\\xff\\x98\\x91@
File size:	63864 bytes
MD5 hash:	739483b900c045ae1374d6f53a86a279

File Activities

File Read

Analysis Process: 8oxYPvmeaT.elf PID: **6239**, Parent PID: **6231**

General

Start time:	17:53:48

Start date:	20/03/2023
Path:	/tmp/8oxYPvmeaT.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: 8oxYPvmeaT.elf PID: **6241**, Parent PID: **6239**

General

Start time:	17:53:48
Start date:	20/03/2023
Path:	/tmp/8oxYPvmeaT.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

Analysis Process: 8oxYPvmeaT.elf PID: **6243**, Parent PID: **6239**

General

Start time:	17:53:48
Start date:	20/03/2023
Path:	/tmp/8oxYPvmeaT.elf
Arguments:	n/a
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9