ID: 1579200
Sample Name: hmips.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 04:26:05
Date: 21/12/2024
Version: 41.0.0 Charoite

Table of Contents

Table of Contents 2
Linux Analysis Report hmips.elf 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
General Information 4
Warnings 4
Runtime Messages 4
Process Tree 4
Malware Threat Intel 5
Yara Signatures 5
Initial Sample 5
Memory Dumps 5
Suricata Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Malware Configuration 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 9
Public IPs 9
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 12
General 12
Static ELF Info 12
ELF header 12
Sections 13
Program Segments 13
Network Behavior 13
Network Port Distribution 13
TCP Packets 14
DNS Queries 14
DNS Answers 16
System Behavior 21
Analysis Process: hmips.elf PID: 6240, Parent PID: 6165 21
General 21
File Activities 21
File Read 21
Directory Enumerated 21
Analysis Process: hmips.elf PID: 6242, Parent PID: 6240 21
General 22
Analysis Process: hmips.elf PID: 6298, Parent PID: 6242 22
General 22
Analysis Process: hmips.elf PID: 6308, Parent PID: 6298 22
General 22
Analysis Process: hmips.elf PID: 6315, Parent PID: 6308 22
General 22
Analysis Process: hmips.elf PID: 6244, Parent PID: 6240 22
General 22
Analysis Process: hmips.elf PID: 6268, Parent PID: 6244 22
General 22
Analysis Process: hmips.elf PID: 6270, Parent PID: 6268 22
General 23

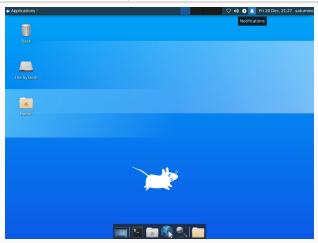
Linux Analysis Report

hmips.elf

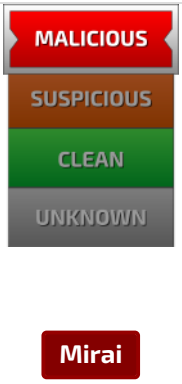
Overview

General Information

Sample name:	hmips.elf
Analysis ID:	1579200
MD5:	40fa65794e145..
SHA1:	c7d7a8f9f2639…
SHA256:	d02adfd870363..
Tags:	elf user-abuse_ch
Infos:	



Detection



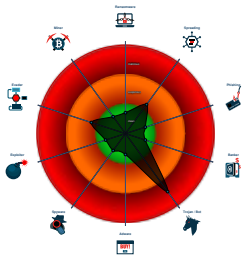
Mirai

Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Mirai
- Connects to many ports of the same…
- Sends malformed DNS queries
- Detected TCP or UDP traffic on non…
- Found strings indicative of a multi-p…
- Sample contains strings indicative o…
- Sample has stripped symbol table
- Sample listens on a socket
- Tries to connect to HTTP servers, b…

Classification



General Information

Joe Sandbox version:	41.0.0 Charoite
Analysis ID:	1579200
Start date and time:	2024-12-21 04:26:05 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 4m 56s
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 name:	hmips.elf
Detection:	MAL
Classification:	mal72.troj.linELF@0/0@69/0

Warnings

Runtime Messages

Command:	/tmp/hmips.elf
PID:	6240
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	I just wanna look after my cats, man.
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- hmips.elf (PID: 6240, Parent: 6165, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/hmips.elf
  - hmips.elf New Fork (PID: 6242, Parent: 6240)
    - hmips.elf New Fork (PID: 6298, Parent: 6242)
      - hmips.elf New Fork (PID: 6308, Parent: 6298)
        - hmips.elf New Fork (PID: 6315, Parent: 6308)
  - hmips.elf New Fork (PID: 6244, Parent: 6240)
    - hmips.elf New Fork (PID: 6268, Parent: 6244)
      - hmips.elf New Fork (PID: 6270, Parent: 6268)
- **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

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
hmips.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
6242.1.00007fd79c400000.00007fd79c415000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6240.1.00007fd79c400000.00007fd79c415000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Suricata Signatures

No Suricata rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Networking

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

Sends malformed DNS queries

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

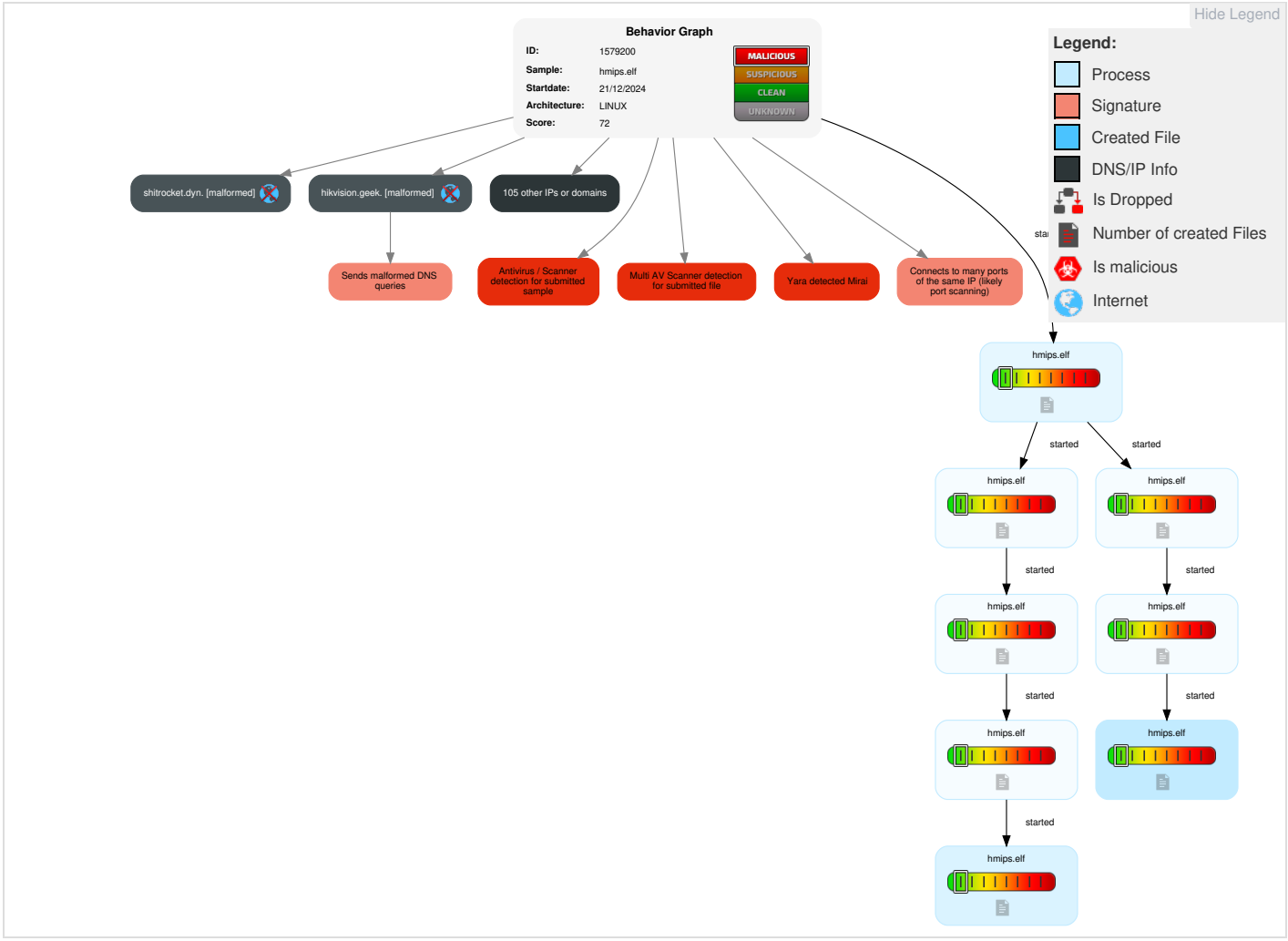
Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	1 Scripting	Valid Accounts	Windows Management Instrumentation	1 Scripting	Path Interception	Direct Volume Access	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	1 Non-Standard Port	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	1 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	2 Application Layer Protocol	Traffic Duplication	Data Destruction

Malware Configuration

No configs have been found

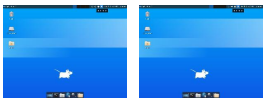
Behavior Graph

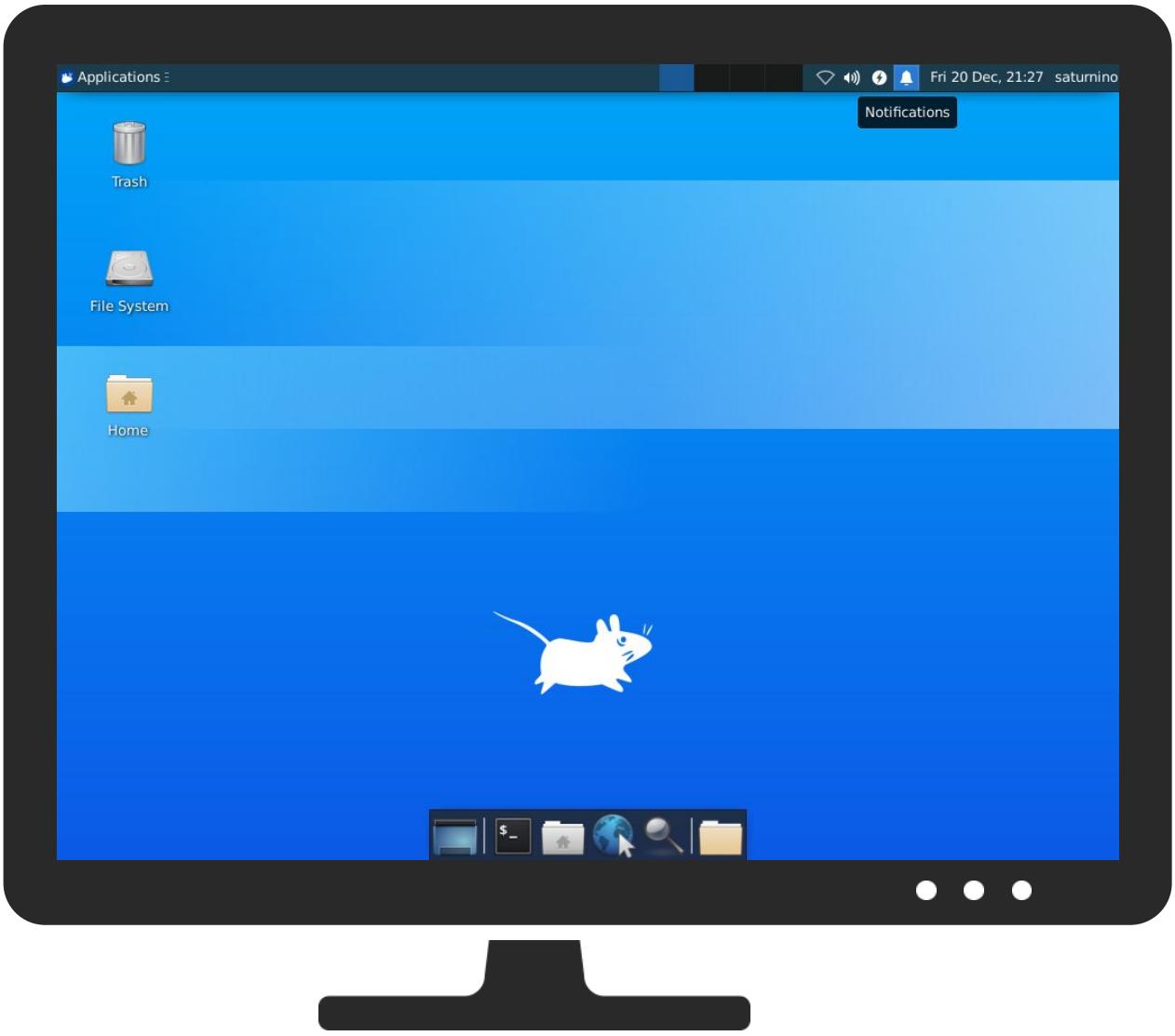


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
hmips.elf	39%	ReversingLabs	Linux.Backdoor.Mirai	
hmips.elf	100%	Avira	EXP/ELF.Agent.J.8	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

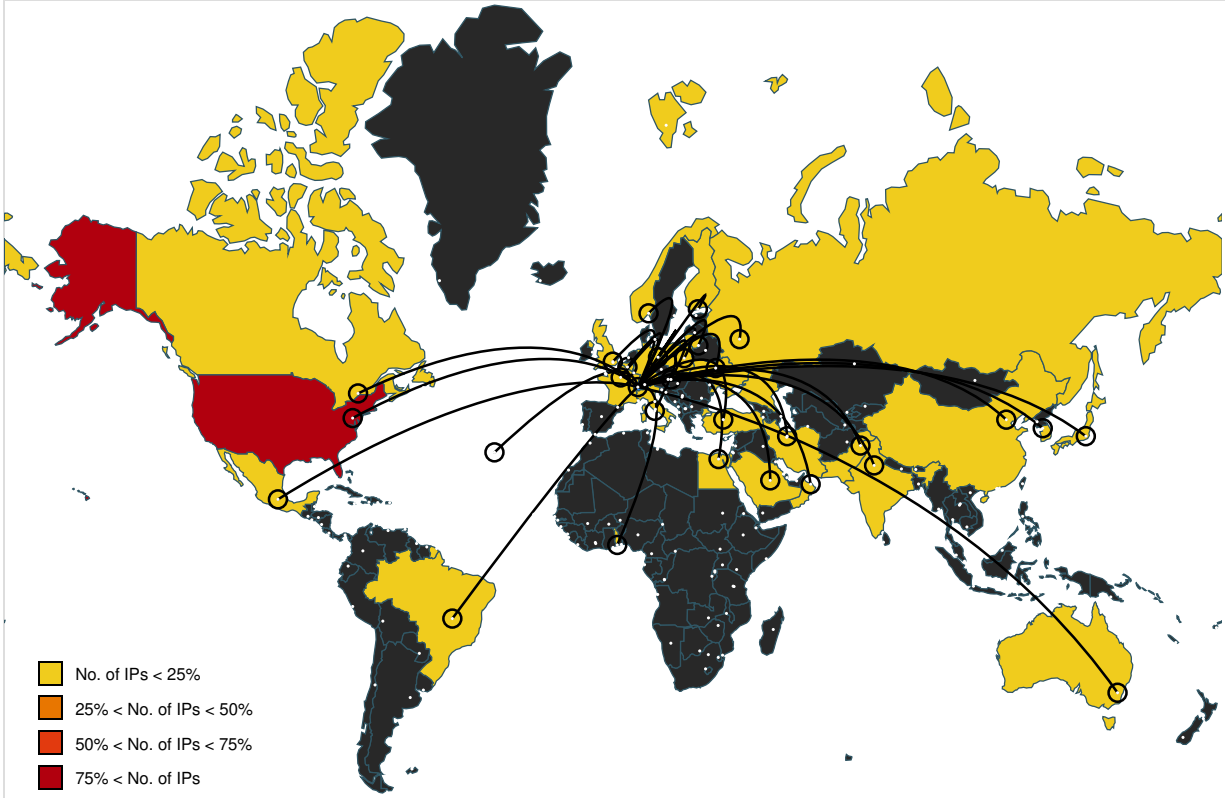
Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
shitrocket.dyn	212.60.5.153	true	false		high
catlovingfools.geek	185.72.8.231	true	false		high
hikvision.geek	185.72.8.231	true	false		high
catlovingfools.geek. [malformed]	unknown	unknown	false		high
hikvision.geek. [malformed]	unknown	unknown	false		high
shitrocket.dyn. [malformed]	unknown	unknown	false		high
catvision.dyn. [malformed]	unknown	unknown	false		high

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
61.248.201.68	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
158.111.69.119	unknown	United States		13611	CDCUS	false
92.243.22.79	unknown	France		203476	GANDI-AS-2Domainnameregistrar-httpwwwgandinetFR	false
59.101.152.237	unknown	Australia		2764	AAPTAAPTLimitedAU	false
147.175.228.70	unknown	Slovakia (SLOVAK Republic)		2607	SANETSlovakAcademicNetworkSK	false
55.84.215.193	unknown	United States		351	DNIC-ASBLK-00306-00371US	false
185.230.47.158	unknown	Ukraine		205692	WEBINVESTPLUSUA	false
28.13.247.181	unknown	United States		7922	COMCAST-7922US	false
84.194.149.212	unknown	Belgium		6848	TELENET-ASBE	false
101.102.207.29	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
78.91.104.110	unknown	Norway		224	UNINETTUNINETTTheNorwegianUniversityResearchNetwork	false
54.185.230.168	unknown	United States		16509	AMAZON-02US	false
188.138.99.78	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.238.216.22	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
4.39.172.234	unknown	United States		46164	ATT-MOBILITY-LABSUS	false
77.181.19.192	unknown	Germany		6805	TDDE-ASN1DE	false
191.123.132.141	unknown	Brazil		26615	TIMSABR	false
129.93.247.90	unknown	United States		7896	NU-ASUS	false
199.33.240.31	unknown	United States		7782	ALSK-7782US	false
205.51.55.180	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
157.151.4.253	unknown	United States		23342	UNITEDLAYERUS	false
196.170.87.186	unknown	Togo		24691	TOGOTEL-ASTogoTelecomTogoTG	false
206.209.124.186	unknown	United States		23548	THEDACAREUS	false
211.17.244.132	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
132.66.186.162	unknown	Israel		378	MACHBA-ASILANIL	false
166.87.167.210	unknown	Saudi Arabia		5080	ARAMCO-ASUS	false
75.128.235.161	unknown	United States		20115	CHARTER-20115US	false
145.224.25.238	unknown	United Kingdom		1101	IP-EEND-ASIP-EENDBVNL	false
30.236.150.145	unknown	United States		7922	COMCAST-7922US	false
121.237.234.92	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
22.238.114.140	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
63.41.135.162	unknown	United States		22394	CELLCOUS	false
203.241.214.22	unknown	Korea Republic of		18401	AS18401-AS-KRDAEGUUNIVERSITYKR	false
220.20.108.56	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
109.142.223.115	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
211.160.25.151	unknown	China		9814	FIBRLINKBeijingFibrLINKNetworksCoLtdCN	false
60.105.182.252	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
183.19.27.115	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
209.248.243.232	unknown	United States		7029	WINDSTREAMUS	false
90.221.106.17	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
223.98.57.231	unknown	China		24444	CMNET-V4SHANDONG-AS-APShandongMobileCommunicationCompany	false
66.9.20.10	unknown	United States		18885	M2NGAGE2US	false
170.101.226.66	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
175.23.41.204	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
131.110.72.47	unknown	United States		6	BULL-HNUS	false
143.225.102.51	unknown	Italy		137	ASGARRConsortiumGARREU	false
156.60.232.255	unknown	United States		1226	CTA-42-AS1226US	false
206.64.5.124	unknown	United States		701	UUNETUS	false
64.79.82.146	unknown	United States		10297	ENET-2US	false
146.211.79.112	unknown	Finland		16086	DNAFI	false
24.66.153.15	unknown	Canada		6327	SHAWCA	false
58.12.166.205	unknown	Japan		17506	UCOMARTERIANetworksCorporationJP	false
54.54.164.172	unknown	United States		14618	AMAZON-AESUS	false
49.30.181.29	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
167.12.63.91	unknown	United States		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
137.27.163.26	unknown	United States		20115	CHARTER-20115US	false
146.20.121.237	unknown	United States		27357	RACKSPACEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
38.207.37.102	unknown	United States		9009	M247GB	false
74.100.71.79	unknown	United States		701	UUNETUS	false
73.105.156.45	unknown	United States		7922	COMCAST-7922US	false
36.50.14.16	unknown	unknown		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
37.206.42.120	unknown	Italy		3269	ASN-IBSNAZIT	false
115.244.44.165	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
156.214.15.151	unknown	Egypt		8452	TE-ASTE-ASEG	false
175.108.110.197	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
101.219.236.184	unknown	India		58519	CHINATELECOM-CTCLOUDCloudComputingCorporationCN	false
78.170.19.203	unknown	Turkey		9121	TTNETTR	false
108.78.15.60	unknown	United States		7018	ATT-INTERNET4US	false
209.92.151.127	unknown	United States		7029	WINDSTREAMUS	false
161.177.38.22	unknown	United States		10695	WAL-MARTUS	false
6.117.134.75	unknown	United States		3356	LEVEL3US	false
78.61.93.100	unknown	Lithuania		8764	TELIA-LIETUVALT	false
146.225.111.145	unknown	United States		25400	TELIA-NORWAY-ASTeliaNorwayCoreNetworksNO	false
30.210.187.13	unknown	United States		7922	COMCAST-7922US	false
153.203.223.211	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
150.179.157.247	unknown	United States		3479	PEACHNET-AS1US	false
99.218.40.105	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
40.99.98.3	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
201.3.136.151	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
58.65.191.39	unknown	Pakistan		23674	NAYATEL-PKNayatelPvtLtdPK	false
61.26.182.226	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
201.143.209.15	unknown	Mexico		8151	UninetSAdeCVMX	false
124.65.32.115	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
142.17.208.176	unknown	Canada		611	NECN-1-611CA	false
213.85.209.25	unknown	Russian Federation		8615	CNT-ASMoscowRussiaRU	false
166.180.68.254	unknown	United States		22394	CELLCOUS	false
37.248.66.142	unknown	Poland		8374	PLUSNETPlusnetworkoperatorinPolandPL	false
94.244.131.127	unknown	Ukraine		34743	NASHNET-ASKievUkraineUA	false
5.36.68.138	unknown	Oman		28885	OMANTEL-NAP-ASOmanTelNAPOM	false
136.48.74.228	unknown	United States		16591	GOOGLE-FIBERUS	false
204.16.157.87	unknown	United States		30686	LVLT-30686US	false
86.55.160.189	unknown	Iran (ISLAMIC Republic Of)		197207	MCCI-ASIR	false
183.9.56.218	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
121.231.38.194	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
132.193.131.201	unknown	United States		668	DNIC-AS-00668US	false
31.59.195.66	unknown	Iran (ISLAMIC Republic Of)		31549	RASANAIR	false
26.227.137.255	unknown	United States		7922	COMCAST-7922US	false
135.33.140.90	unknown	United States		54614	CIKTELECOM-CABLECA	false
135.174.27.80	unknown	United States		14962	NCR-252US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.176.248.215	unknown	Canada		855	CANET-ASN-4CA	false

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.546117135531765
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	hmips.elf
File size:	89'408 bytes
MD5:	40fa65794e145a61bc34ce27581f9fca
SHA1:	c7d7a8f9f26394dfc4d6be2a05ba5e0d0cfaa91d
SHA256:	d02adfd870363610aa7d7862c1627639f7688b7ffaa51f363dd3588cad104b2d
SHA512:	c4d234cb037089769b82aaa424be73f1d31ff403197d5ecc705de3f88f8d17bb1ffee5e0597c6ff5d63d3db0b5cb4febfb3412baac1940197fbbe0efab62ed02
SSDEEP:	1536:PjRdrJyhVuqVuIWu30rJfLueVqCHyOUeE3k1XPSni8VRw/TPm:1dFyWfLcCSO1XPSnid/TO
TLSH:	E793D71E6E71AFADF778C33447774A30A7A863C126E18686D2BCE5101E2034D685FBE4
File Content Preview:	.ELF.....@.`...4..[.....4. ...(.....@...@....M...M.....P..EP..EP.....\H.....dt.Q.....<...'.....!'.....<...'.....!... ....'9... .....<...'.....!.....'9+

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1

ELF header	
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	88848
Section Header Size:	40
Number of Section Headers:	14
Header String Table Index:	13

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	0x12b30	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x412c50	0x12c50	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x412cb0	0x12cb0	0x2100	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x455000	0x15000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x455008	0x15008	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x455014	0x15014	0xdc	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x4550f0	0x150f0	0x3c8	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x4554c0	0x154c0	0x5ec	0x4	0x10000003	WAp	0	0	16
.sbss	NOBITS	0x455aac	0x15aac	0x28	0x0	0x10000003	WAp	0	0	4
.bss	NOBITS	0x455ae0	0x15aac	0x5168	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0xc4e	0x15aac	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x15aac	0x64	0x0	0x0		0	0	1

Program Segments

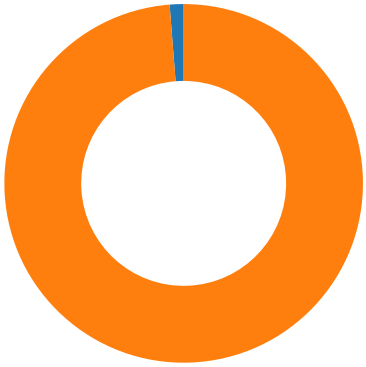
Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x400000	0x400000	0x14db0	0x14db0	5.6089	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x15000	0x455000	0x455000	0xaac	0x5c48	3.7245	0x6	RW	0x10000		.ctors .dtors .data.rel.ro .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution

Total Packets: 80

- 23 (Telnet)
- 443 (HTTPS)



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 21, 2024 04:26:55.424849033 CET	192.168.2.23	168.138.12.137	0x9d89	Standard query (0)	shitrocket.dyn	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:26:55.504049063 CET	192.168.2.23	168.138.12.137	0x9d89	Standard query (0)	shitrocket.dyn	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:26:55.655709028 CET	192.168.2.23	168.138.12.137	0x9d89	Standard query (0)	hikvision.geek	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:26:55.657826900 CET	192.168.2.23	168.138.12.137	0x9d89	Standard query (0)	hikvision.geek	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:00.430489063 CET	192.168.2.23	80.152.203.134	0x2749	Standard query (0)	catlovingf ools.geek	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:00.509527922 CET	192.168.2.23	80.152.203.134	0x2749	Standard query (0)	catlovingf ools.geek	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:00.661626101 CET	192.168.2.23	80.152.203.134	0x2749	Standard query (0)	catvision.dyn. [malformed]	256	388	false
Dec 21, 2024 04:27:00.662024021 CET	192.168.2.23	80.152.203.134	0x2749	Standard query (0)	catvision.dyn. [malformed]	256	388	false
Dec 21, 2024 04:27:05.436629057 CET	192.168.2.23	194.36.144.87	0xb734	Standard query (0)	hikvision.geek. [malformed]	256	393	false
Dec 21, 2024 04:27:05.515305042 CET	192.168.2.23	194.36.144.87	0xb734	Standard query (0)	hikvision.geek. [malformed]	256	393	false
Dec 21, 2024 04:27:05.667881966 CET	192.168.2.23	194.36.144.87	0xb734	Standard query (0)	shitrocket.dyn	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:05.668142080 CET	192.168.2.23	194.36.144.87	0xb734	Standard query (0)	shitrocket.dyn	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:05.681832075 CET	192.168.2.23	81.169.136.222	0xf3d	Standard query (0)	catvision.dyn. [malformed]	256	393	false
Dec 21, 2024 04:27:05.758152962 CET	192.168.2.23	81.169.136.222	0xf3d	Standard query (0)	catvision.dyn. [malformed]	256	393	false
Dec 21, 2024 04:27:11.923083067 CET	192.168.2.23	213.202.211.221	0xccec	Standard query (0)	catvision.dyn. [malformed]	256	399	false
Dec 21, 2024 04:27:12.000170946 CET	192.168.2.23	213.202.211.221	0xccec	Standard query (0)	catvision.dyn. [malformed]	256	400	false
Dec 21, 2024 04:27:12.156678915 CET	192.168.2.23	81.169.136.222	0x3f77	Standard query (0)	catlovingf ools.geek. [malformed]	256	400	false
Dec 21, 2024 04:27:12.232135057 CET	192.168.2.23	81.169.136.222	0x3f77	Standard query (0)	catlovingf ools.geek. [malformed]	256	400	false
Dec 21, 2024 04:27:12.431152105 CET	192.168.2.23	185.181.61.24	0xf3e9	Standard query (0)	hikvision.geek. [malformed]	256	400	false
Dec 21, 2024 04:27:12.486761093 CET	192.168.2.23	185.181.61.24	0xf3e9	Standard query (0)	hikvision.geek. [malformed]	256	400	false
Dec 21, 2024 04:27:12.695307970 CET	192.168.2.23	168.235.111.72	0xe01	Standard query (0)	shitrocket.dyn. [malformed]	256	400	false
Dec 21, 2024 04:27:12.746684074 CET	192.168.2.23	168.235.111.72	0xe01	Standard query (0)	shitrocket.dyn. [malformed]	256	400	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 21, 2024 04:27:12.858846903 CET	192.168.2.23	80.152.203.134	0xb731	Standard query (0)	hikvision.geek	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:12.862814903 CET	192.168.2.23	80.152.203.134	0xb731	Standard query (0)	hikvision.geek	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:17.864353895 CET	192.168.2.23	213.202.211.221	0xccec	Standard query (0)	catvision.dyn. [malformed]	256	405	false
Dec 21, 2024 04:27:17.867774010 CET	192.168.2.23	213.202.211.221	0xccec	Standard query (0)	catvision.dyn. [malformed]	256	405	false
Dec 21, 2024 04:27:18.097522020 CET	192.168.2.23	81.169.136.222	0x3f77	Standard query (0)	catlovingf ools.geek	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.100508928 CET	192.168.2.23	81.169.136.222	0x3f77	Standard query (0)	catlovingf ools.geek	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:24.824223042 CET	192.168.2.23	213.202.211.221	0x6149	Standard query (0)	hikvision.geek. [malformed]	256	412	false
Dec 21, 2024 04:27:25.057166100 CET	192.168.2.23	152.53.15.127	0x10ba	Standard query (0)	catlovingf ools.geek. [malformed]	256	413	false
Dec 21, 2024 04:27:25.302428007 CET	192.168.2.23	81.169.136.222	0x2c79	Standard query (0)	shitrocket.dyn. [malformed]	256	413	false
Dec 21, 2024 04:27:25.544867039 CET	192.168.2.23	152.53.15.127	0x6ac6	Standard query (0)	catvision.dyn. [malformed]	256	413	false
Dec 21, 2024 04:27:25.701735020 CET	192.168.2.23	81.169.136.222	0x2c79	Standard query (0)	shitrocket.dyn. [malformed]	256	413	false
Dec 21, 2024 04:27:25.748473883 CET	192.168.2.23	81.169.136.222	0x2c79	Standard query (0)	shitrocket.dyn. [malformed]	256	413	false
Dec 21, 2024 04:27:25.941761017 CET	192.168.2.23	152.53.15.127	0x6ac6	Standard query (0)	hikvision.geek. [malformed]	256	413	false
Dec 21, 2024 04:27:25.987329006 CET	192.168.2.23	152.53.15.127	0x6ac6	Standard query (0)	hikvision.geek. [malformed]	256	414	false
Dec 21, 2024 04:27:26.184750080 CET	192.168.2.23	194.36.144.87	0x11b0	Standard query (0)	catlovingf ools.geek. [malformed]	256	414	false
Dec 21, 2024 04:27:26.238739014 CET	192.168.2.23	194.36.144.87	0x11b0	Standard query (0)	catlovingf ools.geek. [malformed]	256	414	false
Dec 21, 2024 04:27:26.428466082 CET	192.168.2.23	217.160.70.42	0xea47	Standard query (0)	catvision.dyn. [malformed]	256	414	false
Dec 21, 2024 04:27:26.483891964 CET	192.168.2.23	217.160.70.42	0xea47	Standard query (0)	catvision.dyn. [malformed]	256	414	false
Dec 21, 2024 04:27:27.669857979 CET	192.168.2.23	51.158.108.203	0xcee8	Standard query (0)	hikvision.geek	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:27.724340916 CET	192.168.2.23	51.158.108.203	0xcee8	Standard query (0)	hikvision.geek	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:32.285319090 CET	192.168.2.23	194.36.144.87	0x11b0	Standard query (0)	hikvision.geek	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:45.353216887 CET	192.168.2.23	213.202.211.221	0x6149	Standard query (0)	catlovingf ools.geek	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:54.945265055 CET	192.168.2.23	152.53.15.127	0xec9b	Standard query (0)	shitrocket.dyn	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:54.993377924 CET	192.168.2.23	152.53.15.127	0xec9b	Standard query (0)	shitrocket.dyn	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:59.570246935 CET	192.168.2.23	168.235.111.72	0x9295	Standard query (0)	catlovingf ools.geek. [malformed]	256	447	false
Dec 21, 2024 04:27:59.888437033 CET	192.168.2.23	51.158.108.203	0xcee8	Standard query (0)	hikvision.geek. [malformed]	256	447	false
Dec 21, 2024 04:28:00.129368067 CET	192.168.2.23	194.36.144.87	0xfa80	Standard query (0)	catvision.dyn. [malformed]	256	448	false
Dec 21, 2024 04:28:00.377476931 CET	192.168.2.23	81.169.136.222	0xfbf6	Standard query (0)	shitrocket.dyn	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.134712934 CET	192.168.2.23	168.235.111.72	0x65bc	Standard query (0)	shitrocket.dyn	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.191021919 CET	192.168.2.23	168.235.111.72	0x65bc	Standard query (0)	shitrocket.dyn	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:07.686148882 CET	192.168.2.23	81.169.136.222	0xb2a0	Standard query (0)	shitrocket.dyn	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:09.565018892 CET	192.168.2.23	81.169.136.222	0xb2a0	Standard query (0)	catlovingf ools.geek. [malformed]	256	457	false
Dec 21, 2024 04:28:09.805208921 CET	192.168.2.23	168.138.12.137	0x487a	Standard query (0)	catvision.dyn. [malformed]	256	457	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 21, 2024 04:28:10.208288908 CET	192.168.2.23	109.91.184.21	0xd70	Standard query (0)	shitrocket.dyn	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:10.729099035 CET	192.168.2.23	168.138.12.137	0xc4e7	Standard query (0)	catlovingf ools.geek. [malformed]	256	458	false
Dec 21, 2024 04:28:12.602051020 CET	192.168.2.23	194.36.144.87	0x5232	Standard query (0)	hikvision.geek. [malformed]	256	460	false
Dec 21, 2024 04:28:12.847743988 CET	192.168.2.23	152.53.15.127	0x405a	Standard query (0)	catvision.dyn. [malformed]	256	460	false
Dec 21, 2024 04:28:13.095942974 CET	192.168.2.23	51.158.108.203	0xfee0	Standard query (0)	catlovingf ools.geek. [malformed]	256	461	false
Dec 21, 2024 04:28:13.337104082 CET	192.168.2.23	168.138.12.137	0xe7cf	Standard query (0)	shitrocket.dyn. [malformed]	256	461	false
Dec 21, 2024 04:28:15.734637022 CET	192.168.2.23	81.169.136.222	0xb2a0	Standard query (0)	hikvision.geek. [malformed]	256	463	false
Dec 21, 2024 04:28:15.974493980 CET	192.168.2.23	168.138.12.137	0x487a	Standard query (0)	shitrocket.dyn. [malformed]	256	464	false
Dec 21, 2024 04:28:20.980190039 CET	192.168.2.23	109.91.184.21	0xd70	Standard query (0)	catvision.dyn. [malformed]	256	468	false
Dec 21, 2024 04:28:37.508013964 CET	192.168.2.23	81.169.136.222	0xc7f7	Standard query (0)	shitrocket.dyn	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:40.774159908 CET	192.168.2.23	168.235.111.72	0x9295	Standard query (0)	shitrocket.dyn. [malformed]	256	488	false
Dec 21, 2024 04:28:41.100454092 CET	192.168.2.23	51.158.108.203	0xcee8	Standard query (0)	hikvision.geek. [malformed]	256	489	false
Dec 21, 2024 04:28:41.341579914 CET	192.168.2.23	194.36.144.87	0xfa80	Standard query (0)	catlovingf ools.geek. [malformed]	256	489	false
Dec 21, 2024 04:28:41.588570118 CET	192.168.2.23	81.169.136.222	0xfbf6	Standard query (0)	catvision.dyn. [malformed]	256	489	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 21, 2024 04:27:05.680254936 CET	194.36.144.87	192.168.2.23	0xb734	Format error (1)	hikvision.geek. [malformed]	none	none	256	393	false
Dec 21, 2024 04:27:05.756511927 CET	194.36.144.87	192.168.2.23	0xb734	Format error (1)	hikvision.geek. [malformed]	none	none	256	393	false
Dec 21, 2024 04:27:05.912204027 CET	194.36.144.87	192.168.2.23	0xb734	No error (0)	shitrocket.dyn		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:05.912204027 CET	194.36.144.87	192.168.2.23	0xb734	No error (0)	shitrocket.dyn		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:05.912204027 CET	194.36.144.87	192.168.2.23	0xb734	No error (0)	shitrocket.dyn		212.192.13.95	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:05.912204027 CET	194.36.144.87	192.168.2.23	0xb734	No error (0)	shitrocket.dyn		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:05.912204027 CET	194.36.144.87	192.168.2.23	0xb734	No error (0)	shitrocket.dyn		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:05.912204027 CET	194.36.144.87	192.168.2.23	0xb734	No error (0)	shitrocket.dyn		185.72.8.231	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:05.912204027 CET	194.36.144.87	192.168.2.23	0xb734	No error (0)	shitrocket.dyn		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:05.912329912 CET	194.36.144.87	192.168.2.23	0xb734	No error (0)	shitrocket.dyn		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:05.912329912 CET	194.36.144.87	192.168.2.23	0xb734	No error (0)	shitrocket.dyn		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:05.912329912 CET	194.36.144.87	192.168.2.23	0xb734	No error (0)	shitrocket.dyn		212.192.13.95	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 21, 2024 04:27:05.912329912 CET	194.36.144.87	192.168.2.23	0xb734	No error (0)	shitrocket.dyn		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:05.912329912 CET	194.36.144.87	192.168.2.23	0xb734	No error (0)	shitrocket.dyn		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:05.912329912 CET	194.36.144.87	192.168.2.23	0xb734	No error (0)	shitrocket.dyn		185.72.8.231	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:05.912329912 CET	194.36.144.87	192.168.2.23	0xb734	No error (0)	shitrocket.dyn		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.335809946 CET	81.169.136.222	192.168.2.23	0x3f77	No error (0)	catlovingfools.geek		185.72.8.231	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.335809946 CET	81.169.136.222	192.168.2.23	0x3f77	No error (0)	catlovingfools.geek		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.335809946 CET	81.169.136.222	192.168.2.23	0x3f77	No error (0)	catlovingfools.geek		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.335809946 CET	81.169.136.222	192.168.2.23	0x3f77	No error (0)	catlovingfools.geek		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.335809946 CET	81.169.136.222	192.168.2.23	0x3f77	No error (0)	catlovingfools.geek		212.192.13.95	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.335809946 CET	81.169.136.222	192.168.2.23	0x3f77	No error (0)	catlovingfools.geek		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.335809946 CET	81.169.136.222	192.168.2.23	0x3f77	No error (0)	catlovingfools.geek		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.339787006 CET	81.169.136.222	192.168.2.23	0x3f77	No error (0)	catlovingfools.geek		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.339787006 CET	81.169.136.222	192.168.2.23	0x3f77	No error (0)	catlovingfools.geek		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.339787006 CET	81.169.136.222	192.168.2.23	0x3f77	No error (0)	catlovingfools.geek		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.339787006 CET	81.169.136.222	192.168.2.23	0x3f77	No error (0)	catlovingfools.geek		185.72.8.231	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.339787006 CET	81.169.136.222	192.168.2.23	0x3f77	No error (0)	catlovingfools.geek		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.339787006 CET	81.169.136.222	192.168.2.23	0x3f77	No error (0)	catlovingfools.geek		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:18.339787006 CET	81.169.136.222	192.168.2.23	0x3f77	No error (0)	catlovingfools.geek		212.192.13.95	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:25.301016092 CET	152.53.15.127	192.168.2.23	0x10ba	Format error (1)	catlovingfools.geek. [malformed]	none	none	256	413	false
Dec 21, 2024 04:27:25.787631989 CET	152.53.15.127	192.168.2.23	0x6ac6	Format error (1)	catvision.dyn. [malformed]	none	none	256	413	false
Dec 21, 2024 04:27:26.183645010 CET	152.53.15.127	192.168.2.23	0x6ac6	Format error (1)	hikvision.geek. [malformed]	none	none	256	414	false
Dec 21, 2024 04:27:26.237559080 CET	152.53.15.127	192.168.2.23	0x6ac6	Format error (1)	hikvision.geek. [malformed]	none	none	256	414	false
Dec 21, 2024 04:27:26.427337885 CET	194.36.144.87	192.168.2.23	0x11b0	Format error (1)	catlovingfools.geek. [malformed]	none	none	256	414	false
Dec 21, 2024 04:27:26.482506990 CET	194.36.144.87	192.168.2.23	0x11b0	Format error (1)	catlovingfools.geek. [malformed]	none	none	256	414	false
Dec 21, 2024 04:27:27.910937071 CET	51.158.108.203	192.168.2.23	0xcee8	No error (0)	hikvision.geek		185.72.8.231	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 21, 2024 04:27:27.910937071 CET	51.158.108.203	192.168.2.23	0xcee8	No error (0)	hikvision.geek		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:27.910937071 CET	51.158.108.203	192.168.2.23	0xcee8	No error (0)	hikvision.geek		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:27.910937071 CET	51.158.108.203	192.168.2.23	0xcee8	No error (0)	hikvision.geek		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:27.910937071 CET	51.158.108.203	192.168.2.23	0xcee8	No error (0)	hikvision.geek		212.192.13.95	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:27.910937071 CET	51.158.108.203	192.168.2.23	0xcee8	No error (0)	hikvision.geek		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:27.910937071 CET	51.158.108.203	192.168.2.23	0xcee8	No error (0)	hikvision.geek		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:27.963170052 CET	51.158.108.203	192.168.2.23	0xcee8	No error (0)	hikvision.geek		185.72.8.231	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:27.963170052 CET	51.158.108.203	192.168.2.23	0xcee8	No error (0)	hikvision.geek		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:27.963170052 CET	51.158.108.203	192.168.2.23	0xcee8	No error (0)	hikvision.geek		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:27.963170052 CET	51.158.108.203	192.168.2.23	0xcee8	No error (0)	hikvision.geek		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:27.963170052 CET	51.158.108.203	192.168.2.23	0xcee8	No error (0)	hikvision.geek		212.192.13.95	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:27.963170052 CET	51.158.108.203	192.168.2.23	0xcee8	No error (0)	hikvision.geek		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:27.963170052 CET	51.158.108.203	192.168.2.23	0xcee8	No error (0)	hikvision.geek		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:32.533533096 CET	194.36.144.87	192.168.2.23	0x11b0	No error (0)	hikvision.geek		185.72.8.231	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:32.533533096 CET	194.36.144.87	192.168.2.23	0x11b0	No error (0)	hikvision.geek		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:32.533533096 CET	194.36.144.87	192.168.2.23	0x11b0	No error (0)	hikvision.geek		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:32.533533096 CET	194.36.144.87	192.168.2.23	0x11b0	No error (0)	hikvision.geek		212.192.13.95	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:32.533533096 CET	194.36.144.87	192.168.2.23	0x11b0	No error (0)	hikvision.geek		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:32.533533096 CET	194.36.144.87	192.168.2.23	0x11b0	No error (0)	hikvision.geek		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:32.533533096 CET	194.36.144.87	192.168.2.23	0x11b0	No error (0)	hikvision.geek		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:45.585400105 CET	213.202.211.221	192.168.2.23	0x6149	No error (0)	catlovingfools.geek		212.192.13.95	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:45.585400105 CET	213.202.211.221	192.168.2.23	0x6149	No error (0)	catlovingfools.geek		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:45.585400105 CET	213.202.211.221	192.168.2.23	0x6149	No error (0)	catlovingfools.geek		185.72.8.231	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:45.585400105 CET	213.202.211.221	192.168.2.23	0x6149	No error (0)	catlovingfools.geek		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:45.585400105 CET	213.202.211.221	192.168.2.23	0x6149	No error (0)	catlovingfools.geek		86.107.100.19	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 21, 2024 04:27:45.585400105 CET	213.202.211.221	192.168.2.23	0x6149	No error (0)	catlovingfools.geek		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:45.585400105 CET	213.202.211.221	192.168.2.23	0x6149	No error (0)	catlovingfools.geek		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:55.185673952 CET	152.53.15.127	192.168.2.23	0xec9b	No error (0)	shitrocket.dyn		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:55.185673952 CET	152.53.15.127	192.168.2.23	0xec9b	No error (0)	shitrocket.dyn		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:55.185673952 CET	152.53.15.127	192.168.2.23	0xec9b	No error (0)	shitrocket.dyn		212.192.13.95	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:55.185673952 CET	152.53.15.127	192.168.2.23	0xec9b	No error (0)	shitrocket.dyn		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:55.185673952 CET	152.53.15.127	192.168.2.23	0xec9b	No error (0)	shitrocket.dyn		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:55.185673952 CET	152.53.15.127	192.168.2.23	0xec9b	No error (0)	shitrocket.dyn		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:55.185673952 CET	152.53.15.127	192.168.2.23	0xec9b	No error (0)	shitrocket.dyn		185.72.8.231	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:55.245457888 CET	152.53.15.127	192.168.2.23	0xec9b	No error (0)	shitrocket.dyn		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:55.245457888 CET	152.53.15.127	192.168.2.23	0xec9b	No error (0)	shitrocket.dyn		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:55.245457888 CET	152.53.15.127	192.168.2.23	0xec9b	No error (0)	shitrocket.dyn		212.192.13.95	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:55.245457888 CET	152.53.15.127	192.168.2.23	0xec9b	No error (0)	shitrocket.dyn		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:55.245457888 CET	152.53.15.127	192.168.2.23	0xec9b	No error (0)	shitrocket.dyn		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:55.245457888 CET	152.53.15.127	192.168.2.23	0xec9b	No error (0)	shitrocket.dyn		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:27:55.245457888 CET	152.53.15.127	192.168.2.23	0xec9b	No error (0)	shitrocket.dyn		185.72.8.231	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:00.127276897 CET	51.158.108.203	192.168.2.23	0xcee8	Format error (1)	hikvision.geek.[malformed]	none	none	256	448	false
Dec 21, 2024 04:28:00.375998974 CET	194.36.144.87	192.168.2.23	0xfa80	Format error (1)	catvision.dyn.[malformed]	none	none	256	448	false
Dec 21, 2024 04:28:00.633162022 CET	81.169.136.222	192.168.2.23	0xfbf6	No error (0)	shitrocket.dyn		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:00.633162022 CET	81.169.136.222	192.168.2.23	0xfbf6	No error (0)	shitrocket.dyn		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:00.633162022 CET	81.169.136.222	192.168.2.23	0xfbf6	No error (0)	shitrocket.dyn		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:00.633162022 CET	81.169.136.222	192.168.2.23	0xfbf6	No error (0)	shitrocket.dyn		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:00.633162022 CET	81.169.136.222	192.168.2.23	0xfbf6	No error (0)	shitrocket.dyn		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:00.633162022 CET	81.169.136.222	192.168.2.23	0xfbf6	No error (0)	shitrocket.dyn		212.192.13.95	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:00.633162022 CET	81.169.136.222	192.168.2.23	0xfbf6	No error (0)	shitrocket.dyn		185.72.8.231	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 21, 2024 04:28:02.443694115 CET	168.235.111.72	192.168.2.23	0x65bc	No error (0)	shitrocket.dyn		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.443694115 CET	168.235.111.72	192.168.2.23	0x65bc	No error (0)	shitrocket.dyn		185.72.8.231	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.443694115 CET	168.235.111.72	192.168.2.23	0x65bc	No error (0)	shitrocket.dyn		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.443694115 CET	168.235.111.72	192.168.2.23	0x65bc	No error (0)	shitrocket.dyn		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.443694115 CET	168.235.111.72	192.168.2.23	0x65bc	No error (0)	shitrocket.dyn		212.192.13.95	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.443694115 CET	168.235.111.72	192.168.2.23	0x65bc	No error (0)	shitrocket.dyn		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.443694115 CET	168.235.111.72	192.168.2.23	0x65bc	No error (0)	shitrocket.dyn		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.507653952 CET	168.235.111.72	192.168.2.23	0x65bc	No error (0)	shitrocket.dyn		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.507653952 CET	168.235.111.72	192.168.2.23	0x65bc	No error (0)	shitrocket.dyn		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.507653952 CET	168.235.111.72	192.168.2.23	0x65bc	No error (0)	shitrocket.dyn		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.507653952 CET	168.235.111.72	192.168.2.23	0x65bc	No error (0)	shitrocket.dyn		185.72.8.231	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.507653952 CET	168.235.111.72	192.168.2.23	0x65bc	No error (0)	shitrocket.dyn		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.507653952 CET	168.235.111.72	192.168.2.23	0x65bc	No error (0)	shitrocket.dyn		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:02.507653952 CET	168.235.111.72	192.168.2.23	0x65bc	No error (0)	shitrocket.dyn		212.192.13.95	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:07.925062895 CET	81.169.136.222	192.168.2.23	0xb2a0	No error (0)	shitrocket.dyn		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:07.925062895 CET	81.169.136.222	192.168.2.23	0xb2a0	No error (0)	shitrocket.dyn		185.72.8.231	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:07.925062895 CET	81.169.136.222	192.168.2.23	0xb2a0	No error (0)	shitrocket.dyn		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:07.925062895 CET	81.169.136.222	192.168.2.23	0xb2a0	No error (0)	shitrocket.dyn		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:07.925062895 CET	81.169.136.222	192.168.2.23	0xb2a0	No error (0)	shitrocket.dyn		212.192.13.95	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:07.925062895 CET	81.169.136.222	192.168.2.23	0xb2a0	No error (0)	shitrocket.dyn		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:07.925062895 CET	81.169.136.222	192.168.2.23	0xb2a0	No error (0)	shitrocket.dyn		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:10.491585016 CET	109.91.184.21	192.168.2.23	0xd70	No error (0)	shitrocket.dyn		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:10.491585016 CET	109.91.184.21	192.168.2.23	0xd70	No error (0)	shitrocket.dyn		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:10.491585016 CET	109.91.184.21	192.168.2.23	0xd70	No error (0)	shitrocket.dyn		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:10.491585016 CET	109.91.184.21	192.168.2.23	0xd70	No error (0)	shitrocket.dyn		212.192.13.95	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 21, 2024 04:28:10.491585016 CET	109.91.184.21	192.168.2.23	0xd70	No error (0)	shitrocket.dyn		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:10.491585016 CET	109.91.184.21	192.168.2.23	0xd70	No error (0)	shitrocket.dyn		185.72.8.231	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:10.491585016 CET	109.91.184.21	192.168.2.23	0xd70	No error (0)	shitrocket.dyn		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:12.846244097 CET	194.36.144.87	192.168.2.23	0x5232	Format error (1)	hikvision.geek.[malformed]	none	none	256	460	false
Dec 21, 2024 04:28:13.094410896 CET	152.53.15.127	192.168.2.23	0x405a	Format error (1)	catvision.dyn.[malformed]	none	none	256	461	false
Dec 21, 2024 04:28:13.335596085 CET	51.158.108.203	192.168.2.23	0xfee0	Format error (1)	catlovingfools.geek.[malformed]	none	none	256	461	false
Dec 21, 2024 04:28:21.244559050 CET	109.91.184.21	192.168.2.23	0xd70	Format error (1)	catvision.dyn.[malformed]	none	none	256	469	false
Dec 21, 2024 04:28:37.745575905 CET	81.169.136.222	192.168.2.23	0xc7f7	No error (0)	shitrocket.dyn		176.32.32.113	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:37.745575905 CET	81.169.136.222	192.168.2.23	0xc7f7	No error (0)	shitrocket.dyn		185.72.8.231	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:37.745575905 CET	81.169.136.222	192.168.2.23	0xc7f7	No error (0)	shitrocket.dyn		212.192.13.95	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:37.745575905 CET	81.169.136.222	192.168.2.23	0xc7f7	No error (0)	shitrocket.dyn		86.107.100.19	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:37.745575905 CET	81.169.136.222	192.168.2.23	0xc7f7	No error (0)	shitrocket.dyn		80.78.26.121	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:37.745575905 CET	81.169.136.222	192.168.2.23	0xc7f7	No error (0)	shitrocket.dyn		212.64.215.71	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:37.745575905 CET	81.169.136.222	192.168.2.23	0xc7f7	No error (0)	shitrocket.dyn		212.60.5.153	A (IP address)	IN (0x0001)	false
Dec 21, 2024 04:28:41.340818882 CET	51.158.108.203	192.168.2.23	0xcee8	Format error (1)	hikvision.geek.[malformed]	none	none	256	489	false
Dec 21, 2024 04:28:41.587431908 CET	194.36.144.87	192.168.2.23	0xfa80	Format error (1)	catlovingfools.geek.[malformed]	none	none	256	489	false

System Behavior

Analysis Process: hmips.elf PID: **6240**, Parent PID: **6165**

General

Start time (UTC):	03:26:54
Start date (UTC):	21/12/2024
Path:	/tmp/hmips.elf
Arguments:	/tmp/hmips.elf
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: hmips.elf PID: **6242**, Parent PID: **6240**

General	
Start time (UTC):	03:26:54
Start date (UTC):	21/12/2024
Path:	/tmp/hmips.elf
Arguments:	-
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: hmips.elf PID: **6298**, Parent PID: **6242**

General	
Start time (UTC):	03:26:55
Start date (UTC):	21/12/2024
Path:	/tmp/hmips.elf
Arguments:	-
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: hmips.elf PID: **6308**, Parent PID: **6298**

General	
Start time (UTC):	03:26:55
Start date (UTC):	21/12/2024
Path:	/tmp/hmips.elf
Arguments:	-
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: hmips.elf PID: **6315**, Parent PID: **6308**

General	
Start time (UTC):	03:26:55
Start date (UTC):	21/12/2024
Path:	/tmp/hmips.elf
Arguments:	-
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: hmips.elf PID: **6244**, Parent PID: **6240**

General	
Start time (UTC):	03:26:54
Start date (UTC):	21/12/2024
Path:	/tmp/hmips.elf
Arguments:	-
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: hmips.elf PID: **6268**, Parent PID: **6244**

General	
Start time (UTC):	03:26:54
Start date (UTC):	21/12/2024
Path:	/tmp/hmips.elf
Arguments:	-
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: hmips.elf PID: **6270**, Parent PID: **6268**

General	
Start time (UTC):	03:26:54
Start date (UTC):	21/12/2024
Path:	/tmp/hmips.elf
Arguments:	-
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c