ID: 830828
Sample Name: 6lqMB7o2Ts.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 18:13:53
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

Linux Analysis Report

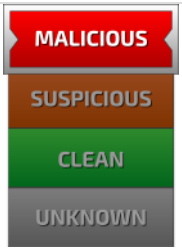
6lqMB7o2Ts.elf

Overview

General Information

Sample Name:	6lqMB7o2Ts.elf
Original Sample Name:	1f34c5bcd411c..
Analysis ID:	830828
MD5:	1f34c5bcd411c..
SHA1:	39a1f8fff95e7c...
SHA256:	a9b25052579b...
Tags:	32 elf mips mirai
Infos:	

Detection



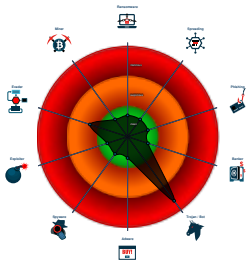
Mirai, Moobot

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.

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830828
Start date and time:	2023-03-20 18:13:53 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 52s
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:	6lqMB7o2Ts.elf
Original Sample Name:	1f34c5bcd411c95d5bdff565afd27afd.elf
Detection:	MAL
Classification:	mal92.troj.linELF@0/0@105/0

Warnings

Runtime Messages

Command:	/tmp/6lqMB7o2Ts.elf
PID:	6230
Exit Code:	0

Exit Code Info:	
Killed:	False
Standard Output:	^p
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- 6lqMB7o2Ts.elf (PID: 6230, Parent: 6125, MD5: 0d6f61f82cf2f781c6eb0661071d42d9) Arguments: /tmp/6lqMB7o2Ts.elf
  - 6lqMB7o2Ts.elf New Fork (PID: 6232, Parent: 6230)
  - sh (PID: 6232, Parent: 6230, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "rm -rf bin/systemd && mkdir bin; >bin/systemd && mv /tmp/6lqMB7o2Ts.elf bin/systemd; chmod 777 bin/systemd"
    - sh New Fork (PID: 6234, Parent: 6232)
    - rm (PID: 6234, Parent: 6232, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -rf bin/systemd
    - sh New Fork (PID: 6235, Parent: 6232)
    - mkdir (PID: 6235, Parent: 6232, MD5: 088c9d1df5a28ed16c726eca15964cb7) Arguments: mkdir bin
    - sh New Fork (PID: 6236, Parent: 6232)
    - mv (PID: 6236, Parent: 6232, MD5: 504f0590fa482d4da070a702260e3716) Arguments: mv /tmp/6lqMB7o2Ts.elf bin/systemd
    - sh New Fork (PID: 6237, Parent: 6232)
    - chmod (PID: 6237, Parent: 6232, MD5: 739483b900c045ae1374d6f53a86a279) Arguments: chmod 777 bin/systemd
  - 6lqMB7o2Ts.elf New Fork (PID: 6238, Parent: 6230)
    - 6lqMB7o2Ts.elf New Fork (PID: 6240, Parent: 6238)
    - 6lqMB7o2Ts.elf New Fork (PID: 6241, Parent: 6238)
- **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
6lqMB7o2Ts.elf	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
6lqMB7o2Ts.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6lqMB7o2Ts.elf	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x11d6c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11d80:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11d94:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11da8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11dbc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11dd0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11de4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11df8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e0c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e20:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e34:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e48:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e5c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e70:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e84:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e98:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11eac:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11ec0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11ed4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11ee8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11efc:$a: 2F 78 33 38 2F 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
6230.1.00007fd3fc400000.00007fd3fc414000.r-x.sdmp	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
6230.1.00007fd3fc400000.00007fd3fc414000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6230.1.00007fd3fc400000.00007fd3fc414000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x11d6c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11d80:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11d94:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11da8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11dbc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11dd0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11de4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11df8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e0c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e20:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e34:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e48:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e5c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e70:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e84:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11e98:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11eac:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11ec0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11ed4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11ee8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x11efc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6240.1.00007fd3fc400000.00007fd3fc414000.r-x.sdmp	JoeSecurity_Moobot	Yara detected Moobot	Joe Security	
6240.1.00007fd3fc400000.00007fd3fc414000.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: 191.61.26.79

Timestamp:	192.168.2.23191.61.26.7952002372152835222 03/20/23-18:15:41.479492
SID:	2835222
Source Port:	52002
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: 41.239.25.98

Timestamp:	192.168.2.2341.239.25.9858734372152835222 03/20/23-18:16:18.194286
SID:	2835222
Source Port:	58734
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: 77.136.237.160

Timestamp:	192.168.2.2377.136.237.16045516372152835222 03/20/23-18:14:44.802279
SID:	2835222
Source Port:	45516
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: 103.54.44.133

Timestamp:	192.168.2.23103.54.44.133503063721528352222 03/20/23-18:15:01.586540
SID:	2835222
Source Port:	50306
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: 104.128.127.228

Timestamp:	192.168.2.23104.128.127.228465443721528352222 03/20/23-18:15:22.996810
SID:	2835222
Source Port:	46544
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: 41.238.196.116

Timestamp:	192.168.2.2341.238.196.1164107637215283522 03/20/23-18:14:59.321194
SID:	2835222
Source Port:	41076
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: 34.120.131.8

Timestamp:	192.168.2.2334.120.131.845438372152835222 03/20/23-18:15:29.072769
SID:	2835222
Source Port:	45438
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: 94.187.108.185

Timestamp:	192.168.2.2394.187.108.18555228372152835222 03/20/23-18:15:36.209617
SID:	2835222
Source Port:	55228
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

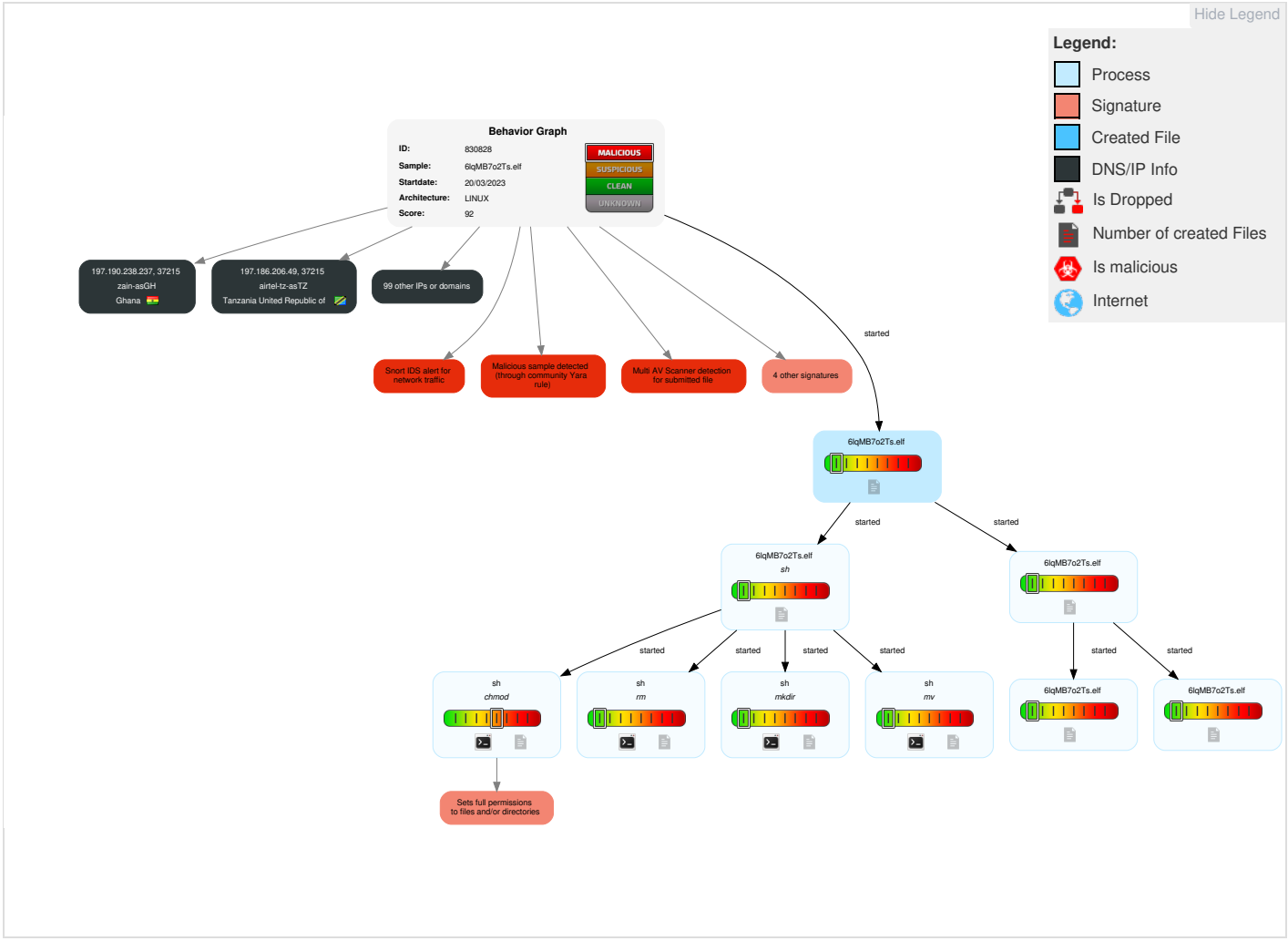
Mitre Att&ck Matrix

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
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
6lqMB7o2Ts.elf	59%	ReversingLabs	Linux.Trojan.Mirai	
6lqMB7o2Ts.elf	61%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

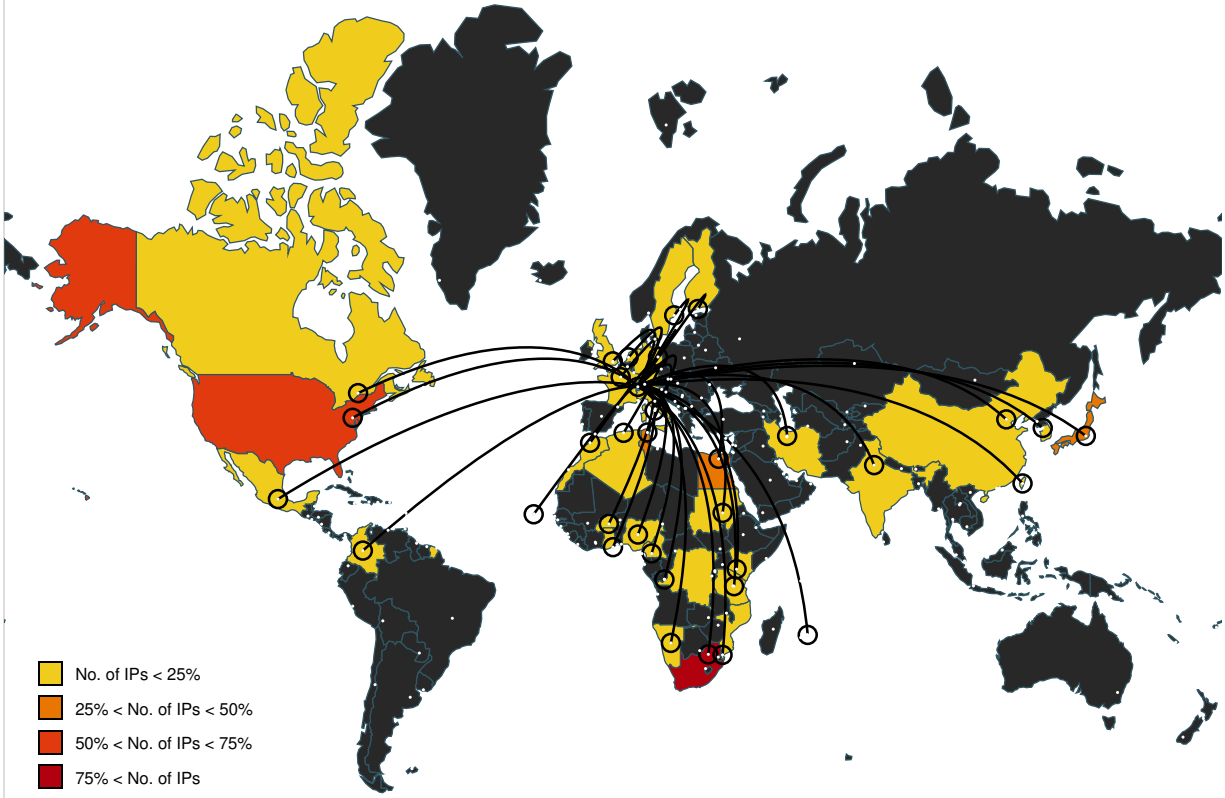
Domains and IPs

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
87.213.190.11	unknown	Netherlands		13127	VERSATELASfortheTrans-EuropeanTele2IPTransportbackbo	false
41.36.131.167	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.58.66.159	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.220.190.33	unknown	Ghana		37341	GLOMOBILEGH	false
197.86.54.125	unknown	South Africa		10474	OPTINETZA	false
157.203.49.95	unknown	United Kingdom		21369	SEMA-UK-ASGB	false
39.79.149.79	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
157.48.46.102	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
75.125.242.147	unknown	United States		36351	SOFTLAYERUS	false
197.13.10.216	unknown	Tunisia		37504	MeninxTN	false
39.117.85.134	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
157.202.188.31	unknown	United States		1759	TSF-IP-CORETeliaFinlandOyjEU	false
157.40.6.77	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
86.55.14.254	unknown	Iran (ISLAMIC Republic Of)		197207	MCCI-ASIR	false
157.129.143.141	unknown	Finland		41701	CAP-FIN-ASFI	false
41.16.118.241	unknown	South Africa		36994	Vodacom-VBZA	false
157.90.119.127	unknown	United States		766	REDIRISRedIRISAutonomousSystemES	false
197.233.216.89	unknown	Namibia		36999	TELECOM-NAMIBIANA	false
41.205.82.241	unknown	Cameroon		36905	Creolink-ASNCM	false
197.210.52.180	unknown	Nigeria		29465	VCG-ASNG	false
197.31.140.190	unknown	Tunisia		37492	ORANGE-TN	false
41.242.195.81	unknown	South Africa		37105	NEOLOGY-ASZA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.220.60.244	unknown	unknown		36900	UNASSIGNED	false
197.240.218.219	unknown	unknown		37705	TOPNETTN	false
177.234.21.222	unknown	Mexico		13591	MexicoReddeTelecomunicacionesSdeRLdeCVMX	false
157.245.2.251	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
41.172.244.43	unknown	South Africa		36937	Neotel-ASZA	false
197.65.94.91	unknown	South Africa		16637	MTNNS-ASZA	false
41.190.129.206	unknown	Mauritius		36997	INFOCOM-UG	false
197.176.2.41	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
157.180.38.236	unknown	Sweden		22192	SSHENETUS	false
41.116.198.169	unknown	South Africa		16637	MTNNS-ASZA	false
157.29.116.114	unknown	Italy		8968	BT-ITALIAIT	false
197.186.206.49	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
41.177.165.227	unknown	South Africa		36874	CybersmartZA	false
197.31.148.1	unknown	Tunisia		37492	ORANGE-TN	false
41.243.103.146	unknown	Congo The Democratic Republic of The		37684	ANGANI-ASKE	false
41.182.10.68	unknown	Namibia		36996	TELECOM-NAMIBIANA	false
41.95.189.153	unknown	Sudan		36998	SDN-MOBITELSD	false
157.77.107.252	unknown	Japan		4678	FINECanonITSolutionsIncJP	false
157.250.6.188	unknown	United States		32934	FACEBOOKUS	false
197.16.224.23	unknown	Tunisia		37693	TUNISIANATN	false
166.248.166.103	unknown	United States		22394	CELLCOUS	false
67.231.248.15	unknown	United States		40244	TURNKEY-INTERNETUS	false
157.74.15.86	unknown	Japan		131932	JEIS-NETJREastInformationSystemsCompanyJP	false
99.255.49.46	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
41.145.58.85	unknown	South Africa		5713	SAIX-NETZA	false
41.133.99.106	unknown	South Africa		10474	OPTINETZA	false
181.155.228.131	unknown	Colombia		26611	COMCELSACO	false
157.47.196.245	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
148.230.177.14	unknown	Mexico		3549	LVLT-3549US	false
197.12.205.119	unknown	Tunisia		37703	ATLAXTN	false
157.1.148.117	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
197.190.238.237	unknown	Ghana		37140	zain-asGH	false
41.216.159.4	unknown	Burkina Faso		37073	IPP-burkina-asBF	false
41.120.89.167	unknown	South Africa		16637	MTNNS-ASZA	false
197.9.0.253	unknown	Tunisia		5438	ATI-TN	false
24.132.41.40	unknown	Netherlands		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
157.94.173.77	unknown	Finland		51164	CYBERCOM-FICybercomFinlandOyFI	false
157.172.225.252	unknown	France		22192	SSHENETUS	false
197.89.97.51	unknown	South Africa		10474	OPTINETZA	false
41.88.141.232	unknown	Egypt		33771	SAFARICOM-LIMITEDKE	false
197.72.190.161	unknown	South Africa		16637	MTNNS-ASZA	false
197.158.15.171	unknown	Mozambique		30619	TDM-ASMZ	false
169.186.225.238	unknown	United States		37611	AfrihostZA	false
157.108.225.9	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
41.143.116.57	unknown	Morocco		36903	MT-MPLSMA	false
41.69.75.113	unknown	Egypt		24835	RAYA-ASEG	false
197.219.202.95	unknown	Mozambique		37342	MOVITELMZ	false
111.71.132.78	unknown	Taiwan; Republic of China (ROC)		17421	EMOME-NETMobileBusinessGroupTW	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
98.30.11.116	unknown	United States		10796	TWC-10796-MIDWESTUS	false
126.32.30.4	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
213.95.251.204	unknown	Germany		12337	NORIS-NETWORKITServiceProviderlocatedinNuernbergGerm	false
95.199.194.164	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
41.179.133.53	unknown	Egypt		24863	LINKdotNET-ASEG	false
197.37.36.139	unknown	Egypt		8452	TE-ASTE-ASEG	false
197.82.246.62	unknown	South Africa		10474	OPTINETZA	false
157.21.225.99	unknown	United States		53446	EVMSUS	false
197.66.218.65	unknown	South Africa		16637	MTNNS-ASZA	false
41.18.169.222	unknown	South Africa		29975	VODACOM-ZA	false
157.232.147.215	unknown	United States		4704	SANNETRakutenMobileIncJP	false
197.204.213.172	unknown	Algeria		36947	ALGTEL-ASDZ	false
197.4.89.169	unknown	Tunisia		5438	ATI-TN	false
64.157.89.206	unknown	United States		3064	AFFINITY-FTLUS	false
41.176.43.255	unknown	Egypt		36992	ETISALAT-MISREG	false
41.182.22.210	unknown	Namibia		36996	TELECOM-NAMIBIANA	false
77.6.87.85	unknown	Germany		6805	TDDE-ASN1DE	false
77.74.199.254	unknown	United Kingdom		42831	UKSERVERS-ASUKDedicatedServersHostingandCo-Location	false
163.208.44.35	unknown	Japan		7502	IP-KYOTOAdvancedSoftwareTechnologyManagementResearch	false
157.37.30.219	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
41.77.59.125	unknown	South Africa		36985	GMSZA	false
41.14.238.56	unknown	South Africa		29975	VODACOM-ZA	false
138.176.152.51	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
41.74.140.210	unknown	Cape Verde		37517	CV-MultimediaCV	false
197.73.232.43	unknown	South Africa		16637	MTNNS-ASZA	false
157.148.116.61	unknown	China		136958	UNICOM-GUANGZHOU-IDCChinaUnicomGuangdongIPnetworkCN	false
41.125.107.227	unknown	South Africa		16637	MTNNS-ASZA	false
157.230.191.4	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
197.185.70.90	unknown	South Africa		37105	NEOLOGY-ASZA	false
157.204.30.224	unknown	United States		54216	GORE-NETWORKUS	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, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.52397672760205
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	6lqMB7o2Ts.elf
File size:	84780
MD5:	1f34c5bcd411c95d5bdff565afd27afd
SHA1:	39a1f8fff95e7c4d693d0d3fbc2d49749f3ba395
SHA256:	a9b25052579b7f41a1f985ed6d95f0eef2f00e8ad0e9a16dafad5ea38cb1b128
SHA512:	e1a92b793af4d9bdba266b6e7c54098a86c87e440d93cb26953a953272d3e783b7c365993d42f346e72dc912971fde5c3311aa38ef17d4d3e111e28579c8822f
SSDEEP:	1536:iVLyu95KRKKkj752dCexuV/8UZlDwfkJ4MYfWa:iVLyMgWFezxu5VD1eX
TLSH:	1683D606BB510FF7DC6FCD370AE91702348C594A22A97B367634D828F65B24B59E3CA4
File Content Preview:	.ELF.....`.@.4....H.....4. ...(.....@...@..;..;.....@...@E..@E.....+.....Q.td.....<\..'!.....'.....<8..'!... .....9'.. .....<...'!.....9

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
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x11b10	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x411c30	0x11c30	0x5c	0x0	0x6	AX	0	0	4

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.rodata	PROGBITS	0x411c90	0x11c90	0x1f00	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x454000	0x14000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x454008	0x14008	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x454014	0x14014	0x44	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x454060	0x14060	0x3a0	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x454400	0x14400	0x498	0x4	0x10000003	WAp	0	0	16
.sbss	NOBITS	0x454898	0x14898	0x1c	0x0	0x10000003	WAp	0	0	4
.bss	NOBITS	0x4548c0	0x14898	0x2250	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x9c6	0x14898	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x14898	0x64	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	0x13b90	0x13b90	5.6031	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x14000	0x454000	0x454000	0x898	0x2b10	3.8763	0x6	RW	0x10000		.ctors .dtors .data.rel.ro .data .got .sbss .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
192.168.2.23191.61.26.79 52002372152835222 03/20/23-18:15:41.479492	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	52002	37215	192.168.2.23	191.61.26.79
192.168.2.2341.239.25.98 58734372152835222 03/20/23-18:16:18.194286	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	58734	37215	192.168.2.23	41.239.25.98
192.168.2.2377.136.237.160455163721528352222 03/20/23-18:14:44.802279	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45516	37215	192.168.2.23	77.136.237.160
192.168.2.23103.54.44.135030637215283522 03/20/23-18:15:01.586540	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	50306	37215	192.168.2.23	103.54.44.133
192.168.2.23104.128.127.228465443721528352222 03/20/23-18:15:22.996810	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	46544	37215	192.168.2.23	104.128.127.228
192.168.2.2341.238.196.116410763721528352222 03/20/23-18:14:59.321194	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	41076	37215	192.168.2.23	41.238.196.116
192.168.2.2334.120.131.845438372152835222 03/20/23-18:15:29.072769	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	45438	37215	192.168.2.23	34.120.131.8
192.168.2.2394.187.108.185552283721528352222 03/20/23-18:15:36.209617	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	55228	37215	192.168.2.23	94.187.108.185

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 18:14:40.710655928 CET	192.168.2.23	8.8.8.8	0xe0a4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:40.729371071 CET	192.168.2.23	8.8.8.8	0xe0a4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:40.748934031 CET	192.168.2.23	8.8.8.8	0xe0a4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:40.767157078 CET	192.168.2.23	8.8.8.8	0xe0a4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:40.786946058 CET	192.168.2.23	8.8.8.8	0xe0a4	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:41.806308031 CET	192.168.2.23	8.8.8.8	0x8e4b	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:41.824856997 CET	192.168.2.23	8.8.8.8	0x8e4b	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:41.845232964 CET	192.168.2.23	8.8.8.8	0x8e4b	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:41.863372087 CET	192.168.2.23	8.8.8.8	0x8e4b	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:41.883501053 CET	192.168.2.23	8.8.8.8	0x8e4b	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:49.903549910 CET	192.168.2.23	8.8.8.8	0x2d96	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:49.923871040 CET	192.168.2.23	8.8.8.8	0x2d96	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:49.944060087 CET	192.168.2.23	8.8.8.8	0x2d96	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:49.964304924 CET	192.168.2.23	8.8.8.8	0x2d96	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:49.984107018 CET	192.168.2.23	8.8.8.8	0x2d96	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:57.002443075 CET	192.168.2.23	8.8.8.8	0x8437	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:57.021122932 CET	192.168.2.23	8.8.8.8	0x8437	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:57.039206028 CET	192.168.2.23	8.8.8.8	0x8437	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:57.059446096 CET	192.168.2.23	8.8.8.8	0x8437	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:57.077682018 CET	192.168.2.23	8.8.8.8	0x8437	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:06.097577095 CET	192.168.2.23	8.8.8.8	0xda8a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:06.116137981 CET	192.168.2.23	8.8.8.8	0xda8a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:06.136562109 CET	192.168.2.23	8.8.8.8	0xda8a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:06.154822111 CET	192.168.2.23	8.8.8.8	0xda8a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:06.175090075 CET	192.168.2.23	8.8.8.8	0xda8a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:10.195401907 CET	192.168.2.23	8.8.8.8	0x4344	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:10.216114044 CET	192.168.2.23	8.8.8.8	0x4344	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:10.236242056 CET	192.168.2.23	8.8.8.8	0x4344	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:10.254297018 CET	192.168.2.23	8.8.8.8	0x4344	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:10.272198915 CET	192.168.2.23	8.8.8.8	0x4344	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:14.292524099 CET	192.168.2.23	8.8.8.8	0xf909	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:14.312907934 CET	192.168.2.23	8.8.8.8	0xf909	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:14.333441973 CET	192.168.2.23	8.8.8.8	0xf909	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:14.351639032 CET	192.168.2.23	8.8.8.8	0xf909	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:14.372216940 CET	192.168.2.23	8.8.8.8	0xf909	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 18:15:15.390887976 CET	192.168.2.23	8.8.8.8	0x8cd2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:15.413100004 CET	192.168.2.23	8.8.8.8	0x8cd2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:15.432490110 CET	192.168.2.23	8.8.8.8	0x8cd2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:15.450932026 CET	192.168.2.23	8.8.8.8	0x8cd2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:15.470230103 CET	192.168.2.23	8.8.8.8	0x8cd2	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:25.488826036 CET	192.168.2.23	8.8.8.8	0xc8a8	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:25.509450912 CET	192.168.2.23	8.8.8.8	0xc8a8	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:25.527558088 CET	192.168.2.23	8.8.8.8	0xc8a8	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:25.545166016 CET	192.168.2.23	8.8.8.8	0xc8a8	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:25.565135002 CET	192.168.2.23	8.8.8.8	0xc8a8	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:30.583404064 CET	192.168.2.23	8.8.8.8	0xcd9a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:30.601807117 CET	192.168.2.23	8.8.8.8	0xcd9a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:30.621901035 CET	192.168.2.23	8.8.8.8	0xcd9a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:30.646783113 CET	192.168.2.23	8.8.8.8	0xcd9a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:30.666836023 CET	192.168.2.23	8.8.8.8	0xcd9a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:32.685048103 CET	192.168.2.23	8.8.8.8	0x68f0	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:32.705912113 CET	192.168.2.23	8.8.8.8	0x68f0	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:32.725862026 CET	192.168.2.23	8.8.8.8	0x68f0	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:32.743865967 CET	192.168.2.23	8.8.8.8	0x68f0	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:32.763892889 CET	192.168.2.23	8.8.8.8	0x68f0	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:38.784017086 CET	192.168.2.23	8.8.8.8	0x9235	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:38.803886890 CET	192.168.2.23	8.8.8.8	0x9235	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:38.821916103 CET	192.168.2.23	8.8.8.8	0x9235	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:38.842101097 CET	192.168.2.23	8.8.8.8	0x9235	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:38.860243082 CET	192.168.2.23	8.8.8.8	0x9235	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:46.879518986 CET	192.168.2.23	8.8.8.8	0x5787	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:46.899801970 CET	192.168.2.23	8.8.8.8	0x5787	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:46.917967081 CET	192.168.2.23	8.8.8.8	0x5787	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:46.937931061 CET	192.168.2.23	8.8.8.8	0x5787	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:46.958604097 CET	192.168.2.23	8.8.8.8	0x5787	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:51.976836920 CET	192.168.2.23	8.8.8.8	0xf25e	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:51.995378017 CET	192.168.2.23	8.8.8.8	0xf25e	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:52.015284061 CET	192.168.2.23	8.8.8.8	0xf25e	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:52.033797026 CET	192.168.2.23	8.8.8.8	0xf25e	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:52.051847935 CET	192.168.2.23	8.8.8.8	0xf25e	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 18:15:55.072233915 CET	192.168.2.23	8.8.8.8	0xd197	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:55.092406034 CET	192.168.2.23	8.8.8.8	0xd197	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:55.110358953 CET	192.168.2.23	8.8.8.8	0xd197	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:55.128492117 CET	192.168.2.23	8.8.8.8	0xd197	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:55.146922112 CET	192.168.2.23	8.8.8.8	0xd197	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:00.165262938 CET	192.168.2.23	8.8.8.8	0xf829	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:00.185560942 CET	192.168.2.23	8.8.8.8	0xf829	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:00.205780029 CET	192.168.2.23	8.8.8.8	0xf829	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:00.223917961 CET	192.168.2.23	8.8.8.8	0xf829	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:00.243792057 CET	192.168.2.23	8.8.8.8	0xf829	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:10.261904955 CET	192.168.2.23	8.8.8.8	0x7773	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:10.281975031 CET	192.168.2.23	8.8.8.8	0x7773	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:10.300118923 CET	192.168.2.23	8.8.8.8	0x7773	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:10.318254948 CET	192.168.2.23	8.8.8.8	0x7773	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:10.338167906 CET	192.168.2.23	8.8.8.8	0x7773	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:19.355822086 CET	192.168.2.23	8.8.8.8	0x13a6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:19.374198914 CET	192.168.2.23	8.8.8.8	0x13a6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:19.391611099 CET	192.168.2.23	8.8.8.8	0x13a6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:19.409610987 CET	192.168.2.23	8.8.8.8	0x13a6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:19.427755117 CET	192.168.2.23	8.8.8.8	0x13a6	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:29.445678949 CET	192.168.2.23	8.8.8.8	0xd685	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:29.465651989 CET	192.168.2.23	8.8.8.8	0xd685	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:29.483763933 CET	192.168.2.23	8.8.8.8	0xd685	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:29.502015114 CET	192.168.2.23	8.8.8.8	0xd685	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:29.519937038 CET	192.168.2.23	8.8.8.8	0xd685	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:35.540028095 CET	192.168.2.23	8.8.8.8	0x3f01	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:35.558434010 CET	192.168.2.23	8.8.8.8	0x3f01	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:35.576556921 CET	192.168.2.23	8.8.8.8	0x3f01	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:35.597016096 CET	192.168.2.23	8.8.8.8	0x3f01	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:35.616880894 CET	192.168.2.23	8.8.8.8	0x3f01	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:44.634846926 CET	192.168.2.23	8.8.8.8	0x958a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:44.652947903 CET	192.168.2.23	8.8.8.8	0x958a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:44.670708895 CET	192.168.2.23	8.8.8.8	0x958a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:44.690668106 CET	192.168.2.23	8.8.8.8	0x958a	Standard query (0)	BC@^]B	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:44.710665941 CET	192.168.2.23	8.8.8.8	0x958a	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 18:14:40.728677988 CET	8.8.8.8	192.168.2.23	0xe0a4	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:40.747214079 CET	8.8.8.8	192.168.2.23	0xe0a4	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:40.766967058 CET	8.8.8.8	192.168.2.23	0xe0a4	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:40.786787033 CET	8.8.8.8	192.168.2.23	0xe0a4	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:40.804503918 CET	8.8.8.8	192.168.2.23	0xe0a4	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:41.824502945 CET	8.8.8.8	192.168.2.23	0x8e4b	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:41.844948053 CET	8.8.8.8	192.168.2.23	0x8e4b	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:41.863142014 CET	8.8.8.8	192.168.2.23	0x8e4b	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:41.883037090 CET	8.8.8.8	192.168.2.23	0x8e4b	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:41.903458118 CET	8.8.8.8	192.168.2.23	0x8e4b	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:49.923542023 CET	8.8.8.8	192.168.2.23	0x2d96	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:49.943679094 CET	8.8.8.8	192.168.2.23	0x2d96	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:49.964112997 CET	8.8.8.8	192.168.2.23	0x2d96	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:49.983896971 CET	8.8.8.8	192.168.2.23	0x2d96	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:50.002075911 CET	8.8.8.8	192.168.2.23	0x2d96	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:57.020864010 CET	8.8.8.8	192.168.2.23	0x8437	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:57.038903952 CET	8.8.8.8	192.168.2.23	0x8437	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:57.059125900 CET	8.8.8.8	192.168.2.23	0x8437	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:57.077517986 CET	8.8.8.8	192.168.2.23	0x8437	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:14:57.097563982 CET	8.8.8.8	192.168.2.23	0x8437	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:06.115888119 CET	8.8.8.8	192.168.2.23	0xda8a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:06.136253119 CET	8.8.8.8	192.168.2.23	0xda8a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:06.154548883 CET	8.8.8.8	192.168.2.23	0xda8a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:06.174738884 CET	8.8.8.8	192.168.2.23	0xda8a	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 18:15:06.194849968 CET	8.8.8.8	192.168.2.23	0xda8a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:10.215801954 CET	8.8.8.8	192.168.2.23	0x4344	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:10.235914946 CET	8.8.8.8	192.168.2.23	0x4344	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:10.254033089 CET	8.8.8.8	192.168.2.23	0x4344	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:10.271939993 CET	8.8.8.8	192.168.2.23	0x4344	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:10.292166948 CET	8.8.8.8	192.168.2.23	0x4344	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:14.312576056 CET	8.8.8.8	192.168.2.23	0xf909	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:14.333122015 CET	8.8.8.8	192.168.2.23	0xf909	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:14.351407051 CET	8.8.8.8	192.168.2.23	0xf909	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:14.371886015 CET	8.8.8.8	192.168.2.23	0xf909	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:14.390366077 CET	8.8.8.8	192.168.2.23	0xf909	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:15.412714005 CET	8.8.8.8	192.168.2.23	0x8cd2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:15.432138920 CET	8.8.8.8	192.168.2.23	0x8cd2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:15.450726986 CET	8.8.8.8	192.168.2.23	0x8cd2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:15.469994068 CET	8.8.8.8	192.168.2.23	0x8cd2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:15.488811016 CET	8.8.8.8	192.168.2.23	0x8cd2	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:25.509138107 CET	8.8.8.8	192.168.2.23	0xc8a8	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:25.527192116 CET	8.8.8.8	192.168.2.23	0xc8a8	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:25.544874907 CET	8.8.8.8	192.168.2.23	0xc8a8	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:25.564853907 CET	8.8.8.8	192.168.2.23	0xc8a8	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:25.583019972 CET	8.8.8.8	192.168.2.23	0xc8a8	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:30.601525068 CET	8.8.8.8	192.168.2.23	0xcd9a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:30.621629000 CET	8.8.8.8	192.168.2.23	0xcd9a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:30.646460056 CET	8.8.8.8	192.168.2.23	0xcd9a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:30.666532040 CET	8.8.8.8	192.168.2.23	0xcd9a	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 18:15:30.684571028 CET	8.8.8.8	192.168.2.23	0xcd9a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:32.705599070 CET	8.8.8.8	192.168.2.23	0x68f0	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:32.725529909 CET	8.8.8.8	192.168.2.23	0x68f0	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:32.743591070 CET	8.8.8.8	192.168.2.23	0x68f0	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:32.763623953 CET	8.8.8.8	192.168.2.23	0x68f0	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:32.783682108 CET	8.8.8.8	192.168.2.23	0x68f0	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:38.803610086 CET	8.8.8.8	192.168.2.23	0x9235	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:38.821660995 CET	8.8.8.8	192.168.2.23	0x9235	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:38.841850996 CET	8.8.8.8	192.168.2.23	0x9235	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:38.860014915 CET	8.8.8.8	192.168.2.23	0x9235	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:38.879367113 CET	8.8.8.8	192.168.2.23	0x9235	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:46.899549007 CET	8.8.8.8	192.168.2.23	0x5787	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:46.917658091 CET	8.8.8.8	192.168.2.23	0x5787	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:46.937635899 CET	8.8.8.8	192.168.2.23	0x5787	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:46.958277941 CET	8.8.8.8	192.168.2.23	0x5787	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:46.976480007 CET	8.8.8.8	192.168.2.23	0x5787	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:51.995114088 CET	8.8.8.8	192.168.2.23	0xf25e	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:52.015002966 CET	8.8.8.8	192.168.2.23	0xf25e	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:52.033480883 CET	8.8.8.8	192.168.2.23	0xf25e	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:52.051573038 CET	8.8.8.8	192.168.2.23	0xf25e	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:52.071703911 CET	8.8.8.8	192.168.2.23	0xf25e	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:55.091957092 CET	8.8.8.8	192.168.2.23	0xd197	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:55.110070944 CET	8.8.8.8	192.168.2.23	0xd197	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:55.128191948 CET	8.8.8.8	192.168.2.23	0xd197	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:15:55.146547079 CET	8.8.8.8	192.168.2.23	0xd197	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 18:15:55.164916039 CET	8.8.8.8	192.168.2.23	0xd197	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:00.185120106 CET	8.8.8.8	192.168.2.23	0xf829	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:00.205375910 CET	8.8.8.8	192.168.2.23	0xf829	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:00.223678112 CET	8.8.8.8	192.168.2.23	0xf829	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:00.243460894 CET	8.8.8.8	192.168.2.23	0xf829	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:00.261671066 CET	8.8.8.8	192.168.2.23	0xf829	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:10.281678915 CET	8.8.8.8	192.168.2.23	0x7773	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:10.299808025 CET	8.8.8.8	192.168.2.23	0x7773	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:10.317961931 CET	8.8.8.8	192.168.2.23	0x7773	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:10.337897062 CET	8.8.8.8	192.168.2.23	0x7773	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:10.355783939 CET	8.8.8.8	192.168.2.23	0x7773	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:19.373778105 CET	8.8.8.8	192.168.2.23	0x13a6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:19.391407967 CET	8.8.8.8	192.168.2.23	0x13a6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:19.409384012 CET	8.8.8.8	192.168.2.23	0x13a6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:19.427515030 CET	8.8.8.8	192.168.2.23	0x13a6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:19.445725918 CET	8.8.8.8	192.168.2.23	0x13a6	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:29.465395927 CET	8.8.8.8	192.168.2.23	0xd685	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:29.483481884 CET	8.8.8.8	192.168.2.23	0xd685	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:29.501699924 CET	8.8.8.8	192.168.2.23	0xd685	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:29.519619942 CET	8.8.8.8	192.168.2.23	0xd685	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:29.539716005 CET	8.8.8.8	192.168.2.23	0xd685	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:35.558115005 CET	8.8.8.8	192.168.2.23	0x3f01	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:35.576301098 CET	8.8.8.8	192.168.2.23	0x3f01	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:35.596678019 CET	8.8.8.8	192.168.2.23	0x3f01	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:35.616626978 CET	8.8.8.8	192.168.2.23	0x3f01	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 18:16:35.634768963 CET	8.8.8.8	192.168.2.23	0x3f01	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:44.652662039 CET	8.8.8.8	192.168.2.23	0x958a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:44.670453072 CET	8.8.8.8	192.168.2.23	0x958a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:44.690440893 CET	8.8.8.8	192.168.2.23	0x958a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:44.710419893 CET	8.8.8.8	192.168.2.23	0x958a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 18:16:44.728445053 CET	8.8.8.8	192.168.2.23	0x958a	Name error (3)	BC@^]B	none	none	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: 6lqMB7o2Ts.elf PID: **6230**, Parent PID: **6125**

General

Start time:	18:14:39
Start date:	20/03/2023
Path:	/tmp/6lqMB7o2Ts.elf
Arguments:	/tmp/6lqMB7o2Ts.elf
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

File Activities

File Read

Analysis Process: 6lqMB7o2Ts.elf PID: **6232**, Parent PID: **6230**

General

Start time:	18:14:40
Start date:	20/03/2023
Path:	/tmp/6lqMB7o2Ts.elf
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: sh PID: **6232**, Parent PID: **6230**

General

Start time:	18:14:40
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	sh -c "rm -rf bin/systemd && mkdir bin; >bin/systemd && mv /tmp/6lqMB7o2Ts.elf bin/systemd; chmod 777 bin/systemd"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: **6234**, Parent PID: **6232**

General

Start time:	18:14:40
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: **6234**, Parent PID: **6232**

General

Start time:	18:14:40
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: **6235**, Parent PID: **6232**

General

Start time:	18:14:40
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mkdir PID: **6235**, Parent PID: **6232**

General

Start time:	18:14:40
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: **6236**, Parent PID: **6232**

General

Start time:	18:14:40
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mv PID: **6236**, Parent PID: **6232**

General

Start time:	18:14:40
Start date:	20/03/2023

Path:	/usr/bin/mv
Arguments:	mv /tmp/6lqMB7o2Ts.elf bin/systemd
File size:	149888 bytes
MD5 hash:	504f0590fa482d4da070a702260e3716

File Activities

File Read

File Moved

Analysis Process: sh PID: **6237**, Parent PID: **6232**

General

Start time:	18:14:40
Start date:	20/03/2023
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: chmod PID: **6237**, Parent PID: **6232**

General

Start time:	18:14:40
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: 6lqMB7o2Ts.elf PID: **6238**, Parent PID: **6230**

General

Start time:	18:14:40
Start date:	20/03/2023
Path:	/tmp/6lqMB7o2Ts.elf
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: 6lqMB7o2Ts.elf PID: **6240**, Parent PID: **6238**

General

Start time:	18:14:40
Start date:	20/03/2023
Path:	/tmp/6lqMB7o2Ts.elf
Arguments:	n/a
File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9

Analysis Process: 6lqMB7o2Ts.elf PID: **6241**, Parent PID: **6238**

General

Start time:	18:14:40
Start date:	20/03/2023
Path:	/tmp/6lqMB7o2Ts.elf
Arguments:	n/a

File size:	5773336 bytes
MD5 hash:	0d6f61f82cf2f781c6eb0661071d42d9