Remcos RAT threat analysis on Windows including, surprisingly enough, IEC 60870-5-104 traffic.

Michał Sołtysik
Cybersecurity Consultant

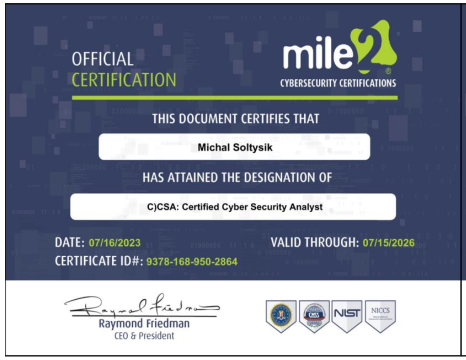
Specializing in deep packet inspection (i.e. network edge profiling and 0-day attacks).

To date, he has identified 253 protocols in the IT, OT and IoT areas used for cyber attacks.

Additionally, a Digital and Network Forensics Examiner, CyberWarfare Organizer and SOC Trainer.

C)CSA - Certified Cyber Security Analyst
C)NFE - Certified Network Forensics Examiner
C)DFE - Certified Digital Forensics Examiner
WCNA - Wireshark Certified Network Analyst
C)PTC - Certified Penetration Testing Consultant
C)PEH - Certified Professional Ethical Hacker
C)VA - Certified Vulnerability Assessor

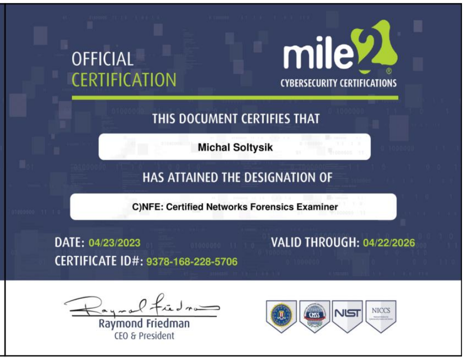
C)CSA - Certified Cyber Security Analyst
C)NFE - Certified Network Forensics Examiner
C)DFE - Certified Digital Forensics Examiner
WCNA - Wireshark Certified Network Analyst
C)PTC - Certified Penetration Testing Consultant
C)PEH - Certified Professional Ethical Hacker
C)VA - Certified Vulnerability Assessor


OFFICIAL
CERTIFICATION
mile2
CYBERSECURITY CERTIFICATIONS

THIS DOCUMENT CERTIFIES THAT
Michal Soltysik
HAS ATTAINED THE DESIGNATION OF
C)CSA: Certified Cyber Security Analyst

DATE: 07/16/2023 VALID THROUGH: 07/15/2026
CERTIFICATE ID#: 9378-168-950-2864

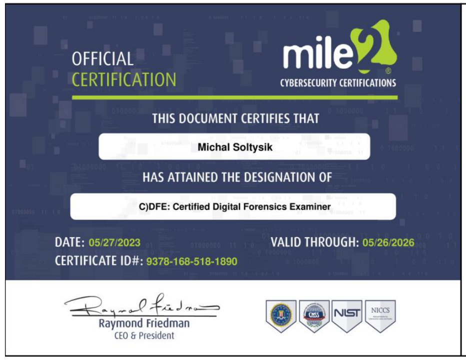
Raymond Friedman
CEO & President


OFFICIAL
CERTIFICATION
mile2
CYBERSECURITY CERTIFICATIONS

THIS DOCUMENT CERTIFIES THAT
Michal Soltysik
HAS ATTAINED THE DESIGNATION OF
C)NFE: Certified Networks Forensics Examiner

DATE: 04/23/2023 VALID THROUGH: 04/22/2026
CERTIFICATE ID#: 9378-168-228-5706

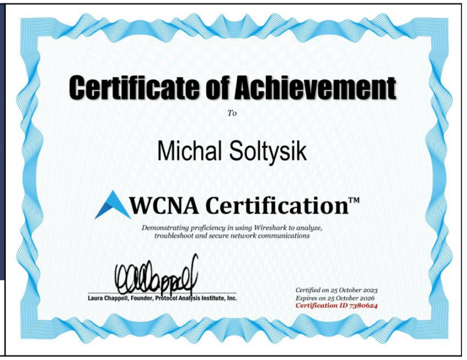
Raymond Friedman
CEO & President


OFFICIAL
CERTIFICATION
mile2
CYBERSECURITY CERTIFICATIONS

THIS DOCUMENT CERTIFIES THAT
Michal Soltysik
HAS ATTAINED THE DESIGNATION OF
C)DFE: Certified Digital Forensics Examiner

DATE: 05/27/2023 VALID THROUGH: 05/26/2026
CERTIFICATE ID#: 9378-168-518-1890

Raymond Friedman
CEO & President


Certificate of Achievement

To

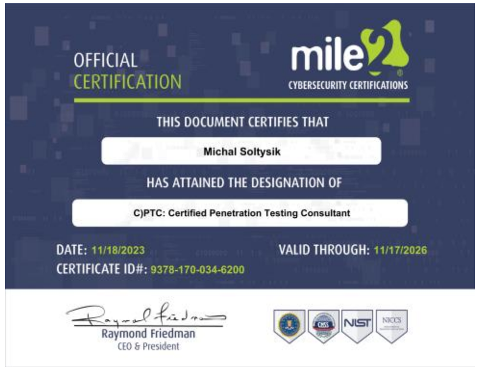
Michal Soltysik

WCNA Certification™

Demonstrating proficiency in using Wireshark to analyze, troubleshoot and secure network communications

Laura Chappell, Founder, Protocol Analysis Institute, Inc.

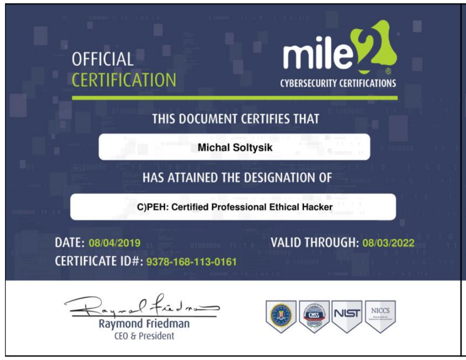
Certified on 25 October 2023
Expires on 25 October 2026
Certification ID 7380624


OFFICIAL
CERTIFICATION
mile2
CYBERSECURITY CERTIFICATIONS

THIS DOCUMENT CERTIFIES THAT
Michal Soltysik
HAS ATTAINED THE DESIGNATION OF
C)PTC: Certified Penetration Testing Consultant

DATE: 11/18/2023 VALID THROUGH: 11/17/2026
CERTIFICATE ID#: 9378-170-034-6200

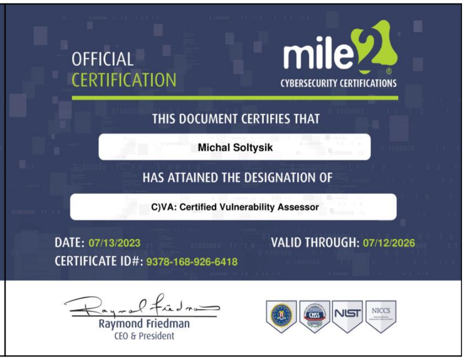
Raymond Friedman
CEO & President


OFFICIAL
CERTIFICATION
mile2
CYBERSECURITY CERTIFICATIONS

THIS DOCUMENT CERTIFIES THAT
Michal Soltysik
HAS ATTAINED THE DESIGNATION OF
C)PEH: Certified Professional Ethical Hacker

DATE: 08/04/2019 VALID THROUGH: 08/03/2022
CERTIFICATE ID#: 9378-168-113-0161

Raymond Friedman
CEO & President


OFFICIAL
CERTIFICATION
mile2
CYBERSECURITY CERTIFICATIONS

THIS DOCUMENT CERTIFIES THAT
Michal Soltysik
HAS ATTAINED THE DESIGNATION OF
C)VA: Certified Vulnerability Assessor

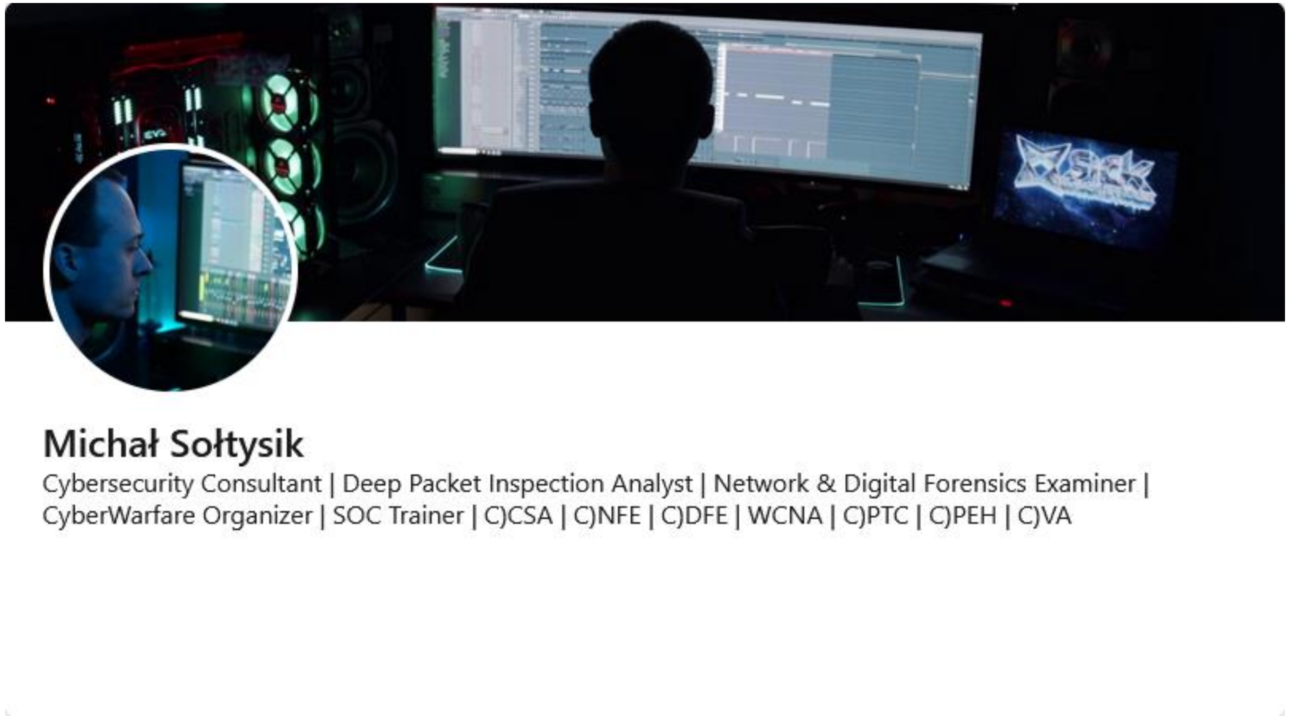
DATE: 07/13/2023 VALID THROUGH: 07/12/2026
CERTIFICATE ID#: 9378-168-926-6418

Raymond Friedman
CEO & President

Contact:

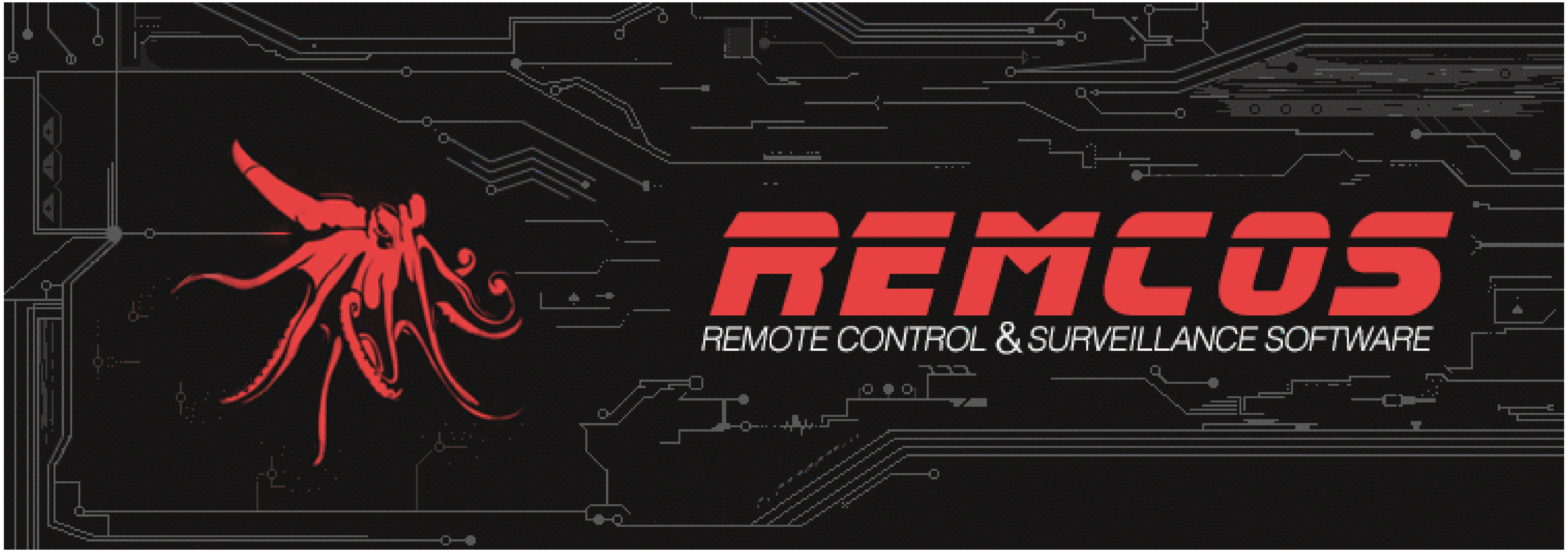
Mail: mikewavepoland@gmail.com

LinkedIn: https://www.linkedin.com/in/michal-soltysik-ssh-soc/



Michał Sołtysik

Cybersecurity Consultant | Deep Packet Inspection Analyst | Network & Digital Forensics Examiner | CyberWarfare Organizer | SOC Trainer | C)CSA | C)NFE | C)DFE | WCNA | C)PTC | C)PEH | C)VA



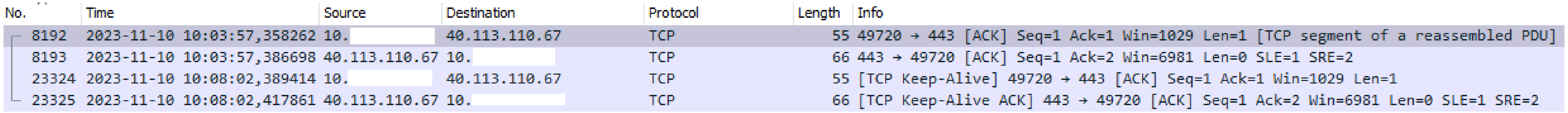
Remcos is **Remote Control and Surveillance** and **RAT** is **Remote Access Trojan.**

Genereally speaking, **Remcos** is a lightweight, fast and highly customizable **Remote Administration Tool** with a wide array of functionalities**.**

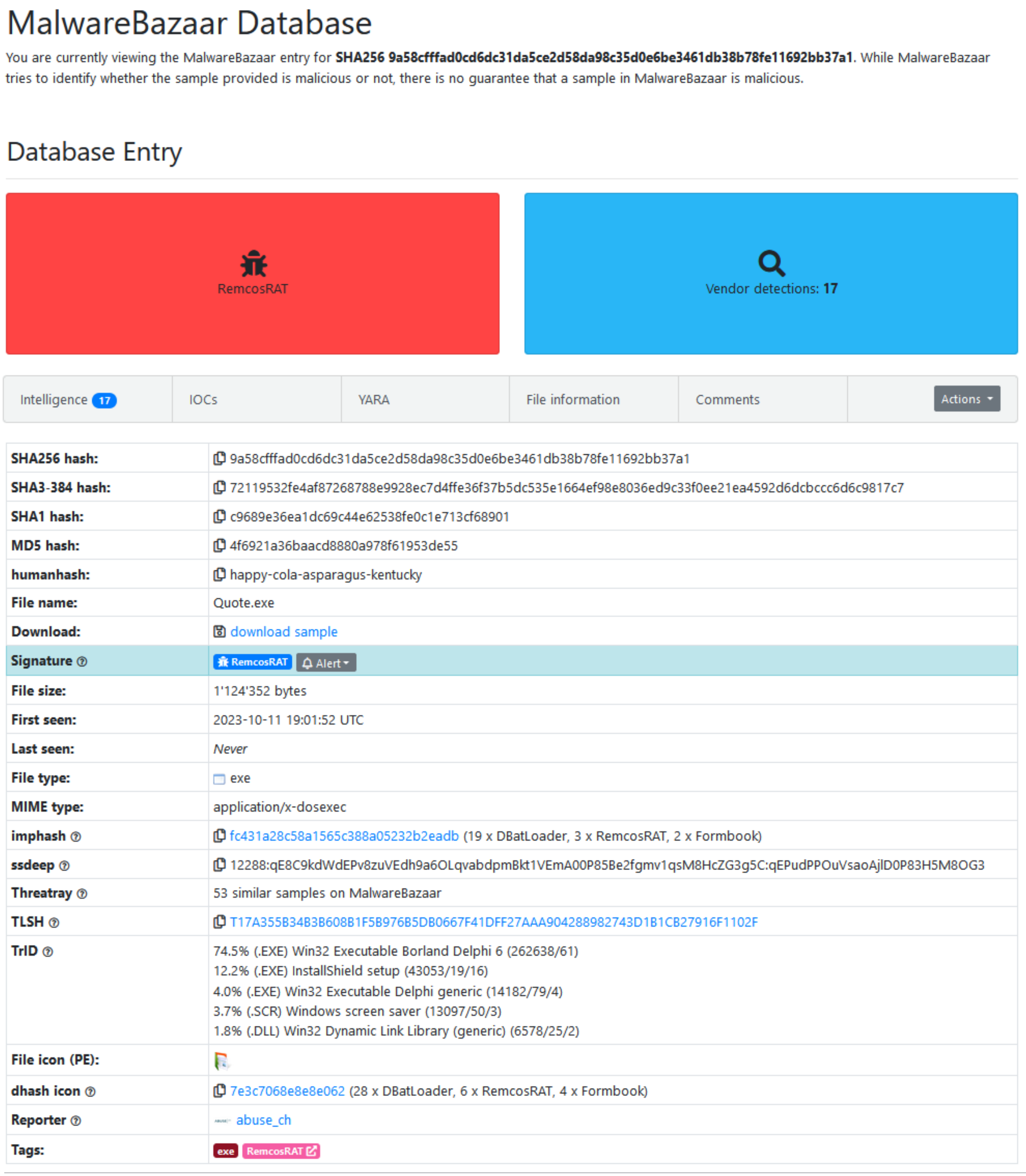
Available at: https://breakingsecurity.net/remcos/

Remcos (short for **Remote Control and Surveillance**) is a commercial system administration application for **Windows** that threat actors have weaponized. **Remcos** is a closed-source application designed for network maintenance, system monitoring, surveillance, and penetration testing, but attackers use it to exploit target systems remotely. Although the vendor **Breaking Security** claims that **Remcos** is a legitimate security tool, it has been labeled as malware by **CISA** (**Cybersecurity and Infrastructure Security Agency**), which is a component of the **United States Department of Homeland Security** (**DHS**) responsible for cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs with **U.S.** states, and improving the government's cybersecurity protections against private and nation-state hackers, and included in its list of top malware strains of 2021.

Remcos's malicious capabilities are nearly unlimited due to its robust feature set and ability to maintain persistent and high-privileged remote control of a victim's system. It is commonly used to steal credentials, for **man-in-the-middle** (**MiTM**) internet connections, and to orchestrate zombie botnets that can launch synchronized distributed **denial-of-service** (**DDoS**) attacks. **Remcos** uses a custom **TCP**-based protocol to establish encrypted connections and keepalive to maintain its **command-and-control** (**C2**) connection over unstable networks. These efficient and robust tools make **Remcos** the malware of choice for maintaining zombie botnets and proxying internet traffic on compromised hosts.



```
No.    Time                       Source          Destination      Protocol   Length Info
 8192  2023-11-10 10:03:57,358262 10.[redacted]   40.113.110.67    TCP            55 49720 → 443 [ACK] Seq=1 Ack=1 Win=1029 Len=1 [TCP segment of a reassembled PDU]
 8193  2023-11-10 10:03:57,386698 40.113.110.67   10.[redacted]    TCP            66 443 → 49720 [ACK] Seq=1 Ack=2 Win=6981 Len=0 SLE=1 SRE=2
23324  2023-11-10 10:08:02,389414 10.[redacted]   40.113.110.67    TCP            55 [TCP Keep-Alive] 49720 → 443 [ACK] Seq=1 Ack=1 Win=1029 Len=1
23325  2023-11-10 10:08:02,417861 40.113.110.67   10.[redacted]    TCP            66 [TCP Keep-Alive ACK] 443 → 49720 [ACK] Seq=1 Ack=2 Win=6981 Len=0 SLE=1 SRE=2
```



MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for **SHA256 9a58cfffad0cd6dc31da5ce2d58da98c35d0e6be3461db38b78fe11692bb37a1**. While MalwareBazaar tries to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

Database Entry

RemcosRAT

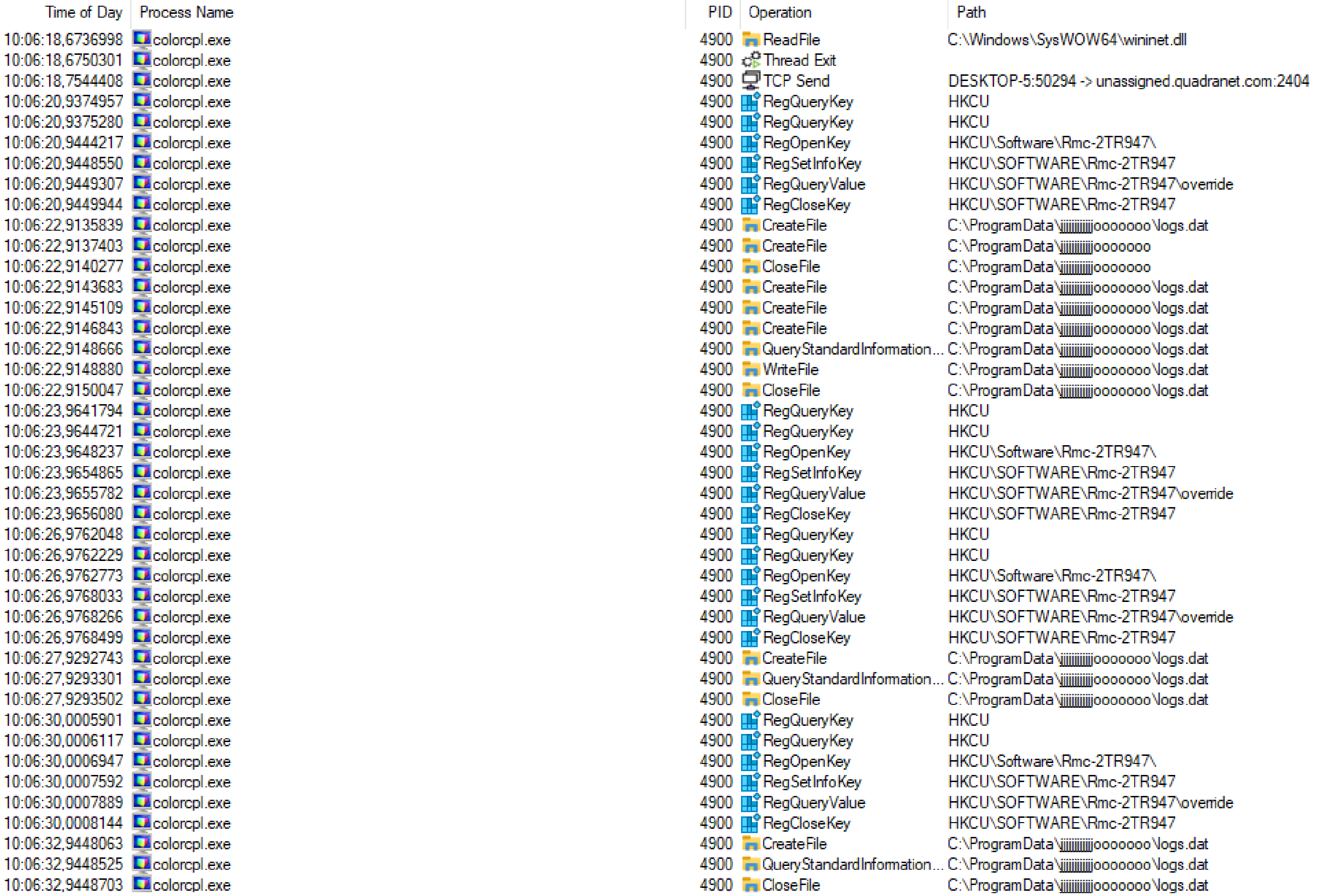
Vendor detections: **17**

SHA256 hash:	9a58cfffad0cd6dc31da5ce2d58da98c35d0e6be3461db38b78fe11692bb37a1
SHA3-384 hash:	72119532fe4af87268788e9928ec7d4ffe36f37b5dc535e1664ef98e8036ed9c33f0ee21ea4592d6dcbccc6d6c9817c7
SHA1 hash:	c9689e36ea1dc69c44e62538fe0c1e713cf68901
MD5 hash:	4f6921a36baacd8880a978f61953de55
humanhash:	happy-cola-asparagus-kentucky
File name:	Quote.exe
Download:	download sample
Signature	RemcosRAT Alert
File size:	1'124'352 bytes
First seen:	2023-10-11 19:01:52 UTC
Last seen:	*Never*
File type:	exe
MIME type:	application/x-dosexec
imphash	fc431a28c58a1565c388a05232b2eadb (19 x DBatLoader, 3 x RemcosRAT, 2 x Formbook)
ssdeep	12288:qE8C9kdWdEPv8zuVEdh9a6OLqvabdpmBkt1VEmA00P85Be2fgmv1qsM8HcZG3g5C:qEPudPPOuVsaoAjlD0P83H5M8OG3
Threatray	53 similar samples on MalwareBazaar
TLSH	T17A355B34B3B608B1F5B976B5DB0667F41DFF27AAA904288982743D1B1CB27916F1102F
TrID	74.5% (.EXE) Win32 Executable Borland Delphi 6 (262638/61) 12.2% (.EXE) InstallShield setup (43053/19/16) 4.0% (.EXE) Win32 Executable Delphi generic (14182/79/4) 3.7% (.SCR) Windows screen saver (13097/50/3) 1.8% (.DLL) Win32 Dynamic Link Library (generic) (6578/25/2)
File icon (PE):	
dhash icon	7e3c7068e8e8e062 (28 x DBatLoader, 6 x RemcosRAT, 4 x Formbook)
Reporter	abuse_ch
Tags:	exe RemcosRAT

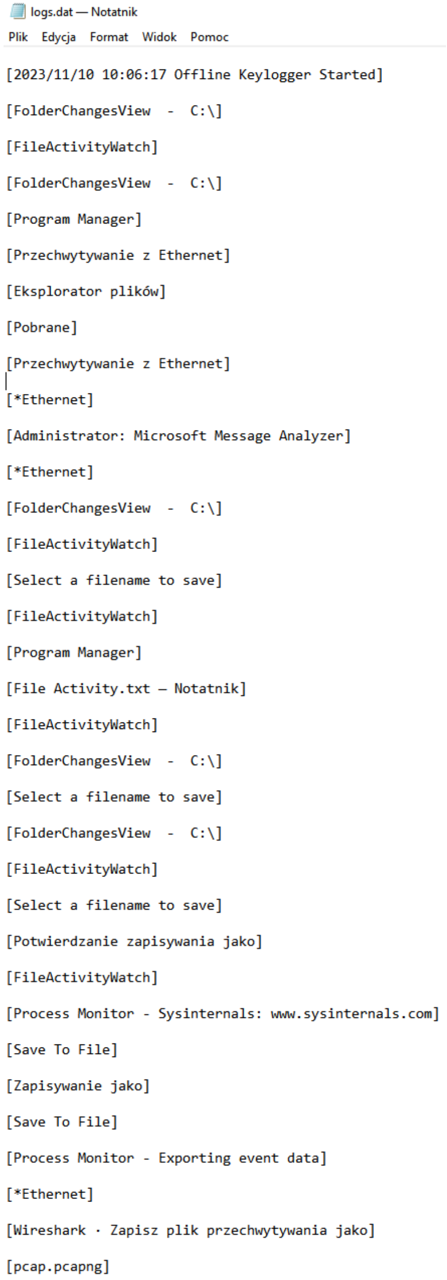
ΛBUSE | ch

MALWARE bazaar by ΛBUSE | ch

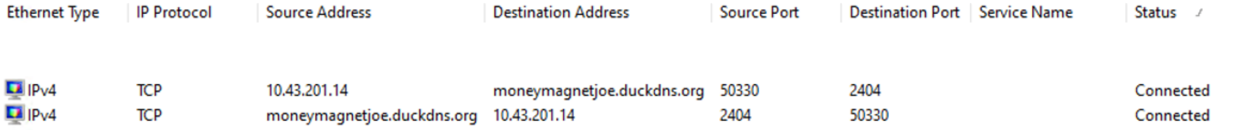
URLhaus by ΛBUSE | ch



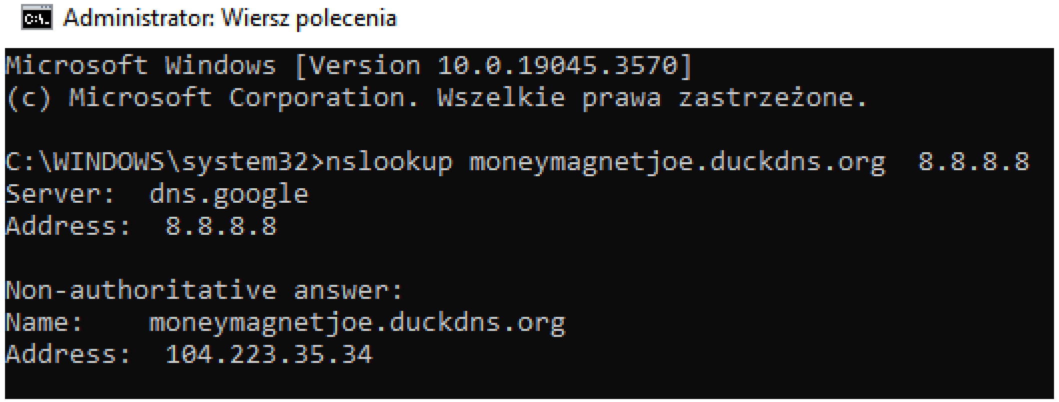
Time of Day	Process Name	PID	Operation	Path
10:06:18,6736998	colorcpl.exe	4900	ReadFile	C:\Windows\SysWOW64\wininet.dll
10:06:18,6750301	colorcpl.exe	4900	Thread Exit	
10:06:18,7544408	colorcpl.exe	4900	TCP Send	DESKTOP-5:50294 -> unassigned.quadranet.com:2404
10:06:20,9374957	colorcpl.exe	4900	RegQueryKey	HKCU
10:06:20,9375280	colorcpl.exe	4900	RegQueryKey	HKCU
10:06:20,9444217	colorcpl.exe	4900	RegOpenKey	HKCU\Software\Rmc-2TR947\
10:06:20,9448550	colorcpl.exe	4900	RegSetInfoKey	HKCU\SOFTWARE\Rmc-2TR947
10:06:20,9449307	colorcpl.exe	4900	RegQueryValue	HKCU\SOFTWARE\Rmc-2TR947\override
10:06:20,9449944	colorcpl.exe	4900	RegCloseKey	HKCU\SOFTWARE\Rmc-2TR947
10:06:22,9135839	colorcpl.exe	4900	CreateFile	C:\ProgramData\jjjjjjjjjjoooooooo\logs.dat
10:06:22,9137403	colorcpl.exe	4900	CreateFile	C:\ProgramData\jjjjjjjjjjoooooooo
10:06:22,9140277	colorcpl.exe	4900	CloseFile	C:\ProgramData\jjjjjjjjjjoooooooo
10:06:22,9143683	colorcpl.exe	4900	CreateFile	C:\ProgramData\jjjjjjjjjjoooooooo\logs.dat
10:06:22,9145109	colorcpl.exe	4900	CreateFile	C:\ProgramData\jjjjjjjjjjoooooooo\logs.dat
10:06:22,9146843	colorcpl.exe	4900	CreateFile	C:\ProgramData\jjjjjjjjjjoooooooo\logs.dat
10:06:22,9148666	colorcpl.exe	4900	QueryStandardInformation...	C:\ProgramData\jjjjjjjjjjoooooooo\logs.dat
10:06:22,9148880	colorcpl.exe	4900	WriteFile	C:\ProgramData\jjjjjjjjjjoooooooo\logs.dat
10:06:22,9150047	colorcpl.exe	4900	CloseFile	C:\ProgramData\jjjjjjjjjjoooooooo\logs.dat
10:06:23,9641794	colorcpl.exe	4900	RegQueryKey	HKCU
10:06:23,9644721	colorcpl.exe	4900	RegQueryKey	HKCU
10:06:23,9648237	colorcpl.exe	4900	RegOpenKey	HKCU\Software\Rmc-2TR947\
10:06:23,9654865	colorcpl.exe	4900	RegSetInfoKey	HKCU\SOFTWARE\Rmc-2TR947
10:06:23,9655782	colorcpl.exe	4900	RegQueryValue	HKCU\SOFTWARE\Rmc-2TR947\override
10:06:23,9656080	colorcpl.exe	4900	RegCloseKey	HKCU\SOFTWARE\Rmc-2TR947
10:06:26,9762048	colorcpl.exe	4900	RegQueryKey	HKCU
10:06:26,9762229	colorcpl.exe	4900	RegQueryKey	HKCU
10:06:26,9762773	colorcpl.exe	4900	RegOpenKey	HKCU\Software\Rmc-2TR947\
10:06:26,9768033	colorcpl.exe	4900	RegSetInfoKey	HKCU\SOFTWARE\Rmc-2TR947
10:06:26,9768266	colorcpl.exe	4900	RegQueryValue	HKCU\SOFTWARE\Rmc-2TR947\override
10:06:26,9768499	colorcpl.exe	4900	RegCloseKey	HKCU\SOFTWARE\Rmc-2TR947
10:06:27,9292743	colorcpl.exe	4900	CreateFile	C:\ProgramData\jjjjjjjjjjoooooooo\logs.dat
10:06:27,9293301	colorcpl.exe	4900	QueryStandardInformation...	C:\ProgramData\jjjjjjjjjjoooooooo\logs.dat
10:06:27,9293502	colorcpl.exe	4900	CloseFile	C:\ProgramData\jjjjjjjjjjoooooooo\logs.dat
10:06:30,0005901	colorcpl.exe	4900	RegQueryKey	HKCU
10:06:30,0006117	colorcpl.exe	4900	RegQueryKey	HKCU
10:06:30,0006947	colorcpl.exe	4900	RegOpenKey	HKCU\Software\Rmc-2TR947\
10:06:30,0007592	colorcpl.exe	4900	RegSetInfoKey	HKCU\SOFTWARE\Rmc-2TR947
10:06:30,0007889	colorcpl.exe	4900	RegQueryValue	HKCU\SOFTWARE\Rmc-2TR947\override
10:06:30,0008144	colorcpl.exe	4900	RegCloseKey	HKCU\SOFTWARE\Rmc-2TR947
10:06:32,9448063	colorcpl.exe	4900	CreateFile	C:\ProgramData\jjjjjjjjjjoooooooo\logs.dat
10:06:32,9448525	colorcpl.exe	4900	QueryStandardInformation...	C:\ProgramData\jjjjjjjjjjoooooooo\logs.dat
10:06:32,9448703	colorcpl.exe	4900	CloseFile	C:\ProgramData\jjjjjjjjjjoooooooo\logs.dat



```
[2023/11/10 10:06:17 Offline Keylogger Started]

[FolderChangesView  -  C:\]

[FileActivityWatch]

[FolderChangesView  -  C:\]

[Program Manager]

[Przechwytywanie z Ethernet]

[Eksplorator plików]

[Pobrane]

[Przechwytywanie z Ethernet]

[*Ethernet]

[Administrator: Microsoft Message Analyzer]

[*Ethernet]

[FolderChangesView  -  C:\]

[FileActivityWatch]

[Select a filename to save]

[FileActivityWatch]

[Program Manager]

[File Activity.txt – Notatnik]

[FileActivityWatch]

[FolderChangesView  -  C:\]

[Select a filename to save]

[FolderChangesView  -  C:\]

[FileActivityWatch]

[Select a filename to save]

[Potwierdzanie zapisywania jako]

[FileActivityWatch]

[Process Monitor - Sysinternals: www.sysinternals.com]

[Save To File]

[Zapisywanie jako]

[Save To File]

[Process Monitor - Exporting event data]

[*Ethernet]

[Wireshark · Zapisz plik przechwytywania jako]

[pcap.pcapng]
```

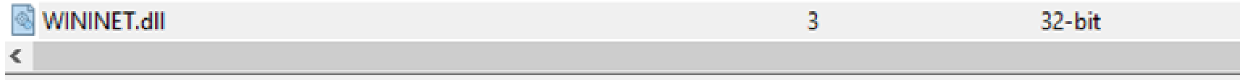


Ethernet Type	IP Protocol	Source Address	Destination Address	Source Port	Destination Port	Service Name	Status
IPv4	TCP	10.43.201.14	moneymagnetjoe.duckdns.org	50330	2404		Connected
IPv4	TCP	moneymagnetjoe.duckdns.org	10.43.201.14	2404	50330		Connected

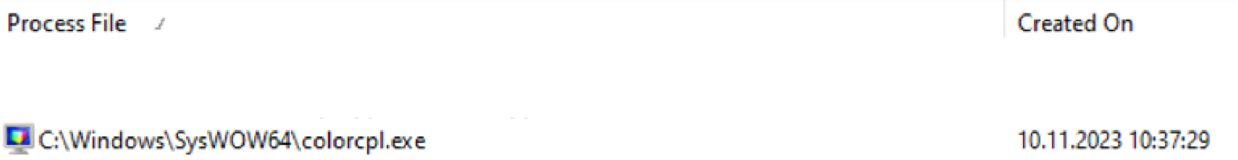


Administrator: Wiersz polecenia

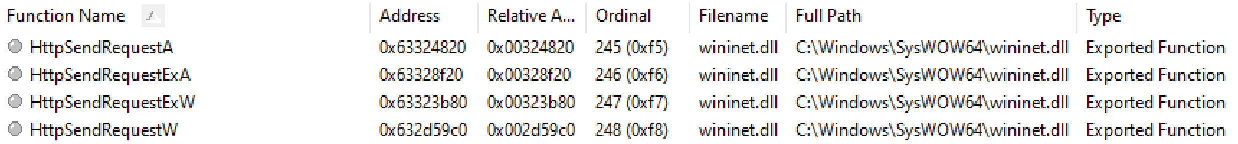
```
Microsoft Windows [Version 10.0.19045.3570]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\WINDOWS\system32>nslookup moneymagnetjoe.duckdns.org  8.8.8.8
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    moneymagnetjoe.duckdns.org
Address:  104.223.35.34
```



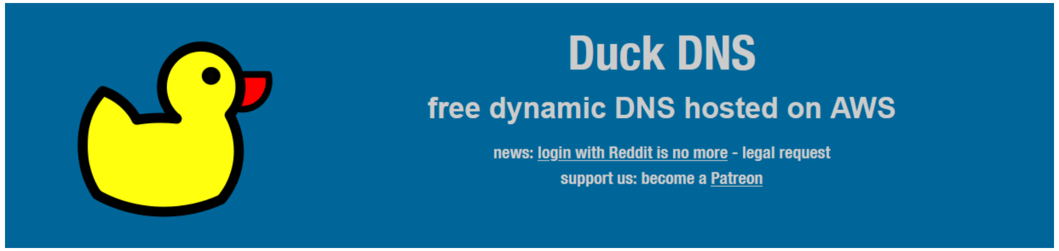
WININET.dll	3	32-bit



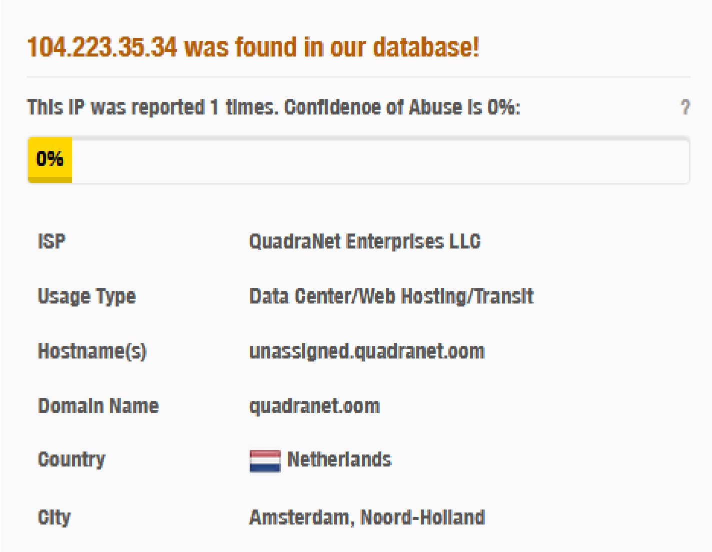
Process File	Created On
C:\Windows\SysWOW64\colorcpl.exe	10.11.2023 10:37:29



Function Name	Address	Relative A...	Ordinal	Filename	Full Path	Type
HttpSendRequestA	0x63324820	0x00324820	245 (0xf5)	wininet.dll	C:\Windows\SysWOW64\wininet.dll	Exported Function
HttpSendRequestExA	0x63328f20	0x00328f20	246 (0xf6)	wininet.dll	C:\Windows\SysWOW64\wininet.dll	Exported Function
HttpSendRequestExW	0x63323b80	0x00323b80	247 (0xf7)	wininet.dll	C:\Windows\SysWOW64\wininet.dll	Exported Function
HttpSendRequestW	0x632d59c0	0x002d59c0	248 (0xf8)	wininet.dll	C:\Windows\SysWOW64\wininet.dll	Exported Function


Duck DNS
free dynamic DNS hosted on AWS
news: login with Reddit is no more - legal request
support us: become a Patreon

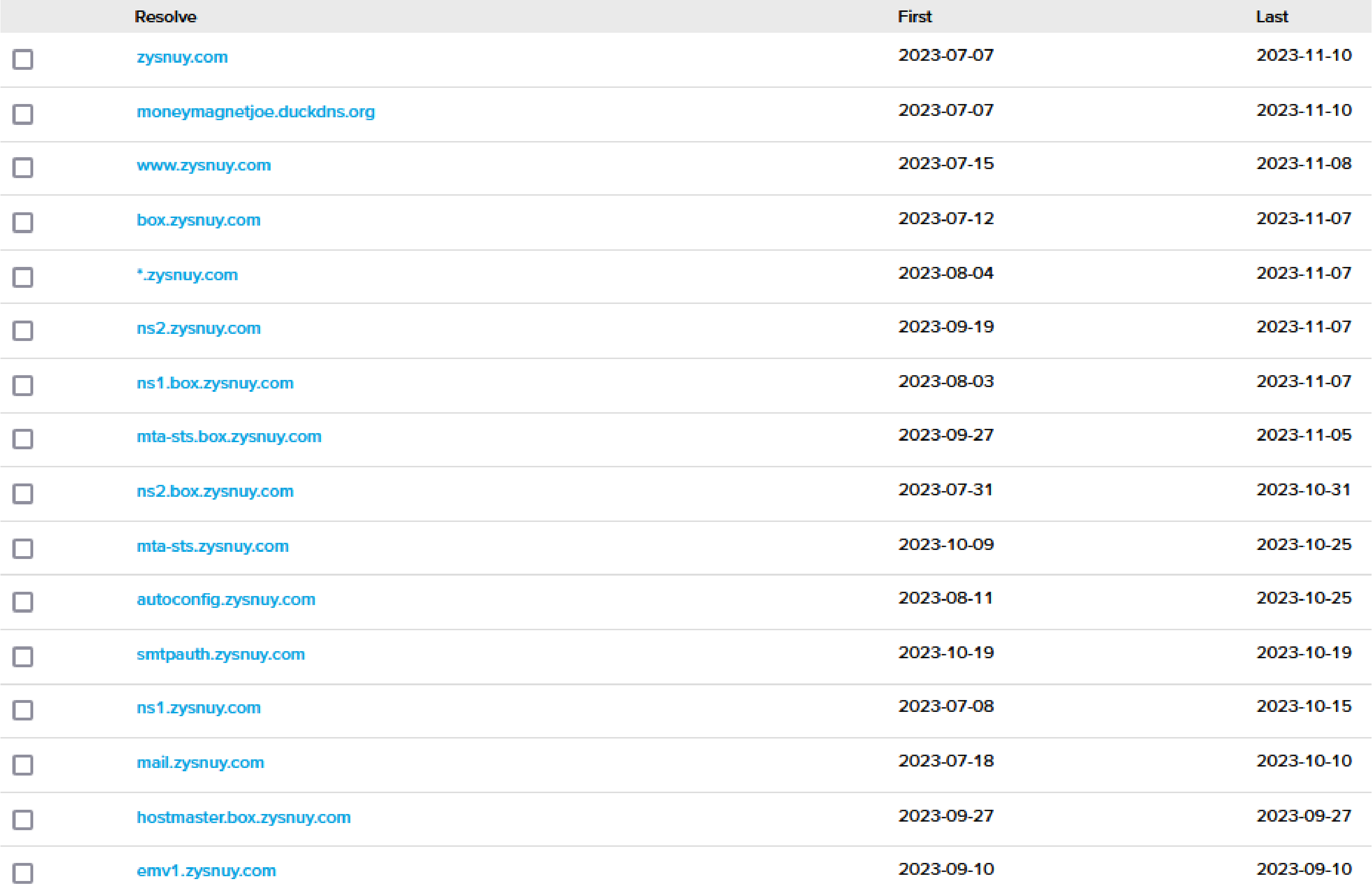
https://www.duckdns.org/



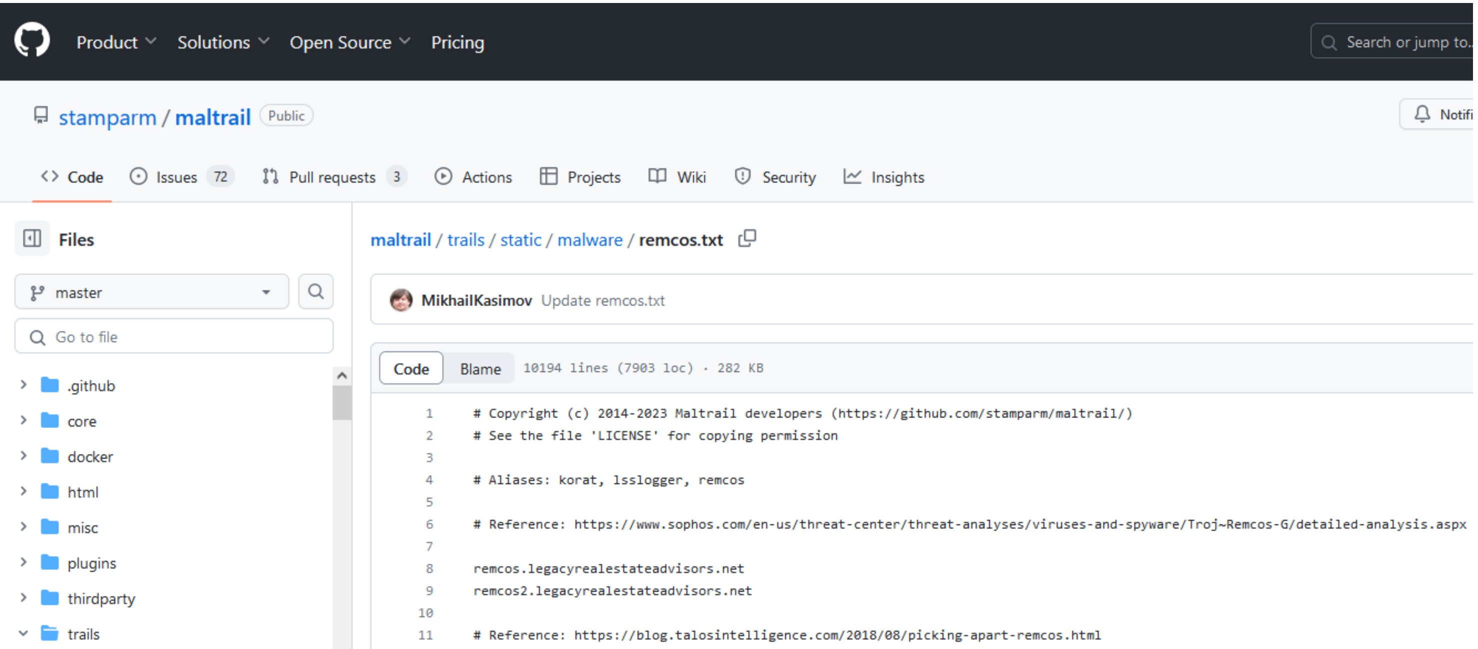
104.223.35.34 was found in our database!

This IP was reported 1 times. Confidence of Abuse is 0%:

ISP	QuadraNet Enterprises LLC
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	unassigned.quadranet.com
Domain Name	quadranet.com
Country	Netherlands
City	Amsterdam, Noord-Holland



	Resolve	First	Last
□	zysnuy.com	2023-07-07	2023-11-10
□	moneymagnetjoe.duckdns.org	2023-07-07	2023-11-10
□	www.zysnuy.com	2023-07-15	2023-11-08
□	box.zysnuy.com	2023-07-12	2023-11-07
□	*.zysnuy.com	2023-08-04	2023-11-07
□	ns2.zysnuy.com	2023-09-19	2023-11-07
□	ns1.box.zysnuy.com	2023-08-03	2023-11-07
□	mta-sts.box.zysnuy.com	2023-09-27	2023-11-05
□	ns2.box.zysnuy.com	2023-07-31	2023-10-31
□	mta-sts.zysnuy.com	2023-10-09	2023-10-25
□	autoconfig.zysnuy.com	2023-08-11	2023-10-25
□	smtpauth.zysnuy.com	2023-10-19	2023-10-19
□	ns1.zysnuy.com	2023-07-08	2023-10-15
□	mail.zysnuy.com	2023-07-18	2023-10-10
□	hostmaster.box.zysnuy.com	2023-09-27	2023-09-27
□	emv1.zysnuy.com	2023-09-10	2023-09-10

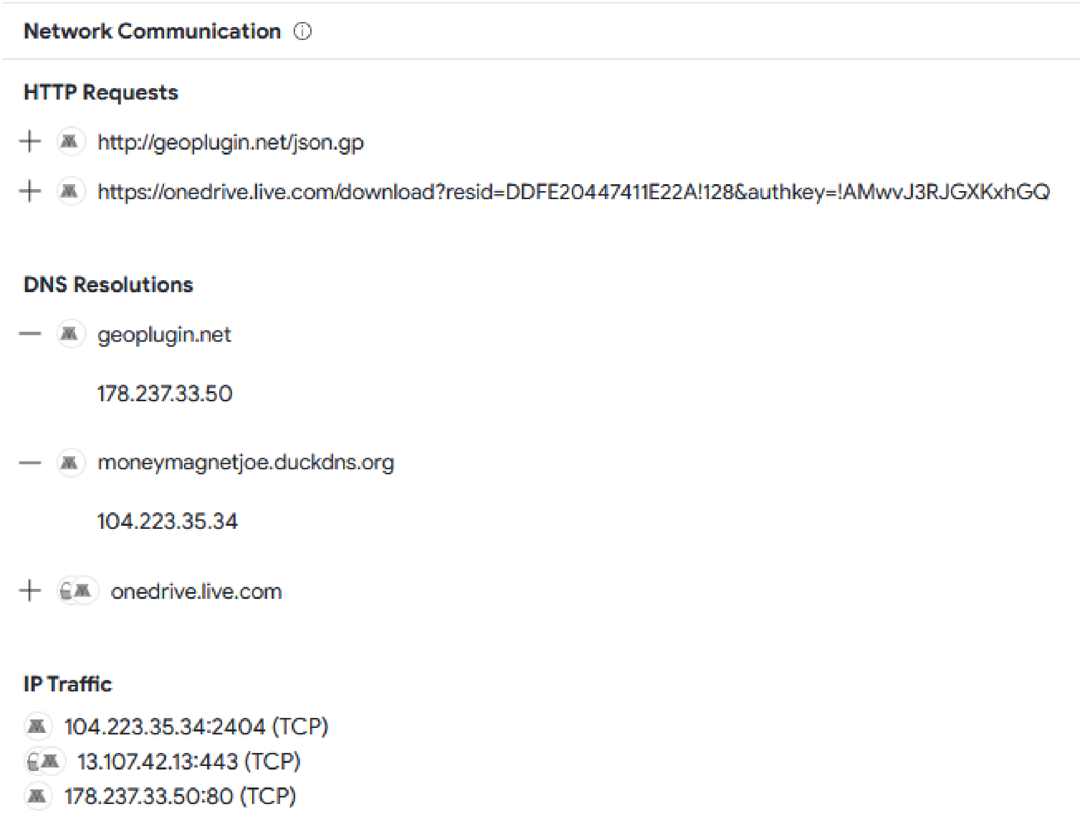


maltrail / trails / static / malware / remcos.txt

MikhailKasimov Update remcos.txt

10194 lines (7903 loc) · 282 KB

```
# Copyright (c) 2014-2023 Maltrail developers (https://github.com/stamparm/maltrail/)
# See the file 'LICENSE' for copying permission

# Aliases: korat, lsslogger, remcos

# Reference: https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Remcos-G/detailed-analysis.aspx

remcos.legacyrealestateadvisors.net
remcos2.legacyrealestateadvisors.net

# Reference: https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html
```



Network Communication

HTTP Requests

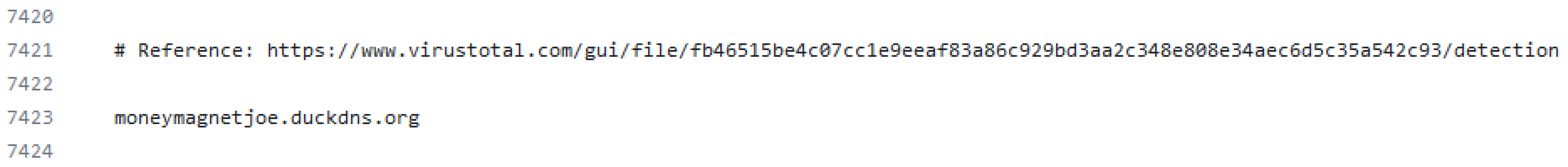
- http://geoplugin.net/json.gp
- https://onedrive.live.com/download?resid=DDFE20447411E22A!128&authkey=!AMwvJ3RJGXKxhGQ

DNS Resolutions

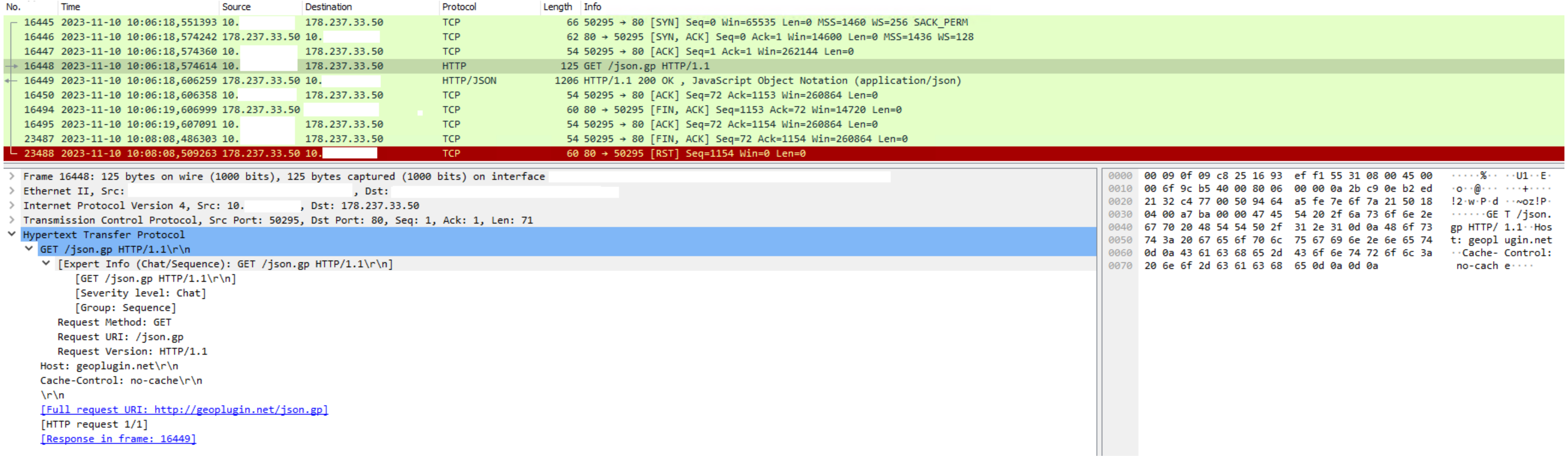
- geoplugin.net
  178.237.33.50
- moneymagnetjoe.duckdns.org
  104.223.35.34
- onedrive.live.com

IP Traffic

104.223.35.34:2404 (TCP)
13.107.42.13:443 (TCP)
178.237.33.50:80 (TCP)



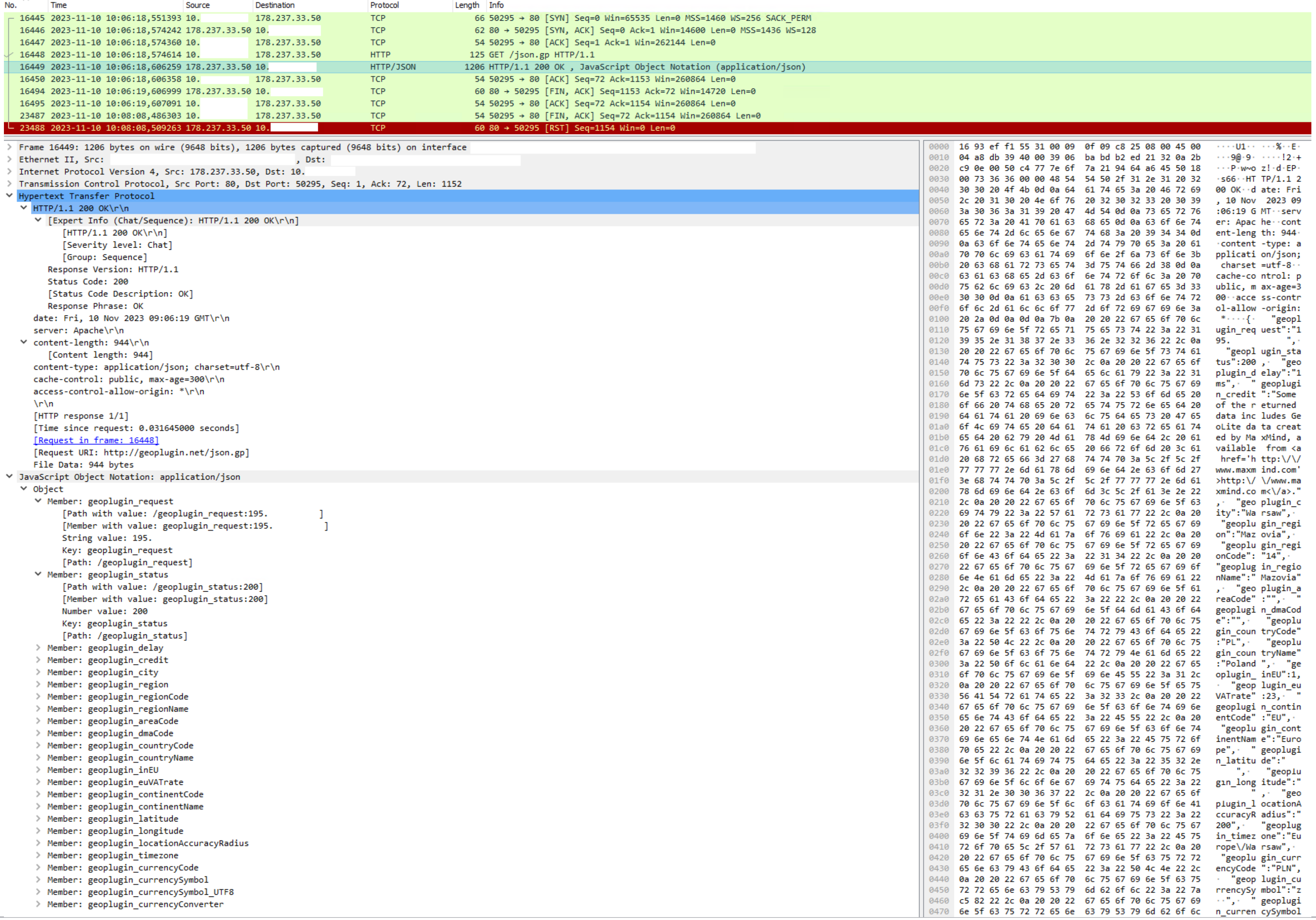
```

# Reference: https://www.virustotal.com/gui/file/fb46515be4c07cc1e9eeaf83a86c929bd3aa2c348e808e34aec6d5c35a542c93/detection

moneymagnetjoe.duckdns.org

```



```
No.    Time                       Source         Destination     Protocol   Length Info
16445 2023-11-10 10:06:18,551393 10.[redacted]  178.237.33.50   TCP          66 50295 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
16446 2023-11-10 10:06:18,574242 178.237.33.50 10.[redacted]   TCP          62 80 → 50295 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1436 WS=128
16447 2023-11-10 10:06:18,574360 10.[redacted]  178.237.33.50   TCP          54 50295 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
16448 2023-11-10 10:06:18,574614 10.[redacted]  178.237.33.50   HTTP        125 GET /json.gp HTTP/1.1
16449 2023-11-10 10:06:18,606259 178.237.33.50 10.[redacted]   HTTP/JSON  1206 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
16450 2023-11-10 10:06:18,606358 10.[redacted]  178.237.33.50   TCP          54 50295 → 80 [ACK] Seq=72 Ack=1153 Win=260864 Len=0
16494 2023-11-10 10:06:19,606999 178.237.33.50 [redacted]      TCP          60 80 → 50295 [FIN, ACK] Seq=1153 Ack=72 Win=14720 Len=0
16495 2023-11-10 10:06:19,607091 10.[redacted]  178.237.33.50   TCP          54 50295 → 80 [ACK] Seq=72 Ack=1154 Win=260864 Len=0
23487 2023-11-10 10:08:08,486303 10.[redacted]  178.237.33.50   TCP          54 50295 → 80 [FIN, ACK] Seq=72 Ack=1154 Win=260864 Len=0
23488 2023-11-10 10:08:08,509263 178.237.33.50 10.[redacted]   TCP          60 80 → 50295 [RST] Seq=1154 Win=0 Len=0
```

```
> Frame 16448: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface [redacted]
> Ethernet II, Src: [redacted], Dst: [redacted]
> Internet Protocol Version 4, Src: 10.[redacted], Dst: 178.237.33.50
> Transmission Control Protocol, Src Port: 50295, Dst Port: 80, Seq: 1, Ack: 1, Len: 71
v Hypertext Transfer Protocol
  v GET /json.gp HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /json.gp HTTP/1.1\r\n]
        [GET /json.gp HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /json.gp
      Request Version: HTTP/1.1
    Host: geoplugin.net\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://geoplugin.net/json.gp]
    [HTTP request 1/1]
    [Response in frame: 16449]
```

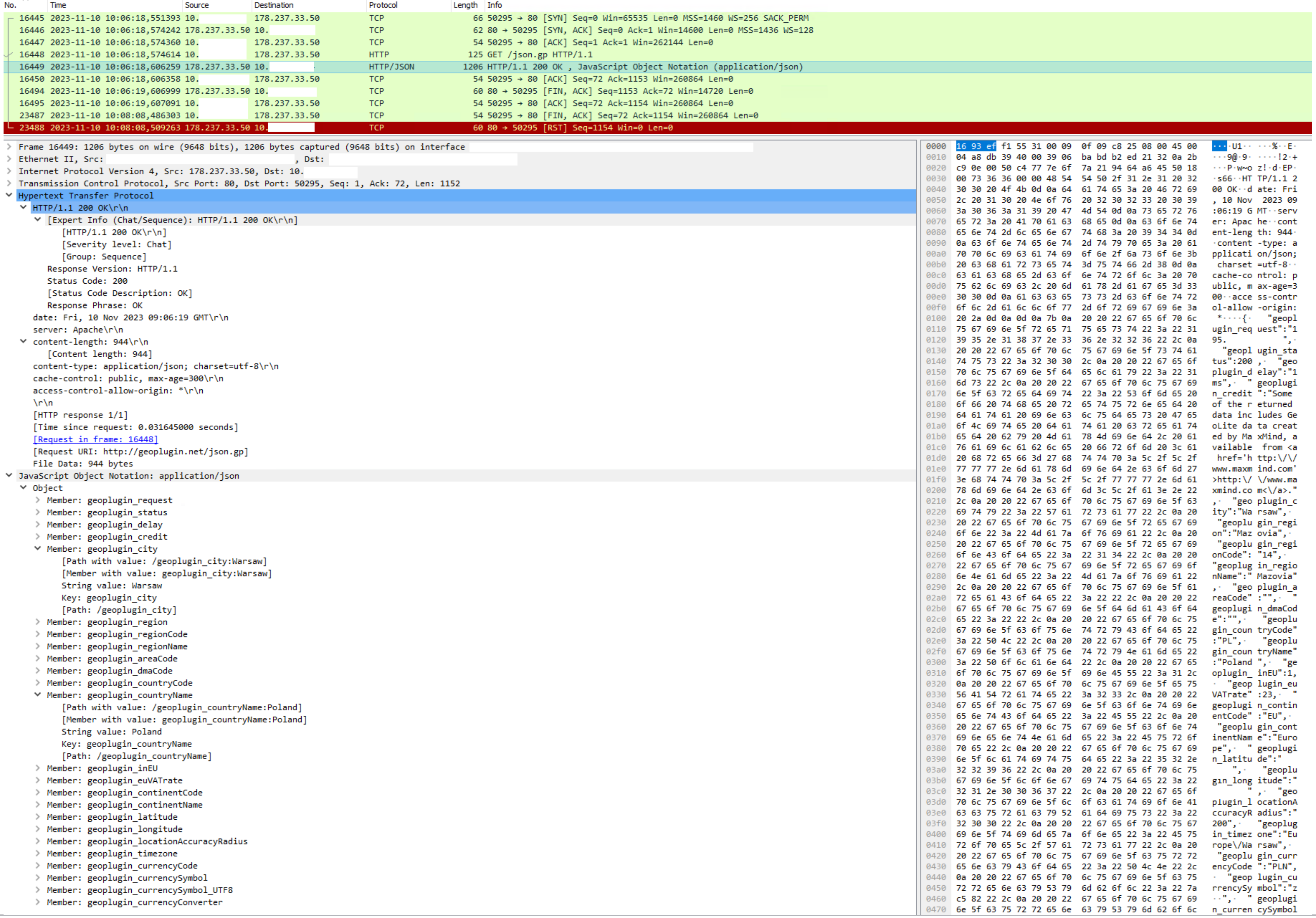
```
0000  00 09 0f 09 c8 25 16 93  ef f1 55 31 08 00 45 00   ·····%·· ··U1··E·
0010  00 6f 9c b5 40 00 80 06  00 00 0a 2b c9 0e b2 ed   ·o··@··· ···+····
0020  21 32 c4 77 00 50 94 64  a5 fe 7e 6f 7a 21 50 18   !2·w·P·d ··~oz!P·
0030  04 00 a7 ba 00 00 47 45  54 20 2f 6a 73 6f 6e 2e   ······GE T /json.
0040  67 70 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   gp HTTP/ 1.1··Hos
0050  74 3a 20 67 65 6f 70 6c  75 67 69 6e 2e 6e 65 74   t: geopl ugin.net
0060  0d 0a 43 61 63 68 65 2d  43 6f 6e 74 72 6f 6c 3a   ··Cache- Control:
0070  20 6e 6f 2d 63 61 63 68  65 0d 0a 0d 0a            no-cach e····
```



```
No.    Time                       Source          Destination     Protocol    Length Info
┌ 16445 2023-11-10 10:06:18,551393 10.[redacted]   178.237.33.50   TCP             66 50295 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
│ 16446 2023-11-10 10:06:18,574242 178.237.33.50   10.[redacted]   TCP             62 80 → 50295 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1436 WS=128
│ 16447 2023-11-10 10:06:18,574360 10.[redacted]   178.237.33.50   TCP             54 50295 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
✓ 16448 2023-11-10 10:06:18,574614 10.[redacted]   178.237.33.50   HTTP           125 GET /json.gp HTTP/1.1
  16449 2023-11-10 10:06:18,606259 178.237.33.50   10.[redacted]   HTTP/JSON     1206 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
  16450 2023-11-10 10:06:18,606358 10.[redacted]   178.237.33.50   TCP             54 50295 → 80 [ACK] Seq=72 Ack=1153 Win=260864 Len=0
  16494 2023-11-10 10:06:19,606999 178.237.33.50   10.[redacted]   TCP             60 80 → 50295 [FIN, ACK] Seq=1153 Ack=72 Win=14720 Len=0
  16495 2023-11-10 10:06:19,607091 10.[redacted]   178.237.33.50   TCP             54 50295 → 80 [ACK] Seq=72 Ack=1154 Win=260864 Len=0
  23487 2023-11-10 10:08:08,486303 10.[redacted]   178.237.33.50   TCP             54 50295 → 80 [FIN, ACK] Seq=72 Ack=1154 Win=260864 Len=0
└ 23488 2023-11-10 10:08:08,509263 178.237.33.50   10.[redacted]   TCP             60 80 → 50295 [RST] Seq=1154 Win=0 Len=0
```

```
> Frame 16449: 1206 bytes on wire (9648 bits), 1206 bytes captured (9648 bits) on interface [redacted]
> Ethernet II, Src: [redacted], Dst: [redacted]
> Internet Protocol Version 4, Src: 178.237.33.50, Dst: 10.[redacted]
> Transmission Control Protocol, Src Port: 80, Dst Port: 50295, Seq: 1, Ack: 72, Len: 1152
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    date: Fri, 10 Nov 2023 09:06:19 GMT\r\n
    server: Apache\r\n
  v content-length: 944\r\n
      [Content length: 944]
    content-type: application/json; charset=utf-8\r\n
    cache-control: public, max-age=300\r\n
    access-control-allow-origin: *\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.031645000 seconds]
    [Request in frame: 16448]
    [Request URI: http://geoplugin.net/json.gp]
    File Data: 944 bytes
v JavaScript Object Notation: application/json
  v Object
    v Member: geoplugin_request
        [Path with value: /geoplugin_request:195.[redacted]]
        [Member with value: geoplugin_request:195.[redacted]]
        String value: 195.
        Key: geoplugin_request
        [Path: /geoplugin_request]
    v Member: geoplugin_status
        [Path with value: /geoplugin_status:200]
        [Member with value: geoplugin_status:200]
        Number value: 200
        Key: geoplugin_status
        [Path: /geoplugin_status]
    > Member: geoplugin_delay
    > Member: geoplugin_credit
    > Member: geoplugin_city
    > Member: geoplugin_region
    > Member: geoplugin_regionCode
    > Member: geoplugin_regionName
    > Member: geoplugin_areaCode
    > Member: geoplugin_dmaCode
    > Member: geoplugin_countryCode
    > Member: geoplugin_countryName
    > Member: geoplugin_inEU
    > Member: geoplugin_euVATrate
    > Member: geoplugin_continentCode
    > Member: geoplugin_continentName
    > Member: geoplugin_latitude
    > Member: geoplugin_longitude
    > Member: geoplugin_locationAccuracyRadius
    > Member: geoplugin_timezone
    > Member: geoplugin_currencyCode
    > Member: geoplugin_currencySymbol
    > Member: geoplugin_currencySymbol_UTF8
    > Member: geoplugin_currencyConverter
```

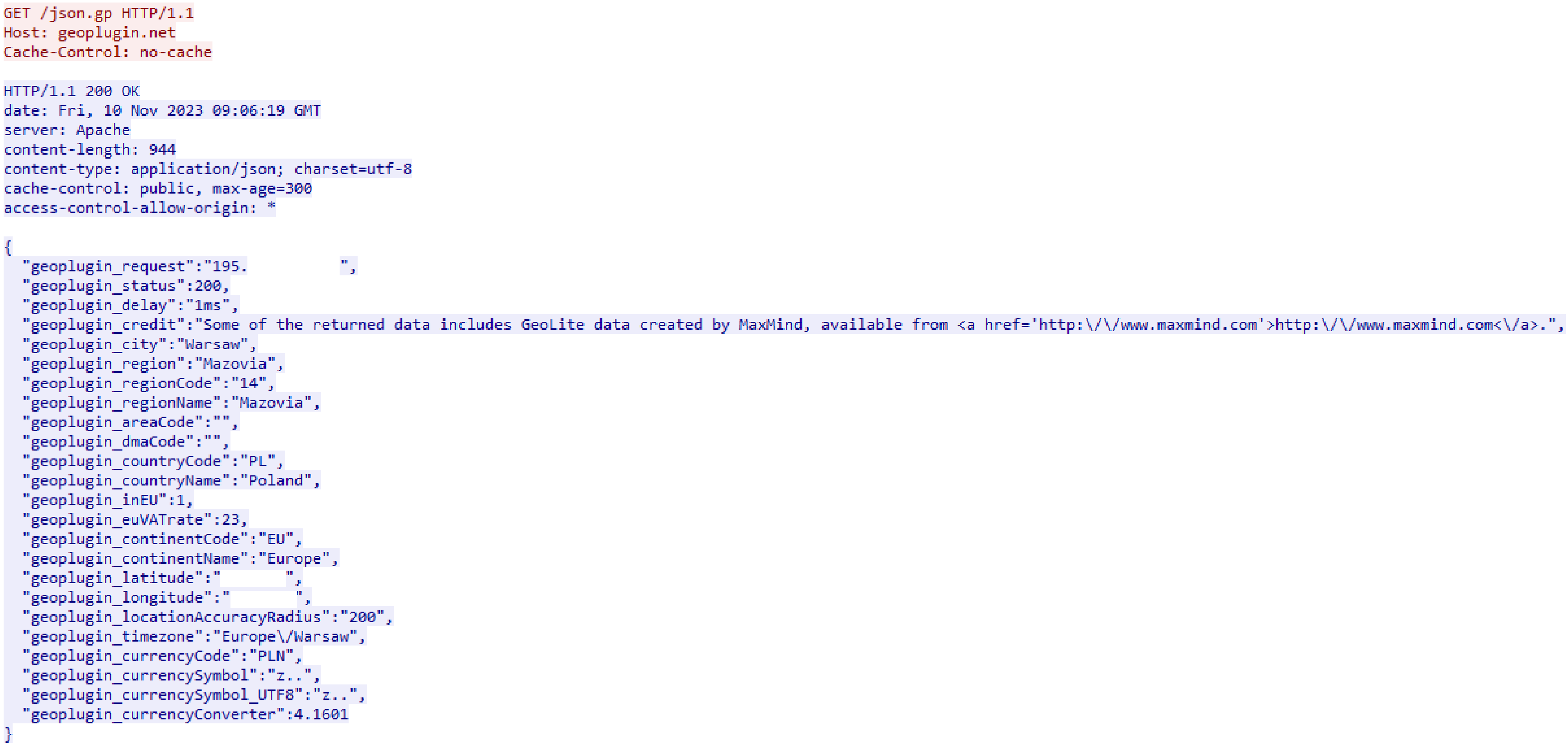
```
0000  16 93 ef f1 55 31 00 09  0f 09 c8 25 08 00 45 00   ····U1·· ···%··E·
0010  04 a8 db 39 40 00 39 06  ba bd b2 ed 21 32 0a 2b   ···9@·9· ····!2·+
0020  c9 0e 00 50 c4 77 7e 6f  7a 21 94 64 a6 45 50 18   ···P·w~o z!·d·EP·
0030  00 73 36 36 00 00 48 54  54 50 2f 31 2e 31 20 32   ·s66··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 64  61 74 65 3a 20 46 72 69   00 OK··d ate: Fri
0050  2c 20 31 30 20 4e 6f 76  20 32 30 32 33 20 30 39   , 10 Nov  2023 09
0060  3a 30 36 3a 31 39 20 47  4d 54 0d 0a 73 65 72 76   :06:19 G MT··serv
0070  65 72 3a 20 41 70 61 63  68 65 0d 0a 63 6f 6e 74   er: Apac he··cont
0080  65 6e 74 2d 6c 65 6e 67  74 68 3a 20 39 34 34 0d   ent-leng th: 944·
0090  0a 63 6f 6e 74 65 6e 74  2d 74 79 70 65 3a 20 61   ·content -type: a
00a0  70 70 6c 69 63 61 74 69  6f 6e 2f 6a 73 6f 6e 3b   pplicati on/json;
00b0  20 63 68 61 72 73 65 74  3d 75 74 66 2d 38 0d 0a    charset =utf-8··
00c0  63 61 63 68 65 2d 63 6f  6e 74 72 6f 6c 3a 20 70   cache-co ntrol: p
00d0  75 62 6c 69 63 2c 20 6d  61 78 2d 61 67 65 3d 33   ublic, m ax-age=3
00e0  30 30 0d 0a 61 63 63 65  73 73 2d 63 6f 6e 74 72   00··acce ss-contr
00f0  6f 6c 2d 61 6c 6c 6f 77  2d 6f 72 69 67 69 6e 3a   ol-allow -origin:
0100  20 2a 0d 0a 0d 0a 7b 0a  20 20 22 67 65 6f 70 6c    *····{·   "geopl
0110  75 67 69 6e 5f 72 65 71  75 65 73 74 22 3a 22 31   ugin_req uest":"1
0120  39 35 2e 31 38 37 2e 33  36 2e 32 32 36 22 2c 0a   95.[redacted]",·
0130  20 20 22 67 65 6f 70 6c  75 67 69 6e 5f 73 74 61     "geopl ugin_sta
0140  74 75 73 22 3a 32 30 30  2c 0a 20 20 22 67 65 6f   tus":200 ,·  "geo
0150  70 6c 75 67 69 6e 5f 64  65 6c 61 79 22 3a 22 31   plugin_d elay":"1
0160  6d 73 22 2c 0a 20 20 22  67 65 6f 70 6c 75 67 69   ms",·  " geoplugi
0170  6e 5f 63 72 65 64 69 74  22 3a 22 53 6f 6d 65 20   n_credit ":"Some 
0180  6f 66 20 74 68 65 20 72  65 74 75 72 6e 65 64 20   of the r eturned 
0190  64 61 74 61 20 69 6e 63  6c 75 64 65 73 20 47 65   data inc ludes Ge
01a0  6f 4c 69 74 65 20 64 61  74 61 20 63 72 65 61 74   oLite da ta creat
01b0  65 64 20 62 79 20 4d 61  78 4d 69 6e 64 2c 20 61   ed by Ma xMind, a
01c0  76 61 69 6c 61 62 6c 65  20 66 72 6f 6d 20 3c 61   vailable  from <a
01d0  20 68 72 65 66 3d 27 68  74 74 70 3a 5c 2f 5c 2f    href='h ttp:\/\/
01e0  77 77 77 2e 6d 61 78 6d  69 6e 64 2e 63 6f 6d 27   www.maxm ind.com'
01f0  3e 68 74 74 70 3a 5c 2f  5c 2f 77 77 77 2e 6d 61   >http:\/ \/www.ma
0200  78 6d 69 6e 64 2e 63 6f  6d 3c 5c 2f 61 3e 2e 22   xmind.co m<\/a>."
0210  2c 0a 20 20 22 67 65 6f  70 6c 75 67 69 6e 5f 63   ,·  "geo plugin_c
0220  69 74 79 22 3a 22 57 61  72 73 61 77 22 2c 0a 20   ity":"Wa rsaw",· 
0230  20 22 67 65 6f 70 6c 75  67 69 6e 5f 72 65 67 69    "geoplu gin_regi
0240  6f 6e 22 3a 22 4d 61 7a  6f 76 69 61 22 2c 0a 20   on":"Maz ovia",· 
0250  20 22 67 65 6f 70 6c 75  67 69 6e 5f 72 65 67 69    "geoplu gin_regi
0260  6f 6e 43 6f 64 65 22 3a  22 31 34 22 2c 0a 20 20   onCode": "14",·  
0270  22 67 65 6f 70 6c 75 67  69 6e 5f 72 65 67 69 6f   "geoplug in_regio
0280  6e 4e 61 6d 65 22 3a 22  4d 61 7a 6f 76 69 61 22   nName":" Mazovia"
0290  2c 0a 20 20 22 67 65 6f  70 6c 75 67 69 6e 5f 61   ,·  "geo plugin_a
02a0  72 65 61 43 6f 64 65 22  3a 22 22 2c 0a 20 20 22   reaCode" :"",·  "
02b0  67 65 6f 70 6c 75 67 69  6e 5f 64 6d 61 43 6f 64   geoplugi n_dmaCod
02c0  65 22 3a 22 22 2c 0a 20  20 22 67 65 6f 70 6c 75   e":"",·   "geoplu
02d0  67 69 6e 5f 63 6f 75 6e  74 72 79 43 6f 64 65 22   gin_coun tryCode"
02e0  3a 22 50 4c 22 2c 0a 20  20 22 67 65 6f 70 6c 75   :"PL",·   "geoplu
02f0  67 69 6e 5f 63 6f 75 6e  74 72 79 4e 61 6d 65 22   gin_coun tryName"
0300  3a 22 50 6f 6c 61 6e 64  22 2c 0a 20 20 22 67 65   :"Poland ",·  "ge
0310  6f 70 6c 75 67 69 6e 5f  69 6e 45 55 22 3a 31 2c   oplugin_ inEU":1,
0320  0a 20 20 22 67 65 6f 70  6c 75 67 69 6e 5f 65 75   ·  "geop lugin_eu
0330  56 41 54 72 61 74 65 22  3a 32 33 2c 0a 20 20 22   VATrate" :23,·  "
0340  67 65 6f 70 6c 75 67 69  6e 5f 63 6f 6e 74 69 6e   geoplugi n_contin
0350  65 6e 74 43 6f 64 65 22  3a 22 45 55 22 2c 0a 20   entCode" :"EU",· 
0360  20 22 67 65 6f 70 6c 75  67 69 6e 5f 63 6f 6e 74    "geoplu gin_cont
0370  69 6e 65 6e 74 4e 61 6d  65 22 3a 22 45 75 72 6f   inentNam e":"Euro
0380  70 65 22 2c 0a 20 20 22  67 65 6f 70 6c 75 67 69   pe",·  " geoplugi
0390  6e 5f 6c 61 74 69 74 75  64 65 22 3a 22 35 32 2e   n_latitu de":"[redacted]
03a0  32 32 39 36 22 2c 0a 20  20 22 67 65 6f 70 6c 75   [redacted]",·   "geoplu
03b0  67 69 6e 5f 6c 6f 6e 67  69 74 75 64 65 22 3a 22   gin_long itude":"
03c0  32 31 2e 30 30 36 37 22  2c 0a 20 20 22 67 65 6f   [redacted]",·  "geo
03d0  70 6c 75 67 69 6e 5f 6c  6f 63 61 74 69 6f 6e 41   plugin_l ocationA
03e0  63 63 75 72 61 63 79 52  61 64 69 75 73 22 3a 22   ccuracyR adius":"
03f0  32 30 30 22 2c 0a 20 20  22 67 65 6f 70 6c 75 67   200",·   "geoplug
0400  69 6e 5f 74 69 6d 65 7a  6f 6e 65 22 3a 22 45 75   in_timez one":"Eu
0410  72 6f 70 65 5c 2f 57 61  72 73 61 77 22 2c 0a 20   rope\/Wa rsaw",· 
0420  20 22 67 65 6f 70 6c 75  67 69 6e 5f 63 75 72 72    "geoplu gin_curr
0430  65 6e 63 79 43 6f 64 65  22 3a 22 50 4c 4e 22 2c   encyCode ":"PLN",
0440  0a 20 20 22 67 65 6f 70  6c 75 67 69 6e 5f 63 75   ·  "geop lugin_cu
0450  72 72 65 6e 63 79 53 79  6d 62 6f 6c 22 3a 22 7a   rrencySy mbol":"z
0460  c5 82 22 2c 0a 20 20 22  67 65 6f 70 6c 75 67 69   ··",·  " geoplugi
0470  6e 5f 63 75 72 72 65 6e  63 79 53 79 6d 62 6f 6c   n_curren cySymbol
```



```
No.    Time                       Source         Destination    Protocol   Length Info
16445 2023-11-10 10:06:18,551393 10.[redacted]  178.237.33.50  TCP          66 50295 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
16446 2023-11-10 10:06:18,574242 178.237.33.50 10.[redacted]   TCP          62 80 → 50295 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1436 WS=128
16447 2023-11-10 10:06:18,574360 10.[redacted]  178.237.33.50  TCP          54 50295 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
16448 2023-11-10 10:06:18,574614 10.[redacted]  178.237.33.50  HTTP        125 GET /json.gp HTTP/1.1
16449 2023-11-10 10:06:18,606259 178.237.33.50 10.[redacted]   HTTP/JSON  1206 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
16450 2023-11-10 10:06:18,606358 10.[redacted]  178.237.33.50  TCP          54 50295 → 80 [ACK] Seq=72 Ack=1153 Win=260864 Len=0
16494 2023-11-10 10:06:19,606999 178.237.33.50 10.[redacted]   TCP          60 80 → 50295 [FIN, ACK] Seq=1153 Ack=72 Win=14720 Len=0
16495 2023-11-10 10:06:19,607091 10.[redacted]  178.237.33.50  TCP          54 50295 → 80 [ACK] Seq=72 Ack=1154 Win=260864 Len=0
23487 2023-11-10 10:08:08,486303 10.[redacted]  178.237.33.50  TCP          54 50295 → 80 [FIN, ACK] Seq=72 Ack=1154 Win=260864 Len=0
23488 2023-11-10 10:08:08,509263 178.237.33.50 10.[redacted]   TCP          60 80 → 50295 [RST] Seq=1154 Win=0 Len=0
```

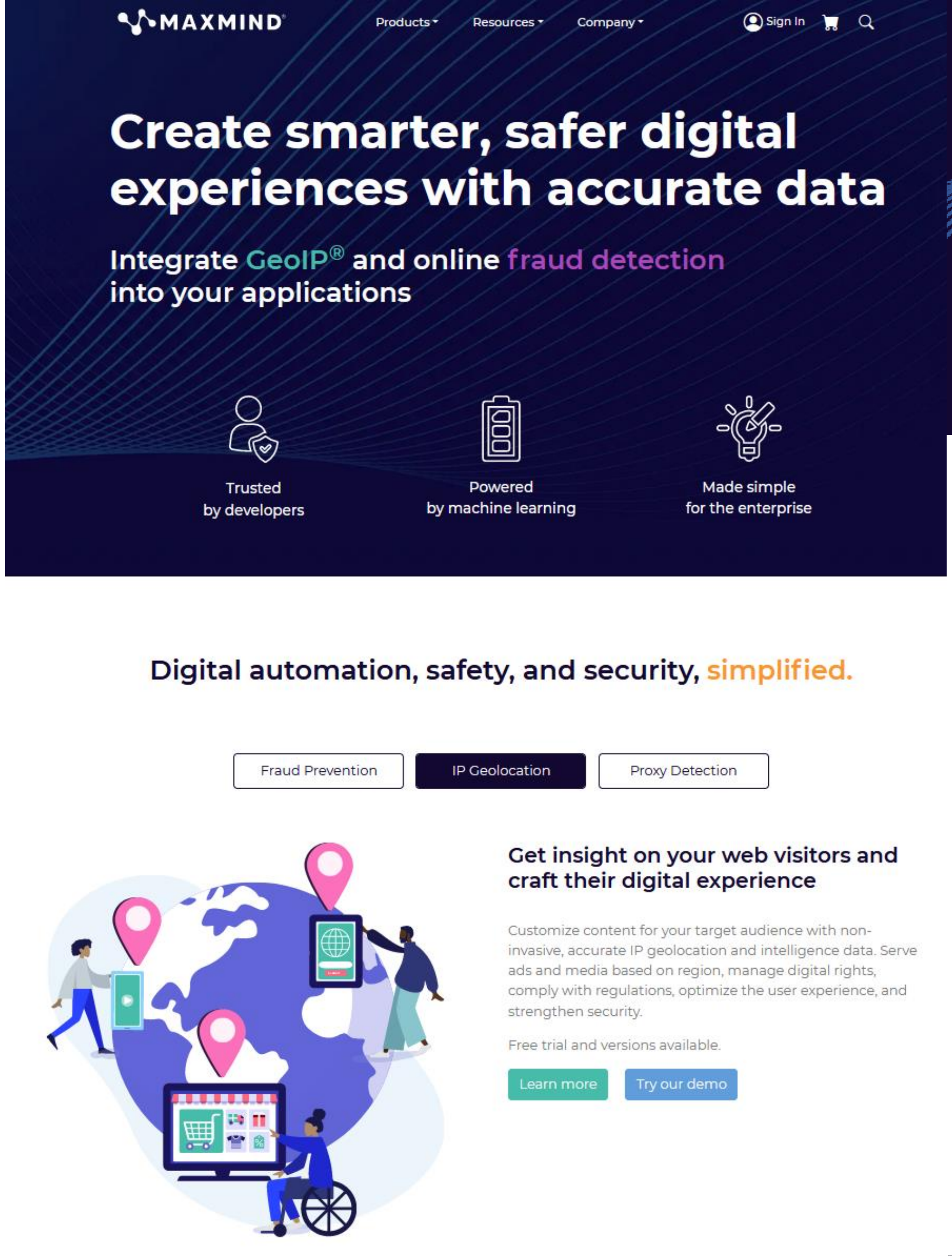
```
> Frame 16449: 1206 bytes on wire (9648 bits), 1206 bytes captured (9648 bits) on interface [redacted]
> Ethernet II, Src: [redacted], Dst: [redacted]
> Internet Protocol Version 4, Src: 178.237.33.50, Dst: 10.[redacted]
> Transmission Control Protocol, Src Port: 80, Dst Port: 50295, Seq: 1, Ack: 72, Len: 1152
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    date: Fri, 10 Nov 2023 09:06:19 GMT\r\n
    server: Apache\r\n
  v content-length: 944\r\n
      [Content length: 944]
    content-type: application/json; charset=utf-8\r\n
    cache-control: public, max-age=300\r\n
    access-control-allow-origin: *\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.031645000 seconds]
    [Request in frame: 16448]
    [Request URI: http://geoplugin.net/json.gp]
    File Data: 944 bytes
v JavaScript Object Notation: application/json
  v Object
    > Member: geoplugin_request
    > Member: geoplugin_status
    > Member: geoplugin_delay
    > Member: geoplugin_credit
    v Member: geoplugin_city
        [Path with value: /geoplugin_city:Warsaw]
        [Member with value: geoplugin_city:Warsaw]
        String value: Warsaw
        Key: geoplugin_city
        [Path: /geoplugin_city]
    > Member: geoplugin_region
    > Member: geoplugin_regionCode
    > Member: geoplugin_regionName
    > Member: geoplugin_areaCode
    > Member: geoplugin_dmaCode
    > Member: geoplugin_countryCode
    v Member: geoplugin_countryName
        [Path with value: /geoplugin_countryName:Poland]
        [Member with value: geoplugin_countryName:Poland]
        String value: Poland
        Key: geoplugin_countryName
        [Path: /geoplugin_countryName]
    > Member: geoplugin_inEU
    > Member: geoplugin_euVATrate
    > Member: geoplugin_continentCode
    > Member: geoplugin_continentName
    > Member: geoplugin_latitude
    > Member: geoplugin_longitude
    > Member: geoplugin_locationAccuracyRadius
    > Member: geoplugin_timezone
    > Member: geoplugin_currencyCode
    > Member: geoplugin_currencySymbol
    > Member: geoplugin_currencySymbol_UTF8
    > Member: geoplugin_currencyConverter
```

```
0000  16 93 ef f1 55 31 00 09  0f 09 c8 25 08 00 45 00   ····U1·· ···%··E·
0010  04 a8 db 39 40 00 39 06  ba bd b2 ed 21 32 0a 2b   ···9@·9· ····!2·+
0020  c9 0e 00 50 c4 77 7e 6f  7a 21 94 64 a6 45 50 18   ···P·w~o z!·d·EP·
0030  00 73 36 36 00 00 48 54  54 50 2f 31 2e 31 20 32   ·s66··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 64  61 74 65 3a 20 46 72 69   00 OK··d ate: Fri
0050  2c 20 31 30 20 4e 6f 76  20 32 30 32 33 20 30 39   , 10 Nov  2023 09
0060  3a 30 36 3a 31 39 20 47  4d 54 0d 0a 73 65 72 76   :06:19 G MT··serv
0070  65 72 3a 20 41 70 61 63  68 65 0d 0a 63 6f 6e 74   er: Apac he··cont
0080  65 6e 74 2d 6c 65 6e 67  74 68 3a 20 39 34 34 0d   ent-leng th: 944·
0090  0a 63 6f 6e 74 65 6e 74  2d 74 79 70 65 3a 20 61   ·content -type: a
00a0  70 70 6c 69 63 61 74 69  6f 6e 2f 6a 73 6f 6e 3b   pplicati on/json;
00b0  20 63 68 61 72 73 65 74  3d 75 74 66 2d 38 0d 0a    charset =utf-8··
00c0  63 61 63 68 65 2d 63 6f  6e 74 72 6f 6c 3a 20 70   cache-co ntrol: p
00d0  75 62 6c 69 63 2c 20 6d  61 78 2d 61 67 65 3d 33   ublic, m ax-age=3
00e0  30 30 0d 0a 61 63 63 65  73 73 2d 63 6f 6e 74 72   00··acce ss-contr
00f0  6f 6c 2d 61 6c 6c 6f 77  2d 6f 72 69 67 69 6e 3a   ol-allow -origin:
0100  20 2a 0d 0a 0d 0a 7b 0a  20 20 22 67 65 6f 70 6c    *····{·   "geopl
0110  75 67 69 6e 5f 72 65 71  75 65 73 74 22 3a 22 31   ugin_req uest":"1
0120  39 35 2e 31 38 37 2e 33  36 2e 32 32 36 22 2c 0a   95.[redacted]",·
0130  20 20 22 67 65 6f 70 6c  75 67 69 6e 5f 73 74 61     "geopl ugin_sta
0140  74 75 73 22 3a 32 30 30  2c 0a 20 20 22 67 65 6f   tus":200 ,·  "geo
0150  70 6c 75 67 69 6e 5f 64  65 6c 61 79 22 3a 22 31   plugin_d elay":"1
0160  6d 73 22 2c 0a 20 20 22  67 65 6f 70 6c 75 67 69   ms",·  " geoplugi
0170  6e 5f 63 72 65 64 69 74  22 3a 22 53 6f 6d 65 20   n_credit ":"Some
0180  6f 66 20 74 68 65 20 72  65 74 75 72 6e 65 64 20   of the r eturned
0190  64 61 74 61 20 69 6e 63  6c 75 64 65 73 20 47 65   data inc ludes Ge
01a0  6f 4c 69 74 65 20 64 61  74 61 20 63 72 65 61 74   oLite da ta creat
01b0  65 64 20 62 79 20 4d 61  78 4d 69 6e 64 2c 20 61   ed by Ma xMind, a
01c0  76 61 69 6c 61 62 6c 65  20 66 72 6f 6d 20 3c 61   vailable  from <a
01d0  20 68 72 65 66 3d 27 68  74 74 70 3a 5c 2f 5c 2f    href='h ttp:\/\/
01e0  77 77 77 2e 6d 61 78 6d  69 6e 64 2e 63 6f 6d 27   www.maxm ind.com'
01f0  3e 68 74 74 70 3a 5c 2f  5c 2f 77 77 77 2e 6d 61   >http:\/ \/www.ma
0200  78 6d 69 6e 64 2e 63 6f  6d 3c 5c 2f 61 3e 2e 22   xmind.co m<\/a>."
0210  2c 0a 20 20 22 67 65 6f  70 6c 75 67 69 6e 5f 63   ,·  "geo plugin_c
0220  69 74 79 22 3a 22 57 61  72 73 61 77 22 2c 0a 20   ity":"Wa rsaw",·
0230  20 22 67 65 6f 70 6c 75  67 69 6e 5f 72 65 67 69    "geoplu gin_regi
0240  6f 6e 22 3a 22 4d 61 7a  6f 76 69 61 22 2c 0a 20   on":"Maz ovia",·
0250  20 22 67 65 6f 70 6c 75  67 69 6e 5f 72 65 67 69    "geoplu gin_regi
0260  6f 6e 43 6f 64 65 22 3a  22 31 34 22 2c 0a 20 20   onCode": "14",·
0270  22 67 65 6f 70 6c 75 67  69 6e 5f 72 65 67 69 6f   "geoplug in_regio
0280  6e 4e 61 6d 65 22 3a 22  4d 61 7a 6f 76 69 61 22   nName":" Mazovia"
0290  2c 0a 20 20 22 67 65 6f  70 6c 75 67 69 6e 5f 61   ,·  "geo plugin_a
02a0  72 65 61 43 6f 64 65 22  3a 22 22 2c 0a 20 20 22   reaCode" :"",·  "
02b0  67 65 6f 70 6c 75 67 69  6e 5f 64 6d 61 43 6f 64   geoplugi n_dmaCod
02c0  65 22 3a 22 22 2c 0a 20  20 22 67 65 6f 70 6c 75   e":"",·   "geoplu
02d0  67 69 6e 5f 63 6f 75 6e  74 72 79 43 6f 64 65 22   gin_coun tryCode"
02e0  3a 22 50 4c 22 2c 0a 20  20 22 67 65 6f 70 6c 75   :"PL",·   "geoplu
02f0  67 69 6e 5f 63 6f 75 6e  74 72 79 4e 61 6d 65 22   gin_coun tryName"
0300  3a 22 50 6f 6c 61 6e 64  22 2c 0a 20 20 22 67 65   :"Poland ",·  "ge
0310  6f 70 6c 75 67 69 6e 5f  69 6e 45 55 22 3a 31 2c   oplugin_ inEU":1,
0320  0a 20 20 22 67 65 6f 70  6c 75 67 69 6e 5f 65 75   ·  "geop lugin_eu
0330  56 41 54 72 61 74 65 22  3a 32 33 2c 0a 20 20 22   VATrate" :23,·  "
0340  67 65 6f 70 6c 75 67 69  6e 5f 63 6f 6e 74 69 6e   geoplugi n_contin
0350  65 6e 74 43 6f 64 65 22  3a 22 45 55 22 2c 0a 20   entCode" :"EU",·
0360  20 22 67 65 6f 70 6c 75  67 69 6e 5f 63 6f 6e 74    "geoplu gin_cont
0370  69 6e 65 6e 74 4e 61 6d  65 22 3a 22 45 75 72 6f   inentNam e":"Euro
0380  70 65 22 2c 0a 20 20 22  67 65 6f 70 6c 75 67 69   pe",·  " geoplugi
0390  6e 5f 6c 61 74 69 74 75  64 65 22 3a 22 35 32 2e   n_latitu de":"[redacted]
03a0  32 32 39 36 22 2c 0a 20  20 22 67 65 6f 70 6c 75   [redacted]",·   "geoplu
03b0  67 69 6e 5f 6c 6f 6e 67  69 74 75 64 65 22 3a 22   gin_long itude":"
03c0  32 31 2e 30 30 36 37 22  2c 0a 20 20 22 67 65 6f   [redacted]",·  "geo
03d0  70 6c 75 67 69 6e 5f 6c  6f 63 61 74 69 6f 6e 41   plugin_l ocationA
03e0  63 63 75 72 61 63 79 52  61 64 69 75 73 22 3a 22   ccuracyR adius":"
03f0  32 30 30 22 2c 0a 20 20  22 67 65 6f 70 6c 75 67   200",·   "geoplug
0400  69 6e 5f 74 69 6d 65 7a  6f 6e 65 22 3a 22 45 75   in_timez one":"Eu
0410  72 6f 70 65 5c 2f 57 61  72 73 61 77 22 2c 0a 20   rope\/Wa rsaw",·
0420  20 22 67 65 6f 70 6c 75  67 69 6e 5f 63 75 72 72    "geoplu gin_curr
0430  65 6e 63 79 43 6f 64 65  22 3a 22 50 4c 4e 22 2c   encyCode ":"PLN",
0440  0a 20 20 22 67 65 6f 70  6c 75 67 69 6e 5f 63 75   ·  "geop lugin_cu
0450  72 72 65 6e 63 79 53 79  6d 62 6f 6c 22 3a 22 7a   rrencySy mbol":"z
0460  c5 82 22 2c 0a 20 20 22  67 65 6f 70 6c 75 67 69   ··",·  " geoplugi
0470  6e 5f 63 75 72 72 65 6e  63 79 53 79 6d 62 6f 6c   n_curren cySymbol
```



```
GET /json.gp HTTP/1.1
Host: geoplugin.net
Cache-Control: no-cache

HTTP/1.1 200 OK
date: Fri, 10 Nov 2023 09:06:19 GMT
server: Apache
content-length: 944
content-type: application/json; charset=utf-8
cache-control: public, max-age=300
access-control-allow-origin: *
```

```
{
  "geoplugin_request":"195.          ",
  "geoplugin_status":200,
  "geoplugin_delay":"1ms",
  "geoplugin_credit":"Some of the returned data includes GeoLite data created by MaxMind, available from <a href='http:\/\/www.maxmind.com'>http:\/\/www.maxmind.com<\/a>.",
  "geoplugin_city":"Warsaw",
  "geoplugin_region":"Mazovia",
  "geoplugin_regionCode":"14",
  "geoplugin_regionName":"Mazovia",
  "geoplugin_areaCode":"",
  "geoplugin_dmaCode":"",
  "geoplugin_countryCode":"PL",
  "geoplugin_countryName":"Poland",
  "geoplugin_inEU":1,
  "geoplugin_euVATrate":23,
  "geoplugin_continentCode":"EU",
  "geoplugin_continentName":"Europe",
  "geoplugin_latitude":"       ",
  "geoplugin_longitude":"       ",
  "geoplugin_locationAccuracyRadius":"200",
  "geoplugin_timezone":"Europe\/Warsaw",
  "geoplugin_currencyCode":"PLN",
  "geoplugin_currencySymbol":"z..",
  "geoplugin_currencySymbol_UTF8":"z..",
  "geoplugin_currencyConverter":4.1601
}
```



Create smarter, safer digital experiences with accurate data

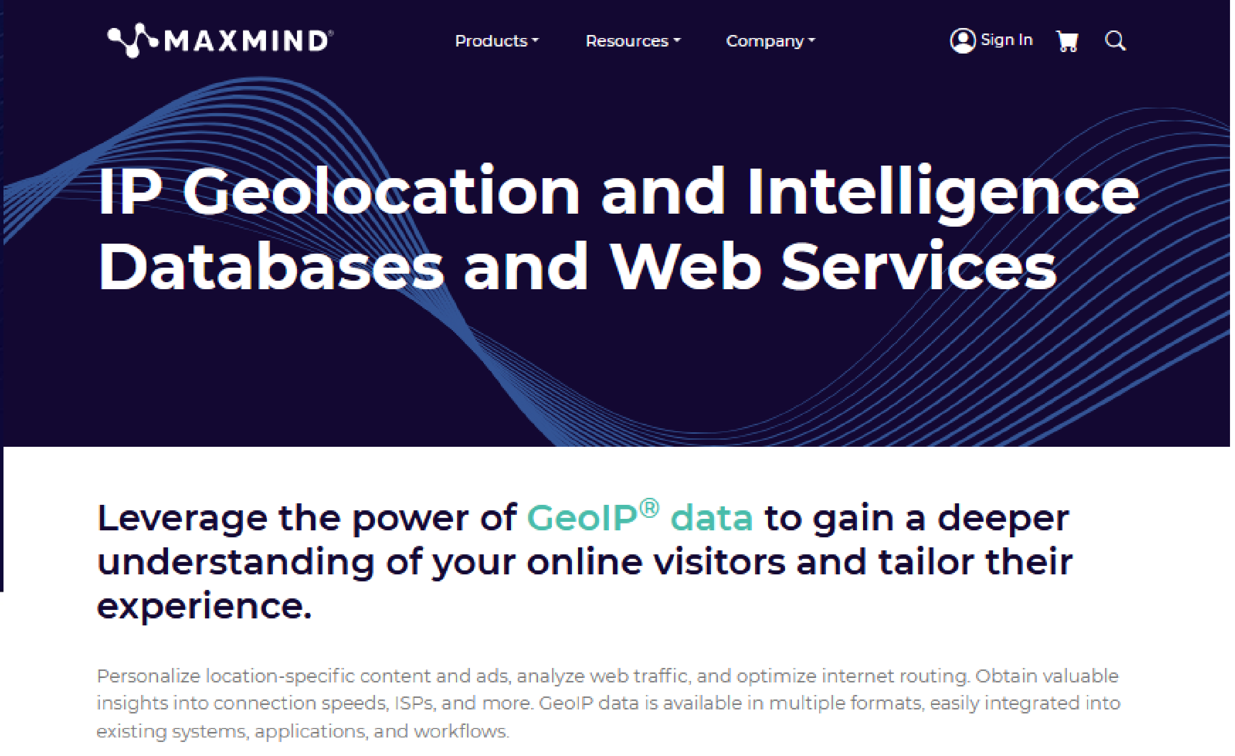
Integrate GeoIP® and online fraud detection into your applications

Digital automation, safety, and security, simplified.

Get insight on your web visitors and craft their digital experience

Customize content for your target audience with non-invasive, accurate IP geolocation and intelligence data. Serve ads and media based on region, manage digital rights, comply with regulations, optimize the user experience, and strengthen security.

Free trial and versions available.

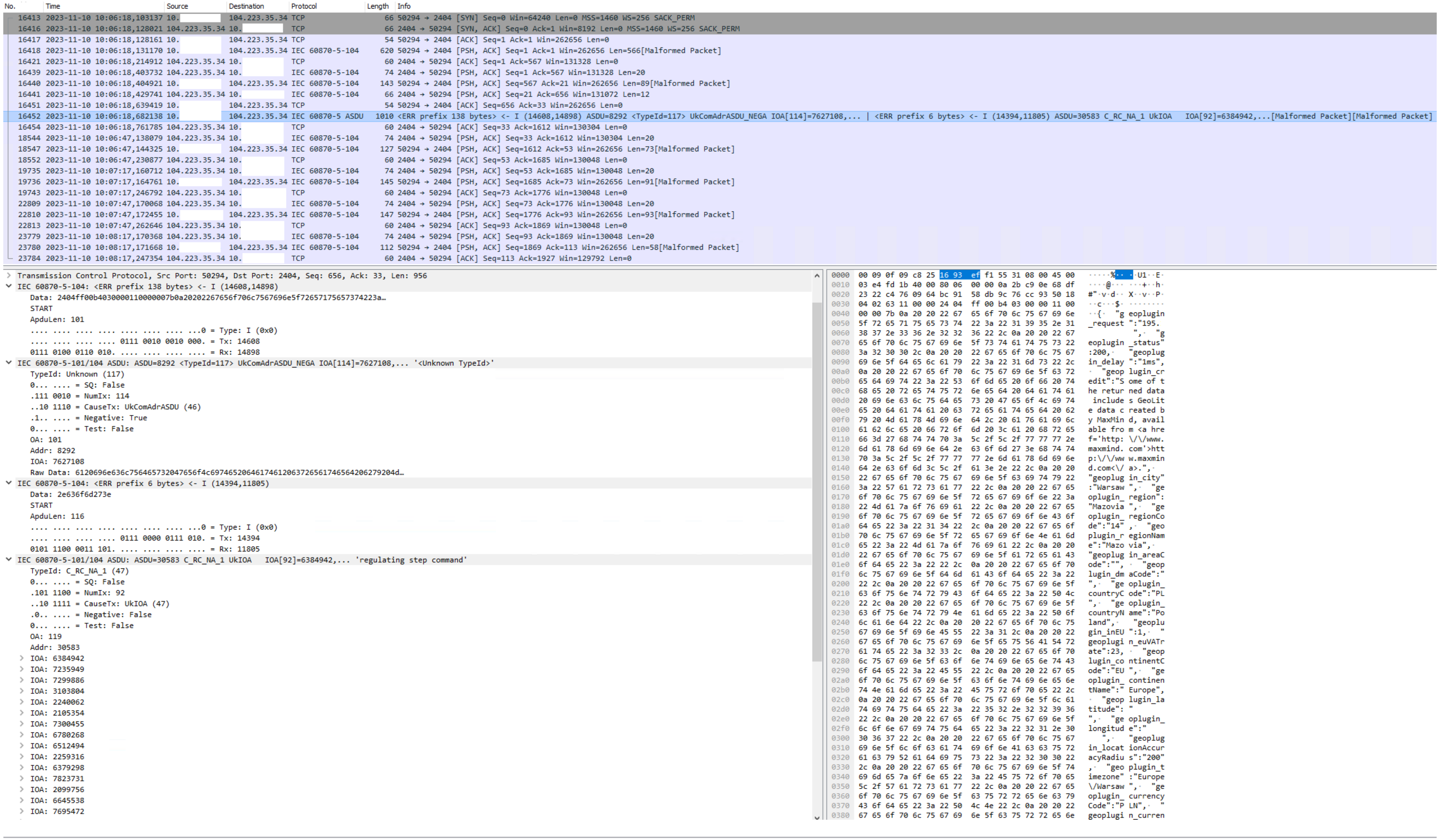


IP Geolocation and Intelligence Databases and Web Services

Leverage the power of GeoIP® data to gain a deeper understanding of your online visitors and tailor their experience.

Personalize location-specific content and ads, analyze web traffic, and optimize internet routing. Obtain valuable insights into connection speeds, ISPs, and more. GeoIP data is available in multiple formats, easily integrated into existing systems, applications, and workflows.

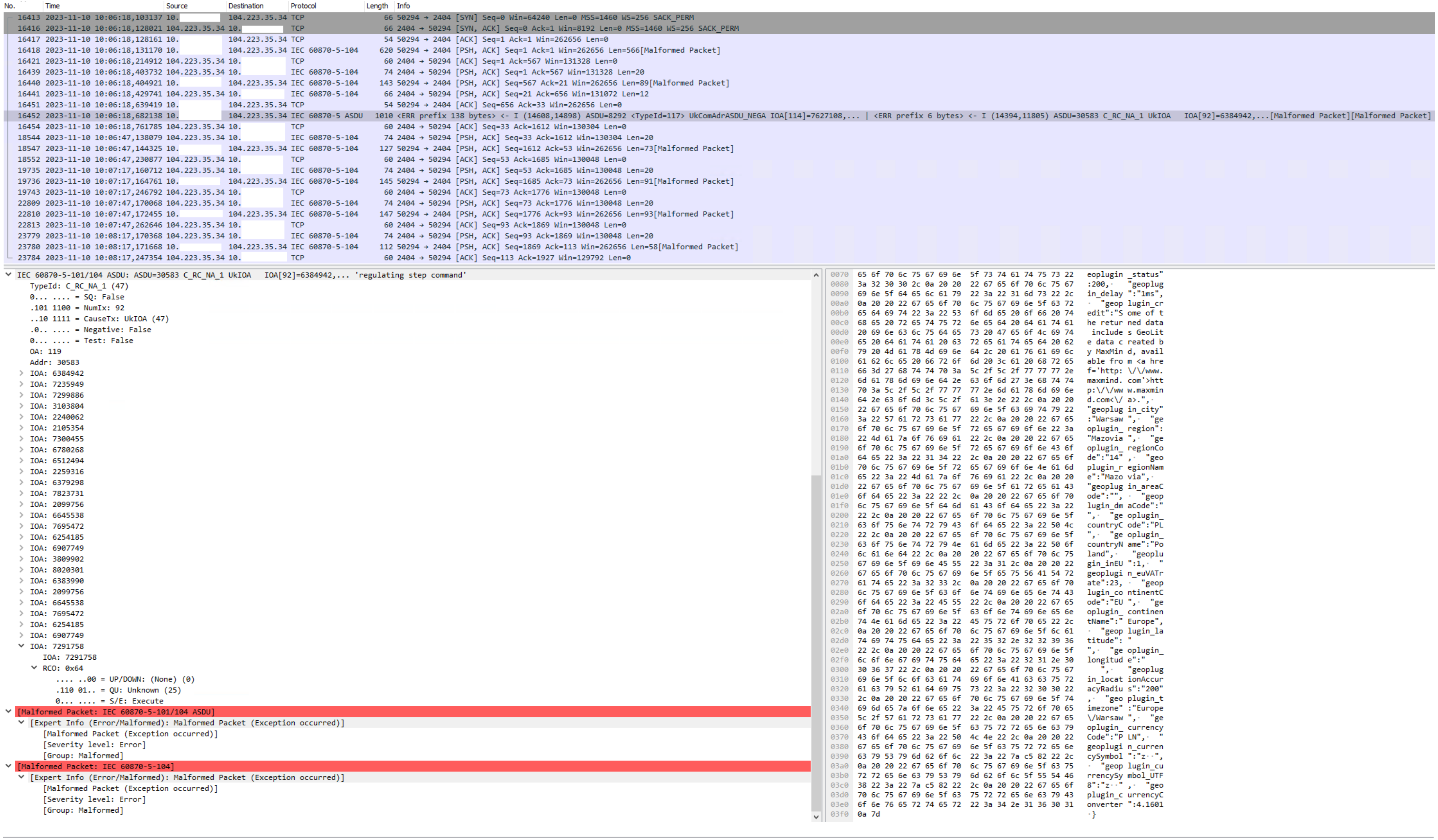
https://www.maxmind.com/en/home
https://www.maxmind.com/en/solutions/ip-geolocation-databases-api-services
https://www.maxmind.com/en/geoip-databases
https://www.maxmind.com/en/geoip-api-web-services
https://www.maxmind.com/en/solutions/geoip2-enterprise-product-suite/enterprise-database
https://dev.maxmind.com/geoip/geolite2-free-geolocation-data



```
No.   Time                       Source         Destination    Protocol            Length Info
16413 2023-11-10 10:06:18,103137 10.[redacted]  104.223.35.34  TCP                 66 50294 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
16416 2023-11-10 10:06:18,128021 104.223.35.34  10.[redacted]  TCP                 66 2404 → 50294 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
16417 2023-11-10 10:06:18,128161 10.[redacted]  104.223.35.34  TCP                 54 50294 → 2404 [ACK] Seq=1 Ack=1 Win=262656 Len=0
16418 2023-11-10 10:06:18,131170 10.[redacted]  104.223.35.34  IEC 60870-5-104    620 50294 → 2404 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=566[Malformed Packet]
16421 2023-11-10 10:06:18,214912 104.223.35.34  10.[redacted]  TCP                 60 2404 → 50294 [ACK] Seq=1 Ack=567 Win=131328 Len=0
16439 2023-11-10 10:06:18,403732 104.223.35.34  10.[redacted]  IEC 60870-5-104     74 2404 → 50294 [PSH, ACK] Seq=1 Ack=567 Win=131328 Len=20
16440 2023-11-10 10:06:18,404921 10.[redacted]  104.223.35.34  IEC 60870-5-104    143 50294 → 2404 [PSH, ACK] Seq=567 Ack=21 Win=262656 Len=89[Malformed Packet]
16441 2023-11-10 10:06:18,429741 104.223.35.34  10.[redacted]  IEC 60870-5-104     66 2404 → 50294 [PSH, ACK] Seq=21 Ack=656 Win=131072 Len=12
16451 2023-11-10 10:06:18,639419 10.[redacted]  104.223.35.34  TCP                 54 50294 → 2404 [ACK] Seq=656 Ack=33 Win=262656 Len=0
16452 2023-11-10 10:06:18,682138 10.[redacted]  104.223.35.34  IEC 60870-5 ASDU  1010 <ERR prefix 138 bytes> <- I (14608,14898) ASDU=8292 <TypeId=117> UkComAdrASDU_NEGA IOA[114]=7627108,... | <ERR prefix 6 bytes> <- I (14394,11805) ASDU=30583 C_RC_NA_1 UkIOA   IOA[92]=6384942,...[Malformed Packet][Malformed Packet]
16454 2023-11-10 10:06:18,761785 104.223.35.34  10.[redacted]  TCP                 60 2404 → 50294 [ACK] Seq=33 Ack=1612 Win=130304 Len=0
18544 2023-11-10 10:06:47,138079 104.223.35.34  10.[redacted]  IEC 60870-5-104     74 2404 → 50294 [PSH, ACK] Seq=33 Ack=1612 Win=130304 Len=20
18547 2023-11-10 10:06:47,144325 10.[redacted]  104.223.35.34  IEC 60870-5-104    127 50294 → 2404 [PSH, ACK] Seq=1612 Ack=53 Win=262656 Len=73[Malformed Packet]
18552 2023-11-10 10:06:47,230877 104.223.35.34  10.[redacted]  TCP                 60 2404 → 50294 [ACK] Seq=53 Ack=1685 Win=130048 Len=0
19735 2023-11-10 10:07:17,160712 104.223.35.34  10.[redacted]  IEC 60870-5-104     74 2404 → 50294 [PSH, ACK] Seq=53 Ack=1685 Win=130048 Len=20
19736 2023-11-10 10:07:17,164761 10.[redacted]  104.223.35.34  IEC 60870-5-104    145 50294 → 2404 [PSH, ACK] Seq=1685 Ack=73 Win=262656 Len=91[Malformed Packet]
19743 2023-11-10 10:07:17,246792 104.223.35.34  10.[redacted]  TCP                 60 2404 → 50294 [ACK] Seq=73 Ack=1776 Win=130048 Len=0
22809 2023-11-10 10:07:47,170068 104.223.35.34  10.[redacted]  IEC 60870-5-104     74 2404 → 50294 [PSH, ACK] Seq=73 Ack=1776 Win=130048 Len=20
22810 2023-11-10 10:07:47,172455 10.[redacted]  104.223.35.34  IEC 60870-5-104    147 50294 → 2404 [PSH, ACK] Seq=1776 Ack=93 Win=262656 Len=93[Malformed Packet]
22813 2023-11-10 10:07:47,262646 104.223.35.34  10.[redacted]  TCP                 60 2404 → 50294 [ACK] Seq=93 Ack=1869 Win=130048 Len=0
23779 2023-11-10 10:08:17,170368 104.223.35.34  10.[redacted]  IEC 60870-5-104     74 2404 → 50294 [PSH, ACK] Seq=93 Ack=1869 Win=130048 Len=20
23780 2023-11-10 10:08:17,171668 10.[redacted]  104.223.35.34  IEC 60870-5-104    112 50294 → 2404 [PSH, ACK] Seq=1869 Ack=113 Win=262656 Len=58[Malformed Packet]
23784 2023-11-10 10:08:17,247354 104.223.35.34  10.[redacted]  TCP                 60 2404 → 50294 [ACK] Seq=113 Ack=1927 Win=129792 Len=0
```

```
> Transmission Control Protocol, Src Port: 50294, Dst Port: 2404, Seq: 656, Ack: 33, Len: 956
v IEC 60870-5-104: <ERR prefix 138 bytes> <- I (14608,14898)
    Data: 2404ff00b4030000110000007b0a20202267656f706c7567696e5f72657175657374223a…
    START
    ApduLen: 101
    .... .... .... .... .... .... .... ...0 = Type: I (0x0)
    .... .... .... .... 0111 0010 0010 000. = Tx: 14608
    0111 0100 0110 010. .... .... .... .... = Rx: 14898
v IEC 60870-5-101/104 ASDU: ASDU=8292 <TypeId=117> UkComAdrASDU_NEGA IOA[114]=7627108,... '<Unknown TypeId>'
    TypeId: Unknown (117)
    0... .... = SQ: False
    .111 0010 = NumIx: 114
    ..10 1110 = CauseTx: UkComAdrASDU (46)
    .1.. .... = Negative: True
    0... .... = Test: False
    OA: 101
    Addr: 8292
    IOA: 7627108
    Raw Data: 6120696e636c756465732047656f4c69746520646174612063726561746564206279204d…
v IEC 60870-5-104: <ERR prefix 6 bytes> <- I (14394,11805)
    Data: 2e636f6d273e
    START
    ApduLen: 116
    .... .... .... .... .... .... .... ...0 = Type: I (0x0)
    .... .... .... .... 0111 0000 0111 010. = Tx: 14394
    0101 1100 0011 101. .... .... .... .... = Rx: 11805
v IEC 60870-5-101/104 ASDU: ASDU=30583 C_RC_NA_1 UkIOA   IOA[92]=6384942,... 'regulating step command'
    TypeId: C_RC_NA_1 (47)
    0... .... = SQ: False
    .101 1100 = NumIx: 92
    ..10 1111 = CauseTx: UkIOA (47)
    .0.. .... = Negative: False
    0... .... = Test: False
    OA: 119
    Addr: 30583
  > IOA: 6384942
  > IOA: 7235949
  > IOA: 7299886
  > IOA: 3103804
  > IOA: 2240062
  > IOA: 2105354
  > IOA: 7300455
  > IOA: 6780268
  > IOA: 6512494
  > IOA: 2259316
  > IOA: 6379298
  > IOA: 7823731
  > IOA: 2099756
  > IOA: 6645538
  > IOA: 7695472
```

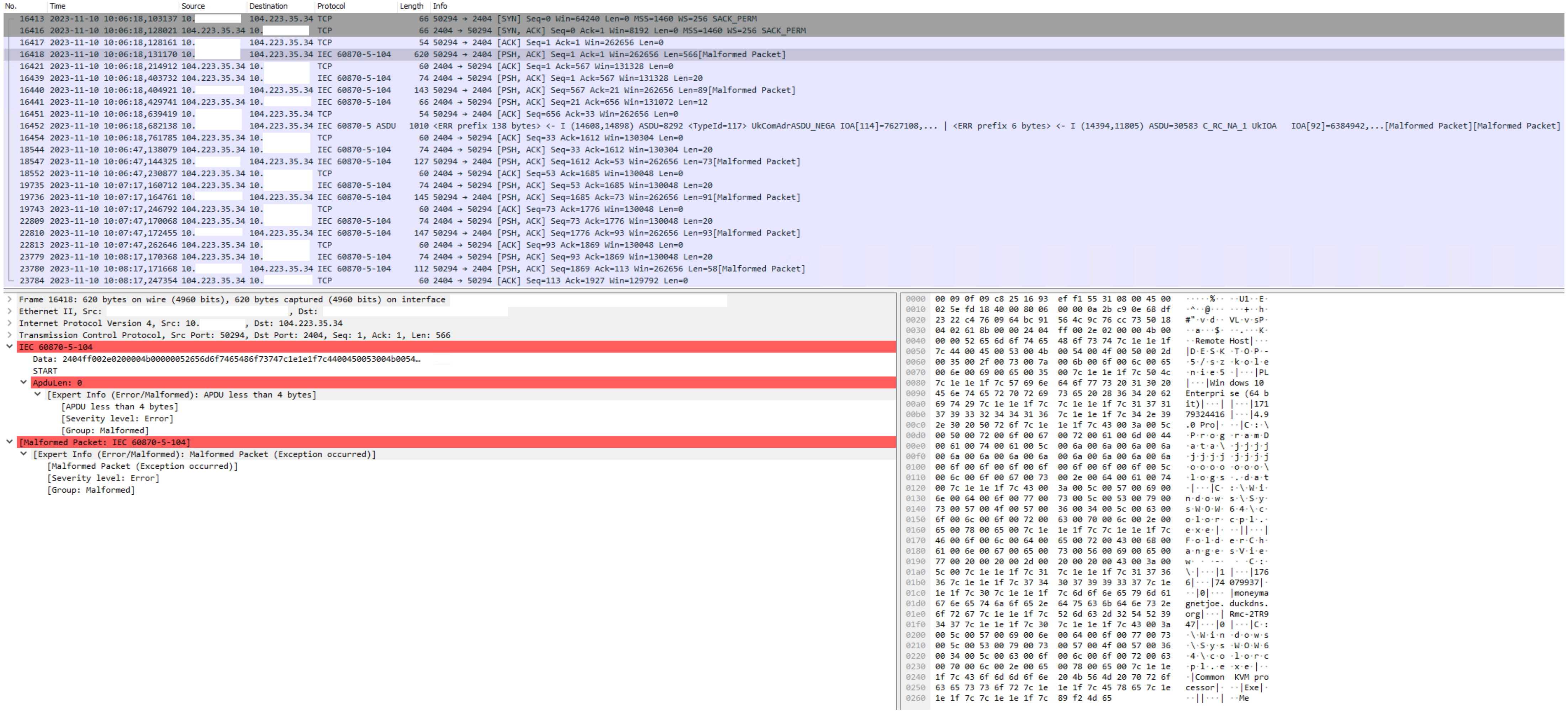
```
0000  00 09 0f 09 c8 25 16 93  ef f1 55 31 08 00 45 00   ·····%·· ··U1··E·
0010  03 e4 fd 1b 40 00 80 06  00 00 0a 2b c9 0e 68 df   ····@··· ···+··h·
0020  23 22 c4 76 09 64 bc 91  58 db 9c 76 cc 93 50 18   #"·v·d·· X··v··P·
0030  04 02 63 11 00 00 24 04  ff 00 b4 03 00 00 11 00   ··c···$· ········
0040  00 00 7b 0a 20 20 22 67  65 6f 70 6c 75 67 69 6e   ··{·  "g eoplugin
0050  5f 72 65 71 75 65 73 74  22 3a 22 31 39 35 2e 31   _request ":"195.
0060  38 37 2e 33 36 2e 32 32  36 22 2c 0a 20 20 22 67   [redacted] ",·  "g
0070  65 6f 70 6c 75 67 69 6e  5f 73 74 61 74 75 73 22   eoplugin _status"
0080  3a 32 30 30 2c 0a 20 20  22 67 65 6f 70 6c 75 67   :200,·   "geoplug
0090  69 6e 5f 64 65 6c 61 79  22 3a 22 31 6d 73 22 2c   in_delay ":"1ms",
00a0  0a 20 20 22 67 65 6f 70  6c 75 67 69 6e 5f 63 72   ·  "geop lugin_cr
00b0  65 64 69 74 22 3a 22 53  6f 6d 65 20 6f 66 20 74   edit":"S ome of t
00c0  68 65 20 72 65 74 75 72  6e 65 64 20 64 61 74 61   he retur ned data
00d0  20 69 6e 63 6c 75 64 65  73 20 47 65 6f 4c 69 74    include s GeoLit
00e0  65 20 64 61 74 61 20 63  72 65 61 74 65 64 20 62   e data c reated b
00f0  79 20 4d 61 78 4d 69 6e  64 2c 20 61 76 61 69 6c   y MaxMin d, avail
0100  61 62 6c 65 20 66 72 6f  6d 20 3c 61 20 68 72 65   able fro m <a hre
0110  66 3d 27 68 74 74 70 3a  5c 2f 5c 2f 77 77 77 2e   f='http: \/\/www.
0120  6d 61 78 6d 69 6e 64 2e  63 6f 6d 27 3e 68 74 74   maxmind. com'>htt
0130  70 3a 5c 2f 5c 2f 77 77  77 2e 6d 61 78 6d 69 6e   p:\/\/ww w.maxmin
0140  64 2e 63 6f 6d 3c 5c 2f  61 3e 2e 22 2c 0a 20 20   d.com<\/ a>.",·
0150  22 67 65 6f 70 6c 75 67  69 6e 5f 63 69 74 79 22   "geoplug in_city"
0160  3a 22 57 61 72 73 61 77  22 2c 0a 20 20 22 67 65   :"Warsaw ",·  "ge
0170  6f 70 6c 75 67 69 6e 5f  72 65 67 69 6f 6e 22 3a   oplugin_ region":
0180  22 4d 61 7a 6f 76 69 61  22 2c 0a 20 20 22 67 65   "Mazovia ",·  "ge
0190  6f 70 6c 75 67 69 6e 5f  72 65 67 69 6f 6e 43 6f   oplugin_ regionCo
01a0  64 65 22 3a 22 31 34 22  2c 0a 20 20 22 67 65 6f   de":"14" ,·  "geo
01b0  70 6c 75 67 69 6e 5f 72  65 67 69 6f 6e 4e 61 6d   plugin_r egionNam
01c0  65 22 3a 22 4d 61 7a 6f  76 69 61 22 2c 0a 20 20   e":"Mazo via",·
01d0  22 67 65 6f 70 6c 75 67  69 6e 5f 61 72 65 61 43   "geoplug in_areaC
01e0  6f 64 65 22 3a 22 22 2c  0a 20 20 22 67 65 6f 70   ode":"", ·  "geop
01f0  6c 75 67 69 6e 5f 64 6d  61 43 6f 64 65 22 3a 22   lugin_dm aCode":"
0200  22 2c 0a 20 20 22 67 65  6f 70 6c 75 67 69 6e 5f   ",·  "ge oplugin_
0210  63 6f 75 6e 74 72 79 43  6f 64 65 22 3a 22 50 4c   countryC ode":"PL
0220  22 2c 0a 20 20 22 67 65  6f 70 6c 75 67 69 6e 5f   ",·  "ge oplugin_
0230  63 6f 75 6e 74 72 79 4e  61 6d 65 22 3a 22 50 6f   countryN ame":"Po
0240  6c 61 6e 64 22 2c 0a 20  20 22 67 65 6f 70 6c 75   land",·   "geoplu
0250  67 69 6e 5f 69 6e 45 55  22 3a 31 2c 0a 20 20 22   gin_inEU ":1,·  "
0260  67 65 6f 70 6c 75 67 69  6e 5f 65 75 56 41 54 72   geoplugi n_euVATr
0270  61 74 65 22 3a 32 33 2c  0a 20 20 22 67 65 6f 70   ate":23, ·  "geop
0280  6c 75 67 69 6e 5f 63 6f  6e 74 69 6e 65 6e 74 43   lugin_co ntinentC
0290  6f 64 65 22 3a 22 45 55  22 2c 0a 20 20 22 67 65   ode":"EU ",·  "ge
02a0  6f 70 6c 75 67 69 6e 5f  63 6f 6e 74 69 6e 65 6e   oplugin_ continen
02b0  74 4e 61 6d 65 22 3a 22  45 75 72 6f 70 65 22 2c   tName":" Europe",
02c0  0a 20 20 22 67 65 6f 70  6c 75 67 69 6e 5f 6c 61   ·  "geop lugin_la
02d0  74 69 74 75 64 65 22 3a  22 35 32 2e 32 32 39 36   titude": "[redacted]
02e0  22 2c 0a 20 20 22 67 65  6f 70 6c 75 67 69 6e 5f   ",·  "ge oplugin_
02f0  6c 6f 6e 67 69 74 75 64  65 22 3a 22 32 31 2e 30   longitud e":"[redacted]
0300  30 36 37 22 2c 0a 20 20  22 67 65 6f 70 6c 75 67   [redacted]",·   "geoplug
0310  69 6e 5f 6c 6f 63 61 74  69 6f 6e 41 63 63 75 72   in_locat ionAccur
0320  61 63 79 52 61 64 69 75  73 22 3a 22 32 30 30 22   acyRadiu s":"200"
0330  2c 0a 20 20 22 67 65 6f  70 6c 75 67 69 6e 5f 74   ,·  "geo plugin_t
0340  69 6d 65 7a 6f 6e 65 22  3a 22 45 75 72 6f 70 65   imezone" :"Europe
0350  5c 2f 57 61 72 73 61 77  22 2c 0a 20 20 22 67 65   \/Warsaw ",·  "ge
0360  6f 70 6c 75 67 69 6e 5f  63 75 72 72 65 6e 63 79   oplugin_ currency
0370  43 6f 64 65 22 3a 22 50  4c 4e 22 2c 0a 20 20 22   Code":"P LN",·  "
0380  67 65 6f 70 6c 75 67 69  6e 5f 63 75 72 72 65 6e   geoplugi n_curren
```



```
No.   Time                       Source         Destination    Protocol          Length Info
16413 2023-11-10 10:06:18,103137 10.[redacted]  104.223.35.34  TCP                   66 50294 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
16416 2023-11-10 10:06:18,128021 104.223.35.34  10.[redacted]  TCP                   66 2404 → 50294 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
16417 2023-11-10 10:06:18,128161 10.[redacted]  104.223.35.34  TCP                   54 50294 → 2404 [ACK] Seq=1 Ack=1 Win=262656 Len=0
16418 2023-11-10 10:06:18,131170 10.[redacted]  104.223.35.34  IEC 60870-5-104     620 50294 → 2404 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=566[Malformed Packet]
16421 2023-11-10 10:06:18,214912 104.223.35.34  10.[redacted]  TCP                   60 2404 → 50294 [ACK] Seq=1 Ack=567 Win=131328 Len=0
16439 2023-11-10 10:06:18,403732 104.223.35.34  10.[redacted]  IEC 60870-5-104      74 2404 → 50294 [PSH, ACK] Seq=1 Ack=567 Win=131328 Len=20
16440 2023-11-10 10:06:18,404921 10.[redacted]  104.223.35.34  IEC 60870-5-104     143 50294 → 2404 [PSH, ACK] Seq=567 Ack=21 Win=262656 Len=89[Malformed Packet]
16441 2023-11-10 10:06:18,429741 104.223.35.34  10.[redacted]  IEC 60870-5-104      66 2404 → 50294 [PSH, ACK] Seq=21 Ack=656 Win=131072 Len=12
16451 2023-11-10 10:06:18,639419 10.[redacted]  104.223.35.34  TCP                   54 50294 → 2404 [ACK] Seq=656 Ack=33 Win=262656 Len=0
16452 2023-11-10 10:06:18,682138 10.[redacted]  104.223.35.34  IEC 60870-5 ASDU   1010 <ERR prefix 138 bytes> <- I (14608,14898) ASDU=8292 <TypeId=117> UkComAdrASDU_NEGA IOA[114]=7627108,... | <ERR prefix 6 bytes> <- I (14394,11805) ASDU=30583 C_RC_NA_1 UkIOA   IOA[92]=6384942,...[Malformed Packet][Malformed Packet]
16454 2023-11-10 10:06:18,761785 104.223.35.34  10.[redacted]  TCP                   60 2404 → 50294 [ACK] Seq=33 Ack=1612 Win=130304 Len=0
18544 2023-11-10 10:06:47,138079 104.223.35.34  10.[redacted]  IEC 60870-5-104      74 2404 → 50294 [PSH, ACK] Seq=33 Ack=1612 Win=130304 Len=20
18547 2023-11-10 10:06:47,144325 10.[redacted]  104.223.35.34  IEC 60870-5-104     127 50294 → 2404 [PSH, ACK] Seq=1612 Ack=53 Win=262656 Len=73[Malformed Packet]
18552 2023-11-10 10:06:47,230877 104.223.35.34  10.[redacted]  TCP                   60 2404 → 50294 [ACK] Seq=53 Ack=1685 Win=130048 Len=0
19735 2023-11-10 10:07:17,160712 104.223.35.34  10.[redacted]  IEC 60870-5-104      74 2404 → 50294 [PSH, ACK] Seq=53 Ack=1685 Win=130048 Len=20
19736 2023-11-10 10:07:17,164761 10.[redacted]  104.223.35.34  IEC 60870-5-104     145 50294 → 2404 [PSH, ACK] Seq=1685 Ack=73 Win=262656 Len=91[Malformed Packet]
19743 2023-11-10 10:07:17,246792 104.223.35.34  10.[redacted]  TCP                   60 2404 → 50294 [ACK] Seq=73 Ack=1776 Win=130048 Len=0
22809 2023-11-10 10:07:47,170068 104.223.35.34  10.[redacted]  IEC 60870-5-104      74 2404 → 50294 [PSH, ACK] Seq=73 Ack=1776 Win=130048 Len=20
22810 2023-11-10 10:07:47,172455 10.[redacted]  104.223.35.34  IEC 60870-5-104     147 50294 → 2404 [PSH, ACK] Seq=1776 Ack=93 Win=262656 Len=93[Malformed Packet]
22813 2023-11-10 10:07:47,262646 104.223.35.34  10.[redacted]  TCP                   60 2404 → 50294 [ACK] Seq=93 Ack=1869 Win=130048 Len=0
23779 2023-11-10 10:08:17,170368 104.223.35.34  10.[redacted]  IEC 60870-5-104      74 2404 → 50294 [PSH, ACK] Seq=93 Ack=1869 Win=130048 Len=20
23780 2023-11-10 10:08:17,171668 10.[redacted]  104.223.35.34  IEC 60870-5-104     112 50294 → 2404 [PSH, ACK] Seq=1869 Ack=113 Win=262656 Len=58[Malformed Packet]
23784 2023-11-10 10:08:17,247354 104.223.35.34  10.[redacted]  TCP                   60 2404 → 50294 [ACK] Seq=113 Ack=1927 Win=129792 Len=0
```

```
IEC 60870-5-101/104 ASDU: ASDU=30583 C_RC_NA_1 UkIOA   IOA[92]=6384942,... 'regulating step command'
  TypeId: C_RC_NA_1 (47)
  0... .... = SQ: False
  .101 1100 = NumIx: 92
  ..10 1111 = CauseTx: UkIOA (47)
  .0.. .... = Negative: False
  0... .... = Test: False
  OA: 119
  Addr: 30583
  IOA: 6384942
  IOA: 7235949
  IOA: 7299886
  IOA: 3103804
  IOA: 2240062
  IOA: 2105354
  IOA: 7300455
  IOA: 6780268
  IOA: 6512494
  IOA: 2259316
  IOA: 6379298
  IOA: 7823731
  IOA: 2099756
  IOA: 6645538
  IOA: 7695472
  IOA: 6254185
  IOA: 6907749
  IOA: 3809902
  IOA: 8020301
  IOA: 6383990
  IOA: 2099756
  IOA: 6645538
  IOA: 7695472
  IOA: 6254185
  IOA: 6907749
  IOA: 7291758
    IOA: 7291758
    RCO: 0x64
      .... ..00 = UP/DOWN: (None) (0)
      .110 01.. = QU: Unknown (25)
      0... .... = S/E: Execute
[Malformed Packet: IEC 60870-5-101/104 ASDU]
  [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
    [Malformed Packet (Exception occurred)]
    [Severity level: Error]
    [Group: Malformed]
[Malformed Packet: IEC 60870-5-104]
  [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
    [Malformed Packet (Exception occurred)]
    [Severity level: Error]
    [Group: Malformed]
```

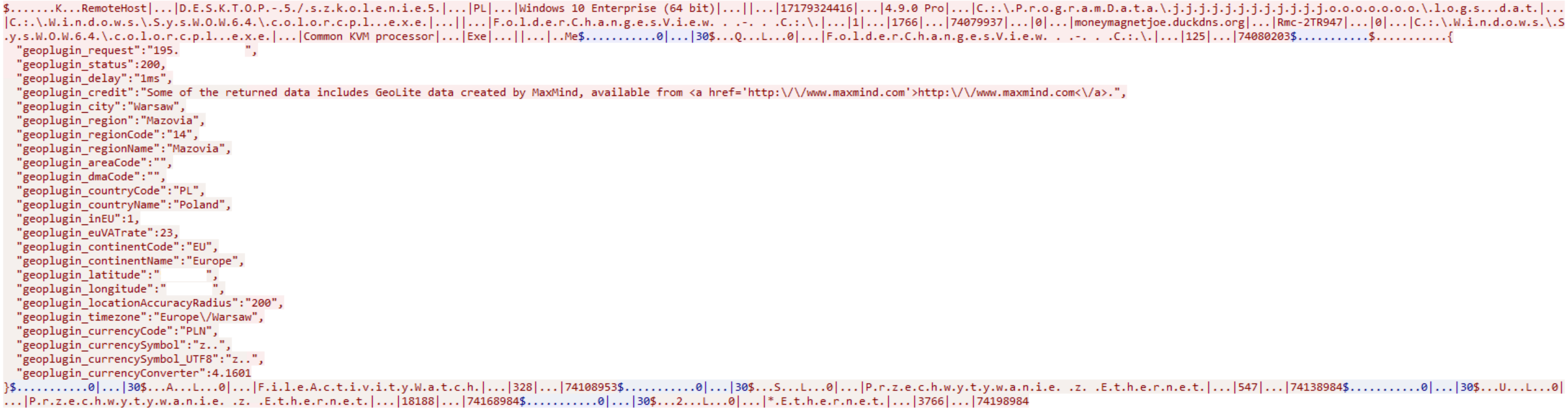
```
0070  65 6f 70 6c 75 67 69 6e  5f 73 74 61 74 75 73 22   eoplugin _status"
0080  3a 32 30 30 2c 0a 20 20  22 67 65 6f 70 6c 75 67   :200,·   "geoplug
0090  69 6e 5f 64 65 6c 61 79  22 3a 22 31 6d 73 22 2c   in_delay ":"1ms",
00a0  0a 20 20 22 67 65 6f 70  6c 75 67 69 6e 5f 63 72   ·  "geop lugin_cr
00b0  65 64 69 74 22 3a 22 53  6f 6d 65 20 6f 66 20 74   edit":"S ome of t
00c0  68 65 20 72 65 74 75 72  6e 65 64 20 64 61 74 61   he retur ned data
00d0  20 69 6e 63 6c 75 64 65  73 20 47 65 6f 4c 69 74    include s GeoLit
00e0  65 20 64 61 74 61 20 63  72 65 61 74 65 64 20 62   e data c reated b
00f0  79 20 4d 61 78 4d 69 6e  64 2c 20 61 76 61 69 6c   y MaxMin d, avail
0100  61 62 6c 65 20 66 72 6f  6d 20 3c 61 20 68 72 65   able fro m <a hre
0110  66 3d 27 68 74 74 70 3a  5c 2f 5c 2f 77 77 77 2e   f='http: \/\/www.
0120  6d 61 78 6d 69 6e 64 2e  63 6f 6d 27 3e 68 74 74   maxmind. com'>htt
0130  70 3a 5c 2f 5c 2f 77 77  77 2e 6d 61 78 6d 69 6e   p:\/\/ww w.maxmin
0140  64 2e 63 6f 6d 3c 5c 2f  61 3e 2e 22 2c 0a 20 20   d.com<\/ a>.",·
0150  22 67 65 6f 70 6c 75 67  69 6e 5f 63 69 74 79 22   "geoplug in_city"
0160  3a 22 57 61 72 73 61 77  22 2c 0a 20 20 22 67 65   :"Warsaw ",·  "ge
0170  6f 70 6c 75 67 69 6e 5f  72 65 67 69 6f 6e 22 3a   oplugin_ region":
0180  22 4d 61 7a 6f 76 69 61  22 2c 0a 20 20 22 67 65   "Mazovia ",·  "ge
0190  6f 70 6c 75 67 69 6e 5f  72 65 67 69 6f 6e 43 6f   oplugin_ regionCo
01a0  64 65 22 3a 22 31 34 22  2c 0a 20 20 22 67 65 6f   de":"14" ,·  "geo
01b0  70 6c 75 67 69 6e 5f 72  65 67 69 6f 6e 4e 61 6d   plugin_r egionNam
01c0  65 22 3a 22 4d 61 7a 6f  76 69 61 22 2c 0a 20 20   e":"Mazo via",·
01d0  22 67 65 6f 70 6c 75 67  69 6e 5f 61 72 65 61 43   "geoplug in_areaC
01e0  6f 64 65 22 3a 22 22 2c  0a 20 20 22 67 65 6f 70   ode":"", ·  "geop
01f0  6c 75 67 69 6e 5f 64 6d  61 43 6f 64 65 22 3a 22   lugin_dm aCode":"
0200  22 2c 0a 20 20 22 67 65  6f 70 6c 75 67 69 6e 5f   ",·  "ge oplugin_
0210  63 6f 75 6e 74 72 79 43  6f 64 65 22 3a 22 50 4c   countryC ode":"PL
0220  22 2c 0a 20 20 22 67 65  6f 70 6c 75 67 69 6e 5f   ",·  "ge oplugin_
0230  63 6f 75 6e 74 72 79 4e  61 6d 65 22 3a 22 50 6f   countryN ame":"Po
0240  6c 61 6e 64 22 2c 0a 20  20 22 67 65 6f 70 6c 75   land",·   "geoplu
0250  67 69 6e 5f 69 6e 45 55  22 3a 31 2c 0a 20 20 22   gin_inEU ":1,·  "
0260  67 65 6f 70 6c 75 67 69  6e 5f 65 75 56 41 54 72   geoplugi n_euVATr
0270  61 74 65 22 3a 32 33 2c  0a 20 20 22 67 65 6f 70   ate":23, ·  "geop
0280  6c 75 67 69 6e 5f 63 6f  6e 74 69 6e 65 6e 74 43   lugin_co ntinentC
0290  6f 64 65 22 3a 22 45 55  22 2c 0a 20 20 22 67 65   ode":"EU ",·  "ge
02a0  6f 70 6c 75 67 69 6e 5f  63 6f 6e 74 69 6e 65 6e   oplugin_ continen
02b0  74 4e 61 6d 65 22 3a 22  45 75 72 6f 70 65 22 2c   tName":" Europe",
02c0  0a 20 20 22 67 65 6f 70  6c 75 67 69 6e 5f 6c 61   ·  "geop lugin_la
02d0  74 69 74 75 64 65 22 3a  22 35 32 2e 32 32 39 36   titude": "[redacted]
02e0  22 2c 0a 20 20 22 67 65  6f 70 6c 75 67 69 6e 5f   ",·  "ge oplugin_
02f0  6c 6f 6e 67 69 74 75 64  65 22 3a 22 32 31 2e 30   longitud e":"[redacted]
0300  30 36 37 22 2c 0a 20 20  22 67 65 6f 70 6c 75 67   [redacted]",·   "geoplug
0310  69 6e 5f 6c 6f 63 61 74  69 6f 6e 41 63 63 75 72   in_locat ionAccur
0320  61 63 79 52 61 64 69 75  73 22 3a 22 32 30 30 22   acyRadiu s":"200"
0330  2c 0a 20 20 22 67 65 6f  70 6c 75 67 69 6e 5f 74   ,·  "geo plugin_t
0340  69 6d 65 7a 6f 6e 65 22  3a 22 45 75 72 6f 70 65   imezone" :"Europe
0350  5c 2f 57 61 72 73 61 77  22 2c 0a 20 20 22 67 65   \/Warsaw ",·  "ge
0360  6f 70 6c 75 67 69 6e 5f  63 75 72 72 65 6e 63 79   oplugin_ currency
0370  43 6f 64 65 22 3a 22 50  4c 4e 22 2c 0a 20 20 22   Code":"P LN",·  "
0380  67 65 6f 70 6c 75 67 69  6e 5f 63 75 72 72 65 6e   geoplugi n_curren
0390  63 79 53 79 6d 62 6f 6c  22 3a 22 7a c5 82 22 2c   cySymbol ":"z··",
03a0  0a 20 20 22 67 65 6f 70  6c 75 67 69 6e 5f 63 75   ·  "geop lugin_cu
03b0  72 72 65 6e 63 79 53 79  6d 62 6f 6c 5f 55 54 46   rrencySy mbol_UTF
03c0  38 22 3a 22 7a c5 82 22  2c 0a 20 20 22 67 65 6f   8":"z··" ,·  "geo
03d0  70 6c 75 67 69 6e 5f 63  75 72 72 65 6e 63 79 43   plugin_c urrencyC
03e0  6f 6e 76 65 72 74 65 72  22 3a 34 2e 31 36 30 31   onverter ":4.1601
03f0  0a 7d                                              ·}
```



```
No.   Time                       Source        Destination   Protocol          Length Info
16413 2023-11-10 10:06:18,103137 10.[redacted] 104.223.35.34 TCP                  66 50294 → 2404 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
16416 2023-11-10 10:06:18,128021 104.223.35.34 10.[redacted] TCP                  66 2404 → 50294 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
16417 2023-11-10 10:06:18,128161 10.[redacted] 104.223.35.34 TCP                  54 50294 → 2404 [ACK] Seq=1 Ack=1 Win=262656 Len=0
16418 2023-11-10 10:06:18,131170 10.[redacted] 104.223.35.34 IEC 60870-5-104     620 50294 → 2404 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=566[Malformed Packet]
16421 2023-11-10 10:06:18,214912 104.223.35.34 10.[redacted] TCP                  60 2404 → 50294 [ACK] Seq=1 Ack=567 Win=131328 Len=0
16439 2023-11-10 10:06:18,403732 104.223.35.34 10.[redacted] IEC 60870-5-104      74 2404 → 50294 [PSH, ACK] Seq=1 Ack=567 Win=131328 Len=20
16440 2023-11-10 10:06:18,404921 10.[redacted] 104.223.35.34 IEC 60870-5-104     143 50294 → 2404 [PSH, ACK] Seq=567 Ack=21 Win=262656 Len=89[Malformed Packet]
16441 2023-11-10 10:06:18,429741 104.223.35.34 10.[redacted] IEC 60870-5-104      66 2404 → 50294 [PSH, ACK] Seq=21 Ack=656 Win=131072 Len=12
16451 2023-11-10 10:06:18,639419 10.[redacted] 104.223.35.34 TCP                  54 50294 → 2404 [ACK] Seq=656 Ack=33 Win=262656 Len=0
16452 2023-11-10 10:06:18,682138 10.[redacted] 104.223.35.34 IEC 60870-5 ASDU  1010 <ERR prefix 138 bytes> <- I (14608,14898) ASDU=8292 <TypeId=117> UkComAdrASDU_NEGA IOA[114]=7627108,... | <ERR prefix 6 bytes> <- I (14394,11805) ASDU=30583 C_RC_NA_1 UkIOA   IOA[92]=6384942,...[Malformed Packet][Malformed Packet]
16454 2023-11-10 10:06:18,761785 104.223.35.34 10.[redacted] TCP                  60 2404 → 50294 [ACK] Seq=33 Ack=1612 Win=130304 Len=0
18544 2023-11-10 10:06:47,138079 104.223.35.34 10.[redacted] IEC 60870-5-104      74 2404 → 50294 [PSH, ACK] Seq=33 Ack=1612 Win=130304 Len=20
18547 2023-11-10 10:06:47,144325 10.[redacted] 104.223.35.34 IEC 60870-5-104     127 50294 → 2404 [PSH, ACK] Seq=1612 Ack=53 Win=262656 Len=73[Malformed Packet]
18552 2023-11-10 10:06:47,230877 104.223.35.34 10.[redacted] TCP                  60 2404 → 50294 [ACK] Seq=53 Ack=1685 Win=130048 Len=0
19735 2023-11-10 10:07:17,160712 104.223.35.34 10.[redacted] IEC 60870-5-104      74 2404 → 50294 [PSH, ACK] Seq=53 Ack=1685 Win=130048 Len=20
19736 2023-11-10 10:07:17,164761 10.[redacted] 104.223.35.34 IEC 60870-5-104     145 50294 → 2404 [PSH, ACK] Seq=1685 Ack=73 Win=262656 Len=91[Malformed Packet]
19743 2023-11-10 10:07:17,246792 104.223.35.34 10.[redacted] TCP                  60 2404 → 50294 [ACK] Seq=73 Ack=1776 Win=130048 Len=0
22809 2023-11-10 10:07:47,170068 104.223.35.34 10.[redacted] IEC 60870-5-104      74 2404 → 50294 [PSH, ACK] Seq=73 Ack=1776 Win=130048 Len=20
22810 2023-11-10 10:07:47,172455 10.[redacted] 104.223.35.34 IEC 60870-5-104     147 50294 → 2404 [PSH, ACK] Seq=1776 Ack=93 Win=262656 Len=93[Malformed Packet]
22813 2023-11-10 10:07:47,262646 104.223.35.34 10.[redacted] TCP                  60 2404 → 50294 [ACK] Seq=93 Ack=1869 Win=130048 Len=0
23779 2023-11-10 10:08:17,170368 104.223.35.34 10.[redacted] IEC 60870-5-104      74 2404 → 50294 [PSH, ACK] Seq=93 Ack=1869 Win=130048 Len=20
23780 2023-11-10 10:08:17,171668 10.[redacted] 104.223.35.34 IEC 60870-5-104     112 50294 → 2404 [PSH, ACK] Seq=1869 Ack=113 Win=262656 Len=58[Malformed Packet]
23784 2023-11-10 10:08:17,247354 104.223.35.34 10.[redacted] TCP                  60 2404 → 50294 [ACK] Seq=113 Ack=1927 Win=129792 Len=0
```

```
> Frame 16418: 620 bytes on wire (4960 bits), 620 bytes captured (4960 bits) on interface [redacted]
> Ethernet II, Src: [redacted], Dst: [redacted]
> Internet Protocol Version 4, Src: 10.[redacted], Dst: 104.223.35.34
> Transmission Control Protocol, Src Port: 50294, Dst Port: 2404, Seq: 1, Ack: 1, Len: 566
v IEC 60870-5-104
    Data: 2404ff002e0200004b00000052656d6f7465486f73747c1e1e1f7c4400450053004b0054…
    START
  v ApduLen: 0
    v [Expert Info (Error/Malformed): APDU less than 4 bytes]
        [APDU less than 4 bytes]
        [Severity level: Error]
        [Group: Malformed]
v [Malformed Packet: IEC 60870-5-104]
  v [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
      [Malformed Packet (Exception occurred)]
      [Severity level: Error]
      [Group: Malformed]
```

```
0000  00 09 0f 09 c8 25 16 93  ef f1 55 31 08 00 45 00   ·····%·· ··U1··E·
0010  02 5e fd 18 40 00 80 06  00 00 0a 2b c9 0e 68 df   ·^··@··· ···+··h·
0020  23 22 c4 76 09 64 bc 91  56 4c 9c 76 cc 73 50 18   #"·v·d·· VL·v·sP·
0030  04 02 61 8b 00 00 24 04  ff 00 2e 02 00 00 4b 00   ··a···$· ·.····K·
0040  00 00 52 65 6d 6f 74 65  48 6f 73 74 7c 1e 1e 1f   ··Remote Host|···
0050  7c 44 00 45 00 53 00 4b  00 54 00 4f 00 50 00 2d   |D·E·S·K ·T·O·P·-
0060  00 35 00 2f 00 73 00 7a  00 6b 00 6f 00 6c 00 65   ·5·/·s·z ·k·o·l·e
0070  00 6e 00 69 00 65 00 35  00 7c 1e 1e 1f 7c 50 4c   ·n·i·e·5 ·|···|PL
0080  7c 1e 1e 1f 7c 57 69 6e  64 6f 77 73 20 31 30 20   |···|Win dows 10 
0090  45 6e 74 65 72 70 72 69  73 65 20 28 36 34 20 62   Enterpri se (64 b
00a0  69 74 29 7c 1e 1e 1f 7c  7c 1e 1e 1f 7c 31 37 31   it)|···| |···|171
00b0  37 39 33 32 34 34 31 36  7c 1e 1e 1f 7c 34 2e 39   79324416 |···|4.9
00c0  2e 30 20 50 72 6f 7c 1e  1e 1f 7c 43 00 3a 00 5c   .0 Pro|· ··|C·:·\
00d0  00 50 00 72 00 6f 00 67  00 72 00 61 00 6d 00 44   ·P·r·o·g ·r·a·m·D
00e0  00 61 00 74 00 61 00 5c  00 6a 00 6a 00 6a 00 6a   ·a·t·a·\ ·j·j·j·j
00f0  00 6a 00 6a 00 6a 00 6a  00 6a 00 6a 00 6a 00 6a   ·j·j·j·j ·j·j·j·j
0100  00 6f 00 6f 00 6f 00 6f  00 6f 00 6f 00 6f 00 5c   ·o·o·o·o ·o·o·o·\
0110  00 6c 00 6f 00 67 00 73  00 2e 00 64 00 61 00 74   ·l·o·g·s ·.·d·a·t
0120  00 7c 1e 1e 1f 7c 43 00  3a 00 5c 00 57 00 69 00   ·|···|C· :·\·W·i·
0130  6e 00 64 00 6f 00 77 00  73 00 5c 00 53 00 79 00   n·d·o·w· s·\·S·y·
0140  73 00 57 00 4f 00 57 00  36 00 34 00 5c 00 63 00   s·W·O·W· 6·4·\·c·
0150  6f 00 6c 00 6f 00 72 00  63 00 70 00 6c 00 2e 00   o·l·o·r· c·p·l·.·
0160  65 00 78 00 65 00 7c 1e  1e 1f 7c 7c 1e 1e 1f 7c   e·x·e·|· ··||···|
0170  46 00 6f 00 6c 00 64 00  65 00 72 00 43 00 68 00   F·o·l·d· e·r·C·h·
0180  61 00 6e 00 67 00 65 00  73 00 56 00 69 00 65 00   a·n·g·e· s·V·i·e·
0190  77 00 20 00 20 00 2d 00  20 00 20 00 43 00 3a 00   w· · ·-·  · ·C·:·
01a0  5c 00 7c 1e 1e 1f 7c 31  7c 1e 1e 1f 7c 31 37 36   \·|···|1 |···|176
01b0  36 7c 1e 1e 1f 7c 37 34  30 37 39 39 33 37 7c 1e   6|···|74 079937|·
01c0  1e 1f 7c 30 7c 1e 1e 1f  7c 6d 6f 6e 65 79 6d 61   ··|0|··· |moneyma
01d0  67 6e 65 74 6a 6f 65 2e  64 75 63 6b 64 6e 73 2e   gnetjoe. duckdns.
01e0  6f 72 67 7c 1e 1e 1f 7c  52 6d 63 2d 32 54 52 39   org|···| Rmc-2TR9
01f0  34 37 7c 1e 1e 1f 7c 30  7c 1e 1e 1f 7c 43 00 3a   47|···|0 |···|C·:
0200  00 5c 00 57 00 69 00 6e  00 64 00 6f 00 77 00 73   ·\·W·i·n ·d·o·w·s
0210  00 5c 00 53 00 79 00 73  00 57 00 4f 00 57 00 36   ·\·S·y·s ·W·O·W·6
0220  00 34 00 5c 00 63 00 6f  00 6c 00 6f 00 72 00 63   ·4·\·c·o ·l·o·r·c
0230  00 70 00 6c 00 2e 00 65  00 78 00 65 00 7c 1e 1e   ·p·l·.·e ·x·e·|··
0240  1f 7c 43 6f 6d 6d 6f 6e  20 4b 56 4d 20 70 72 6f   ·|Common  KVM pro
0250  63 65 73 73 6f 72 7c 1e  1e 1f 7c 45 78 65 7c 1e   cessor|· ··|Exe|·
0260  1e 1f 7c 7c 1e 1e 1f 7c  89 f2 4d 65               ··||···| ··Me
```



```
$.......K...RemoteHost|...|D.E.S.K.T.O.P.-.5./.s.z.k.o.l.e.n.i.e.5.|...|PL|...|Windows 10 Enterprise (64 bit)|...||...|17179324416|...|4.9.0 Pro|...|C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.j.j.j.j.j.j.j.j.j.j.j.j.o.o.o.o.o.o.o.o.\.l.o.g.s...d.a.t.|...
|C.:.\.W.i.n.d.o.w.s.\.S.y.s.W.O.W.6.4.\.c.o.l.o.r.c.p.l...e.x.e.|...||...|F.o.l.d.e.r.C.h.a.n.g.e.s.V.i.e.w. . .-. . .C.:.\.|...|1|...|1766|...|74079937|...|0|...|moneymagnetjoe.duckdns.org|...|Rmc-2TR947|...|0|...|C.:.\.W.i.n.d.o.w.s.\.S
.y.s.W.O.W.6.4.\.c.o.l.o.r.c.p.l...e.x.e.|...|Common KVM processor|...|Exe|...||...|..Me$..........0|...|30$...Q...L...0|...|F.o.l.d.e.r.C.h.a.n.g.e.s.V.i.e.w. . .-. . .C.:.\.|...|125|...|74080203$..........$..........{
  "geoplugin_request":"195.            ",
  "geoplugin_status":200,
  "geoplugin_delay":"1ms",
  "geoplugin_credit":"Some of the returned data includes GeoLite data created by MaxMind, available from <a href='http:\/\/www.maxmind.com'>http:\/\/www.maxmind.com<\/a>.",
  "geoplugin_city":"Warsaw",
  "geoplugin_region":"Mazovia",
  "geoplugin_regionCode":"14",
  "geoplugin_regionName":"Mazovia",
  "geoplugin_areaCode":"",
  "geoplugin_dmaCode":"",
  "geoplugin_countryCode":"PL",
  "geoplugin_countryName":"Poland",
  "geoplugin_inEU":1,
  "geoplugin_euVATrate":23,
  "geoplugin_continentCode":"EU",
  "geoplugin_continentName":"Europe",
  "geoplugin_latitude":"       ",
  "geoplugin_longitude":"       ",
  "geoplugin_locationAccuracyRadius":"200",
  "geoplugin_timezone":"Europe\/Warsaw",
  "geoplugin_currencyCode":"PLN",
  "geoplugin_currencySymbol":"z..",
  "geoplugin_currencySymbol_UTF8":"z..",
  "geoplugin_currencyConverter":4.1601
}$..........0|...|30$...A...L...0|...|F.i.l.e.A.c.t.i.v.i.t.y.W.a.t.c.h.|...|328|...|74108953$..........0|...|30$...S...L...0|...|P.r.z.e.c.h.w.y.t.y.w.a.n.i.e. .z. .E.t.h.e.r.n.e.t.|...|547|...|74138984$..........0|...|30$...U...L...0|
...|P.r.z.e.c.h.w.y.t.y.w.a.n.i.e. .z. .E.t.h.e.r.n.e.t.|...|18188|...|74168984$..........0|...|30$...2...L...0|...|*.E.t.h.e.r.n.e.t.|...|3766|...|74198984
```

Contact:

Mail: mikewavepoland@gmail.com

LinkedIn: https://www.linkedin.com/in/michal-soltysik-ssh-soc/

Michał Sołtysik

Cybersecurity Consultant | Deep Packet Inspection Analyst | Network & Digital Forensics Examiner | CyberWarfare Organizer | SOC Trainer | C)CSA | C)NFE | C)DFE | WCNA | C)PTC | C)PEH | C)VA

Thank you for watching!

Remember to leave your questions and rate the presentation in the comment section below.